

А. В. Бабаш, Д.А. Ларин

Серия Информационная безопасность

**История защиты информации в зарубежных
странах**

Москва 2013

УДК

Пособие предназначено для студентов высших учебных заведений, обучающихся по направлению информационной безопасности и прикладной информатики.

УДК

ББК

Бабаш А.В., Ларин Д.А

История защиты информации в зарубежных странах.
Учебно-методическое пособие — М.:, 2013. — **с.**

ISBN

Учебно-методическое пособие знакомит студентов с историей криптографической защиты информации. Оно написано в соответствии с программой ФГОС 3-го поколения по дисциплинам направления «Криптографические методы защиты информации»

ББК

ISBN

© Бабаш А.В., Ларин Д.А. 2013

© Российский государственный социальный университет
(г. Москва), 2013

Подписано в печать 25.07.2013. Формат 60x88/16.

Гарнитура Newton. Бумага офсетная.

Усл. печ. л. 15,0. Уч.изд. л. 18,72.

Тираж 500 экз. Заказ №

Цена свободная.

Издательский Дом

127282, Москва,

E-mail:

Отпечатано по технологии «печать по требованию»

Тел.: (495) 363-92-15; e-mail: info@rior.ru

Содержание

Оглавление

Предисловие авторов	4
Введение.....	6
Криптография в древние времена и античную эпоху	16
Криптография средневековья.....	38
Криптография в эпоху возрождения	69
Криптография в эпоху «черных кабинетов».....	119
Научно-технический прогресс в XIX веке и криптография	156
Машинная криптография	194
Охота за «Энигмой».....	256
Использованные литература и ресурсы INTERNET	

Памяти Генриха Петровича Шанкина посвящается

Предисловие авторов

Данная работа предназначена для лиц, начинающих знакомство с одним из наиболее мощных способов защиты информации – использованием шифров для преобразования защищаемого сообщения (текста) в хаотический набор знаков некоторого алфавита. При этом "законный" получатель шифрованного сообщения, для которого оно и предназначено, по этому набору легко восстанавливает исходное сообщение. "Противник", перехвативший шифрованное сообщение, сталкивается с серьезными проблемами при попытках применить методы дешифрования, то есть раскрытия истинного содержания сообщения.

В работе дается краткое изложение истории криптографии с исторически известного в настоящее время момента возникновения криптографии (древняя Греция, Рим). При изложении материала мы хотели не только показать и разъяснить появлявшиеся в историко-хронологическом порядке криптографические идеи, конкретные способы шифрования, но и в некоторой степени дать характеристику культуры конкретной исторической эпохи, в которой эти идеи и шифры появлялись. В этом смысле, как представляется, интересен список имен крупных исторических личностей, так или иначе связанных с развитием криптографии. Среди этих имен – руководители государств, видные деятели культуры, науки и техники своего времени, крупные ученые-математики, представители церковной иерархии и т. д.

При написании данной работы были использованы многочисленные исторические источники. Они указаны в разделе литература и ресурсы internet. В первую очередь здесь следует упомянуть фундаментальный исторический труд: David Kahn "The codebreakers", New York, 1967, к сожалению, до сих пор не переведенный полностью на русский язык. Наша цель – дать разъяснение и популяризацию криптографического подхода к защите информации; при этом, читатель должен получить достаточно содержательное представление о конкретных методах и средствах защиты информации, появившихся в рассматриваемый исторический отрезок времени.

В основу пособия положены изданные ранее отдельные лекции и материалы, читаемые авторами в течении многих лет в различных

курсах учебных заведений РФ, а также материалы книги Бабаши А.В., Шанкина Г.П. «История криптографии», М., Гелиос АРВ, 2002.

Книга рекомендуется студентам, обучающимся в высших учебных заведениях, специализирующихся в области информационной безопасности.

Представляется, что предлагаемая работа может заинтересовать и специалистов по защите информации, интересующихся вопросами возникновения и становления криптографии как искусства и науки.

Благодарим всех своих коллег, принявших участие в обсуждении подготовленных материалов и представивших новые данные и сведения по истории криптографии. Особую благодарность выражаем бывшей редакции журнала ФСБ России "Служба безопасности – новости разведки и контрразведки" и, в первую очередь, его главному редактору А.Д. Витковскому за внимание и поддержку проводимых исторических исследований. Без этой поддержки предлагаемая работа едва ли могла бы появиться. Благодарим Вице-президента Академии криптографии Российской Федерации В.Н. Сачкова за обращение к читателю, помещенное в книге А.В. Бабаши, Г.П. Шанкина «История криптографии», поддержавшее авторов.

А. В. Бабаши

Д.А. Ларин

Введение

Криптография (в переводе с греческого языка — тайнопись) - это область научных, прикладных, инженерно-технических исследований и практической деятельности, которая связана с обеспечением информационной безопасности, а также преодолением криптографических средств защиты информации.

Основным понятием криптографии является понятие шифра. Шифр является совокупностью некоторых алгоритмов, преобразующих открытый конфиденциальный текст в хаотический набор знаков (букв, чисел или специально придуманных символов), называемый шифртекстом. Алгоритмы шифрования являются обратимыми, то есть позволяют из шифртекста восстановить исходный текст. Преобразование шифрованного текста в открытый называется расшифрованием. Эти преобразования (шифрование и расшифрование) зависят от секретного ключа. Смена ключа приводит к появлению другого шифртекста.

Вообще в историческом контексте следует говорить о более широком понятии – криптографической деятельности. Под криптографической деятельностью понимается не только шифрование и дешифрование, но и организация каналов передачи сообщений (системы связи), использование различных методов защиты информации (криптография, стеганография, физическая защита собственных линий связи и т.д.), организация перехвата шифрованной информации противника. Дешифрование без перехвата невозможно. Разумеется, сюда входят меры по добыванию информации, облегчающей дешифрование (добывание ключей, описания шифрсистем и т.д.). С другой стороны, при разработке методов и средств защиты информации необходимо учитывать возможные аналогичные действия противника и предпринимать соответствующие меры для их пресечения. Если действия по добыванию информации связаны с разведывательными операциями, то при защите главную роль играют контрразведывательные мероприятия. Поэтому криптографические службы работают в тесном контакте с разведкой и контрразведкой.

Вообще криптографическая деятельность является составной частью информационного противоборства, которое включает в себя организацию пропаганды и информационного воздействия на потенциального и реального противника и своего населения

(поддержка патриотического духа, разъяснение политики государства и т.д.), ведение контрпропаганды, проведение операций по дезинформации противника. В случае проведения операций по информационному воздействию на противника нередко используют криптографию. С одной стороны, узнав о дешифровании своих секретных сообщений, можно не усиливать защиту, а продолжать использовать тот же шифр, передавая дезинформацию, которую, другая сторона, будет принимать за истинную информацию. Такая ситуация называется дезинформацией «под шифром». В этом случае для передачи достоверной информации используют другие шифры и другие каналы связи. С другой стороны, тайно захватив шифры и ключи противника, или вскрыв их аналитическим путем (дешифрованием), можно попытаться от имени истинного отправителя передать противнику дезинформацию. [Гольев, 2008].

Фактически, как только где-то на Земле происходило становление того или иного государства как тут же начиналась его криптографическая деятельность. С развитием государственных институтов учреждались специальные криптографические службы. Известный американский историк Дэвид Кан считает, что признаками великой державы являются наличие у страны ядерного оружия, успехов в освоении космоса и достижений в области криптографии [Кан, 2004].

Изучение достижений современной криптографии невозможно без знания исторических закономерностей развития этой науки. Только знание истории криптографии позволяет понять истоки и закономерности развития ее фундаментальных идей, представить в полной мере картину постоянного соперничества разработчиков шифров и дешифровальщиков. Нередко успехи и неудачи криптографов оказывали серьезное влияние на ход войн, революций, внешнюю и внутреннюю политику, проводимую различными государствами. Изучение достижений современной криптографии невозможно без знания исторических закономерностей развития этой науки. Только знание истории криптографии позволяет понять истоки и закономерности развития ее фундаментальных идей, представить в полной мере картину постоянного соперничества разработчиков шифров и дешифровальщиков.

Нередко успехи и неудачи криптографов оказывали серьезное влияние на ход войн, революций, внешнюю и внутреннюю политику, проводимую различными государствами. Характерным примером

служит операция «Ультра» (дешифрование английскими криптографами основного шифратора вооруженных сил Германии «Энигма» в ходе Второй Мировой войны), результаты которой в значительной мере переломили ход боевых действий в Атлантическом океане, Средиземноморье и на Западном фронте в пользу антигитлеровской коалиции.

Довольно часто авторы публикаций по истории криптографии ограничиваются описанием исторических шифров и криптографической деятельности известных исторических личностей (Ришелье, Виет, Петр I и т.д.). Но помимо этого важно проследить связи между становлением и развитием криптографии, событиями мировой истории и научно-техническим прогрессом. Достижения научно-технического прогресса нередко способствуют созданию новых способов защиты информации, развитию известных и появлению новых методов криптографического анализа. Например, развитие элементной базы вычислительной техники привело к тому, что в 1950-е годы на смену дисковым шифраторам пришли электронные шифраторы. В то же время, потребности криптографии иногда являлись стимулом к интенсивному освоению многих областей науки и техники. Например, с середины 1970-х годов значительно активизировались исследования по проблемам факторизации чисел и дискретного логарифмирования в алгебраических структурах. В этих областях дискретной математики были получены значительные результаты. Это произошло благодаря появлению такого нового направления криптографии, как криптография с открытым ключом.

Исторический процесс развития средств и методов защиты тайных посланий указывает на три основных способа такой защиты.

Первый способ защиты информации – это физическая защита от противника материального носителя информации (пергамент, бумага, магнитная лента, физические каналы передачи: проводная линия связи, радио-канал, вибро-акустический канал и т. д.). Одновременно появляются приемы и способы, затрудняющие перехват сообщений. Главную роль здесь играет выбор канала связи, труднодоступного для перехвата (ласточки, голуби, специальный курьер, кабельные линии связи, специальные виды радиопередач, волоконно-оптические линии связи и т. д.).

Наряду с физической защитой носителя информации предусматриваются и другие меры. В их числе можно отметить следующие.

При реальной угрозе захвата противником материального носителя информации и наличии сомнений по поводу достойного отражения этой угрозы предпринимаются меры по быстрому и эффективному уничтожению носителя информации (или самой информации, записанной на нем). Спектр действий здесь достаточно широк: выбросить носитель в недоступное для “захватчиков” место, разорвать, стереть, проглотить и т. д. Естественно, сам физический носитель информации и способ ее записи в этом случае должны соответствовать требованиям эффективного уничтожения. В настоящее время, как впрочем, и в древние времена, этой проблеме уделялось и уделяется достойное внимание.

Важной задачей при физической защите информации является своевременное обнаружение факта “утечки” секретной информации, наличия тайной перлюстрации корреспонденции. Это обнаружение позволяет принять меры к локализации негативных последствий от действий противника, обладающего этой информацией. Поэтому необходимо предусматривать меры по обнаружению перехвата и перлюстрации. Нападающая сторона, со своей стороны, должна принимать меры к безуликовости перехвата и перлюстрации, к сокрытию факта наличия у нее полученной информации. Особенно строго следует сохранять тайну источника информации.

Второй способ защиты информации – это так называемая стеганографическая защита информации. Термин стеганография (в переводе с латино-греческого – тайнопись) было использовано для определения метода защиты, основанного на попытке сокрытия от противника самого факта наличия интересующей его информации. Такую защиту можно было бы осуществить несколькими принципиально различными способами.

Во-первых, можно было бы попытаться сделать “невидимым” для противника сам физический носитель информации. В современных условиях к таким способам относится, например, использование так называемых “микроточки – микрофотографии” (размером в “точку” письменного текста), подклеиваемой под клапан конверта, почтовую марку

и т. д. На этой микроточке фотографическим способом передается защищаемый текст. Сюда же относятся исторически древние приемы: “запирывание” носителя информации в корешках книг, в каблуках, в пломбе зуба, в медицинских препаратах и т. д.

Во-вторых, можно было бы попытаться поступить таким образом, чтобы противник, даже имея в руках носитель секретной информации, саму эту информацию не увидел. В этом направлении наибольшее распространение получили так называемые симпатические (химические) чернила. Текст, написанный этими чернилами между строк "невинного послания", невидим; он проявляется только в результате применения определенной технологии проявления.

В-третьих, на носителе информации, попадающем в руки противника, нет ничего, кроме того текста, рисунка, графика и т. д., который он видит. Однако истинное, секретное сообщение скрывается в буквах, точках рисунка, графика и т. д., стоящих на заранее оговоренных местах "невинного" сообщения.

В целом нужно отметить, что имеется огромный спектр стеганографических методов защиты информации. Здесь фантазия не ограничена.

Третий способ защиты информации, наиболее надежный и распространенный в наши дни – криптография.

Следует отметить, что наиболее эффективная защищенность информации достигается при комплексном использовании всех указанных выше способов. История предлагает многочисленные примеры такой комплексной защиты. Следует также заметить, что в историческом плане даже незашифрованный текст (тем более на иностранном языке, или написанный буквами иностранного языка) сам по себе уже определяет первую ступень защиты. В то время, когда подавляющее большинство населения было безграмотно, прочтение таких текстов "простолюдинами" было затруднительным. С древних времен использовались различные украшения букв текста, которые также затрудняли его понимание и делали это возможным лишь для "посвященных" (к которым, в первую очередь, относился сам автор: жрец, философ и т. д.).

Изобретение стенографии (скорописи), которое относят к временам древнего Рима и связывают с именем Тимона (вольноотпущенника Цицерона), привело к появлению "символических" записей, понятных лишь тем, кто владеет искусством стенографии.

Однако перечисленные методы записи сообщений можно отнести собственно не к их защите, а лишь к "маскировке", к попыткам создать способ записи, совместимый со скоростью речи оратора, чьи

высказывания фиксируются. Секрета здесь нет, нужно лишь освоить соответствующие навыки записи текстов.

Одно из требований, предъявляемое к методам и средствам защиты – это требование оперативности связи. Использование средств защиты не должно существенным образом задерживать передачу сообщения. С другой стороны, нападающая сторона также должна учитывать временной фактор. Информация “стареет”, и ее получение с большим запозданием может свести все усилия по ее добыванию “на нет”.

Отдельно следует упомянуть об организационных, административно-правовых мерах, направленных на защиту информации. В частности, предусматриваются серьезные наказания за разглашение секретной информации. Аналогичные меры применяются и при попытке несанкционированного доступа к этой информации. В истории имеются многочисленные факты таких наказаний, вплоть до смертной казни.

Известно, что лучшей формой защиты является нападение. Это относится и к защите информации. В частности, нападающей стороне можно “подсунуть” дезинформацию и тем самым заставить нападающего действовать вопреки своим интересам. Ниже будут приведены примеры использования такой активной формы защиты.

Информационные проблемы (как в защите, так и в нападении) приходится решать в условиях наличия ограниченных сил и средств. Эффективность решения указанных проблем в значительной мере зависит от этих ограничений. Чрезмерная экономия обычно приводит к плачевным результатам. Соответствующие примеры будут приведены ниже.

Наряду с государственными методами защиты информации развивались и негосударственные.

К защите информации прибегали оппозиционеры (“диссиденты”) правящего режима, уголовный мир, религиозно-мистические общества, коммерсанты, ученые, скрывающие свои идеи от преследования государства и церкви и т. д. К защите прибегали и частные лица, желающие сохранить в тайне от окружающих, от постороннего взгляда передаваемую информацию (например, любовного содержания). Следует отметить, что вклад таких дилетантов в историю криптографии иногда был весьма заметным.

Необходимо отметить одно существенное обстоятельство. Исторические исследования в области криптографии опираются на

изучение дошедших до наших дней материалов. Однако государственная криптографическая деятельность всегда велась под покровом великой тайны. Как правило, все секретные материалы уничтожались. Открытые же источники, которые, в частности, используются по тексту данной работы, обычно не отражают уровня развития государственной криптографии. Тем не менее, они дают определенное представление об уровне развития методов защиты и нападения в области обеспечения информационной безопасности государств.

Эволюция криптографической деятельности в различных странах обычно не является прямолинейной. Как правило, здесь имеются взлеты и падения, вызванные конкретной исторической обстановкой. Нередко оригинальные методы защиты информации забывались и изобретались заново через столетия. Иногда плодотворные идеи возникали параллельно в различных странах. Имеются определенные объективные трудности в сопоставлении уровня развития криптографии в различных странах. Так, например, пусть некоторая страна "А" успешно дешифрует переписку страны "В", а "В", со своей стороны, не дешифрует переписку стороны "А"; прибегая к футбольной терминологии, имеет место счет 1:0 в пользу "А". Такой счет может косвенно свидетельствовать о превосходстве (в данный исторический период) стороны "А" как в защите, так и в нападении. Счет 1:1, нередко встречающийся в истории криптографии, может свидетельствовать о равенстве криптографических возможностей обеих сторон, причем приводит к выводу об опережающем развитии средств и методов "нападения". Счет 0:0 говорит об обратном: общие возможности обеих сторон одинаковы, но средства и методы защиты опережают соответствующие средства и методы нападения. Однако это лишь общая и достаточно поверхностная оценка. Так, например, успехи в дешифровании опираются на возможности перехвата сообщений. Если эти возможности недостаточны, то даже при хорошо развитых средствах и методах дешифрования общий эффект в нападении становится невысоким.

Криптография в историческом аспекте развивалась не "сама по себе". Внимание, уделяемое развитию криптографии, зависело от активности деятельности государства в различных сферах: политической, дипломатической, военной, экономической и т. д. Криптография выполняла заказы государства и развивалась при его соответствующей поддержке. Среди внутренних противоречий,

стимулирующих развитие криптографии, в первую очередь следует выделить противостояние двух сторон криптографической деятельности: защита и нападение (противостояние "снаряда и брони"). Успехи в дешифровании шифров приводили к разработке новых шифров; в свою очередь, разработка новых шифров – к поиску новых методов их дешифрования.

Огромное влияние на развитие криптографии во всей истории ее существования оказывали достижения научно-технического прогресса.

Криптография (в современном понимании этого слова) появилась практически сразу же после появления письменности. Мощный импульс ее развитию дало изобретение алфавитной письменности. Широкому распространению криптографических способов защиты информации способствовало совершенствование технологической базы обмена письменными сообщениями: от записи на камнях – к глиняным табличкам (Месопотамия), затем к папирусу (Египет), бересте (Россия), шелковой ткани (Китай), пергаменту (Египет, Греция, Рим), деревянным дощечкам (Греция, Рим), к бумаге (Китай, I век н. э.) и, наконец, к современным носителям информации.

Особенно ярко влияние научно-технического прогресса на криптографию проявилось в XIX–XX вв., когда появились принципиально новые методы и средства защиты информации и нападения. Следует подчеркнуть, что криптография является не только "пассивным потребителем" достижений научно-технического прогресса, но и стимулирует развитие этого прогресса, ставя перед исследователями специфические проблемы. Не вдаваясь в серьезный анализ влияния криптографии на научно-технический прогресс, отметим лишь тот факт, что первые электронно-вычислительные машины (в современном их понимании) появились в Англии в значительной мере благодаря влиянию криптографии. В настоящее время для решения криптографических проблем создаются уникальные вычислительные комплексы, по своим характеристикам намного превосходящие аналогичную "массовую" продукцию. Ту же мысль можно высказать и по отношению к развитию математики, физики, электроники, теории связи и т. д.

Научно-технический прогресс заставил по-новому взглянуть на криптографические проблемы. Исходная проблема – защита информации, оставаясь основной, пополнилась в XX веке и другими проблемами, при решении которых существенно используются

криптографические методы. К этим проблемам относятся в настоящее время такие, как защита от имитации ("дезинформации под шифром"), идентификация абонентов ("электронная подпись"), проблема создания различных криптографических протоколов обмена информацией и т. д.

Во все времена учитывались затраты на защиту информации и на реализацию методов нападения. Как защита, так и нападение требуют сопоставления затрат с возможными доходами от успехов в их воплощении. Вопрос о том, что и как защищается (и какой ценой), что и как достается (и какой ценой) – это очень серьезный вопрос. Один древний мудрец сказал: "нельзя ловить рыбу на золотой крючок". Потеря крючка не окупается стоимостью выловленной рыбы. В наши дни известный специалист в области защиты информации Л. Дж. Хоффман (США) справедливо отметил: "На практике всегда следует стремиться к достижению компромисса между стоимостью шифрования и требуемой степенью обеспечения безопасности".

Наряду с развитием криптографии, как искусства и науки, развивались и совершенствовались государственные криптографические структуры. Если у истоков криптографической деятельности стояли специалисты-одиночки, то далее появились такие мощные государственные организации как Федеральное Агентство Правительственной Связи и Информации (ФАПСИ) при Президенте РФ, Агентство Национальной Безопасности (АНБ) США, Штаб Квартира Правительственной связи (ШКПС) Великобритании и др.

Одновременно совершенствовалась законодательно-правовая база функционирования криптографических служб. Из "подпольных", "нелегальных", "полулегальных" служб и организаций они стали официально объявленными органами государственного управления. Создано достаточное правовое поле для их деятельности. Введена практика сертификации и лицензирования в области обеспечения информационной безопасности. Постепенно появилось понимание того, что криптографической деятельностью в государстве должны заниматься не только талантливые одиночки – самоучки (их оказалось явно недостаточно), но и специально подготовленные к этой деятельности специалисты – криптографы. С конца XVII – начала XVIII вв. в развитых государствах мира создаются учебные заведения по подготовке таких специалистов. В настоящее время в передовых государствах мира созданы уникальные системы подготовки криптографов, предполагающие наличие у выпускников таких знаний

и умений, которые в своей области на несколько лет опережают знания и умения выпускников неспециализированных высших учебных заведений.

Официальная криптография охватывает не только государственные службы, но и финансовые, коммерческие и другие организации. Появляется заметный спрос на специалистов, в той или иной мере знакомых с принципами криптографической защиты информации. В многочисленных высших учебных заведениях организуются специальные "потоки" подготовки соответствующих специалистов. Однако не всегда эта подготовка осуществляется достаточно профессионально. Представляется, что содержательное изучение истории криптографии должно стать необходимой составляющей в этой подготовке.

История учит не только прошлому, но и пониманию настоящего, а также прогнозированию будущего. В этой связи уместно напомнить высказывания известных людей.

У. Черчилль: "Размышления над прошлым могут послужить руководством для будущего ...".

Д. С. Лихачев: "Для того чтобы протянуть очень длинную мысленную нить в будущее, нужно иметь ей достаточно длинный же противовес в прошлом – линию, столь же протяженную в прошлых столетиях".

В. Г. Белинский: "Мы вопрошаем и допрашиваем прошедшее, чтобы оно объяснило нам наше настоящее и намекнуло о нашем будущем".

В заключении – несколько слов о терминологии.

Как указывалось выше, слово "криптография" в переводе с греческого языка означает "тайнопись". В современной терминологии нередко используется термин "криптология" ("учение о тайне"); криптология, в свою очередь, включает в себя две составляющие: "криптография" (как наука о защите информации), "криптоанализ" (наука о нападении с целью преодоления защиты и получения интересующей нападающего информации). Термин "криптоанализ" часто используется наравне с термином "дешифрование".

Основное понятие в криптографии – "шифр". Напомним еще раз, что шифр – это совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты; эти исходные сообщения обычно называются "открытыми текстами". Выбор конкретного преобразования открытого текста определяется

наиболее секретной частью криптографической защиты – так называемым “ключом шифра” (или просто ключом). Этот ключ должен быть известен как отправителю сообщения, так и его законному получателю. Поэтому заранее, до обмена информацией, отправители сообщений и их получатели должны строго конфиденциально договориться об используемых шифрах и ключах. Бессмысленный набор знаков заранее оговоренного алфавита, получаемый в результате преобразования открытого текста, называется шифрованным сообщением (“криптограммой”). Преобразование открытого текста в криптограмму называется шифрованием (зашифрованием). Обратное преобразование криптограммы в открытый текст, осуществляемый законным получателем сообщения (знающим шифр и ключ), называется расшифрованием. Действия “противника”, получившего перехват (криптограмму), с целью обладания секретной информацией называется “дешифрованием” криптограммы.

Криптография в древние времена и античную эпоху

Криптография ровесница письменности. Эта наука прошла путь от папируса до компьютера и по возрасту старше Египетских пирамид. Она в своем развитии прошла через этапы: «криптография как искусство» и «криптография как ремесло» к этапу «криптография как наука». Криптография всегда развивались в тесном взаимодействии с математикой. Эти науки взаимно дополняли и обогащали друг друга. Математический аппарат продолжает оставаться основным в криптографии. Ведь не случайно в многовековую историю криптографии вписано много имен видных математиков.

Шифры активно использовали древние цивилизации Вавилона, Египта, Греции, Рима, Китая и Индии. Почти четыре тысячи лет тому назад в древнеегипетском городе Менет-Хуфу на берегу Нила один опытный писец нарисовал иероглифы, рассказавшие историю жизни его господина. Сделав это, он стал родоначальником документально зафиксированной истории криптографии. Его система не является тайнописью в том виде, в каком она известна современному миру. Для засекречивания своей надписи он не использовал никакого полноценного шифра. Эта надпись, вырезанная им примерно в 1900 году до нашей эры на гробнице знатного человека по имени Хнумхотеп, лишь в отдельных местах состоит из необычных

иероглифических символов вместо более привычных иероглифов. Большинство их встречается в ее последних двадцати столбцах, в которых перечисляются монументы, созданные Хнумхотепом на службе у египетского фараона Аменемхета II. Неизвестный писец старался не затруднить чтение текста, а придать ему важность, подобно тому, как это делается в каком-нибудь заявлении по торжественному поводу, в котором пишут «в год одна тысяча восемьсот шестьдесят третий от Рождества Христова», вместо того чтобы просто и без затей написать «в 1863 году». Таким образом, хотя писец применил не тайнопись, он, бесспорно, воспользовался одним из существенных элементов шифрования – умышленным преобразованием письменных символов. Это самый древний известный нам текст, который претерпел такие изменения.

По мере расцвета древнеегипетской цивилизации и совершенствования ее письменности росло количество усыпальниц почитаемых умерших, и все более изощренными становились преобразования текстов, которые вырезались на камнях гробниц. Со временем писцы стали заменять обычную иероглифическую форму буквы, например, рот, изображенный анфас, иной формой, например, ртом, изображенным в профиль. Они вводили в употребление новые иероглифы, первый звук произношения которых выражал желательную букву, как, например, изображение свиньи. Иногда произношение двух иероглифов различалось, но их изображение напоминало друг друга. Время от времени писцы использовали иероглиф по принципу ребуса, подобно тому, как, например, в английском языке изображение пчелы (Bee) может означать букву «В». Эти преобразования были изначально свойственны обычному египетскому письму: именно с их помощью иероглифы приобрели свои звуковые значения. В дальнейшем они лишь усложнялись и делались все более искусственными.

Такие преобразования были обнаружены во многих местах – в надгробных надписях, восхвалявших пройденный путь умерших, в гимне в честь Тота (Тот – бог Луны, письма, счета и письменности в Древнем Египте) и на саркофагах фараона Сети I. В них нет ничего такого, что преследовало бы цель скрыть смысл текста. И действительно, большинство надписей повторяются в обычной форме рядом с измененной. Для чего же тогда делать преобразования? Часто с той же целью, что и в гробнице Хнумхотепа, а именно – чтобы произвести впечатление на читателя. Иногда – чтобы показать

хорошую каллиграфию или ради украшения. Реже – чтобы отразить соответствующее тому времени произношение.

Но постепенно многие надписи начинают преследовать другую, важную для криптографии цель – секретность. В некоторых случаях секретность была нужна для усиления тайны и, следовательно, колдовской силы поминальных текстов. Гораздо чаще секретность проистекала из понятного желания древних египтян заставить прохожего прочитать их эпитафии и тем самым выразить умершим благословения, которые содержались в надгробных надписях. В Древнем Египте, с характерной для него непоколебимой верой в загробную жизнь, количество надписей быстро выросло до такой степени, что внимание к ним прохожих пошатнулось. Чтобы возродить их интерес, писцы нарочно делали надписи несколько туманными. Они ввели криптографические знаки, дабы привлечь внимание читателя, заставить его задуматься и вызвать у него желание разгадать их смысл. Но эти приемы совершенно не удались. Вместо того чтобы заинтересовать читателя, они губили даже малейшее желание прочитать набившие всем оскомину эпитафии. А посему вскоре после появления «надгробной» криптографии от нее отказались.

С другой стороны шифрование стали применять древнеегипетские жрецы, чтобы скрыть свои предсказания и другую информацию от посторонних. Итак, добавление элемента секретности в преобразование иероглифов породило криптографию. Правда, это напоминало скорее игру, поскольку преследовалась цель задержать разгадку только на самое короткое время. Поэтому криптоанализ также заключался всего лишь в раскрытии головоломки. Таким образом, древнеегипетский криптоанализ был весьма примитивен и не являлся наукой, в отличие от этой современной, чрезвычайно серьезной области научных знаний. Однако как утверждает американский историк криптографии Д. Кан «всем великим делам свойственны скромные начинания» [Кан, 2004, с. 116].

Шифрованные тексты древнего Египта – это чаще всего религиозные тексты и медицинские рецепты. Древним Египтянам была известна и стеганография. Они использовали так называемое «загадочное», или «играющее», письмо. Вот лишь один пример. На картинке (оттиск печати) изображен властный мужчина с пером в руках, над которым восходит солнце. Одновременно рядом помещен похожий рисунок, но составленный из иероглифов. Слова звучали так:

«Владыка» — «НИБ», «Перо» — «МА» (правда), «Солнце» — «РЭ» — все читалось как: «Владыка правды — РЭ». Но одновременно можно было прочесть и слово «НИБМАРЭ» — престольное имя Аменхотепа III, которому и принадлежала печать [Бабаш, 2002, с. 22].

По свидетельству древнегреческого историка Геродота в древнем Египте роль шифра обычно играл специально созданный жрецами язык. Там параллельно существовали три алфавита: письменный, священный и загадочный. Первый из них отображал обычный разговорный язык, второй мог использоваться для изложения религиозных текстов, а третий применялся предсказателями или для сокрытия смысла сообщений [Жельников, 1996].

Древние египтяне использовали и символический язык. Так, в 1998 году был дешифрован текст, записанный на каменных плитах. Этому тексту более 6000 лет, он получил название Великие Арканы Таро. В нем в символической форме трактуются принципы мироздания, говорится об абсолютной и относительной истине, и своеобразно обсуждаются законы диалектики, с которой, как выяснилось, древние египтяне были знакомы.

Наряду с защитой информации широко использовалась и дезинформация. Античные полководцы нередко прибегали к приему, заключающемуся в доведении до сведения противника ложных известий, чтобы побудить его к действиям во вред собственным интересам. Таких приемов история знает немало. Они родились еще задолго до античных времен. Так, например, еще в 1312 году до н. э. египетский фараон Рамсес II провел неудачную битву против хеттов вблизи Кадеша. До начала битвы два мнимых хеттских дезертира сообщили фараону ложные сведения. Построив битву на основе этих сведений, фараон ее начисто проиграл и едва спас собственную жизнь путем позорного бегства.

Иероглифы Древнего Египта действительно включали, хотя и в несовершенной форме, два элемента — секретность и преобразование письма, которые составляют основные атрибуты криптографии, а попытки их разгадать соответственно были элементами криптоанализа [Алферов, 2005], [Бабаш, 2002], [Кан, 2004].

Так родилась криптология (На западе часто употребляется этот термин для обозначения науки о криптографических методах защиты информации. Криптология разделяется на криптографию (науку о создании шифров) и криптоанализ, изучающий методы их взлома. В России для обозначения данной сферы человеческой деятельности

принят термин криптография). В течение первых 3000 лет ее развитие не было неуклонным. В одних местах криптология появилась самостоятельно и потом умерла вместе с породившими ее цивилизациями. В других она выжила, проникнув в литературу. Опираясь на ее литературную основу, следующее поколение могло карабкаться к новым высотам криптологии. Но продвижение к ним было медленным и прерывистым. Больше было потеряно, чем сохранено. Значительная часть древней истории криптологии представляет собой плохо подобранный букет, составленный из расцветающих, распустившихся и увядающих цветов. Накопленные знания получили простор только в начале эпохи европейского Возрождения.

Упоминания о криптоанализе имеются и в древнеиндийских источниках. В Индии, стране с древней высокоразвитой цивилизацией, люди с незапамятных времен пользовались несколькими разновидностями тайнописи. В древнеиндийских рукописях содержится изложение 64-х способов преобразования текста, а также упоминается, что тайнопись является одним из 64 искусств, которым следует владеть как мужчинам, так и женщинам [elitarium]. В учебнике Ватсыяны об искусстве любви («Камасутра») среди 64 искусств, которыми должна овладеть женщина, на 45 месте упоминается тайнопись в виде шифра простой замены. При этом отмечается, что криптография обязательна к изучению, как мужчинами, так и женщинами, и рекомендуется, как средство для связи любовников. В многих древнеиндийских рукописях содержится изложение 64-х способов преобразования текста. Среди них написание знаков не по порядку, а вразброс по некоторому правилу. Многие из приводимых способов следует рассматривать как криптографические. Приведена система замены букв. В религиозных книгах Индии указывается, что сам Будда знал несколько десятков способов письма, среди которых (по современной классификации) присутствовали шифры перестановки [Бабаш, 2002, с. 21].

В классическом древнеиндийском трактате об искусстве управлять государством, написанном между 321 и 300 годами до нашей эры, рекомендуется, чтобы глава разведывательной службы зашифровывал задания своим агентам. Там же дипломатам дается совет прибегать к криптоанализу для получения ценной информации: «При невозможности беседовать с людьми пусть посол осведомится о происходящем у врага из речей нищих, пьяных, сумасшедших,

спящих или из условных знаков, надписей, рисунков в храмах и местах паломничества» [Кан, 2004, с. 117]. И хотя автор трактата не дает никакого намека, как именно нужно читать тайнопись, тот факт, что он знает о возможности ее дешифрования, свидетельствует о некоторой искусственности в области криптоанализа. Более того, впервые в истории человечества здесь упоминается о криптоанализе в политических целях.

Не избежала соприкосновения с шифрами (или, если говорить точнее, с предшественниками шифров, так как в ней нет элемента секретности) и Библия. Как в случае с иероглифами на гробнице Хнумхотепа, преобразования письма сделаны в Библии без какого-либо явного желания скрыть содержание текста. Главной причиной, очевидно, было стремление переписчика обессмертить себя путем изменения текста, который позднее будет снова тщательно переписан и позволит пронести частицу его личности через века.

Самая знаменитая «криптограмма» в Библии связана с историей о том, как в разгар пира у вавилонского царя Валтасара человеческая рука стала писать на стене зловещие слова: «мене, текел, упарсин». Однако тайна заключается не в том, что означают эти слова. Непонятно, почему мудрецы царя не смогли разгадать их смысл.

Сами слова «мене», «текел» и «упарсин» взяты из арамейского языка, родственного древнееврейскому, и означают «исчислил», «взвешен» и «разделено». Когда Валтасар вызвал к себе пророка Даниила, последний без труда прочитал надпись и дал толкование этих трех слов: «мене – исчислил Бог царство твое и положил конец ему; текел – ты взвешен и найден очень легким; фарес – разделено царство твое и отдано мидянам и персам». При этом было обыграно значение слова «фарес», которое в арамейском языке идентично слову «упарсин». «Надпись «мене, текел, упарсин» может также означать названия денежных единиц – мина, текел (1/60 мины) и фарес (1/2 мины). Их перечисление именно в такой последовательности символизирует крушение Вавилонской империи. Учитывая возможность всех этих интерпретаций, кажется странным, что вавилонские священники не сумели прочитать зловещую надпись на стене. Возможно, они боялись сообщить Валтасару плохую новость, или, может быть, Господь открыл глаза только Даниилу. Как бы там ни было, одному Даниилу удалось разгадать эту загадку, и в результате он стал первым известным криптоаналитиком. А поскольку это библейское сказание, то и награда за успешный

криптоанализ, согласно Библии, намного превзошла какие-либо более поздние вознаграждения за аналогичные успехи в дешифровании: «Тогда... одели Даниила в багряницу, и возложили золотую цепь на шею его, и провозгласили его третьим властелином в царстве» [Кан, 2004, с. 117-118]. Вот еще один пример своеобразного «криптоанализа». В VI веке до н.э. персидский царь Дарий вторгся в скифские земли Причерноморья. Этот поход могущественного царя оказался неудачным. Скифы оказали достойное сопротивление.

Скифские послы преподнесли Дарию загадочный «подарок»: птицу, мышь, лягушку и пять стрел. Долго персы ломали голову над его смыслом. Наконец, появился один мудрый «переводчик», который растолковал это так: «Если вы, персы, не улетите, как птицы в небеса, или не спрячетесь в землю, как мыши, или не укачете в озёра, как лягушки, то не вернётесь назад и погибнете от наших стрел». Дарий отступил [Очерки, 1999, т.1, с. 15].

В Древней Греции и Риме некоторые политические, военные и религиозные деятели использовали криптографию. Среди них были греческие историк Полибий (201 – 120 годы до нашей эры) и полководец Эней, римский император Юлий Цезарь, общественный деятель Цицерон. При этом Полибий, Эней и Цезарь являются изобретателями шифров, которые впоследствии были названы их именами.

Шифр Полибия является оригинальным шифром простой замены. Приведем пример этого шифра для русского языка. Буквы алфавита в произвольном порядке вписываются в прямоугольник 5x6 (заполнение квадрата и является ключом) например, так:

	1	2	3	4	5
1	К	Р	Б	Ю	Ы
2	Ф	Т	А	Щ	О
3	Д	Н	Я	И	Е
4	С	Ь	В	М	Ш
5	Э	Г	Л	Ц	П
6	Ж	У	Х	З	Ч

Шифртекст представляет собой координаты буквы открытого текста (номер строки и номер столбца или наоборот). При шифровании слова «Греция» по данному ключу получим следующий шифртекст: 52 12 35 54 34 33.

Полибий в своей девятой книге «Всеобщая история» указал способ передачи сведений на расстояние при помощи световой факельной сигнализации из 10 факелов. Для этого он предложил использовать квадратную табличку размерами 5X5 клеток, куда в произвольном порядке выписывалась 24-буквенная греческая азбука. Сигнализируя последовательно координаты нужных букв на расстояние видимости факелов, греки достигали быстрой и безошибочной связи. Меняя же порядок букв в таблице, легко было изменять и ключ для шифрования сообщений.

Вообще греки внесли большой вклад в развитие средств передачи информации на большие расстояния. Нет сомнения, что желание передать свою волю удаленным на расстояние лицам весьма содействовало изобретению письма. У шумеров и их наследников – вавилонян и ассирийцев, так же как и у египтян, это открытие уходит в седую древность. Владыки микенской эпохи также располагали развитым, к сожалению, еще не прочитанным письмом. Представление о том, что певцы гомеровской эпохи не имели никакой письменности, оказалось на основании открытий, сделанных в течение последнего поколения, ложным. Даже обыкновенное греческое письмо, которое древние сами называли финикийским, так как оно фактически было заимствовано у финикийцев, было известно уже в IX веке до н.э., стало быть, в гомеровское время. Поэтому мы должны иначе смотреть на знаменитое место из Илиады, где царь Пройт передает с Беллерофоном предательское письмо своему тестю. Он вручил ему, повелев доставить в Азию родственному царю “злосоветные знаки, много на дщице (дощечке) складной, начертав их ему на погибель”. Так как это послание, содержавшее тайное приказание убить Беллерофона, последний не должен был видеть, то, как обычно в древности, оно должно было состоять из сложенной вдвое дощечки, обе половинки которой с одной стороны были скреплены вместе, а другой – “закрывались при помощи нитки и печати. Это мог быть весьма обычный в более древнее время, перегнутый пополам, кусок березовой коры, на внутренней стороне которого нацарапывались письма; или же, применявшаяся позже, двойная деревянная пластинка с выдолбленной поверхностью,

залитой воском, на котором при помощи грифеля нацарапывалось письмо. Какова бы ни была форма предательского письма, описанного Гомером, оно нам указывает на древнейшую разновидность секретных депеш [Дильс, 1934].

С течением времени в Греции изобреталось все более и более различных приемов передачи секретных сообщений. Один древний военный писатель Эней Тактик, написавший в середине IV в. до н.э. книгу об осаде городов, считает этот предмет, играющий естественно большую роль при осаде, настолько важным, что посвящает ему целую большую главу. Он насчитывает там 16 различных способов передачи секретных депеш и шифрованных донесений, из которых некоторые имеют применение еще и ныне. Например, первый способ секретных сообщений достигается при помощи любой книги, в которой точкой отмечаются соответствующие буквы. У тайно влюбленных он должен встречаться еще и теперь. Возлюбленной посылают томик стихов Шиллера, а отмеченные точкой буквы какого-либо стихотворения, будучи расположены вместе в ряд, передают тайное сообщение.

Подобные сигналы должны были находить применение в тех случаях, когда было желательно быстро собрать союзников для отражения нападения. Так, Демосфен в своей речи о венце описывает знаменитый эпизод, когда при известии о нападении Филиппа на Элатею (339 год до н.э.) афиняне воспользовались сплетенными из ивняка рыночными палатками для разведения сигнального огня, который должен был поднять по тревоге всех жителей Аттики, способных носить оружие. Подобным же образом были устроены и сторожевые вышки в Швейцарии, описанные Штольбергом; “Такие сторожевые вышки расставлены по всей Швейцарии, благодаря чему обеспечивается возможность предупредить всех союзников-швейцарцев в случае готовящегося нападения. Как только замечен один огонь, зажигают соседний, и в течение 24 часов все союзные отряды приводятся в боевую готовность” [Дильс, 1934].

Еще Гомер упоминает о сигнальных огнях, которые ночью передавались жителями из осажденного города. Послегомеровский эпос “О возвращении” повествует о ложных сигнальных огнях Навплия, из чего можно заключить, что такие огни и маяки сооружались на островах и утесах Эгейского моря. Древние считали Паламеда, сына Навплия, изобретателем сигнализации при помощи огней. Геродот упоминает о том, что Мардоний после битвы при

Саламине надеялся при помощи сигнальных огней передать через острова в Азию обратившемуся в бегство царю Ксерксу известие о взятии Афин персами; но отсюда следует вывод, что такие приспособления существовали, по крайней мере, в Азии. Во время персидской войны греки-островитяне также поддерживали подобные посты сигнальных огней, поскольку Геродот упоминает, что эллины у Артемизия, на северной оконечности острова Эвбеи, получили с лежащего напротив острова Скиатоса сообщение огнями о том, что два греческих корабля взяты персами [Дильс, 1934].

Наиболее наглядное описание связи при помощи сигнальных огней, существовавшей в V веке в Греции, мы имеем в драме Эсхила “Агамемнон”. Немыслимо, чтобы автор все это мог выдумать сам, если допустить, что подобное телеграфирование сигнальными огнями не имело применения хотя бы по временам (рис. 1.1). “Хор спрашивает Клитемнестру, когда пала Троя. Царица на это отвечает:

Клитемнестра.

В ночь самую, родившую день этот.

Хор.

Кто ж из гонцов пройти так скоро мог бы?

Клитемнестра.

Гефест сам с Иды яркий свет послал.

Костры же, меж собой передаваясь,

Несли сюда тот вестовой огонь.

Шлет Ида на Гермесову скалу

На Лемнос, с острова ж великий светоч

Утес Афонский Зевса принял третьим

С своим костром такой могучей силы,

Чтоб весело бегущий свет понесся

Через море и, златым лучом, как солнце,

Сверкнув, оповестил Макиста выси.

А тот без замедленья, сну безопасно

Не отдаваясь, дело вестника

Исполнить не преминул.

И далеко к струям Эврипа на гору Мессапий

Тот свет костра, придя, сигнал приносит

Для сторожей. Те тоже засветили

И дальше весть послали, разведя

Огонь там кучей вереску сухого.

Он, разгоревшись, не ослабевая,

Перескочил долину всю Асопа,
Как ясный свет луны, и Киферона
Достиг высот, где новую уж смену
Огня посыльного он пробудил.
Далекий свет не ускользал от стражи.
И больший, чем приказано то было,
Костер там разводили. Свет сверкнул
Через озеро Горгопу и, горы
Достигнув Эгипланкта, не давал
Огня завету даром пропадать.
Оттуда шлют огромный столб огня,
Нескупо разжигая, чтоб глядящий
Над Сароническим заливом мыс
Превысил он и дальше бросил, свет
Взвился и вот на Арахнейские
Пришел высоты – пост дозорный наш,
Соседний уж, затем на кровлю эту
Дворца Атридов падает сей свет,
Не первый тот костра на Иде отблеск.
Такой порядок бега был огней.
Один другому свой черед вручал.
А побеждает тот, кто начал бег,
А кто последним в беге том бежал.
О знаке этом я тебе и говорю.
Супруг прислал его из Трои мне.

В столь высоко поэтической форме описан древнейший оптический телеграф, который передал весть о победе над Троей от горы Иды через остров Лемнос на Афон, затем на юг через Эвбею и Беотию и Киферон, далее через Истм до Арахнейских высот у Эпидавра и, наконец, в Микенский замок. Все же это художественное описание не может претендовать на буквальную истинность. Точные арифметические вычисления показали, что расстояние в 180 км (между Афоном и Макистом на Эвбее) едва ли позволило сигнализировать огнями. В действительности здесь следовало бы ввести, по крайней мере, еще одну промежуточную станцию [Дильс, 1934].



Рис. 1.1. Расположение постов сигнальных огней по “Агамемнону”
Эсхила.

Несмотря на это, мы должны принять, что ни одна из упомянутых автором станций не могла быть выбрана, если бы не

имелись в виду существующие или когда-либо раньше существовавшие в этих местах сигнализационные приспособления [Дильс, 1934].

Подобное телеграфирование при помощи огней имеет, однако, тот большой недостаток, что допускает передачу лишь таких сообщений, содержание которых заранее твердо установлено. И если даже посредством согласования известных сигналов, как в описываемом Гомером случае, и было возможно точное извещение, все же этот способ не осуществлял телеграфию в нашем смысле слова. Уже упомянутый Эней Тактик сообщает в отрывке, сохранившемся у Полибия, об остроумном приборе, который можно назвать водяным телеграфом (см. рис. 1.2):

“Если хотят доставить срочное сообщение, то нужно взять два глиняных сосуда одинаковой ширины и глубины. Глубина их должна составлять около 3 локтей (1 1/3 м), ширина 1 локоть (44 см). Затем следует вырезать два куска пробки, имеющие ширину, немного меньшую, чем размер обоих глиняных сосудов. На них укрепляется стойка, имеющая зарубки, удаленные друг от друга на расстояние 3 дюймов (5,5 см). Таким образом, вся стойка разграничена на 24 поля или деления. На них наносятся события, обычные во время войны. Например, на первом делении – “всадники вторглись в страну”; на втором – “тяжело вооруженная пехота” и т.д.; на третьем – “легко вооруженная” и т.д.; затем – “корабли”, “провиант”, пока на 24 делениях не будут поставлены наиболее вероятные, могущие быть заранее предвиденными события. Разумеется, надписи и деления на обеих стойках должны быть совершенно одинаковы. Затем оба глиняных сосуда нужно снабдить выпускными отверстиями, расположенными у дна и имеющими, конечно, одинаковое сечение и положение. Потом отверстия сосудов затыкают, наполняют сосуды до краев водой, а пробку с размеченной стойкой устанавливают в виде поплавка. Теперь аппараты готовы для телеграфирования. Один остается на станции отправления, другой передается на станцию назначения.

Когда происходит один из предусмотренных случаев, ночью на станции отправления, прежде всего, подается сигнал факелом. Соответствующим сигналом станция назначения сообщает о своей готовности. Следовательно, в этот момент оба факела подняты вверх. Тогда на станции отправления факел опускается. Это является

условным знаком, что отверстие глиняного цилиндра открыто, и вода медленно вытекает.

Как только станция назначения заметила, что на той стороне факел опустил, пробка из сосуда вытаскивается, и здесь вода начинает вытекать с такой же скоростью, как и на станции отправления. Между тем при равномерном понижении уровня воды в сосудах оба пробковых поплавка вместе со стойками также погружаются в сосуд.



Рис. 1.2. Водяной “телеграф”.

Когда надпись, содержащая нужное донесение, поравняется с краем сосуда, станция отправления снова подымает факел. Этот сигнал означает: “Закрыть отверстие”. На станции назначения, тотчас смотрят, какая надпись видна над краем. Это и будет передаваемое сообщение.

Недостатком этой остроумной системы Полибий считал, что количество предусматриваемых случаев слишком ограничено и что, прежде всего, никакие точные числовые указания не могут быть переданы. Ведь желательно было знать не только тот факт, что в страну вторглись всадники, а также и количество последних.

Так как из указанных Энеем размеров следует, что должно быть сделано именно 24 деления, мы предполагаем, что изобретатель намеревался создать телеграфный алфавитный аппарат. Греческий алфавит, как тогда было принято, имел 24 буквы, и не 24 происшествия, но всевозможные извещения должны были

передаваться при помощи 24 делений с буквами. Правда, это было несколько сложно, потому что, когда буквы не следовали одна за другой, приходилось особый сигнал приказывать вновь наполнить сосуды. Но даже если каждая отдельная буква передавалась со свежим наполнением сосуда, можно было в течение одного часа с удобством передать 20 букв и, следовательно, в течение всей ночи множество сообщений.

Эней говорит лишь о сигналах, передаваемых ночью, но ясно, что при помощи флагов этим аппаратом можно пользоваться также и днем. Конечно, такая передача депеши была несколько длительной и требовала крайней тщательности от обслуживающего персонала. Военный практик, подобный Энею или предшественнику, у которого Эней позаимствовал эту систему, сделал аппарат применимым к обычной практике посредством готовых надписей на каждом из 24 делений. Происхождение сокращенного способа удастся проследить на целое поколение ранее Энея. Эней писал между 360-346 годами до н.э., сокращенная же система возникает в Сицилии во время царствования Дионисия Старшего (в 410-367 годы до н.э.) и берет свое начало от карфагенян. Более поздний военный писатель Полиэн сообщает, что во время войны с Дионисием карфагеняне пользовались парой одинаковых (стеклянных) сосудов клепсидр, охваченных одинаково расположенными кольцами. На этих кольцах имелись различные краткие распоряжения, например: “прислать военные корабли” или “баржи”, или “не хватает денег” или же “машины”. Одни такие водяные часы карфагеняне оставили в Сицилии, другие же отправили в Карфаген. Вытекание воды и ее остановка у определенного кольца регулировались сигналами факелов, подобно тому как и в описанном выше аппарате.

Следует, конечно, заметить, что нельзя передать сигналы факелом прямо с Сицилии на расстояние 220 км. Надлежало бы, следовательно, ввести промежуточную станцию: (примерно на о. Коссира), но даже и в этом случае расстояние было бы чрезмерным. Вероятно, аппарат действовал вовсе не между Африкой и Сицилией, как указывает Полиэн, а между отдельными местами на самой Сицилии. Мы упомянул о гипотетическом алфавитном телеграфе с 24 делениями, а также о карфагенском телеграфе с клепсидами и, наконец, остановились на водяном аппарате Энея, представлявшем как бы нечто среднее между двумя предыдущими системами. Теперь покажем, что добавила к этим изобретениям наиболее блестящая

эпоха античной техники. К счастью, знаменитый историк и стратег Полибий дал нам точное описание одного сигнального телеграфа (см. рис. 1.3), изобретенного александрийскими инженерами Клеоксеном и Демоклетом и усовершенствованного самим Полибием. Станции отправления и назначения приспособлены только для действия ночью. На каждой станции устраиваются две стены с зубцами, имеющими по 5 промежутков между зубцами на расстоянии 2 футов один от другого. При помощи факелов, выставляемых в эти промежутки, можно подавать сигналы станции, расположенной напротив. Далее, каждая станция имеет код, содержащий 24 буквы греческого алфавита в следующей порядке:

Таблица

I $\alpha - \varepsilon$

II $\zeta - \kappa$

III $\lambda - \omicron$

IV $\pi - \upsilon$

V $\varphi - \omega$

Телеграфируют же следующим образом: пусть, например, нужно передать такое сообщение: “Критян дезертировало 100”. Прежде всего, передается буква “к”. Она находится во второй таблице. Следовательно, в промежутках между зубцами левой стены, предназначенной для указания номера таблиц, выставляется 2 факела. Станция назначения отмечает это у себя. Затем на стене справа выставляется 5 факелов, так как “к” является 5-й по порядку буквой во второй таблице. (Стена справа предназначена для указания последовательности отдельных букв в каждой из 5 групп, сигнализируемых со стены слева.) Итак, станция назначения отмечает – таблица 2-я, буква 5-я. Это и будет “к”. Далее идут буквы “р”, “и”, “т” и следующие. Эта система явно содержит зародыш нашей нынешней телеграфии. Сомнительно, в какой мере Полибий и его александрийские предшественники подверглись влиянию со стороны описанной мною системы сигнализации 24 буквами. Возможно, что это древнее изобретение, поскольку оно не вошло в практику, было забыто подобно многим идеям такого рода [Дильс, 1934].



Рис. 1.3. Факельный телеграф, описываемый Полибием.

Нет ссылки в тексте на этот рис стр 31

Легко заметить, что эта система весьма сложна; даже сам Полибий заранее предвидит подобное возражение. Но, рассуждает он, сначала и обычная жизнь довольно сложна до тех пор, пока к ней не привыкнешь. Высчитали, что вышеупомянутое сообщение “критян дезертировало 100” потребует для передачи до 200 сигналов факелами и что это может быть проделано в течение около получаса. При удовлетворительном обслуживании это время, наверное, могло быть еще значительно сокращено. Но если даже мы примем и максимальную величину, то все же эта затрата времени никоим образом не является причиной неуспеха системы Полибия на практике. Вернее всего, главной причиной здесь является незначительная дальность действия сигналов, подаваемых факелом. Вследствие рассеяния света отдельные факелы можно ясно различать лишь на расстоянии примерно 700 метров. Некоторое улучшение этого способа может быть достигнуто, путем применения лишь одного факела; его поднятием и опусканием за стену дают один за другим сперва 2, а затем 5 сигналов. В этом случае, во избежание путаницы темп передачи должен быть значительно более медленным.

Во всяком случае, для таких оптических телеграфов древности нужно было множество промежуточных станций. Такая система промежуточных пунктов показалась, по-видимому, древним слишком громоздкой и дорогостоящей. По этой причине изобретение и не имело никакого практического успеха. Также, очевидно, не нашло никакого практического применения и улучшение, сделанное в аппарате Полибия каким-то неизвестным римлянином, о чем нам сообщает Юлий Африканский.

В 1659 году один немец, Вэгелин из Клерберга, смотритель дворца в Нассау, выдумал подобную же систему, вероятно,

позаимствовав ее у Полибия. Но при этом он воспользовался уже изобретенной тогда подзорной трубой и приспособил эту систему для работы в дневное время. Писатель римского времени Вегеций кратко упоминает (*de re militari* III) о телеграфировании при помощи балок, поднимаемых и опускаемых на башне [Дильс, 1934].

Шифр Полибия применяли декабристы, когда после восстания 1825 года некоторые из них находились в заключении в Петропавловской крепости. Этот шифр нередко называли «тюремным шифром». Он был удобен тем, что им можно было легко перестукиваться через стенки тюремных камер, в данном случае буквы вписывались в прямоугольник в алфавитном порядке. Например, буква Б стояла в первой строке на втором месте, тогда она передавалась при перестукивании следующим образом: удар – длинная пауза – два коротких удара.

Неоднократно упомянутый выше Эней Тактик в IV веке до н.э. предложил устройство, названное впоследствии "диском Энея" (см. рис. 1.4). Принцип его был прост. На диске диаметром 10-15 см и толщиной 1-2 см высверливались отверстия по числу букв алфавита. В центре диска помещалась "катушка" с намотанной на ней ниткой достаточной длины. При зашифровании нитка "вытягивалась" с катушки и последовательно протягивалась через отверстия, в соответствии с буквами шифруемого текста. Диск и являлся посланием. Получатель послания последовательно вытягивал нитку из отверстий, что позволяло ему получать передаваемое сообщение, но в обратном порядке следования букв. При перехвате диска недоброжелатель имел возможность прочесть сообщение тем же образом, что и получатель. Но Эней предусмотрел возможность легкого уничтожения передаваемого сообщения при угрозе захвата диска. Для этого было достаточно выдернуть "катушку" с закрепленным на ней концом нити до полного выхода всей нити из всех отверстий диска.

Идея Энея была использована при создании и других оригинальных шифров замены. Скажем, в одном из вариантов вместо диска использовалась линейка с числом отверстий, равных количеству букв алфавита. Каждое отверстие обозначалось своей буквой; буквы по отверстиям располагались в произвольном порядке. К линейке была прикреплена катушка с намотанной на нее ниткой. Рядом с катушкой имелась прорезь. При шифровании нить протягивалась через прорезь, а затем через отверстие, соответствующее первой букве

шифруемого текста, при этом на нити завязывался узелок в месте прохождения ее через отверстие; затем нить возвращалась в прорезь и аналогично зашифровывалась вторая буква текста и т.д. После окончания шифрования нить извлекалась и передавалась получателю сообщения. Тот, имея идентичную линейку, протягивал нить через прорезь до отверстий,

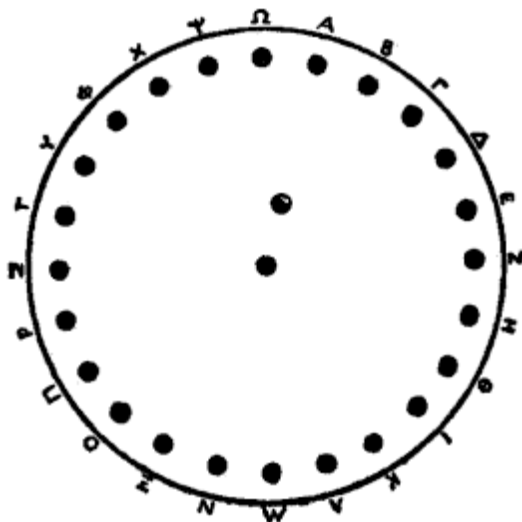


Рис. 1.4. Диск с отверстиями для пересылки секретных сообщений

Нет ссылки в тексте на этот рис стр 33

определяемых узлами, и восстанавливал исходный текст по буквам отверстий. Это устройство получило название "линейка Энея". Такой шифр является одним из примеров шифра замены: когда буквы заменяются на расстояния между узелками с учетом прохождения через прорезь. Ключом шифра являлся порядок расположения букв по отверстиям в линейке. Посторонний, получивший нить (даже имея линейку, но без нанесенных на ней букв), не сможет прочитать передаваемое сообщение. Аналогичное "линейке Энея" "узелковое письмо" получило распространение у индейцев Центральной Америки. Свои сообщения они также передавали в виде нитки, на которой завязывались разноцветные узелки, определявшие содержание сообщения. Заметным вкладом Энея в криптографию является предложенный им так называемый книжный шифр,

описанный в сочинении "Об обороне укрепленных мест". Эней предложил прокалывать малозаметные дырки в книге или в другом документе над буквами (или под ними) секретного сообщения. Интересно отметить, что во время Первой мировой войны германские шпионы использовали аналогичный шифр, заменив дырки на точки, наносимые симпатическими (невидимыми) чернилами на буквы газетного текста. Книжный шифр в современном его виде имеет несколько иной вид. Суть этого шифра состоит в замене букв на номер строки и номер этой буквы в строке и заранее оговоренной странице некоторой книги. Ключом такого шифра является книга и используемая страница в ней. Этот шифр оказался "долгожителем" и применялся даже во времена Второй мировой войны.

Одним из первых полководцев, использовавших массовый перехват писем, был Александр Македонский. Во время азиатских походов его солдаты испытывали многочисленные лишения. Росло количество недовольных солдат. Шли разговоры о прекращении войны и возвращении домой. Македонский решил выявить и наказать зачинщиков смуты. Для этого он разрешил солдатам писать домой. Одновременно был организован перехват солдатских писем. Смутьяны были выявлены и направлены в первые в мире создавшиеся штрафные отряды. Учителем Македонского был Аристотель. В беседах с учеником великий ученый внушал будущему полководцу, что далеко не все тайны и откровения можно доверять письму. Как видим, советы учителя оказались для Македонского весьма полезными. В дальнейшем правило цензурного просмотра писем военнослужащих было принято во всех армиях мира [Гольев, 2008].

Помимо шифрования для защиты сообщений от перехвата использовались различные стеганографические способы. Упоминание об одном интересном способе сокрытия факта передачи информации имеется в работе древнегреческого историка Геродота. В древней Греции было распространено письмо на восковых дощечках. Слова писались на поверхности воска при помощи специального стила. Для передачи секретного послания делали следующее. Воск соскабливали с дощечек, писали послание прямо на дереве, а потом дощечки заново покрывали воском. Написанный текст становился невидимым, при этом сами таблички выглядели без изменений и потому не вызывали подозрений. Таким образом, скрывалось не только сообщение, но вообще факт его существования. Кроме Древней Греции, этот способ использовался в Древнем Риме.

Геродот описал и еще один оригинальный способ тайной передачи сообщений. Передача послания производилась с использованием головы раба. В 474 году до нашей эры один из греческих правителей — тиран Гистий попал в плен к персидскому царю Дарию. Пленник жил в Сузах и не имел возможности послать письмо своим родным в азиатский город Милет. Дарий обязательно задержал бы письмо. Тогда Гистий выбрил голову своему рабу и вытатуировал на ней короткое сообщение. Через некоторое время, когда волосы отросли, раб отправился в Милет. Он добрался до родственников Гистия, которым оставалось лишь побрить ему голову и прочитать сообщение.

Другой стеганографический способ придумали китайцы. В Китае письма писали на полосках шелка. Для сокрытия сообщений полоски с текстом письма сворачивали в шарики и покрывали воском. После этого посыльные их глотали.

Шифр Цезаря представлял собой упрощенный вариант шифра простой замены. Вот, что пишет про него римский историк Гай Светоний: «...существуют и его (Цезаря - авт.) к Цицерону и письма к близким о домашних делах: в них, если нужно было сообщить что-нибудь негласно, он пользовался тайнописью, т.е. менял буквы так, чтобы из них не складывалось не одного слова. Чтобы разобрать и прочитать их, нужно читать всякий раз четвертую букву вместо первой, D вместо A и так далее» [Алферов, 2005, с. 11]. Таким образом, нижняя строка замены образовывалась циклическим сдвигом алфавита открытого текста на 3 буквы влево:

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC

Тогда слово CAESAR (Цезарь) шифровалось бы так ZXHVXU. Преемник Цезаря - Октавиан Август использовал такой же шифр, но со сдвигом на 4 буквы.

Первый шифровальный прибор – сциталу (другой вариант написания скитала) (см. рис. 1.5) создали в Спарте примерно в V–VI веках до нашей эры. В отличие от применявшихся в древности шифров замены здесь был реализован шифр перестановки. Сцитала упоминается в трудах историка Ксенофонта [Ксенофонт, 1996]. Другой греческий историк Плутарх так описывает способ шифрования с помощью этого прибора:

«Отправляя к месту службы начальника флота или сухопутного войска, эфоры (военачальники – авт.) вручают отъезжающему круглую палку (цилиндрической формы – авт.). Другую, совершенно одинаковой длины и толщины, оставляют себе. Эти палки и называют скиталами. Когда эфорам нужно сообщить какую-нибудь важную тайну, они вырезают длинную и узкую, вроде ремня, полосу папируса, плотно, без промежутков наматывают ее на свою скиталу и пишут на нем текст. Затем снимают полосу и без палки отправляют ее военачальнику. Так как буквы на ней стоят без всякой связи, разбросаны в беспорядке, прочитать написанное он может, только взяв свою скиталу и намотав на нее вырезанную полосу, чтобы,водя глазами вокруг палки и переходя от предыдущего к последующему, иметь перед собой связное сообщение» [Плутарх 1994, с. 496.]. Ключом является диаметр цилиндра.

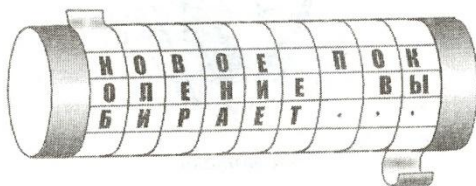


Рис. 1.5 Считала.

Нет ссылки в тексте на этот рис стр 36

Одним из первых дешифровальщиков древности был знаменитый греческий философ Аристотель (384-322 до н.э.). Этот выдающийся ученый, участник Академии Платона, учитель Александра Македонского, охватил почти все доступные в то время знания. Перед математикой его заслуга в том, что он дал первое систематическое изложение логики и теории доказательств. В криптографии Аристотель известен как автор способа дешифрования считалы. Он предложил использовать для этого конусообразное «копье», на которое наматывался перехваченный ремень, который передвигался по оси до того положения, пока не появлялся осмысленный текст.

Применял шифрование и другой великий математик древности – Пифагор. Знаменитый греческий философ Платон отмечает, что "с великим трудом и большой ценой добыл один из манускриптов

Пифагора, который никогда не записывал свое эзотерическое учение иначе, как тайными знаками и под различными символами". Впоследствии Платон передал шифрованный текст Пифагора Аристотелю.

Использовали в Древней Греции и способ получения секретной информации, известный теперь как технические каналы утечки. Сиракузский тиран Дионисий Старший (IV в до нашей эры), отличавшийся крайней подозрительностью, содержал своих пленников в помещениях, своды которых были устроены таким образом, что малейший шорох оттуда доходил до тайника, сделанного в форме уха, где Дионисий подслушивал их разговоры. Этот тайник получил название Дионисова уха.

Криптография средневековья

После распада Римской империи в Европе наступили так называемые «темные века», народы фактически опустились до варварства. Наука, ремесла, торговля, искусство пришли в полный упадок. По свидетельству святого Джерома "весь мир погрузился в руины". Лишь к концу средневековья применение криптографии начинает возрождаться [Жельников, 1996, с. 23]. Большинство населения Европы того времени было неграмотным, что уж говорить о шифровании. В условиях, когда грамотность была крайне низка, зашифровывать сообщения не было необходимости, да и самих письменных сообщений практически не было. Так, король франков и Римский император Карл Великий (742-814 г.г.) (см. рис. 2.1) научился читать и писать в возрасте 50 лет, а после этого захотел сохранять свои послания в тайне. Один из приемников Карла император Лотар (Lothar) (840-855 г.г.) посылал своим корреспондентам сообщения, замаскированные под цитаты из священного писания [Черняк, 1991, с. 12].



Рис. 2.1 Карл Великий. **Нет ссылки в тексте на этот рис стр 38**

Хотя в целом в Европе криптография находилась в состоянии застоя вплоть до наступления эпохи Возрождения, шифры все же применялись. Однако это были весьма примитивные криптосистемы - фразы писались по вертикали или в обратном порядке, гласные заменялись точками, использовались иностранные алфавиты (например, древнееврейский и армянский). В шифрах простой замены использовался упрощенный шифр Цезаря, где каждая буква заменялась на последующую в алфавитном порядке, а в более сложных системах буквы заменялись на специально придуманные знаки. По выражению советского историка Е. Черняка, «в эпоху, когда мало кто мог бы прочесть и простое письмо, редко было нужно прибегать к шифровке» [Черняк, 1991, с. 12]. Однако здесь, по-видимому, имеется в виду защита частной информации от «простолюдинов», а не сохранение государственных тайн от вполне образованного противника [Бабаш, 2002, с. 46]. Не таким сильным был упадок криптографии в Византии, сохранившей многие античные традиции. Но и здесь криптографические системы предельно упростились и были легко уязвимы.

В раннем средневековье шифры появились и в регионах, которые в те времена не относились к развитым. Сектанты в Ираке пользовались таинственными знаками из-за страха перед мусульманами. Аналогичная картина наблюдается у тибетцев, у членов тайных обществ в Нигерии, в Таиланде и т.д. Эти шифры представляли собой простую замену знаков открытого текста на другие, в том числе и специально придуманные, нередко похожие на

обычные знаки письма. Использованные шифры интересны тем, что в них нередко буквы заменялись на экзотически написанные координаты их положения в специальном расположении букв алфавита (некоторое подобие шифра Полибия). Интересен и другой прием. Слово писалось побуквенно так, как сами буквы фонетически звучат в алфавите. Например, слово ФОНТАН могло быть записано в виде ЭФОЭНТЭАЭН. Были предложены и другие экзотические замены.

В раннем средневековье в Скандинавии, Британии, Ирландии и территории нынешней Германии, а так же землях, заселенных древними славянами широко использовалось руническое письмо. Руны (то есть знаки древнескандинавского алфавита) в алфавите были разбиты на три группы по восемь в каждой (см. рис. 2.2).

III						II						I					
ƿ						:*						↑					
f						h						t					
1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6

Рис. 2.2 Скандинавские руны.

Основная система шифрования представляла собой шифр замены – каждой руне соответствовали два знака шифртекста (обычно косые черточки разной длины). Число черточек сверху обозначало номер группы, а снизу – номер руны в группе. Встречались и усложнения этой системы, например руны в группах перемешивались (см. рис. 2.3).

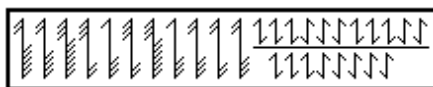


Рис. 2.3 Рунный шифр простой замены

До наших дней дошел памятник древней шведской криптографии – рёкский камень. Этот камень высотой более 4 метров находится на кладбище деревни Рёк. На нем нанесено 770 зашифрованных рун. Встречаются шифрованные рунические надписи и в других регионах Швеции.

Несмотря на то, что позднее в странах Скандинавии стала применяться латинская графика, руническое письмо употреблялось там до XIX века. Однако в XVI-XVIII веках весьма небольшое количество людей знало рунические алфавиты, поэтому руническая запись даже без шифрования обеспечивала сохранение тайны переписки. В частности руны для защиты информации использовал шведский генерал Якоб де ла Гарди во время тридцатилетней войны (1618-1646 годов) [Бутырский, 2007].

Отметим, что в течении всей эпохи средневековья криптология была поражена болезнью, которая сохранилась до более позднего времени, а именно – убежденностью многих людей в том, что криптография, а тем более криптоанализ являются разновидностями черной магии. Набор непонятных букв или символов, сам по себе похожий на заклинание, воспринимался как нечто магическое, а люди, извлекающие из этого набора символов смысл, расценивались как колдуны или гадалы, что не могло не наложить свой отпечаток на отношение к ним в христианской Европе. С первых дней своего существования криптография преследовала цель спрятать содержание важных разделов письменных документов, имевших отношение к таким сферам магии, как гадание и заклинание. В одной из рукописей о магии, датируемой III веком, используется шифр, чтобы скрыть важные части колдовских рецептов. Криптография часто была на службе магии во времена средневековья, и даже в эпоху Возрождения с помощью шифров алхимики засекречивали важные части формул получения философского камня. Сходство между магией и криптографией подчеркивалось и другими факторами. Помимо криптографии, таинственные символы использовались в таких понятных лишь посвященным в областях магических знаний, как астрология и алхимия, где, подобно знакам открытого текста, каждая планета и каждое химическое вещество имели специальный знак. Как и зашифрованные слова, заклинания и магические формулы, вроде «абракадабры», походили на чепуху, но в действительности были сильны скрытым значением.

Во времена средневековья европейская криптография приобрела сомнительную славу, отголоски которой слышатся и в наши дни. Криптографию стали отождествлять с черной магией, с некоторой формой оккультизма, астрологией, алхимией, еврейской каббалой. К шифрованию информации призывались мистические

силы. Так, например, рекомендовалось использовать "магические квадраты".

В квадрат размером 4 на 4 (размеры могли быть и другими) вписывались числа от 1 до 16. Его магия состояла в том, что сумма чисел по строкам, столбцам и полным диагоналям равнялась одному и тому же числу – 34. Впервые эти квадраты появились в Китае, где им и была приписана некоторая "магическая сила". Приведем пример:

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Шифрование по магическому квадрату производилось следующим образом. Например, требуется зашифровать фразу: "Приезжаю сегодня". Буквы этой фразы вписываются последовательно в квадрат согласно записанным в них числам, а в пустые клетки ставятся произвольные буквы.

16У	3И	2Р	13Д
5З	10Е	11Г	8Ю
9С	6Ж	7А	12О
4Е	15Я	14Н	1П

После этого зашифрованный текст записывается в строку:

УИРДЗЕГЮСЖАОЕЯНП

При **расшифровывании** в разных местах это понятие пишется по-разному (расшифрование, тоже правильно в зависимости от контекста, зашифрованный текст вписывается в квадрат, и открытый текст читается в последовательности чисел "магического квадрата". Данный шифр – обычный шифр перестановки, но считалось, что особую стойкость ему придает волшебство "магического квадрата".

Иногда мистика, чародейство, магия, оккультизм сознательно объединялись с криптографией. Тем самым человек, знакомый с криптографией, надевал на себя маску чародея, чем вызывал трепет у окружающих. Как заметил один из крупнейших криптографов XX века У. Фридман (США), человек, утверждающий связь криптографии с

черной магией, должен «поневоле ежедневно общаться с нечистой силой, чтобы добиться больших успехов в криптографии» [Бабаш, 2002, с. 51].

Вдобавок многие люди, которые хвастались своей способностью разгадывать шифры, одновременно похвалялись и умением слышать человеческие голоса, будучи глубоко под землей, или даром телепатии. Естественно, что впоследствии эти две области стали обсуждаться вместе – поскольку, мол, они всегда развивались бок о бок. Мнение о том, что криптоанализ является по своей природе черной магией, происходит и от поверхностного сходства между криптоанализом и гаданием. Извлечение смысла из шифртекста казалось точно таким же делом, что и получение знаний путем изучения расположения звезд и планет, длины линий и мест их пересечения на ладони, внутренностей овец, положения кофейного осадка в чашке. Видимость брала верх над реальностью. Простодушные усматривали магию даже в обычном процессе расшифрования. Другие, более искушенные, видели ее в криптоанализе, так как вскрытие чего-то глубоко спрятанного казалось им непостижимым и сверхъестественным.

Ни в одном из упомянутых выше случаев применения тайнописи нет подтверждения существованию криптоанализа как науки. Время от времени факт дешифрования текста имел место. Подтверждением тому служат истории с пророком Даниилом или с какими-нибудь египтянами, которые разгадали отдельные иероглифические надписи на могильных памятниках. Но научного криптоанализа не существовало ни в Египте с Индией, ни в Европе в период примерно до начала XV века. Была только криптография.

При этом все же следует отметить, что шифрами пользовались не только колдуны и чернокнижники. Случалось и так, что даже к богу обращались с зашифрованными посланиями. Богу все доступно, а шифр защищает послание от постороннего любопытства. Так в VI веке верующий человек нацарапал на стене коптского монастыря в Египте зашифрованную шифром простой замены просьбу: «Во имя бога, я, Виктор, бедный человек, прошу – помните меня!». Бог, по-видимому, выполнил просьбу Виктора; его имя открыли и прочитали археологи много веков спустя [Бабаш, 2002, с. 45].

Первыми открыли и описали научные методы криптоанализа арабы примерно в VIII - IX веках. Этот народ создал одну из самых развитых цивилизаций, которую когда-либо знала история. Арабская наука процветала. Медицина и химия, астрономия и математика у

арабов стали самыми лучшими в мире (отметим, что многие научные термины, например «алгебра», «щелочь», «зенит» пришли к нам от арабов) [Сингх, 2007, с. 29]. Мощная созидательная энергия арабской культуры, которую ислам лишил портретной живописи и скульптуры, дала плоды на ниве литературы. Распространились различные ремесла, от исламских мастеров дошли до нас великолепные картины, изысканны резные украшения и ткани исключительной отделки. Развивалась система государственного управления, а как уже неоднократно упоминалось, с развитием государственных институтов появляется необходимость применения различных методов защиты информации. Разумеется, не обошли своим вниманием арабы и криптографию. Получило широкое распространение составление словесных загадок, ребусов и каламбуров. Грамматика стала главным учебным предметом и включала в себя тайнопись. Тайнопись и ее значение упоминается в сказках Шехерезады "Тысяча и одна ночь". Да и само слово «шифр» - имеет корни в арабском слове "цифра". Кстати цифры, которыми мы сейчас пользуемся, называются «арабскими», хотя на самом деле они пришли в Европу через Ближний Восток из Индии. Сейчас арабы, как и все в мире, пользуются десятичной системой счисления, однако написание цифр серьезно отличается от принятого на Западе (см. рис. 2.4).

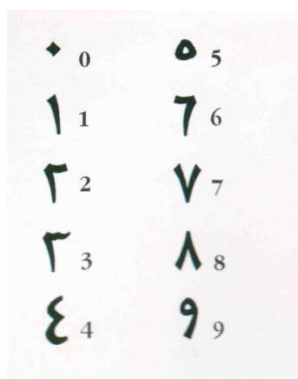


Рис. 2.4 Современные арабские цифры

Арабская цивилизация была способна не только приобретать и накапливать знания, но и распространять их, поскольку к этому времени она уже обладала искусством изготовления бумаги, проникшим сюда из Китая. Изготовление бумаги дало толчок

появлению профессий переписчиков и изготовителей бумаги (warrāqīn, или “тех, кто занимается бумагой”, - людей, которые копировали рукописи и поставляли бумагу для расцветающего издательского дела). В пору максимального расцвета арабской культуры ежегодно издавались десятки тысяч книг, причем только в предместье Багдада было более сотни книжных лавок. Помимо таких классических произведений, как упомянутая выше, «Тысяча и одна ночь», в здесь продавались также учебники и пособия по различным наукам, благодаря чему арабское общество оставалось самым грамотным и образованным в мире.

Процветание арабской цивилизации было в значительной степени обусловлено тем, что общество было богатым и мирным. В отличие от своих предшественников, халифы династии Аббасидов (Династия арабских халифов в 750-1258 гг., происходят от Аббаса, дяди пророка Мухаммеда, во времена их правления в VIII-IX веках арабский Халифат достиг своего наивысшего расцвета. Он включал в себя страны Ближнего и Среднего востока, Северной Африки, а также одно время почти всю территорию современной Испании, столица Халифата была в Багдаде) не так уж стремились завоевывать новые территории и покорять другие народы; вместо этого они приступили к созданию организованного и процветающего общества. Низкие налоги поощряли развитие коммерческой деятельности и вели к росту торговли и предпринимательства, а строгие законы сократили взяточничество и обеспечили защиту населения. Все это опиралось на эффективно действующую систему управления, чиновники же, в свою очередь, полагались на систему передачи сообщений, безопасность которой обеспечивалась за счет использования шифрования. Документально подтверждено, что, помимо политической и военной информации, чиновники зашифровывали также сообщения о различных аспектах функционирования системы государственного управления, например, сведения о налогах. То есть уже в то время криптография у арабов уже широко применялась и ее использование было обычным делом. В связи с этим во многие руководства для чиновников, к примеру, в “Adab al-Kuttāb” (“Руководство для секретарей”) X века, вошли разделы, посвященные криптографии.

Некоторые историки даже считают, что криптография как наука зародилась именно в арабском мире. На Арабском Востоке, появились книги не только с описаниями, известных на тот момент, систем шифрования, но и впервые в истории было рассказано о

криптоанализе (дешифровании). [Бабаш, 2002, с. 52], [Сингх, 2007, с. 29-30] [Кан, 2004, с. 120].

Однако прежде чем подробно рассказать о достижениях арабов в области криптоанализа, рассмотрим системы шифрования, используемые в те времена на Арабском Востоке. В 855 году арабский ученый по имени Абу Бакр Ахмед бен-Али бен-Вахшия ан-Набати включил несколько шифроалфавитов, реализующих шифр простой замены, в свою «Книгу о большом стремлении человека разгадать загадки древней письменности». Пожалуй, эта первая из дошедших до нас книг, содержание которой в значительной степени посвящено криптографии. Описания античных шифров встречаются в основном в исторических трудах и трактатах по военному искусству. Один шифроалфавит, называвшийся «дауди» (см. рис. 2.5) по имени израильского царя Давида. Он был составлен из видоизмененных букв древнееврейского алфавита, применялась скоропись, добавления к буквам различных хвостиков, завитушек, удаления некоторых частей букв и т.д. Шифр «дауди» использовался для зашифрования трактатов по черной магии (иногда он также назывался «рейхани» - магия), так в 1076 году переписчик одного из подобных сочинений зашифровал по этой системе слово «опиум».

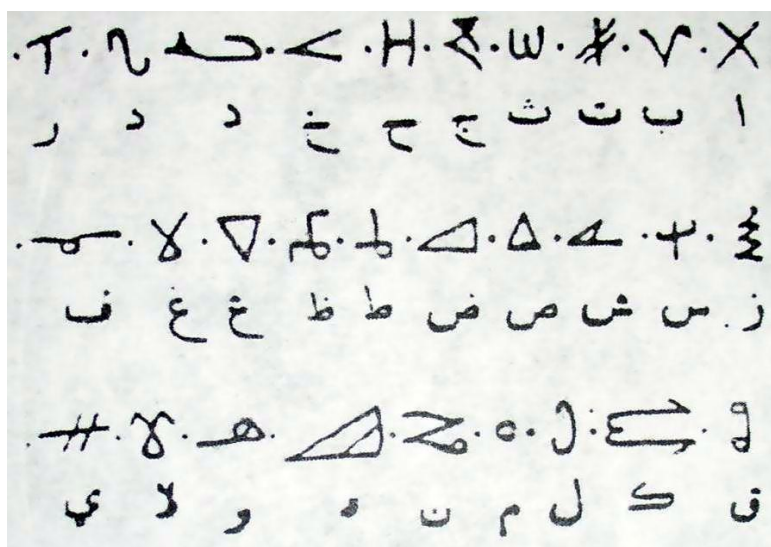


Рис. 2.5. Арабский “давидовский” шифр замены

Другой вариант шифра простой замены, описанный в книге, был использован почти тысячу лет спустя в 1775 году в письме шпиона, направленном регенту Алжира [Бабаш, 2002], [Сингх, 2007], [Kahn, 1967]. Этот шифр был широко распространен на Востоке, в Турции он назывался «Мысырлы», в Египте – «Шаами» (сирийский), а в Сирии «Тадмури» (пальмирский, Пальмира древний город в Сирии, крупный центр караванной торговли в I-III веках н.э., в настоящее время в результате археологических раскопок восстановлена планировка античного города, представлены храмы, статуи, некрополи, мозаики, росписи и т.д. Памятник античной архитектуры мирового значения. На самом деле название шифра происходит от до сих пор существующего в Сирии вблизи Пальмиры города Тадмор). В рукописи о военном искусстве, написанной в Египте в XIV веке этим шифром были зашифрованы составы и компоненты зажигательных смесей, которые забрасывались во вражеские крепости, что бы вызвать пожар. Такой шифр использовал и один из министров Халифата, живший в VIII веке Муллюль Бен Ибрагим Бен Яхья аш-Шанхаги. В одном из арабских генеалогических трактатах о нем говорится, что: «Он был красноречив и быстро изучил язык птиц; он писал по древнесирийски (т.е. использовал шифр «Шаами» - авт.) и весьма преуспел в этом» [Kahn, 1967].

В монументальном историческом обзоре «Мукаддима» («Введение»), который известный английский историк Арнолд Тойнби (Toynbee) оценил как величайшую работу своего рода, которая когда-либо и где либо была создана, содержится описание весьма оригинальных вариантов шифра простой замены, использовавшихся арабскими чиновниками. Этот обзор был написан в Египте в XIV веке Абдель Рахманом ибн Халдуном, вот что в нем говорится о шифровании: «сборщики налогов и военачальники в переписке между собой пользуются специальным шифром, который похож на загадку. В нем используются названия благовоний, фруктов, птиц или цветов для указания букв или же формы, отличные от принятых форм букв. Те, кто состоит в переписке, согласовывают между собой такой шифр, чтобы иметь возможность излагать свои мысли в письменной форме» [Kahn, 1967]. Использование названий птиц для шифрования очевидно арабы переняли у персов, которые с давних пор использовали данный прием, и творчески дополнили использовав для замены также и другие предметы. Скорее всего эти сведения взяты ибн Халдуном из «руководства для министров»,

написанном в X веке Абу Бакр Мухаммедом Бен Яхья ас-Суни, который описал способы шифрования путем замены букв на названия птиц и положений луны, он также указал, что данный способ шифрования заимствован из Персии. В «Мукаддиме» упоминаются и приемы криптоанализа, вот что поэтому поводу пишет ее автор: «Иногда умные министры, хотя они и не являются первыми изобретателями шифра и раньше не знали о нем, находят правила его разгадки путем применения комбинаций, которые они разрабатывают для этой цели благодаря своим умственным способностям и которые они называют решением головоломки. У людей есть хорошо известные произведения на эту тему. Бог мудр и всемогущ» [Kahn, 1967]. Как видим описание криптоаналитической работы весьма туманно. Однако важна ссылка на «хорошо известные произведения», вероятнее всего речь идет о работах ряда арабских ученых в области криптоанализа о которых будет рассказано ниже.

Арабские сборщики налогов использовали особый шифр под названием «кирма». Этот шифр предполагает упрощение формы арабских букв путем уменьшения их размеров, продления «хвостиков», удаления точек, слова не отделялись друг от друга, мало того они часто накладывались друг на друга и перемешивались. Шифр «кирма» появился в Египте в XVI веке, большинство турецких, египетских и сирийских финансовых документов шифровались данной системой до второй половины XIX века. «Кирма» использовалась только в налоговых ведомствах Арабского Востока [Kahn, 1967].

Известно также, что арабские чиновники длительное время широко применяли шифры перестановки. Кроме государственных ведомств и составителей магических трактатов, шифрование использовали секты исламских религиозных фанатиков, чтобы скрыть свои планы и намерения от госструктур и добропорядочных граждан [Сингх, 2007], [Kahn, 1967].

Если бы арабы были просто знакомы с использованием ряда систем шифрования, то в истории криптографии об этом упоминалось бы лишь вскользь. Однако наряду с использованием шифров, арабские специалисты оказались способны раскрывать шифры. Они фактически создали криптоанализ - науку о дешифровании криптограмм без знания ключа. В то время как специалисты по криптографии разрабатывают и создают новые способы шифрования, криптоаналитики стараются выявить слабости этих способов, чтобы

получить доступ к содержанию секретных сообщений. Главным успехом арабских криптоаналитиков был, разработанный ими способ дешифрования шифра простой замены. Этот шифр к тому времени использовался в разных странах уже несколько тысяч лет.

Одним из первых арабских криптоаналитиков был широко известный арабский филолог Абу Абдель Рахман аль-Халиль ибн Ахмед ибн Омар ибн Таммам аль-Фарахиди аз-Зади аль-Ахмади, живший в VIII веке. Он впервые использовал возможность наличия стандартных слов и выражений (стандартов) для дешифрования. В процессе криптоанализа зашифрованного простой заменой сообщения на греческом языке, которое ему переслал византийский император с просьбой о дешифровании, аль-Ахмади сделал следующее предположение: «Я сказал себе, что письмо должно начинаться со слов "Во имя Бога" или как-нибудь в этом роде. Итак, я составил на основе этого первые буквы, и все оказалось правильным». На основе открытого им метода дешифрования он написал книгу «Китаб аль-Маумма» («Книга тайного языка»). Аль-Ахмади затратил на дешифрование криптограммы примерно месяц, что говорит об скорее интуитивном характере работы аль-Ахмади. [Бабаш, 2002], [Сингх, 2007], [Kahn, 1967].

Данный метод с тех времен нашел широкое применение, криптоаналитики пытаются узнать тематику открытого текста и высказывая предположения о наличии в нем тех или иных слов и фраз пытаются провести атаку «открытый – зашифрованный текст». Поясним вышеизложенное.

Например, криптоаналитику стало известно (допустим из агентурных источников, тайные операции по добыче криптографических секретов проводились с глубокой древности, подробнее о них можно прочитать в книге [Гольев, 2008], она охватывает временной интервал от античных времен до Второй мировой войны включительно), что зашифрованный текст касается проведения некоторой военной операции. Тогда он может предположить, что в открытом тексте встречаются такие слова как «атака», «прорыв», «наступление», «оборона», наименования воинских подразделений «батальон», «полк», «дивизия» и т.п. Часто вероятными словами служат фамилии получателя и отправителя (последняя обычно стоит в конце криптограммы), общепринятые обращения, например, «Ваше превосходительство», «товарищ полковник». Задача криптоаналитика состоит в том, чтобы найти

шифрованный эквивалент стандарта и реализовать атаку «открытый – шифрованный текст». Заметим, что атака при помощи стандартов возможна не только на примитивные шифры (типа простой замены), так значительное количество ключей знаменитого немецкого шифратора «Энигма» во время Второй мировой войны была вскрыта англичанами именно с помощью стандартов (англичане называли их «подстрочниками»).

Однако главным достижением арабов в области криптоанализа стало использование частотного анализа для дешифрования шифра простой замены. Одним из первых кто догадался, что подсчет частоты появления знаков, встречающихся в шифртексте, может быть использовано для взлома шифров, был Абу Юсуф Якуб ибн Исхак ибн ас-Сабах ибн Умран ибн Исмаил аль-Кинди, более известный на западе как Алькиндус. Он жил в IX веке и является одним из крупнейших арабских ученых того времени. Аль-Кинди родом из царского южно-аравийского племени Кинда. Он известен как “философ арабского мира”, является автором 290 книг по медицине, астрономии, математике, лингвистике и музыке. Большое влияние на Аль-Кинди оказали греческие философы, в особенности Сократ и Аристотель, переводы произведений которых он использовал в своих работах. Подтверждение этому можно видеть в многочисленных работах Аль-Кинди по философии. Своему народу Аль-Кинди был известен, прежде всего, философскими трудами, однако он занимался также исследованиями в области математики, медицины, оптики, астрономии и многих других наук. Кстати именно Аль-Кинди внедрил индийские числительные в арабскую письменность, а уже оттуда они перекочевали в христианскую, именно ему мы обязаны, появлением крайне удобной записи цифр и чисел, которая используется во всем мире и в наши дни.

Его самый знаменитый трактат, с точки зрения истории криптографии был обнаружен лишь в 1987 году в турецком архиве Сулайманийа в Стамбуле. Он называется «Рукопись по дешифрованию криптографических сообщений», первая страница которой показана на рис. 2.6. В нём содержится подробный анализ статистики, фонетики и синтаксиса арабского языка, а также методика криптоанализа шифра простой замены. Работая над зашифрованными сообщениями греческого и римского происхождения, Аль-Кинди так описал свою дешифровальную работу всего в двух коротких абзацах своего трактата:

«Один из способов прочесть зашифрованное сообщение, если мы знаем язык, на котором оно написано, - это взять другой незашифрованный текст на том же языке, размером на страницу или около того, и затем подсчитать появление в нем каждой из букв. Назовем наиболее часто встречающуюся букву «первой», букву, которая по частоте появления стоит на втором месте, назовем «второй», букву, которая по частоте появления стоит на третьем месте, назовем «третьей» и так далее, пока не будут сочтены все различные буквы в незашифрованном тексте.

Затем посмотрим на зашифрованный текст, который мы хотим прочитать, и таким же способом проведем сортировку его символов. Найдём наиболее часто встречающийся символ и заменим его «первой» буквой незашифрованного текста, второй по частоте появления символ заменим «второй» буквой, третий по частоте появления символ заменим «третьей» буквой и так далее, пока не будут заменены все символы зашифрованного сообщения, которое мы хотим дешифровать» [Сингх, 2007, с. 32].

Методика Аль-Кинди получила в криптоанализе название «частотный анализ», в ходе которого происходит подсчет количества букв определенного языка в открытом тексте и процентного соотношения знаков шифртекста, а затем осуществляется замена символов на буквы с равным показателем частотности их появления в текстах. Тем не менее, для данного метода дешифрования идеальным является достаточно длинное сообщение, к тому же буквы, обычно часто встречающиеся на письме и в речи, могут употребляться в зашифрованном сообщении реже, произвольно или же намеренно, чтобы ввести в заблуждение криптоаналитиков. Большой опыт, серьезные усилия и рассуждения с использованием догадок во многих случаях позволяют вскрывать самые сложные шифры [Сингх, 2007], [Al-Kadi, 1992].

Криптоанализ на Арабском Востоке не смог бы появиться до тех пор, пока цивилизация там не достигла бы достаточно высокого уровня в ряде дисциплин, включая математику, статистику и лингвистику. Мусульманская цивилизация являлась идеальной колыбелью для криптоанализа, поскольку ислам требовал соблюдения законов во всех областях человеческой деятельности, а для этого нужны знания, по-арабски *ilm*. Каждый мусульманин был обязан стараться приобретать знания во всех областях. Экономический расцвет Халифата Аббасидов означал, что у ученых было время,

деньги и материалы, необходимые для выполнения ими своих обязанностей. Они старались овладеть знаниями предшествующих цивилизаций, приобретая древнеегипетские, вавилонские, индийские, китайские, персидские, сирийские, армянские, еврейские и латинские рукописи и переводя их на арабский язык. В 815 году халиф Аль-Мамун основал в Багдаде Bait al-Hikmah (Дом мудрости) - библиотеку и центр переводов [Сингх, 2007].

Истоки достижений арабов в области криптоанализа, очевидно, следует искать в интенсивном и скрупулезном изучении Корана многочисленными школами арабских грамматиков. Наряду с другими исследованиями, они занимались подсчетом частоты встречаемости слов, пытаясь составить хронологию глав Корана, изучали фонетику слов, чтобы установить, являлись ли они подлинно арабскими или были заимствованы из других языков.

Большую роль в обнаружении лингвистических закономерностей, приведших к возникновению криптоанализа у арабов, сыграло также развитие лексикографии. Ведь при составлении словарей авторам фактически приходилось учитывать частоту встречаемости букв, а также то, какие буквы могут стоять рядом, а какие никогда не встречаются по соседству.

Кроме лучшего понимания светских дисциплин, появление криптоанализа было обусловлено также и развитием религиозного образования. Основные медресе были основаны в Басре, Куфе и Багдаде, где теологи тщательно изучали содержащиеся в Коране откровения пророка Мухаммеда. Теологи пытались составить хронологию этих откровений, а также найти в них скрытый смысл. Для этого они подсчитывали частоту появления слов, содержащихся в каждой из сур Корана. Теоретические предпосылки состояли в том, что определенные слова появились сравнительно недавно, и поэтому, чем больше новых слов содержится в откровении, тем к более позднему периоду оно относится. Теологи также изучали Хадисы, которые состояли из ежедневных изречений Пророка. Они попытались показать, что каждое изречение действительно может быть приписано Мухаммеду. Это проводилось путем изучения этимологии слов и структуры предложений, чтобы проверить, согласуются ли отдельные тексты с лингвистическим стилем Пророка. Также эти исследователи пытались выяснить, какие слова были исконно арабскими, а какие заимствованы из других языков [Сингх, 2007], [Kahn, 1967].

Это привело к обобщению структуры арабского языка. Например, один арабский лингвист, упоминая о язычных согласных «Ра», «Лам», «Нун» и губных согласных «Фа», «Ба», «Мин», заявил следующее: «После того, как эти шесть букв были произнесены, оказалось, что их легко образовывать, и они стали обычными в речи. Поэтому ни один из истинных пятибуквенных корней не свободен от них или по крайней мере одного из них» [Kahn, 1967].

Толкование мусульманских религиозных текстов арабами привело к появлению «тафсира» – учения, имеющего официальную трактовку Священных текстов и “таавиля” (аналог еврейской каббалы) – учение о символично-аллегорическом истолковании Священных текстов (в первую очередь - Корана). К учению “таавиль” прибегали “свободно-мыслящие” - противники догматического

ислама. Одновременно свои собственные мысли они скрывали с помощью «таких» - набора приёмов сокрытия тайны. Сторонник таавилия испано-арабский философ Ибн Туфейль (XII век) писал: «Мы не лишали совершенно эти тайны, доверенные нами сим немногим листкам, лёгкой завесы, которую быстро прорвет тот, кто достоин её, но которая окажется непроницаемой и недоступной для того, кто не достоин переступить её». Широко применяли «такую» ученые, поэты и писатели того времени [Al-Kadi, 1992].

Важно, что религиозные ученые не остановились в своем исследовании на уровне слов. Они также проанализировали отдельные буквы; в частности, выяснилось, что некоторые буквы встречаются чаще других. На основании этого арабские криптоаналитики и достигли своих выдающихся на тот момент результатов.

Своеобразный итог работе арабов в области криптографии и криптоанализа был подведен в 14 томной энциклопедии "Шауба аль-Аша" ("Светоч для незрячего в ремесле писца"). Автором этого грандиозного труда был Шехаб эд-Дин Абу аль-Аббас Ахмед Бен Али бен Ахмед Абдулла аль-Калкашанди, живший в Египте. Работу над энциклопедией аль-Калкашанди закончил в 1412 году, цели издания - дать систематический обзор всех важных областей человеческого знания. Энциклопедия предназначалась для служащих государственной канцелярии (Дивана документов и переписки, диванами на Арабском Востоке называются различные министерства и ведомства, главным из них был Большой Диван), она объединяет в себе универсальный справочник и учебное пособие и содержит самые разнообразные сведения по истории и географии, вопросам делопроизводства и внешней политики, каллиграфии и титулатуре и многим другим наукам. В качестве образцов в ней приводятся уникальные подлинные документы и письма из архива государственной канцелярии Египта. Энциклопедия также содержит множество цитат из трудов предшественников аль-Калкашанди, многие из которых не дошли до нашего времени.

Аль-Калкашанди много лет прослуживший в государственной канцелярии Египта, был хорошо знаком с работой этого ведомства. Арабская разведка была в ведении государственной канцелярии вышеупомянутого Дивана, которая не только следила за прохождением бумаг через свое ведомство, но и ведала официальной перепиской султана, почтовой службой, организацией ежегодного паломничества в Мекку и Медину. В энциклопедии аль-Калкашанди

приоткрываются секреты средневековых арабских шпионов, чиновников государственной канцелярии, послов, служащих многочисленных ведомств - диванов, применявших различные средства для сокрытия написанного от посторонних глаз. Параграф энциклопедии, посвященный защите информации, называется «Относительно сокрытия в буквах тайных сообщений» и содержит две части. Одна касается символических действий, иносказаний и намеков (в современной криптографии такой способ защиты информации получил название «жаргонный код»), а другая была посвящена стеганографии (в частности рецептам и вариантам использования симпатических (невидимых) чернил) и криптографии. Этот параграф является частью главы, которая называется «О технических методах, применяемых в переписке министрами в восточных и западных странах и на египетских территориях в течение всего периода от появления ислама и до наших дней». Эта глава является частью большого раздела, который имеет название «О формах переписки» [Kahn, 1967].

Криптографический раздел энциклопедии аль-Калкашанди, по его собственному утверждению, написал на основе работ двух арабских ученых ибн ад Дурахийма (какой-либо информации о нем автору найти не удалось) и Тадж эд-Дин Али ибн ад-Маусыли (1312-1361). Этот человек занимал ряд административных постов в Сирии и Египте, а также занимался преподавательской деятельностью. Он является автором двух трудов по криптографии, к сожалению утраченных, но подробно изученных аль-Калкашанди. Первым из них была поэма «Урджуза фи аль-Мутарджам», вторым комментарий в прозе к поэме «Мифтах аль-Кунуз фи ядаху аль-Мармуз» [Kahn, 1967].

Рассмотрим криптографическую часть энциклопедии аль-Калкашанди подробнее. Автор начинает этот параграф с объяснения необходимости мероприятий по защите информации «потому что враг создает какое-нибудь препятствие или нечто подобное между отправителем и адресатом, например, между двумя правителями или двумя другими лицами. Это необходимо, когда существует опасность перехвата или тщательной проверки всех писем, исходящих от любой из двух переписывающихся сторон» [Kahn, 1967]. Одним из самых простых способов сохранить сообщение в тайне, по мнению аль-Калкашанди, написать его на неизвестном для противника языке. Этот вид защиты информации неоднократно применялся в истории

криптографии. Например, американцы в обеих мировых войнах XX века использовали практически неизвестные в воюющих странах языки некоторых малочисленных индейских племен. С этой целью на этих узлах связи работали специально подготовленные представители этих племен. Аналогичным образом поступили ирландские военнослужащие, входившие в 1960 году в миротворческий контингент в Конго – они вели радиопереговоры на гэльском языке (язык малочисленной народности – потомков древнего кельтского населения, проживающих на территории Великобритании и Ирландии) [Архипов, 2002], [Сингх, 2007], [Kahn, 1967].

Далее аль-Калкашанди приводит описание криптографических систем защиты информации, со ссылкой на ибн ад-Дурайхима рассказывает о 7 системах шифрования:

1. Одна буква может заменять другую; При шифровании арабские буквы могли заменяться буквами из древних или иностранных языков, цифрами. В числе языков используемых при шифровании упоминаются монгольский, армянский, тюркский, персидский, еврейский, сирийский, греческий, латинский и коптский.
2. Можно писать слово в обратном порядке, например, слово "Мухаммед" (МХМД – в арабском алфавите, состоящем из согласных) примет вид ДМХМ; в этом случае, лицу, проводящему расшифрование не нужно заучивать аналоги всех букв, ему достаточно лишь знать общий принцип.
3. Можно переставлять в обратном порядке чередующиеся буквы слов;
4. Можно заменять буквы на цифры в соответствии с принятой заменой арабских букв на числа. Тогда слово "Мухаммед" превращается в $40+8+40+4$ ($M=40$, $X=8$, $D=4$). При этом криптограмма выглядит как перечень каких-то цифр.
5. Можно заменять каждую букву открытого текста на две арабские буквы, которые используются и в качестве чисел, и сумма которых равна цифровой величине шифруемой буквы открытого текста;

6. Похожий на предыдущий, но более сложный способ - буквы сперва заменяются соответствующими цифрами, Мухаммад = $40+8+40+4$, а затем каждая цифра записывается как сумма двух букв (с учетом их числового значения). В итоге имя Мухаммад будет выглядеть как Л-и Б-у Л-и А-дж.
7. Можно заменять каждую букву именем какого-либо человека, так же при шифровании можно использовать словарь замены, описывающий положения луны, названия стран (в определенном порядке), названия фруктов, деревьев и т. д., либо рисовать птиц или другие живые существа, либо просто изобрести специальные символы в качестве знаков шифртекста [Бабаш, 2002, с. 52-53], [Al-Kadi, 1992], [Kahn, 1967].

Опишем арабские цифровые системы шифрования подробнее. В арабской криптографии известны свои названия шифров, относящихся к буквам и цифрам: Это АБДЖАТ - соответствие каждого слова, или буквы в слове, своему цифровому значению, что позволяло заменять при письме слово его суммарным числовым значением. ДЖАФР - шифрование с помощью букв, цифр и символов. Каждое слово в арабском алфавите имеет определенное цифровое значение. Иными словами, каждая арабская буква имеет определенное числовое значение, то есть число может быть выражено буквами и наоборот. Таким образом, каждое слово, помимо своего буквального смысла, имеет также числовое значение. Исходя из этого, можно производить кодировку слов и различные расчеты (см. рис. 2.7).

Нет ссылки в тексте на этот рис

Порядковые номера и числовые значения арабского алфавита														
Номер буквы	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Арабские буквы	ا	ب	ج	د	ه	و	ز	ح	ط	ي	ك	ل	م	ن
Латинское звучание	alf	ba	cin	dal	ha	vav	ze	ha	ta	ya	kaf	lam	mim	nun
Численное значение	1	2	3	4	5	6	7	8	9	10	20	30	40	50
Номер буквы	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Арабские буквы	س	ع	ف	ص	ق	ر	ش	ت	ث	خ	ذ	ض	ظ	غ
Латинское звучание	sin	ayn	fa	sad	kaf	ra	shin	ta	sa	ha	zal	dad	za	gayn
Численное значение	60	70	80	90	100	200	300	400	500	600	700	800	900	1000

Рис. 2.7. Численные значения арабских букв.

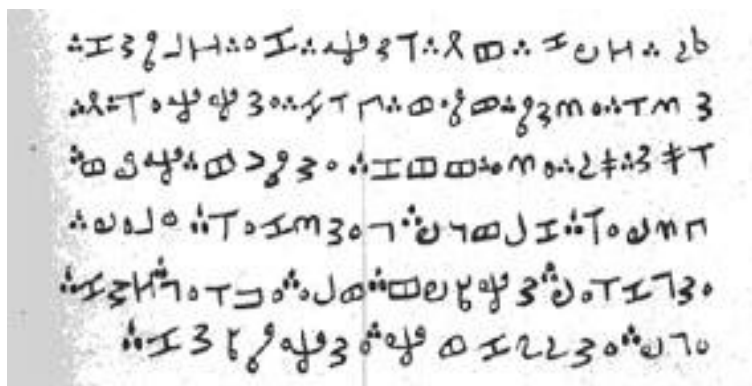
Цифровое кодирование арабы использовали в мистических исследованиях, в частности для предсказания будущего. Даты всех событий в истории древних арабов, персов и тюрков записывались с помощью букв, которым были даны численные значения, таким образом, буквы описывали и событие, и, одновременно, содержали информацию о его дате. Эти даты получались путем сложения суммы численных значений всех использованных для описания этого события букв. Соответствие каждого слова цифровому значению (абджад) мусульмане использовали в различных областях. Шифрование буквами, цифрами и символам (джафр) является одной из сфер применения данной особенности арабского алфавита.

Джафр – название особой области знания лингвистики арабского языка, которая дешифрует и изучает предсказания будущих событий, сокрытые в словах, составленных методом абджад. Одним из способов джафра, к которому прибегают обладающие знанием этого метода предсказатели – это комментарии будущих событий по суммарному подсчету букв, слогов и символов. Самое главное отличие кодировки (абджада) от толкования предсказаний (джафра) можно выразить так: кодировка (абджад) – это наука о свершившихся событиях, даты которых были заключены в буквенные значения, а толкование предсказаний (джафр) – это наука дешифровки слов и толкований, сокрытых в цифрах дат вероятных будущих событий. 240. Этот метод подсчета восходит к глубокой древности и был широко распространенной формой арабского письма еще до ниспослания

Священного Корана. Все события, происходившие в истории арабов, записывались специально составляемыми буквами с учетом их цифровых значений и, таким образом, фиксировалось как само описание события, так и его дата. Эта дата получалась из суммирования особого цифрового значения каждой используемой в слове буквы. Это один из многочисленных примеров использования криптографии в, своего рода, оккультных, магических, в общем далеких от научных целей.

Первый раз за всю историю шифров в энциклопедии аль-Калкашанди приводился описание, как систем перестановки, так и систем замены (см. рис. 2.8). Более того, в пятом пункте списка впервые упоминался шифр, для которого была характерна более чем одна замена букв открытого текста [Kahn, 1967].

Это весьма важный факт. Однако главным достижением аль-Калкашанди считается обобщение криптоаналитических методов того времени.



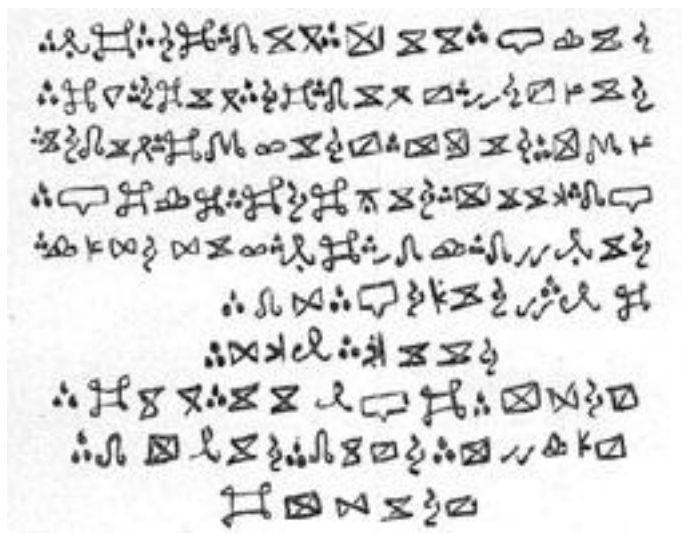


Рис. 2.8. Фрагменты рукописи аль-Калкашанди,
(соч., т.IX, стр. 240 и 245)

Нет ссылки в тексте на этот рис стр. 60

Аль-Калкашанди приводит список букв арабского алфавита с указанием частоты их встречаемости в текстах Корана. Аль-Калкашанди, опять же со ссылкой на ибн ад-Дурайхима начинает изложение криптоаналитических методов с азов: «Криптоаналитик должен знать язык, на котором написана криптограмма. (Это может быть сделано разными способами, например, по числу употребляемых знаков шифртекста и в соответствии с количеством букв в различных алфавитах определить, на каком языке написан документ, используя оперативную и агентурную информацию и т.д. - примеч. авт.). Поскольку арабский язык, самый благородный и самый прекрасный из всех языков, является одним из наиболее распространенных» [Кан, 2004, с 121]. Далее дается пространное описание его лингвистических характеристик. Приводятся перечни букв, которые никогда не стоят вместе в одном слове, и букв, которые редко появляются по соседству, а также буквенные комбинации, которые в словах встретить невозможно, «так например буква «Та» не может предшествовать букве «Шин». Последним идет список букв в порядке «частоты их использования в арабском языке в свете результатов изучения

священного Корана». (Заметим, что буква “Алиф” встречается в тексте Корана 650 раз, буква “Лям” 480 раз, буква “Мим” - 260 раз, буква “Ра” 137 раз). Автор отмечает, что «в произведениях, не связанных с Кораном, частота использования может быть иной» [Кан, 2004, с 122], [Kahn, 1967].

Предоставив читателю статистические характеристики арабского языка (т.е. главный «инструмент» вскрытия шифра простой замены), аль-Калкашанди продолжает: «Ибн ад-Дурайхим сказал: Если вы хотите прочесть сообщение, которое вы получили в зашифрованном виде, то, прежде всего, начните подсчет букв, а затем сосчитайте, сколько раз повторяется каждый знак, и подведите итог в каждом отдельном случае. Если изобретатель шифра был очень внимателен и скрыл в сообщении все границы между словами, то первая задача, которая должна быть решена, заключается в нахождении знака, разделяющего слова. Это делается так: вы берете букву и работаете, исходя из предположения, что следующая буква является знаком, делящим слова. И таким образом вы изучаете все сообщение с учетом различных комбинаций букв, из которых могут быть составлены слова... Если получается, тогда все в порядке; если нет, то вы берете следующую по счету букву и т. д., пока вы не сможете установить знак раздела между словами. Затем нужно найти, какие буквы чаще всего встречаются в сообщении, и сравнить их с образцом частоты встречаемости букв, о котором упоминалось прежде. Когда вы увидите, что одна буква попадает чаще других в данном сообщении, вы предполагаете, что это буква «Алиф». Затем вы предполагаете, что следующая по частоте встречаемости будет буквой «Лам» (третьей по частоте встречаемости в арабском языке является буква «Мим», а самой редкой буква «За» - примеч. авт.). Точность вашего предположения должна подтверждаться тем фактом, что в большинстве контекстов буква «Лам» следует за буквой «Алиф»... Затем первые слова, которые вы попытаетесь разгадать в сообщении, должны состоять из двух букв. Это делается путем оценки наиболее вероятных комбинаций букв до тех пор, пока вы не убедитесь в том, что вы стоите на правильном пути. Тогда вы смотрите на их знаки и выписываете их эквиваленты всякий раз, когда они попадают в сообщении. Нужно применять точно такой же принцип по отношению к трехбуквенным словам этого сообщения, пока вы не убедитесь, что вы на что-то напали. Вы выписываете эквиваленты из всего сообщения. Этот же принцип применяется по отношению к

словам, состоящим из четырех и пяти букв, причем метод работы прежний. Всякий раз, когда возникает какое-либо сомнение, нужно высказать два, три предположения или еще больше и выписать каждое из них, пока оно не подтвердится на основании другого слова» [Кан, 2004, с 122-123].

Дав это четкое разъяснение, аль-Калкашанди приводит пример вскрытия шифра. Дешифруемая криптограмма состоит из двух стихотворных строк, зашифрованных с помощью условных символов. В заключение аль-Калкашанди отмечает, что восемь букв не было использовано и что это как раз те самые буквы, которые стоят в конце перечня, составленного по частоте встречаемости. Он отмечает: «Однако это простая случайность: буква может быть поставлена не на то место, которое она должна занимать в вышеупомянутом перечне». Такое замечание свидетельствует о наличии большого опыта в области криптоанализа. Чтобы расставить все точки над «i», аль-Калкашанди приводит из книги ибн ад-Дурайхима второй пример криптоанализа довольно длинной криптограммы. Этим примером на трех страницах он и заканчивает раздел о криптологии [Кан, 2004, с. 123], [Kahn, 1967].

Аль-Калкашанди в своей энциклопедии описывает и такой способ защиты информации, как стеганография. В частности о нескольких рецептах симпатических (невидимых) чернил, среди которых - письмо молоком с разведенным в нем аммиаком, письмо луковым соком и раствором квасцов в дождевой воде. Надписи эти "чернилами" производились на бумаге и проявлялись при помощи нагревания. На бумаге или каком-либо другом материале можно было писать водным раствором медного купороса. Для проявления текста необходимо было протереть место, где нанесен текст, водным раствором истолченного чернильного орешка, более того аль-Калкашанди предлагает писать желчью черепахи (она должна светиться в темноте!), а также пастой, приготовленной из равных частей черного лимона и корней колоквинта, поджаренных на оливковом масле и смешанных с яичным желтком. Через некоторое время на месте, где была сделана надпись этой пастой, должны прорасти ... волосы! По утверждению нашего энциклопедиста, этот удивительный способ особенно хорош, когда послание требуется отправить далекому адресату: к тому времени, как письмо дойдет по назначению, волосы уже прорастут и его можно будет прочесть! Конечно, последние два способа, видимо, навеяны трактатами по

магии и другой подобной литературой и на практике не применимы, а вот первые успешно применяются в разных странах на протяжении многих веков [Бабаш, 2002], [Al-Kadi, 1992], [Kahn, 1967].

Безусловно, нельзя не оценить огромный теоретический вклад арабов в криптоанализ, однако практическое применение своих знаний было весьма и весьма скромным. По некоторым сведениям арабские криптоаналитики дешифровали какое-то количество византийских криптограмм, хотя возможно это лишь искаженная версия о работе Аль-Ахмади. Каких-либо других успехов не было.

Возможно это связано с тем, что в XIII-XIV веках Арабский Восток был завоеван турками, которые не стремились воспользоваться знаниями покоренного народа. Это подтверждает следующий факт. Турецкий султан Баязид II (XV век), узнав, что венецианский байюло (глава дипломатической миссии) Дж. Марчелло посылает своему правителю зашифрованные письма, приказал ему в три дня покинуть страну. Султан заявил, что он вообще не намерен терпеть у себя при таких условиях венецианского байюло. Несмотря на длительные переговоры, венецианская колония в Константинополе долго после этого случая оставалась без главы [Гольев, 2008, с. 8]. А ведь в его распоряжении были работы арабских ученых в области криптоанализа и вместо того чтобы запрещать шифрпереписку можно было ее дешифровать и получать важную информацию. Но султан и его окружение не удосужились обратиться к работам арабских специалистов.

О полной деградации арабского криптоанализа свидетельствует эпизод, произошедший в 1600 году. Марокканский султан Ахмед аль-Мансур направил к английской королеве Елизавете I посольство во главе с доверенным человеком – министром Абдель Вахид ибн Масуд ибн Мухаммед Ануном. Посольство должно было заключить с Англией союз, направленный против Испании. Анул отправил на родину зашифрованную простой заменой депешу, которая вскоре после этого каким-то образом попала в руки одного араба. Араб тот был, возможно, умным человеком, но, к сожалению, он ничего не знал о великом арабском наследии в области криптоанализа. Свидетельством тому – памятная записка, в которой он написал: «Хвала Аллаху! Относительно письма министра Абдель Вахид ибн Масуд ибн Мухаммед Ануна. Я нашел письмо, написанное его рукой, в котором он с помощью тайных знаков изложил некоторые сведения, предназначенные для нашего покровителя Ахмеда аль-

Мансура. Эти сведения касаются султанши христиан (да покарает их Аллах!), которая жила в стране под названием Лондон... С того момента, как это письмо попало ко мне, я постоянно время от времени изучал содержащиеся в нем знаки. Прошло примерно 15 лет, пока не наступило то время, когда Аллах позволил мне понять эти знаки, хотя никто не обучал меня этому...» [Бабаш, 2002, с. 53-55]. Пятнадцать лет!!! Подобную задачу аль-Кинди, ибн ад-Дурайхим и другие вышеупомянутые арабы решили бы за несколько часов.

Достижения арабов в области криптографии в стихотворной форме выразил выдающийся ученый и философ конца XI начала XII веков, поэт Омар Хайям. В своих произведениях он нередко упоминал тайнопись, вот одно четверостишие из его произведений («Рубаи»):

Все что видишь ты, - видимость только одна,

Только форма - а суть никому не видна.

Смысл этих картинок понять не пытайся –

Сядь спокойно в сторонке и выпей вина! [Бабаш, 2002, с. 55]

Здесь Хайям весьма пессимистично относится к попыткам проникнуть в тайный смысл сообщений, скрывающийся за внешней формой их представления (шифром, стеганографией). Как было сказано выше, некоторые его современники были настроены гораздо оптимистичнее.

Неизвестно, насколько тесной была связь между развитием европейской и арабской криптографии. Безусловно, подобного рода контакты могли происходить в Испании (в частности через эту страну попали в Европу многие арабские математические трактаты) и во время Крестовых походов, а так же в ходе дипломатических и торговых контактов. Скорее всего, можно утверждать, что европейская криптология в то время использовала арабский опыт. Хотя труды аль-Калкашанди и его предшественников не были переведены с арабского языка, европейские ученые вполне могли с ними ознакомиться. По всей видимости, именно с Арабского Востока Святой Бонифаций, осуществлявший в VIII веке миссионерскую деятельность на территории Германии и основавший там ряд монастырей, привез "Сборник криптозагадок", где гласные буквы заменялись различными комбинациями точек [Бабаш, 2002], [Kahn, 1967].

В эпоху позднего средневековья, с началом возрождения интереса к античному наследию и просвещению, криптография в Европе обретает «второе рождение». Наиболее передовые позиции в

криптографии на долгое время заняли итальянцы. В архивах Венеции можно отыскать шифр, датированный 1226 годом. Суть его заключается в том, что точки и кресты заменяют гласные в нескольких словах, находящихся в разных местах послания.

Огромное влияние в описываемый период на все стороны жизни Европы, в первую очередь политическую, оказывала католическая церковь. Разумеется, обойтись без шифров было не возможно. Но даже церковные системы шифрования пребывали в зачаточном виде, хотя тогда Церковь пользовалась наибольшим влиянием в обществе. Все же именно с этого времени криптография развивается без продолжительных периодов стагнации и регресса, ее совершенствование становится неуклонным. Самый древний шифрованный документ, хранящийся в архивах Ватикана, представляет собой небольшой список имен, составленный в 1326-1327 годах, когда в Италии шла борьба между гвельфами (сторонниками папы римского) и гибеллинами (приверженцами императора Священной Римской империи). В нем гибеллины называются «египтянами», а гвельфы – «детьми Израилевыми». Также некто обозначен буквой О (от OFFICIAL – влиятельное лицо, чиновник). Спустя 10 лет в другом документе отказываются от использования жаргона, и все имена обозначены буквами, так например, Христос обозначен буквой А. Вместе с этим документом хранится другой листок бумаги (очевидно написанный несколько позже), на которой написан первый сохранившейся код: А=король, ... D=папа римский и т.д. [Kahn, 1967].

В 1379 году антипапа Климентий VII, за год до этого бежавший во французский город Авиньон, чтобы внести раскол в Римскую Католическую Церковь (тогда на папский трон претендовали два кандидата), объявив себя законным владельцем папского трона, повелел своей канцелярии ввести в действие новые шифры. Один из секретарей антипапы Габриэли ди Лавинде, уроженец итальянского города Пармы, работавший в его представительстве в одном из североитальянских городов-государств, изготовил индивидуальные ключи для всех 24 корреспондентов антипапы. Среди прочих ключи получили епископ Венеции, герцог Монтевидский, и некий Никколо из Неаполя. Ключи Лавинде, самые древние среди сохранившихся на Западе, сочетают в себе элементы кода и шифра. Помимо шифралфавита простой замены с пустышками, почти каждый такой ключ включает небольшой список из более десятка широко

распространенных слов или имен, которым ставятся в соответствие двухбуквенные кодовые эквиваленты. Это самый ранний образец номенклатора – гибридной системы шифрования, которой в последующие 450 лет суждено было распространиться по всей Европе, а в последствии и в Америке. Номенклатор – шифр, представлявший собой сочетание шифра замены и небольшого кода. Номенклатор обычно содержал кодовые эквиваленты букв алфавита и наиболее употребительных слогов, слов и словосочетаний, а также ряд специальных символов. Чаще всего в нем встречались специально созданные для этой цели символы, но нередко также использовалась астрологическая и оккультная символика. Номенклатор был разработан как система шифрования, наилучшим образом приспособленная к наиболее употребительным в то время методам криптоанализа, которые, как правило, включали подсчет частоты появления в тексте каждого шифрового символа и поиск в тексте слов и выражений, содержащих характерные для данного языка сочетания букв. [Kahn, 1967].

Применялись шифры в эпоху позднего средневековья и в среде интеллектуальной элиты того времени. Многие ученые средневекового периода стремились скрыть сделанные ими изобретения и открытия. Объясняя широкое распространение тайнописи среди ученых средневековья, А.И. Герцен писал: «Гонимые, скитальцы из страны в страну, окруженные опасностями, они не зарыли из благоразумного страха истины, о которой были призваны свидетельствовать; они высказывали ее везде; где не могли высказать прямо – одевали ее в маскарадное платье, облекали аллегориями, прятали под условными знаками, прикрывали тонким флером, который для зоркого, для желающего ничего не скрывал, но скрывал от врага: любовь догадливее и проницательнее ненависти. Иногда они это делали, чтобы не испугать робкие души современников; иногда – чтобы не тотчас попасть на костер» [Бабаш, 2002, с. 47-48].

Одним из ученых, активно использовавших криптографию, был английский монах-францисканец, профессор в Оксфорде, универсальный ученый, математик, оптик, астроном и химик Роджер Бэкон (1214-1292). Он придавал большое значение математике и опыту – как научному эксперименту, так и внутреннему «мистическому» озарению. В середине XIII века Бэкон написал книгу "Тайные опыты и недействительность магии". В предисловии он заметил: "Дурак тот, кто пишет о тайне каким-либо способом, но не

так, чтобы скрыть ее от простонародья" [Бабаш, 2002, с. 47]. Здесь же Бэкон приводит несколько методов сокрытия тайны: пропуск гласных букв, использование метафор, букв из иностранных алфавитов, стеганографии. Таким образом, это одна (пусть примитивная) из первых обзорных работ по криптографии в Европе.

Бэкон сделал ряд изобретений (самое известное его изобретение – очки), однако многие из них при жизни не были опубликованы, считается, что Бэкон предвосхитил многие позднейшие открытия. Так современные исследователи установили, что состав черного пороха был открыт Р. Бэконом в XIII веке, почти за сто лет до «официальной» даты создания пороха Бертольдом Шварцем. В одном из его трудов присутствовало незашифрованное описание свойств этого вещества, но сам состав был зашифрован таким сложным шифром перестановки, что вскрыть его удалось лишь в наши дни с применением ЭВМ.

За свои научные работы Роджер Бэкон был осужден церковным судом и провел 14 лет в заточении. Его обвинили в черной магии. Особенно много суеверных толков связано с его лабораторией. Говорили, будто в ней Бэкон вместе со своим учеником монахом Бунгеем изготовил бронзовую голову, которую с помощью дьявола пытался оживить и заставить говорить. Сам же Бэкон писал: «... одни отрицают все необычное, – а другие, выходя за пределы разума, впадают в магию» [Бабаш, 2002, с. 47]. Этим высказыванием он хотел подчеркнуть, что он – ученый, который не отрицает все необычное, но изучает это необычное, не выходя за пределы разума, то есть, не впадая в черную магию. В конце жизни Роджер Бэкон покался и стал отшельником. А в XVI веке, после появления легенды о докторе Фаусте, его стали считать прообразом этого героя.

Одним из известных европейских криптографов был английский писатель, астроном-любитель, таможенный чиновник Джеффри Чосер (1340-1400). Сама жизнь заставила автора знаменитых "Кентеберийских рассказов" овладеть искусством криптографии. Еще мальчиком он был определен пажом при дворе, а затем рыцарским оруженосцем в окружении английского короля. Во время похода на Францию он попал в плен, но вместе с двумя чистокровными скакунами был выкуплен своим монархом, который заплатил 120 ливров за лошадей и всего 16 – за своего подданного. В 1370-х годах в звании эсквайра Чосер, как человек надежный и сведущий, выполнял секретные дипломатические поручения своего

короля в Италии и Франции. Всю тайную переписку он вел, используя шифр простой замены. Даже в свои стихи он включал зашифрованные строфы. Преуспев в делах дипломатических, он оставался в тени, получив за многолетнюю службу "высочайшую милость" – всего-то должность таможенного надсмотрщика лондонского порта по шерсти, коже и мехам. Но величайшим делом его жизни была поэзия, астрономия и криптография. Однако, ни то, ни другое, ни третье не принесло ему ни славы, ни денег. Он кончил жизнь смотрителем стен, валов, канав, сточных труб, прудов, дорог и мостов вдоль Темзы и был похоронен в Вестминстерском аббатстве [Бабаш, 2002, с. 48].

Криптография в эпоху возрождения

Новая культурная парадигма возникла вследствие кардинальных изменений общественных отношений в Европе, в первую очередь в Италии. Рост городов-республик привёл к росту влияния сословий, не участвовавших в феодальных отношениях: мастеровых и ремесленников, торговцев, банкиров. Всем им была чужда иерархическая система ценностей, созданная средневековой, во многом церковной культурой и её аскетичный, смиренный дух. Это привело к появлению гуманизма — общественно-философского движения, рассматривавшего человека, его личность, его свободу, его активную, созидающую деятельность как высшую ценность и критерий оценки общественных институтов. В городах стали возникать светские центры науки и искусства, деятельность которых находилась вне контроля церкви. Новое мировоззрение обратилось к античности, видя в ней пример гуманистических отношений. Таким образом, Эпоха Возрождения (Ренессанс) началась в Италии, где первые признаки были заметны ещё в XIII и XIV веках, она выдвинула новые факторы необходимости применения криптографии. Появившаяся интеллектуальная элита в виде гуманистов приходит на службу могущественным меценатам, все более отдалялась от простого народа. В сфере коммуникаций это проявляется тем, что главенствующим языком сообщений становится античная латынь, которая отходит от живого языка даже в Италии. Древние системы шифрования восстанавливаются и развиваются целой плеядой крупных ученых. Наряду с традиционными применениями криптографии в политике и военном деле возникают неожиданно

близкие к нашему времени задачи ее применения для охраны интеллектуальной собственности от преследований инквизицией или заимствования другими учеными. [Жельников 1996, с. 23].

Серьезные успехи в области криптографии были достигнуты в XIV-XVI веках в Италии, а центром мировой криптографической науки на длительное время стал Ватикан. При этом специалисты папской курии (учреждение, являющееся аналогом администрации президента) в этот период не только создавали шифры, но и разрабатывали криптоаналитические методы их вскрытия. При этом в отличие от арабов полученные результаты широко применялись для проникновения в тайны европейских монархов, политических деятелей, военачальников и т.д.

Не отставали от папских криптографов и правители итальянских городов-государств. В XIII-XIV веках методы криптографической защиты информации широко использовались в государствах Италии. Уже в эти времена венецианское правительство имело особых специалистов-шифровальщиков, а за всей криптографической деятельностью было поручено следить «Совету Десяти» - верховному органу исполнительной власти. В Венеции в это время находилась одна из самых организованных дипломатических служб. Ее приемы оказали сильнейшее влияние на дипломатию складывавшихся в это время в Европе монархий. Купечество захватившее власть в Венеции, внесло и в дипломатическое дело тот дух тайны и ревнивого недоверия и в то же время ту систематичность и целеустремленность, которыми было проникнуто все государственное управление. А уже тогда понимали, что дипломатическая деятельность без криптографии невозможна. Шифры обычно заключались в замене букв латинского алфавита либо другими буквами, либо арабскими цифрами, чёрточками, точками, произвольными фигурами, шифрованный текст нередко вводились знаки, не имевшие никакого значения для того, чтобы усложнить шифр. Эти знаки впоследствии стали называться пустышками. Как видим, пока еще простая замена господствовала в криптографии того времени.

РевOLUTIONный шаг был сделан в 1401 году в Мантуанском герцогстве. Секретарь герцога Симеон де Крема предложил шифр, в котором для гласных букв имелись по несколько шифробозначений (для одной буквы обычно использовали от 2 до 4 замен). Тот факт, что это применялось именно для гласных букв (при этом наиболее часто

встречающихся) свидетельствует о знании криптоаналитических методов дешифрования, основанных на частоте встречаемости знаков шифртекста. Это первый подобный шифр, дошедший до нас, хотя по некоторым сведениям подобные шифры стали применяться в Италии несколько ранее с 1390 годов [Kahn, 1967].

Большое внимание криптоанализу уделяли правители Милана герцоги Сфорца. Эти злые и жестокие олигархи постоянно интриговали с целью увеличения своих прибылей и расширения политического влияния, с помощью шифров они защищали свои тайны, а с помощью криптоанализа проникали в секреты своих конкурентов и других противников. Работы по криптоанализу начались в Милане примерно с начала XV века, успехи миланцев весьма своеобразно оценили их оппоненты из Модены, которые вручили своему послу в Милане самый сложный номенклатор из всех использовавшихся в этом герцогстве. На Сфорца в городе Павия работал один из секретарей криптоаналитик Чикко Симонетти. В 1474 году Симонетти написал свой трактат, посвященный исключительно криптоанализу. В нем Симонетти установил 13 правил вскрытия шифров простой замены, в которых сохранены разделители слов. Рукопись, написанная на трех кусках пергамента, начинается со слов: «Первое необходимое условие состоит в выяснении того, написан ли документ на латинском или на местном языке, а это можно установить следующим образом: выясните, имеют ли слова в данном документе только пять различных окончаний, меньше или больше. Если их только пять или меньше, вы правы, считая, что документ написан на местном языке...» [Кан, 2004, с. 128-129]. Через 9 лет после публикации работы Симонетти миланские криптографы стали использовать по два символа-пустышки для обозначения границ шифртекста. В этот период в Милане применяется шифр, названный «Миланский ключ», представляющий собой значковый шифр пропорциональной замены.

Главный революционный прорыв в европейской криптографической науке в XV веке совершил флорентиец Леон Баттиста Альберти (1404-1472) итальянский ученый, архитектор, теоретик искусства (см. рис.3.1). Альберти намного превосходил своих современников и талантом, и любознательностью, и многосторонностью, и особой живостью ума. В нем счастливо сочетались тонкое эстетическое чувство и способность разумно и логично мыслить, опираясь при этом на опыт, почерпнутый от

общения с людьми, природой, искусством, наукой, классической литературой. Болезненный от рождения, он сумел сделать себя здоровым и сильным. Из-за жизненных неудач склонный к пессимизму и одиночеству, он постепенно пришел к приятию жизни во всех ее проявлениях. Альберти получил юридическое образование в университете в Болонье. После тяжелой болезни Альберти переключил свое внимание с юриспруденции на искусство и науку. Его талант был универсален. Альберти обладал выдающимися способностями. Он является автором десяти научных трактатов по архитектуре (в т.ч. "О статуе", "О живописи", "О зодчестве"), он также писал поэмы, басни, комедии, музыку, был одним из лучших органистов своего времени. Будучи теоретиком искусства, он обобщил опыт гуманистической науки в изучении античного наследия. Альберти создал палаццо Ручеллаи, церковь Иль Джезу и ряд других замечательных произведений зодчества Италии. Трудолюбие Альберти было поистине безмерно. Он полагал, что человек, подобно морскому кораблю, должен проходить огромные пространства и "стремиться трудом заслужить похвалу и плоды славы". Как писателя, его одинаково интересовали и устои общества, и жизнь семьи, и проблематика человеческой личности, и вопросы этики [wikipedia].

В области криптографии заслугой Альберти стали 25 страничный «Трактат о шифрах» - он опубликовал первую в Европе книгу, посвященную криптоанализу, и изобрел устройство, реализующее шифр многоалфавитной замены, получившее название «диск Альберти».



Рис. 3.1 Л. Альберти

Нет ссылки в тексте на этот рис стр.71

Интерес Альберти к криптографии побудили встречи с папским секретарем Леонардо Дато, вот что об этом вспоминает он

сам, в начале «Трактата о шифрах»: «Мы с Дато гуляли в папских садах в Ватикане и заговорили, как мы часто это делали о литературе. Наше немалое восхищение вызвал немецкий изобретатель, который может сегодня взять до трех оригинальных работ какого-либо автора и за 100 дней с помощью подвижных литер изготовить более 200 копий. За один лишь контакт он может воспроизвести на своей печатной машине копию целой страницы большой рукописи (Здесь идет речь об изобретении в 1440 году книгопечатания Иоганном Гуттенбергом (Германия, г. Майнц), оно заметно повысило грамотность населения Европы. Ожилась переписка, возрос объем обмена секретной информацией. С другой стороны, доступные всем книги сами по себе породили "книжные" шифры, идею которых высказал еще древнегреческий полководец Эней, о чем было рассказано выше). Так мы переходили от одной темы к другой, изумляясь человеческой изобретательности, пока Дато не выразил своего неподдельного восхищения людьми, которые могут использовать то, что называют шифрами... Вы всегда интересовались этими секретами бытия – сказал Дато. Что Вы думаете об этих дешифровальщиках? Вы не пробовали свои силы в этом в меру своих познаний?». Альберти знал, что в обязанности Дато входила работа с шифрами. Вот, что он сказал папскому чиновнику: «Вы начальник папского секретариата. Не приходится ли Вам иногда пользоваться этими вещами в делах очень важных для его святейшества? Поэтому-то я и заговорил об этом – ответил Дато. Занимая свою должность, я хочу научиться делать это самостоятельно, не прибегая к помощи посторонних лиц. Ибо, когда мне приносят письма, шифр которых перехвачен шпионами, то тут уж не до шуток. Так что, пожалуйста, если Вы обдумывали какие-нибудь новые идеи на этот счет, расскажите мне о них» [Kahn, 1967].

Результатом этой беседы стала рукопись, написанная Альберти в 1466 или начале 1467 года, где излагаются основы частотного анализа, при этом Альберти заявляет, что додумался до этого метода совершенно самостоятельно. Тракtrat начинается с описания характерных особенностей латинского языка, затем Альберти коротко останавливается на особенностях итальянского языка и переходит к решению задачи вскрытия шифра простой замены на основе анализа повторяемости букв в тексте. Вот как он описывает процесс дешифрования: «Сначала я рассмотрю вопрос о количестве букв и те явления, которые зависят от количественных

закономерностей. Здесь гласные претендуют на первое место. Без гласной нет и слога. Поэтому, если вы возьмете страницу какого - либо стихотворного или прозаического латинского текста и отдельно подсчитаете в строках гласные и согласные, то вы наверняка убедитесь, что гласных очень много. Если все гласные на одной странице будут насчитывать, скажем, 300 букв, то количество всех согласных, вместе взятых, составит около 400 букв. Я заметил, что среди гласных буква „О“ хотя и встречается не менее часто, чем согласные, но реже других гласных. Когда в конце слова согласные следуют за гласной, этой конечной согласной всегда будет „Т“, „S“ и „X“, к которой может быть добавлена „С“ [Кан, 2004, с. 138]. Оставшаяся часть трактата посвящена вопросу повышения стойкости шифров. В дальнейшем преклонный возраст не позволил Альберти развить идеи из области криптоанализа, изложенные им в своем трактате. Работа Альберти положила конец почти полной монополии шифра простой замены, теперь стало ясно, что использование данного шифра небезопасно.

Однако Альберти предложил выход из положения – шифр многоалфавитной замены, являющийся стойким к частотному анализу. Принцип построения этого шифра заключается в следующем, для шифрования используются не один как в простой замене, а несколько шифралфавитов. Первая буква шифруется по первому шифралфавиту, вторая по второму и т.д. «Диск Альберти» (см. рис. 3.2) состоял из двух дисков – внешнего неподвижного (на нем были нанесены буквы в алфавитном порядке и цифры 1,2,3,4) и подвижного внутреннего диска, на котором буквы были переставлены. Процесс шифрования заключался в нахождении буквы открытого текста на внешнем диске и замене ее на букву с внутреннего диска, стоящую под ней. После этого внутренний диск сдвигался на одну позицию и шифрование второй буквы производилось уже по новому шифралфавиту.

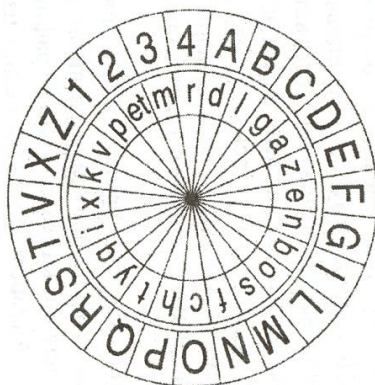


Рис. 3.2 Диск Альберти

Нет ссылки в тексте на этот рис стр74

Ключом данного шифра являлся порядок расположения букв на внутреннем диске и его начальное положение относительно внешнего диска. Другим изобретением Альберти стали коды, он предложил заменять на упорядоченные двух-, трех- и четырех цифровые комбинации слоги, слова и целые предложения (всего таких комбинаций 336). После этого цифры перешифровывались многоалфавитной заменой. Таким образом, Альберти одним из первых выдвинул идею «двойного шифрования» - текст, полученный в результате первого шифрования, подвергался повторному шифрованию другим шифром. «Диск Альберти» является одним из первых механических устройств шифрования. Идеи Альберти использовались при создании дисковых шифрмашин в первой половине XX века, некоторые из них использовались в разных странах до 1980-х годов. В многоалфавитном шифре Альберти количество алфавитов равно числу букв в алфавите открытого текста плюс четыре. Альберти - изобретатель многоалфавитных шифров, которые, в основном, используются и в наши дни. Однако способ выработки последовательности алфавитов шифрованного текста и их выбор существенно усложнен; у Альберти он определялся циклическим сдвигом на единицу через заранее оговоренное количество шифруемых букв. Таким образом, процесс шифрования стал

«динамичным» [Васин, 2008]. Многоалфавитные шифры явились большим шагом вперед, но на практике не использовались в течение более четырех столетий. Потому, что многоалфавитная замена по сравнению с номенклатором отнимала слишком много времени, а «незначительная» ошибка при письме, например, пропуск буквы, приводила к таким искажениям, что получателю сообщения было не суждено расшифровать его даже при наличии верного ключа. В заключении рассказа о криптографической деятельности Альберти приведем следующую цитату: "Должен был появиться человек, - писал Леонардо Ольшки, - который, владея теорией и имея призвание к искусству и практике, поставил бы стремления своего времени на прочную основу и придал бы им определенное направление, в котором им предстояло развиваться в будущем. Этим многосторонним, но в то же время гармоническим умом был Леон Баттиста Альберти" [wikipedia].

К итальянским разработкам в области криптографии и криптоанализа мы еще вернемся. Но криптографические идеи в Европе в Эпоху Возрождения появлялись не только на Апеннинском полуострове. Первым немцем, внесшим значительный вклад в криптографию, был Иоганнес Тритемий (1462—1516), он родился 2 февраля 1462 года в городе Триттенхайме, в семье богатого винодела. В 17 лет Иоганнес поступил в Гейдельбергский университет, где и выбрал себе латинизированный псевдоним Тритемий (настоящая его фамилия – Гейденберг). В 20-летнем возрасте Тритемий избирает путь монашества и вскоре, несмотря на молодость, становится аббатом монастыря Святого Мартина в городе Шпанхайме, с 1506 года Тритемий становится настоятелем монастыря Святого Иакова в городе Вюрцбурге. В 24 года публикует первую книгу проповедей, которая пользуется успехом. Вообще Тритемий был разносторонним ученым, занимался богословием, историей, алхимией, оккультизмом (в частности классификацией ведьм и ангелов, ведьм Тритемий разделил на 4 тщательно описанные категории, а ангелов на 12 иерархий), магией, библиографией, а также криптографией. Среди его учеников был знаменитый врач Парацельс, а читателей книг - Джордано Бруно. Римская католическая церковь сочла некоторые труды Тритемиев еретическими и в 1609 году внесла его книги в список запрещенных книг. Этот запрет длился 250 лет. Сам Тритемий еще при жизни приобрел репутацию чародея.

Следует отметить следующие труды Тритемия: биографический справочник знаменитых немцев, описание жизни Святого Максима, ряд исторических хроник, а так же «Книгу о писателях духовных» (1494 год) – хронологический перечень 7000 работ в области теологии 963 авторов. Последняя работа принесла Тритемию титул «отца библиографии». Помимо собственных трудов Тритемий активно занимался формированием монастырской библиотеки. К 1503 году в его библиотеке насчитывалось уже две тысячи томов - невероятное богатство для того времени! Люди из других городов Германии, из Италии и Франции приезжали посмотреть на его коллекцию и на знаменитого аббата, эрудиция которого вошла в пословицу. В переписке с Тритемием состояли крупные ученые, представители знати, религиозные и политические деятели. Среди последних можно назвать императора Священной Римской империи Максимилиана I (Интересно отметить, что по приказу Максимилиана в первом десятилетии XVI века была организована одна из первых в Европе служб перлюстрации почтовой корреспонденции, которую можно считать прародительницей европейских «черных кабинетов» [Черняк, 1991, с 248]), Маркграфа Бранденбургского, пфальцграфа Филиппа из Гейдельберга и др. Правители приглашали Тритемия для познавательных бесед и советов по различным вопросам.

Существует легенда, что в 1482 году Тритемия вызвали ко двору императора по срочному делу. Императрица Мария Бургундская погибла в результате несчастного случая, и Максимилиан, прежде чем избрать себе новую супругу, пожелал выслушать совет мудрого аббата. Утверждают, что Тритемий предложил императору вызвать дух покойной императрицы, дабы та сама назначила свою преемницу. Максимилиан согласился. Тритемий вызвал дух покойной, и Мария явилась во всей своей красе. Побеседовав с ней, Максимилиан забыл об осторожности и вышел из магического круга, чтобы обнять любимую жену, - но тотчас же упал наземь, как громом пораженный, а призрак сию минуту исчез. Впрочем, до того Мария успела предсказать множество будущих событий и, в том числе, назвать новую императрицу - Бьянку Сфорца.

Одно из знакомств Тритемия было весьма экзотическим, это был прототип знаменитого героя Гёте – доктора Фауста. Тритемию он был известен под именем Георгия Сабелликуса и произвел впечатление "глупого и дерзкого человека, ничего не смыслящего в

настоящих науках" [Бабаш, 2002, с. 60]. Интересно отметить, что согласно преданию математик, астроном, астролог Фауст владел символическими способами письма, знал шифры перестановки («анаграммы»).

Первым трудом Тритемия в котором появляется криптография является эзотерическая книга «Стеганография» (Книга не имеет отношения к защите информации подобным методом). В первых двух главах книги описаны некоторые элементарные системы шифрования, представляющие из себя простые взаимные замены гласных и согласных, а также несколько вариантов шифра, в котором только определенные буквы бессмысленных слов имеют осмысленное значение, а остальные не несут никакой информации. Приведем пример (для русского языка):

Пусть имеется сообщение: ВРАНАХ МОРТУН ГЕВБДА ПИМРБА НУКБИР РАСАЕХ УРТАНГ СОРЕЙД. Если прочитать каждую пятую букву каждого второго слова, то получится секретное сообщение «УБЕЙ».

Однако в целом «Стеганография» не являлась пособием по криптографии, а была посвящена различным эзотерическим вопросам. Эта рукопись вызывает интерес до сих пор, первоначально она распространялась в списках, а полная версия была напечатана в городе Дармштадте в 1621 году (Steganographia. Darmstadt 1621). Современные эзотерики считают, что Тритемий, писал «Стеганографию» шифром и каждое слово его имеет скрытый смысл; однако ключ к этому шифру великий аббат унес с собой в могилу. Поскольку для верного понимания труда Тритемия важно учитывать определенные сочетания слов, эта книга - написанная по-латыни - становится совершенно бессмысленной в переводе.

В 1508 году Тритемий приступил к написанию книги «Полиграфия» (см. рис. 3.3), посвященной криптографии, эта книга была издана в 1518 году, спустя два года после смерти автора, «Полиграфия» стала первой печатной книгой, посвященной криптографии. Там описывались известные на тот момент шифры, но помимо этого Тритемий предложил два шифра многоалфавитной замены, которые вписали его имя золотыми буквами в историю криптографии.

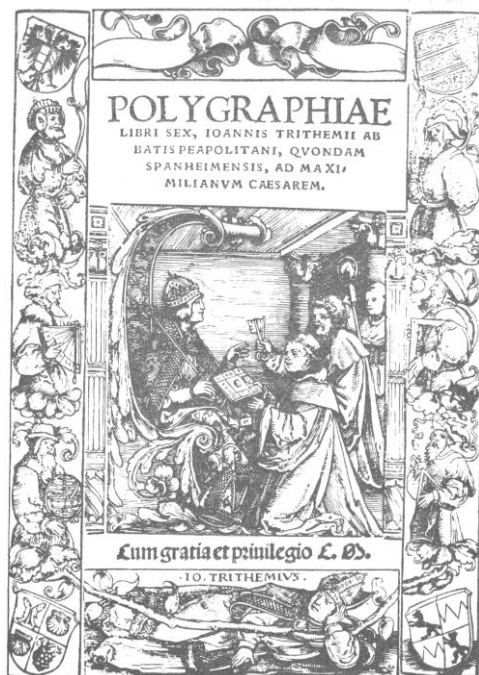


Рис. 3.3 Гравюра по дереву, которая является первой страницей книги «Полиграфия».

На этой гравюре изображен автор в своем бенедиктинском одеянии со своей аббатской митрой, лежащей на полу перед ним. Стоя на коленях, он преподносит свою книгу, закрытую на замок, что подчеркивает ее секретное содержание, императору Священной Римской империи Максимилиану, которому ее посвящает. Сидя на своем троне во дворце в городе Аугсбург с императорской короной на голове и в мантии, Максимилиан в одной руке держит свой скипетр, а другой благославляет Тритемия. За Тритемием изображено еще одно лицо – или монах или издатель, который протягивает Максимилиану два ключа от книги, символизирующие духовную и мирскую власть Максимилиана. На заднем фоне капеллан Тритемия, юный монах, держит посох своего аббата. Внизу изображен Тритемий, лежащий с веткой, унизанной плодами, которая символизирует его девиз - "Я буду судить о дереве по его плодам". В левом верхнем углу – герб Священной Римской империи. Напротив – герб гравера. Слева внизу – герб самого Тритемия – два окуня спина к спине – символ его

религиозного положения, гроздь винограда – его отец был виноделом, и две раковины, смысл которых можно разгадать как замкнутость, тайна, богатство. Внизу справа герб епископа Вюрцбурга. По бокам философы держат сферу, секстант, компас и угольник [Kahn, 1967].

Полное название работы Тритемия звучит так: «Шесть книг о полиграфии Иоганнеса Тритемия, аббата в Вюрцбурге, прежде в Шпанхайме, для императора Максимилиана», она была написана на латинском языке. Книга содержала 540 страниц относительно небольшого формата, она переиздавалась в 1550, 1571, 1600 и 1613 годах. В 1541 году вышел французский перевод, а чуть позже книга вышла на немецком языке. В 1561 году появился сильно искаженный французский перевод книги Тритемия, выполненный Габриелем де Колланжем, который был переиздан в 1625 году. Интересно отметить, что в 1620 году некий Доменик де Хоттинга опубликовал работу Колланжа, как свою собственную, при этом публично жаловался, как трудно было ее написать, таким образом, с книгой Тритемия связан один из ранних случаев плагиата в истории книгопечатания [Kahn, 1967].

«Полиграфия» разделена на 6 частей (книг), первая и вторая посвящены изобретенному Тритемием шифру "Аве Мария". Этот шифр **ЭТО К ЧЕМУ?** основан на принципе замены букв шифруемого текста на заранее оговоренные слова (см. рис. 3.4).

a	Deus	a	clemens
b	Creator	b	clementissimus
c	Conditor	c	pius
d	Opifex	d	pissimus
e	Dominus	e	magnus
f	Dominator	f	excelsus
g	Consolator	g	maximus
h	Arbiter	h	optimus

Рис. 3.4 Первая страница ключа Тритемия к шифру "Аве Мария" [Kahn, 1967].

При этом каждой букве соответствует несколько слов, то есть это оригинальный шифр многоалфавитной замены. Из этих сообщений составлялось внешне "невинное" сообщение. Таким образом, при использовании данного шифра реализуются два метода

защиты информации – криптография и стеганография. Соединение этих методов для того времени было новаторским.

Как видно из рисунка Тритемий использовал слова религиозного содержания, при этом они выбирались таким образом, что практически любому открытому тексту можно было подобрать осмысленный шифрованный текст. При этом шифртекст получался в виде не вызывавшей подозрений молитвы.

Поясним использование шифра "Аве Мария" на примере с использованием русского языка:

Заменим буквы Е, Н, Т на следующие слова:

Е = "ЗЕЛЕНый", "ЖДУ", "МОЙ", «ОН».

Н = "И", "Я", "ЗДЕСЬ".

Т = "ДОМА", "ВЕЧЕРОМ", "ОКОЛО", "КЛЮЧ".

Тогда отрицательный секретный ответ "нет" на заданный вопрос может иметь несколько "невинных" вариантов: "Я жду дома", "Я жду вечером", "Здесь мой ключ", «И зеленый ключ», «Здесь он дома», «И он вечером» [Бабаш, 2002, с. 60].

Первая книга, напечатанная крупным готическим шрифтом, содержит 384 буквы и соответствующих им слов, разбитых на две колонки на странице, вторая - другой ключ для шифра «Аве Мария» на 274 величины. Третья книга представляет собой шифр многоалфавитной замены, где буквы заменяются на искусственно придуманные «слова» типа HUBA, HUBE, HUBI, HUBO и т.п. Всего имеется 1056 пронумерованных строк, в каждой из которых по 3 «слова», пользоваться этим шифром нужно также как «Аве Марией», но стеганографическая составляющая отсутствует. Заметим, что числа 384, 284, 1056 не кратны 26 (количеству букв в латинском алфавите для которого предназначались эти шифры), очевидно Тритемий придумал большее количество эквивалентов для чаще встречаемых букв и меньшее для редких. Четвертая книга насчитывает 117 колонок искусственных слов, в которых вторая буква в алфавитном порядке менялась от А до W (Тритемий поставил ее в конце алфавита после Z): BALDACH, ABZACH, ECOZACH, ADONACH и т.д. Из этих слов составлялся шифртекст, читалась каждая вторая буква, то есть приведена система, которая очень похожа на то, что Тритемий описал в «Стеганографии».

Наиболее серьезное предложение Тритемия по защите информации, с помощью шифров изложено в пятой книге. Это квадратная таблица алфавитов подписанных один под другим и

циклически сдвинутых на одну позицию влево. Эта таблица получила название «таблица Тритемия». Ее эквивалент для современного английского алфавита приведен на рис. 3.5.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Рис. 3.5 Таблица Тритемия [Бабаш, 2002, с. 61].

Рассмотрим процесс шифрования по этой системе. Здесь первая строка таблицы является одновременно и строкой букв открытого текста. Первая буква текста шифруется простой заменой по второй строке, вторая буква по третьей и так далее после использования последней строки возвращаются к первой. Так слово *Trithemius* зашифровывается следующим образом: *UTLYMLTQDS*.

То есть, как и в случае с шифром "Аве Мария", это шифр многоалфавитной замены, но реализованный совершенно иным способом. Тритемий развил идею Альберти о многоалфавитных шифрах.

Преимущество этого метода шифрования по сравнению с методом Альберти состоит в том, что с каждой буквой задействуется новый алфавит. Альберти рекомендовал менять алфавиты лишь после трех или четырех слов, хотя возможность смены алфавита на каждом такте шифрования уже была возможна. Поэтому его шифртекст состоял из отрезков, каждый из которых обладал закономерностями открытого текста, которые помогали вскрыть криптограмму. Побуквенное зашифрование не дает такого преимущества. Шифр Тритемия является также первым нетривиальным примером периодического шифра. Так называется многоалфавитный шифр, правило зашифрования которого состоит в использовании периодически повторяющейся последовательности простых замен.

Реализация таблицы Тритемия не требует использования каких-либо механических приспособлений. Однако в первоначальном варианте в шифре Тритемия отсутствовал ключ. Секретом являлся сам способ шифрования. В дальнейшем усложнения шифра пошли по двум путям:

- введение произвольного порядка расположения букв исходного алфавита шифрованного текста вместо лексикографически упорядоченного алфавита;

- применение усложненного порядка выбора строк таблицы при шифровании.

Эти усложнения позволили применять ключевые множества значительного объема [Бабаш, 2002, с. 62].

Шестая книга посвящена «историческим шифрам». В ней приводятся шифрсистемы, которые использовались норманнами и франками (это в основном вариации на тему простой замены, своеобразная реинкарнация античных шифров), а также одно из первых изложений записок Тирона. Это шифр, который по преданию был изобретен Туллием Тироном – рабом, отпущенным Цицероном на свободу. Шифр представлял собой, так называемое, силлабическое письмо – это слоговое письмо, являющиеся видом фонетического письма, в котором одним знаком изображается последовательность согласных и гласных (как правило, один слог). Можно сказать, что силлабическое письмо является предком системы шифрования с

помощью кодов (как было отмечено выше, «классические» коды были изобретены Л. Альберти в XV веке и применяются до наших дней). Силлабическое письмо использовал для защиты информации римский папа Сильвестр II (занимал престол Святого Петра с 999 по 1003 годы), кстати, он упомянул имя изобретателя этой системы Тирона в зашифрованном виде в двух своих буллах. Силлабическое письмо использовалось также в Индии, Тибете, Эфиопии, местные ученые изобрели его независимо от Тирона и друг друга [Словарь, 1984], [Kahn, 1967].

В заключение отметим, что идеи Тритемия оказали огромное влияние на развитие криптографии. Автор первой печатной книги, посвященной криптографии, придумал шифр, построенный на основе периодически сдвигаемого ключа – Таблицу Тритемия, которая стала основой многочисленных шифрсистем в более позднее время.

Вернемся к итальянцам. Пожалуй наиболее развитой криптографической службой в XVI веке обладала Венеция. Главным криптоаналитиком здесь был секретарь по шифрам (с 1506 года) Венецианской республики Джованни Соро. Одним из первых его успехов стало дешифрование послания Марка Антония Колонны, командующего армией императора Священной Римской империи Максимилиана I, фактически германского императора. Из этой депеши итальянцам удалось узнать, что имперская армия испытывает серьезные проблемы, Марк Антоний просил прислать 20000 дукатов или лично прибыть императору в распоряжение войск для поднятия морального духа [Kahn, 1967]. Как было сказано выше, в этот период Тритемий уже работал над своей «Полиграфией», но результаты его работы стали известны несколько позже, пока же германский император и его военачальники использовали традиционные для того времени шифры – номенклаторы и различные варианты шифра простой замены.

В дальнейшем Соро прославился тем, что с успехом вскрывал шифры многочисленных европейских государств. Слава Соро была столь велика, что во многих государствах Европы были приняты срочные меры по увеличению стойкости используемых шифров. Интересно отметить, что Соро работал и на Папскую курию. Начиная с 1510 года из Ватикана ему присылали для вскрытия шифры, с которыми не могли справиться папские криптоаналитики. Так, например, в 1526 году Папа Климент VII (Не путать с Антипапой носившем то же имя) дважды направлял Соро перехваченные

сообщения для дешифрования, и оба раза Соро добился успеха. В первом случае это были 3 весьма объемные депеши императора Священной Римской империи (он стал приемником Максимилиана I) и по совместительству короля Испании Карла V, а во втором – письма герцога Феррасского к своему послу в Испании. Занимался Соро и анализом стойкости папских шифров. Так, когда одно из посланий Климента попало в руки его противников, тот воскликнул: «Соро может вскрыть любой шифр!» [Кан, 2004, с. 127] – и направил Соро копию этого послания, чтобы выяснить, надежно ли оно зашифровано. Соро успокоил Папу, сообщив, что не может его прочесть. Хотя есть предположения, что Соро мог преднамеренно ввести Папу в заблуждение, не желая огорчать, а также давая Венеции возможность читать зашифрованную корреспонденцию. Помимо криптоанализа Соро занимался и разработкой шифров, в частности им был создан «общий шифр» (это был номенклатор) для связи венецианских послов в разных странах между собой. У дипломатов имелся также «специальный шифр» для связи с родиной. Такое разделение было сделано для того, чтобы в случае вскрытия (или кражи) противником одного шифра, связь по другому направлению была бы возможна.

15 мая 1542 года Соро получил двух помощников, таким образом, с этого времени Венеция обрела первую в мире дешифровальную службу. Криптоаналитикам было предоставлено помещение во дворце дожа (венецианского правителя), где они работали за запертыми дверями. Никому не позволялось их беспокоить, а им самим, по слухам, не разрешалось покидать свое рабочее помещение, пока не будет найден открытый текст очередной перехваченной криптограммы. Работа по криптоанализу зашифрованных сообщений начиналась немедленно после того как они попадали в руки венецианцев.

Венецианские криптоаналитики также писали трактаты, в которых разъясняли методы своей работы. К сожалению, труд Соро о дешифровании переписки на латинском, итальянском, испанском и французском языках, написанный им в начале XVI века, утерян. Однако уцелели отрывочные записи его преемника, а также исследования в этой области других венецианских секретарей по шифрам. Это были Джиованни Батиста де Людовичис, Джироламо Франческа, Джиованни Франческо Марина и Агостино Амади. Учебное пособие последнего высоко оценили руководители Венеции -

двум его сыновьям был назначен пожизненный пенсион в 10 дукатов ежемесячно каждому.

Необходимо отметить, что именно в Венеции впервые в мире был применен системный подход в отношении криптографии. Криптографическая служба имела четкую структуру, были организованы каналы шифрованной связи с заграничными представителями, были организованы перехват и дешифрование иностранных секретных сообщений. В продолжение дела Соро было создано учебное заведение для обучения криптографии, кстати, не только обучаемые, но и действующие специалисты каждый год в сентябре сдавали экзамен. Не оставлялась без внимания материальная сторона, жалование криптографов составляло 10-12 дукатов в месяц, что было весьма неплохо, для Венеции того времени. При этом специалист, внесший ценные предложения по улучшению функционирования криптографической службы получал солидную надбавку к жалованию, при этом однако раскрывшего секреты венецианской криптографической службы могли казнить.

«Совет десяти» способствовал притоку свежих идей в криптографическую службу из вне, для этого регулярно проводились конкурсы по шифрам, отличившиеся в них щедро награждались. Так весьма значительную сумму в 100 дукатов получил Марко Рафаэль (позднее он стал фаворитом короля Англии Генриха VIII) за рецепт симпатических (невидимых) чернил не известный ранее.

Весьма внимательно относились в «Совете десяти» к надежности шифрсвязи, при малейшем подозрении о возможности компрометации того или иного шифра он тут же заменялся, для этого всегда в запасе имелись несколько номенклаторов, неиспользуемых ранее. Так, например, 31 августа 1547 года новые шифры были направлены послам в Англии, Милане, Риме, Турции, Франции и при императоре Священной Римской Империи. 5 июня 1595 года один из вернувшихся из за рубежа дипломатов сообщил руководству, что венецианские шифры дешифрованы. На основании этой информации 12 июня Совет отдал распоряжение заменить все посольские шифры. Это было немедленно сделано, послам были посланы новые номенклаторы, которые были разработаны самым опытным на тот момент из венецианских секретарей по шифрам Пьетро Партенио. Сами венецианские дипломаты хорошо понимали особенности использования шифров, так венецианский посол при дворе английского короля Генриха VIII (1491-1547) узнал, что его письма

перлюстрируются. Впрочем, это относилось и к переписке других дипломатов работавших в то время в Лондоне. Венецианец предположил, что англичане будут пытаться дешифровать их. С целью исключения атаки «открытый – зашифрованный текст», посол перефразировал и максимально изменял ноты и заявления перед тем как довести их до сведения англичан [Kahn, 1967].

Венеция была не единственным в Италии местом обитания искусных криптоаналитиков в эпоху европейского Возрождения. Во Флоренции Пирро Музефили, граф Сассетский, с 1546 по 1557 годы прочел множество зашифрованных сообщений, вскрыв среди прочих номенклатуры, использовавшиеся в переписке между французским королем Генрихом II и его посланцами в Дании и Сиене, шифр кардинала Неаполя ди Мендоце. Музефили был очень квалифицированным криптоаналитиком, поэтому к нему как и к Соро, обращались зарубежные представители с просьбой вскрыть для них шифры. Среди клиентов Музефили были в частности король Англии, который прислал ему криптограмму, найденную в подметках пары золотых туфель, доставленных к его двору из Франции и герцог Альба. Один из папских криптографов, рассуждая о вкладе своих современников сказал: «Музефили по праву положено первое место и все почести» [Kahn, 1967]. Однако его приемник Камилло Джусти оказался еще более опытным специалистом. Так же как и Соро, Музефили и Джусти занимались не только дешифрованием, но и созданием шифров. Созданные ими шифры для правителей Флоренции Медичи, в особенности для Лоренцо Великолепного показывают, что при их разработке были учтены известные флорентийцам методы криптоанализа [Kahn, 1967]. Отметим также, что о криптографии в своей книге «О военном искусстве» упоминает уроженец Флоренции, знаменитый политический и государственный деятель, мыслитель, писатель Николо Макиавелли (1469-1527).

Еще одним итальянцем, внесшим вклад в развитие криптографии был Джероламо Кардано (1501-1576) (см. рис. 3.6) математик, философ, врач и изобретатель. Издал ряд трудов по алгебре, а так же является автором первой в мире книги по теории вероятности. С именем Кардано связывают формулу

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

для решения неполного кубического уравнения $x^3 + px + q = 0$. Так же в его работах впервые появились мнимые

величины (комплексные числа). Жизнь Кардано была омрачена тяжелым и некрасивым спором – ссорой со своим другом – математиком Тарталья. Кардано «позаимствовал» свою знаменитую «формулу Кардано» (решение уравнения третьей степени) у своего друга и опубликовал ее под собственным именем. Этот факт вызвал весьма негативную оценку со стороны современников Кардано и у последующих поколений математиков.

Судьба Кардано сложилась трагически. Как астролог, он заранее предсказал себе 75 лет жизни. Чтобы не нарушать собственное предвидение, согласно легенде он покончил с собой в отведенный им срок со словами: "Если и неверно, то неплохо придумано". Перед смертью, находясь в религиозном экстазе, Кардано сжег свои книги, усмотрев в них противоречие «с волей божьей».

Кардано изобрел и шарнирный механизм для соединения двух валов под переменным углом, впоследствии получивший название карданный вал.



Рис. 3.6 Д. Кардано

Нет ссылки в тексте на этот рис стр 87

В криптографии он (известно, что Кардано тесно сотрудничал с папской курией и возможно этот шифр изначально предназначался для Ватикана) известен изобретением оригинального шифра, называемого «решеткой Кардано». Из плотного материала вырезался прямоугольник произвольных размеров, например, 7×10 клеток. В прямоугольнике проделывались окна. Секретный текст вписывался в эти окна, затем решетка снималась и оставшиеся клетки заполнялись так, чтобы получалось сообщение, не вызывающее подозрений. Суровую команду на английском языке: «YOU KILL AT ONCE» с

помощью решетки можно спрятать в текст любовного содержания, например такой: «I LOVE YOU. I HAVE YOU DEEP UNDER MY SKIN. MY LOVE LASTS FOREVER IN HYPERSPACE».

I		L	O	V	E		Y	O	U
I		H	A	V	E		Y	O	U
D	E	E	P		U	N	D	E	R
M	Y		S	K	I	N		M	Y
L	O	V	E		L	A	S	T	S
F	O	R	E	V	E	R	I	N	
H	Y	P	E	R	S	P	A	C	E

Этот

шифр

использовался во многих странах в разные времена, в том числе и во время Второй мировой войны. Вот пример, в 1828 году должность российского представителя в Персии занимал известный русский писатель, общественный деятель и дипломат Александр Сергеевич Грибоедов. Он использовал в своих письмах «решетку Кардано». Грибоедов писал своей жене «невинные» послания, с которыми знакомились сотрудники МИД. Они расшифровывали сообщения и затем доставляли письма адресату. Жена Грибоедова, видимо, не догадывалась о двойном назначении этих посланий.

Уже в Советское время некоторых биографов Грибоедова смутил тот факт, что в отдельных письмах из Персии нарушался характерный стиль знаменитого писателя. При исследовании оказалось, что эти письма содержали дипломатические послания Александра Сергеевича. Раскрыли эту систему очень просто. Сложили все листочки в стопку и просветили мощной лампой. Буквы, стоявшие на местах окон решетки, давали темные пятна, так как лежали строго друг под другом. По этим пятнам легко восстанавливалась решетка, то есть ключ (см. рис 3.7).

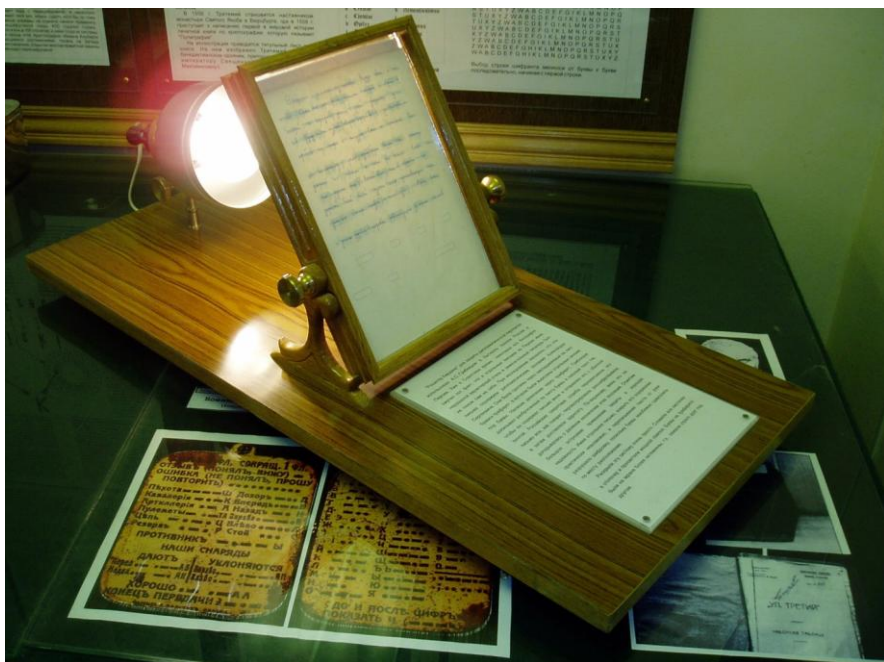


Рис. 3.7. Реконструкция прибора для дешифрования «решеток Кардано». Нет ссылки в тексте на этот рис стр 69

Идеи Альберти и Тритемия развил Джованни Батиста Белазо. Факты из его жизни очень немногочисленные и даже противоречивые, но его заслуги в криптографической сфере, безусловно, заслуживают признания. Уже про происхождение Белазо разные источники выдают разную информацию. По некоторым документам родился Джованни в 1505 году в древней и благородной брешианской семье. Его семье принадлежала большая территория в окрестностях города Фениллы. Там до сих пор сохранилась часовня, принадлежавшая этому знатному роду. Следующее, документально подтвержденное, звено жизни Джованни – это обучение в Университете города Падуи, о чем свидетельствует его регистрация как студента, и успешное его окончание с присуждением диплома в гражданском праве в 1538.

Заинтересовавшись математикой, Белазо занимается секретными письмами. Белазо пользовался большой популярностью у местных судей и папской курии. Белазо был одним из немногих

секретарей, которые скорее из любопытства и менее из за необходимости, пробовали новые методы шифрования в своей ежедневной практике. Некоторые придуманные им шифры считались совершенными на протяжении последующих практически 4-х веков.

Белазо в этот период своей жизни написал 3 работы на криптографические темы, в которых он щедро поделился своим опытом работы криптографа в свите кардинала Карпи. В 1553 году в Италии вышла небольшая книга «Шифр синьора Белазо». Белазо предложил использовать таблицу Тритемия совместно с легко запоминаемым ключом, так называемым паролем. Таким паролем могло бы служить, например, легко запоминаемое стихотворение. Буквы, входящие в стихотворение, последовательно определяют строки таблицы Тритемия, по которым шифруются буквы открытого сообщения. Сам пароль стал ключом шифра. Однако Белазо, как и Тритемий, использовал в качестве шифралфавитов обычные алфавиты. Кроме этих автобиографических данных, имеются несколько источников, в которой Белазо упомянут его современниками. Так, например, Белазо приписывается изобретение полиалфавитного шифра с автоключом [Бабаш, 2002], [Buonafalce, 2006], [Kahn, 1967].

Как уже упоминалось выше, весьма высокое значение криптографии придавали в Ватикане, шифровальная служба при папской курии к тому времени действовала уже примерно пару столетий. Занимались там и криптоанализом, однако до поры до времени делалось это без какой либо системы, а в наиболее сложных обращались к криптоаналитикам итальянских городов-государств. Римский Папа Павел III, сменивший Климента VII, быстро сообразил, что не в его интересах посылать шифры для вскрытия за границу, а надо бы использовать собственные кадры. Все вопросы, связанные с криптографией были поручены специалисту Антонио Элио, «который умел с большой легкостью дешифровать шифры» [Kahn, 1967]. Этот криптоаналитик сделал блестящую карьеру, став впоследствии личным секретарем Папы. Позднее он получил сан епископа города Пулы (Хорватия, в описываемые времена находился под контролем Венеции) и наконец стал иерусалимским патриархом. В 1555 году в папской курии была учреждена должность секретаря по шифрам, которую занял Трифон Бенчо де Ассизи. В 1557 году под его руководством папские криптоаналитики достигли грандиозного успеха, они вскрыли шифр испанского короля Филиппа II (1527-1598),

который тогда воевал с Папой Римским (см. рис. 3.8). Это был очень сложный номенклатор, описание которого будет приведено ниже. В частности было дешифровано письмо Филиппа к кардиналу Бургундии. А вскоре был вскрыт и весь шифр.

[1557.]

Cifra del card. di Burgos¹ con il re Philipppo, decifratra alli X febraro 1557
in Bologna.

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	y	z
⌘	⌘	.	L	⌘	.	.	.	G	∞	.	Γ	⌘	.	.	Δ	⌘	.	a	⌘	
ω	Λ			+				T			b				ε	-e		ot		
ba	be	bi	bo	bu							pa	pe	pi	po	pu					
m	m̄	-m	m+	m̄							u	ù	-u	u+	ū					
											61	62	63	64	65					
ca	ce	ci	co	cu							qua	que	qui							
16	17	18	19	20							τ	τ̄	-τ							
n	n̄	-n	n+	n̄							66	67	68							
da	de	di	do	du							ra	re	ri	ro	ru					
21	22	23	24	25							φ	φ̄	-φ	φ+	φ̄					
e	ē	-e	e+	ē							71	72	73	74	75					
fa	fe	fi	fo	fu							sa	se	si	so	su					
a	à	-a	a+	ā							∞	∞̄	∞	∞+	∞̄					
ga	ge	gi	go	gu							76	77	78	79	80					
Q	Q̄	-Q	Q+	Q̄							ta	te	ti	to	tu					
31	32	33	34	35							×	×	-×	×	×					
ha	he	hi	ho	hu							81	82	83	84	85					
36	37	38	39	40							va	ve	vi	vo	vu					
ia	ie	ii	io	iu							p	p̄	-p	p+	p̄					
e	ē	-e	e+	ē							86	87	88	89	90					
41	42	43	44	45							xa	xe	xi	xo	xu					
⌘	⌘̄	-⌘	⌘+	⌘̄							g	ḡ	-g	g+	ḡ					
											91	92	93	94	95					
la	le	li	lo	lu							za	ze	zi	zo	zu					
5-	5̄	-5	5+	5̄							ε	ε̄	-ε	ε+	ε̄					
46	47	48	49	50							96	97	98	99	-					
ma	me	mi	mo	mu							gra	gre	gri	gro	gru					
ω-	ω̄	-ω	ω+	ω̄							ψ	ψ̄	-ψ	ψ+	ψ̄					
51	52	53	54	55																
na	ne	ni	no	nu							cha	che	chi	cho	chu					
o-	ō	-o	o+	ō							g	ḡ	-g	g+	ḡ					
56	57	58	59	60																

Рис. 3.8. Результат работы папских криптоаналитиков над письмом испанского короля кардиналу Бургундии.

Нет ссылки в тексте на этот рис стр 92

Здесь сделаем небольшое отступление и рассмотрим криптографическую деятельность в Испании в описываемый период. Первые испанские шифрсистемы были внедрены в Испании в 1480 году советником Мигелем Пересом Альсаманом. Это были

преобразования открытого текста в римские цифры, то есть простая замена. Христофор Колумб, будучи в Новом Свете, использовал такой шифр в письме к брату, где предлагал выгнать присланного из Испании губернатора.

24 мая 1556 года, начавший править только год назад испанский король Филипп II написал письмо своему дяде Императору Священной Римской империи и королю Венгрии Фердинанду I, где сообщил, что хочет изменить шифры своего отца, так как они были скомпрометированы. И шесть месяцев спустя "общий шифр" Филиппа II начал использоваться. Испанские шифры того времени были весьма совершенны, они представляли собой номенклаторы. В состав номенклатора входил код и шифр пропорциональной замены (для гласных букв использовались по три шифробозначения (знаки открытого текста обычно называются шифрвеличинами, а шифрованного шифробозначениями), для согласных – два), так же имелись свои обозначения для наиболее часто встречающихся биграмм и триграмм (это могли быть двузначные числа или специальные знаки). В шифртексте имелись «пустышки» (ни чего не значащие знаки), они помечались точкой стоящей над знаком. Если в открытом тексте встречалось удвоение букв, то вторая буква пропускалась, а над шифробозначением первой ставились две точки.

Существовал общий шифр, который использовался для защиты переписки между королем и испанскими дипломатами в различных странах и особые шифры для связи короля с военачальниками, губернаторами колоний и другими корреспондентами, а также их связи между собой.

Приведем пример одного из вариантов общего шифра Филиппа II, сохранившегося в испанских архивах [Devos, 1950].

Пропорциональная замена:

a	b	c	d	e	f	g	h	i	l	m	n
4	3	u	o	и	g	f	p	g	1	L	Г
7	^	>	<	+	g	q	d	f	∞	θ	6
ω	1			+o							
o	p	q	r	s	t	v	x	y	z		
L	1	1	E	Ze	Z	o	D	g	u		
Le	v	Δ	+	ℓ	x	∫	d	2	ω		
4						a					

Таблицы замены биграмм и триграмм:

ba	be	bi	bo	bu
m-	m	m	m	me
11	12	13	14	15
da	de	di	do	du
e-	e	e	e	ee
21	22	23	24	25
ga	ge	gi	go	gu
q-	q	q	q	qe
31	32	33	34	35
ja	je	ji	jo	ju
o-	o	o	o	oe
41	42	43	44	45
ma	me	mi	mo	mu
ω-	ω	ω	ω	ωe
51	52	53	54	55

ca	ce	ci	co	cu
n-	n	n	n	ne
16	17	18	19	20
fa	fe	fi	fo	fu
a-	a	a	a	ae
26	27	28	29	30
ha	he	hi	ho	hu
b-	b	b	b	be
36	37	38	39	40
la	le	li	lo	lu
s-	s	s	s	se
46	47	48	49	50
na	ne	ni	no	nu
o-	o	o	o	oe
56	57	58	59	60

pa	pe	pi	po	pu
u-	u	u	u	ue
61	62	63	64	65
ra	re	ri	ro	ru
q-	q	q	q	qe
71	72	73	74	75
ta	te	ti	to	tu
x-	x	x	x	xe
81	82	83	84	85
xa	xe	xi	xo	xu
g-	g	g	g	ge
91	92	93	94	95
za	ze	zi	zo	zu
c-	c	c	c	ce
01	02	03	04	05
ca	ce	ci	co	cu
g-	g	g	g	ge
11	12	13	14	15
ga	ge	gi	go	gu
ψ-	ψ	ψ	ψ	ψe
21	22	23	24	25
pa	pe	pi	po	pu
o-	o	o	o	oe
31	32	33	34	35

qua	que	qui	quo	quu
r-	r	r	r	re
66	67	68	69	70
sa	se	si	so	su
u-	u	u	u	ue
76	77	78	79	80
va	ve	vi	vo	vu
p-	p	p	p	pe
86	87	88	89	90
ya	ye	yi	yo	yu
v-	v	v	v	ve
96	97	98	99	00
cha	che	chi	cho	chu
g-	g	g	g	ge
11	12	13	14	15
fra	fre	fri	fro	fru
z-	z	z	z	ze
21	22	23	24	25
pla	plic	piz	pilo	pliu
h-	h	h	h	he
31	32	33	34	35
tra	tre	tri	tro	tru
h-	h	h	h	he
41	42	43	44	45

Пример шифрования удвоенных букв открытого текста (нижняя строка рукописного текста):

Duplices
seran todas qualesquier letras del
alfabeto de la cifra, que tuvieran
dos puntos en cima ó de bajo, como:
ñ vale por ñ, y ð por dos ff y así de las otras.

NULLAS
seran todas las letras ó caracteres que tuvieran un punto solo
en cima ó de bajo ó de qualquier forma que sean, y á lo menos se
pongan en cada renglon quatro.

Кодовая книга.

A				
Alemania	ab	adonde		it
Alemanes	eb	aun		ot
Argel	ib		B	
Africa	ob	Beatitud		ut
Alexandria	ub	Bohemia		ba
armas	al	baxa		be
armada	el	Bugia		bi
artilleria	il	Berberia		bo
arcabuzes	ol	Barcelona		bu
amigo	ul	Bonifacio		bla
amistad	am	batalla		ble
año	em	bateria		bli
aviso	im	bastimentos		blo
amotin	om	bastante		blu
aca	um		C	
aquí	ar			
alla	er	Cartagena		bra
alli	ir	Cerdeña		bre
ay	or	Corcega		bri
assi	ur	Calabria		bro
ante	at	Constantinopla		bru
allende	et	Corfu		bal

Candía	bel	Dorgui	dri
ciudad	bil	daño	dro
castillo	bol	designo	dru
campo	bul	despach	dal
campana	ca	dinero	del
Christiandad	ce	diligencia	dil
carestía	ci	donde	dol
cardenal	co	despues	dul
concilio	cu	desde	dar
collegio	cla	de manera	der
consejo	cle		
capitan general	cli	E	
capitan	clo	emperador	dir
coronel	clu	España	dor
cavallos	cra	Espanoles	dur
cavalleria	cre	Escocia	das
carta	cri	embaxador	des
correo	cro	embaxada	dis
compania	cru	exercito	dos
casa	cam	effecto	dus
capítul	cem	empresa	fa
correspon	cim	enemigo	fe
como	com	estado	fi
con	cum	espia	fo
		escri	fu
D		esto	fla
Díos	car	ello	fle
Duque de Saboya	cer	esta	fli
Duque Octavio	cir	ella	flo
Duque d'Alva	cor	esendo	flu
Duque de Cleves	cur		
Duque de Florencia	da	F	
Duque de Ferrara	de	Flandes	fia
Duque de Mantua	di	Francia	fie
Duque de Urbino	do	Franceses	fii
Duque	du	Florencia	fio
Duquesa	dra	Florentin	fiu
Ducado	dre	Ferrara	fal

ocasion	nos	quan	quil
ocurre	nus	quanto	quol
orden	pa	quantidad	quul
officio	pe	qual	quam
obediencia	pi	qualidad	quem
obede	po	question	quim
ocupacion	pu	quasi	quom
occup	pla		
		R	
P		Roma	quum
Papa	ple	rey	quar
principe	pli	reyna	quer
Principe de España	plo	reyno	quir
Principe Andrea Doria	plu	Rey de España	quor
potentado	pra	Rey de Inglaterra	quur
Portugal	pre	Rey de Romanos	quas
Portugueses	pri	Rey de Francia	ques
Piamonte	pro	Rey de Portugal	quis
Pomblin	pru	Rey de Bohemia	quos
Pulla	pal	Reyna de Escocia	quus
puerto	pel	Rey de Polonia	ra
Puerto Hercules	pil	Rey de Dinamarca	re
provincia	pol	Rey de Tunez	ri
principal	pul	Rey de Argel	ro
persona	pam	Ragusa	ru
polvora	pem	Reverendissimo	ral
pilota	pim	religion	rel
pacific	pom	república	ril
paz	pun	razón	rol
provision	qua	remedio	rul
prone	que	resolucion	ram
para	qui	resolvi	rem
paraque	quo	respuesta	rim
porque	qua		
pero	qual	S	
		Santopadre	rom
Q		Su Santidad	rum
quando	quel	Su Beatitud	ras

Su Magestad	res	V	
Su Alteza	ris	Vuestra Magestad	vol
Su Excellencia	ros	Vuestra Alteza	vul
Sede Apostolica	rus	Vuestra Excellencia	vam
Serenisimo	rat	Vuestra Señoria	vem
Serenisima	ret	Vuestra merced	vim
Saboya	rit	Virey de Napoles	vom
Suiça	rot	Virey de Sicilia	vum
Suiços	rut	Virey de Cataluña	vaz
Sicilia	ta	Virey de Navarra	vez
secta	te	Virey de Cerdeña	viz
secretario	ti	Virey de Mallorca	voz
secret	to	Virey de Menorca	vuz
señor	tu	Venecia	vas
señoria	tra	Venecianos	ves
satisfaction	tre	Ungria	vis
sazón	tri	Ungaros	vos
socorro	tro	Villafranca	vus
suma	tru	villa	xa
successo	tam	verdad	xe
servicio	tem	virtud	xi
siempre	tim	vitoria	xo
		virtualla	xu
T		Vizcocho	xal
Toscana	tom	vandera	xel
Trento	tum	vela	xil
Turquia	tas	vuestro	xol
Turco	tes	vuestra	xul
Tunez	tis	union	xam
tierra	tos	unido	xem
tregua	tus	unida	xom
trigo	va		
trato	ve	Z	
tractado	vi	Zante	xim
todo	vo	zabra	xon
toda	vu		
tanto	val		
tanta	vel		
tiempo	vil		

Слова, входившие в кодовую книгу, шифровались, соответствующими обозначениями, остальные с помощью комбинаций из буквенных замен, замен биграмм и триграмм. Особые

шифры были гораздо более простыми, чем общий, отличия заключались в объеме кодовой книги. Для общего шифра применялись книги, содержавшие более 1000 слов, для особых 100-200, иногда в особых шифрах были совсем небольшие коды, обычно набор имен и географических названий, часто встречавшихся в переписке. Испанцы считали свои шифры принципиально недешифруемыми, они глубоко ошибались.

Теперь вернемся к криптографической деятельности Ватикана. Спустя 10 лет (1567 год) после дешифрования номенклатора Филиппа II отличился викарий собора Святого Петра в Риме, который менее чем за шесть часов сумел прочесть криптограмму, написанную «на большом листе бумаги, на турецком языке, на котором викарий не знал и четырех слов» [Кан, 2004, с. 128].

Весьма значительный вклад в развитие папской криптографии внесла семья Ардженти. Первым на службу Папе поступил Джованни Батиста Ардженти, он стал личным секретарем ведущего на тот момент папского криптографа А. Элио, который и обучил его криптографии. Д.Б. Ардженти долго мечтал стать папским секретарем по шифрам, но значительный период времени этот пост занимали другие люди, нередко использовавшие для назначения на этот престижный пост, родственные и личные связи. Наконец, когда Папой стал Сикст V, ранее покровительствовавший Ардженти, его мечта исполнилась, в это время ему было далеко за 50. Следующему Папе Григорию XIV взошедшему на престол в 1590 году пришлось долго уговаривать Д.Б. Ардженти остаться на своем посту, так как по состоянию здоровья не ему было трудно сопровождать Папу в зарубежных поездках. Предчувствуя скорую смерть, Джованни Батиста поспешил обучить криптографии своего племянника Маттео. 24 апреля 1591 года Джованни Батиста Ардженти скончался.

Маттео Ардженти в возрасте 30 лет унаследовал должность своего дяди. Он занимал этот пост при пяти Папах, надеясь продолжить семейную традицию Маттео обучил криптографии своего младшего брата Марчелло, работавшего секретарем у одного из кардиналов. Но неожиданно 15 июня 1605 года М Ардженти был уволен со своего поста в результате интриг внутри папской курии. Однако папа, признав Ардженти невиновным, назначил ему солидную пенсию в 100 дукатов [Бабаш, 2002], [Kahn, 1967].

Выйдя в отставку, Маттео решил обобщить дядины и свои достижения в области криптографии. Результатом стало пособие,

вышедшее в начале XVII века. Оно представляло собой книгу объемом 135 страниц, изданную в переплете из телячьей кожи. Ардженти первыми предложили использовать некоторое слово-лозунг в качестве ключа для смешанного алфавита. Началом смешанного алфавита служило ключевое слово (как правило, без повторяющихся букв), за которым следовали остальные буквы в их естественном порядке. Например, ключевое слово PIETRO дает такой смешанный латинский алфавит:

PIETROABCDGHIJKLMNOPQSUUVWXYZ

Такие смешанные алфавиты часто использовались в качестве алфавитов шифртекста в шифрах простой, разнзначной (кстати сама идея разнзначной замены принадлежит Ардженти) и многоалфавитной замены. Например:

ABCDEFGHIJKLMNPOQRSTUVWXYZ

PIETROABCDGHIJKLMNOPQSUUVWXYZ

Очевидно, что такой вариант не самый удачный, так как последние 6 букв переходят сами в себя.

Ардженти, безусловно, знали о частотном анализе и успехах папских криптоаналитиков, эти знания использовались при составлении шифров. С целью усложнения шифра простой замены Ардженти вводили пустышки, которые добавлялись в зашифрованное сообщение, использовали шифробозначения разной значности, для некоторых частых сочетаний букв текста вводились отдельные шифробозначения (элемент номенклатора), частым буквам придавалось несколько шифробозначений (пропорциональная или по другому омофонная замена). Так, например, зная, что для большинства романских языков после буквы Q всегда следует буква U, Ардженти вводили для этой биграммы специальное шифробозначение, вместо удвоенных букв писалась и зашифроввалась одна, так например итальянское слово SIGILLO (печать, штампель) писалось как SIGILO и т.п.

Ардженти представляли и способ дешифрования пропорциональной замены, заключающейся в поиске повторений. Так например, если криптоаналитик видит в шифртексте, зашифрованном пропорциональной замены такие фрагменты:

13 24 81 66 41

12 24 49 66 41

Очевидно, что 81 и 49 обозначают одну и ту же букву, если текст достаточно большой длины, то можно определить значительное

количество таких эквивалентов и тогда дешифрование подобной криптограммы сводится к криптоанализу шифра простой замены. Чтобы избежать подобного Ардженти настоятельно рекомендовали насыщать текст пустышками, считая, что в каждой строке их должно быть от 3 до 7. При этом в их рекомендациях категорически запрещалось разбивать шифртекст на слова, соблюдать пунктуацию, а также смешивать открытый и зашифрованный тексты (не смотря на это на протяжении многих веков в разных странах для ускорения процессов шифрования/расшифрования шифровался не весь текст, а отдельные наиболее «секретные» фразы и слова, очевидно, что прочитав открытые фрагменты текста (клер), может сделать весьма далеко идущие выводы относительно содержания зашифрованного). НЕ ЧИТАЕТСЯ Прошу оставить

Для обеспечения стойкости смешивались одно и многозначные шифробозначения, при этом существовало четкое правило их разделения при расшифровании. Вводились так называемые полифоны когда одному шифробозначению соответствовали разные знаки открытого текста, разумеется, подбирались они таким образом, чтобы при расшифровании из контекста однозначно определялось бы какой конкретно знак получается в данном случае. Криптоаналитиков противника подобные вещи должны были привести в тупик. Позже подобные идеи получили широкое распространение.

Приведем пример шифра Маттео Ардженти для итальянского языка (см. рис. 3.9).

A	B	C	D	E	F	G	H	I	L	M	N	O
1	86	02	20	62 82	22	06	60	3	24	26	84	9

P	Q	R	S	T	U	Z	ET	CON	NON	CHE	Ø
66	68	28	42	80	04 40	88	08	64	00	44	5 7

Рис. 3.9. Один из шифров Маттео Ардженти

Слово ARGENTI может быть зашифровано многими способами, например, так:

5128068285480377 (5 – пустышка, 1 – А, 28 – R, 06 – G, 82 – E, 84 (через пустышку 5) – N, 80 – T, 3 – I, 77 – две пустышки).

или же так:

172850675628455803 (соответствие шифробозначений знакам открытого текста читателю предлагается восстановить самому).

Наибольшим достижением Ардженти считается разработанный им буквенный код — один из шифров замены, в котором буквы, слоги, слова и целые фразы заменялись группами букв. Необходимым количеством словарных величин в коде в то время считалось 1200.

Ардженти старались оптимизировать шифры для разных языков. В итальянском языке крайне редки буквы J, K, W, X и Y. Поэтому используется либо 21-буквенный алфавит, либо 22-буквенный (без J, K, W, Y), соответственно шифробозначения для этих букв не нужны (в вышеприведенном примере, как видим, отсутствует еще и V). При необходимости можно произвести вполне прозрачную замену, например, J на I, X на CS, V на B и т.п.

Во французском языке практически не используются буквы K и W. Эти буквы встречаются только в некоторых словах иностранного происхождения, например tramway, kilo, wagon, weekend. Поэтому часто используют 24-буквенный алфавит (без K и W).

В немецком языке исключительно редки буквы Q, X и Y. Зато без K и W уже обойтись сложно. Буква Q появляется в виде начальной буквы лишь в некоторых малоупотребительных словах, большей частью иностранного происхождения, например quelle, quarta, quitting. Помимо латинских букв немецкий язык использует еще три буквы: ö, ä, ё, которые часто заменяют эквивалентами OE, AE и UE соответственно, например, в словах kaempfen, moebel, glueck. Буквы X и Y практически не используются, поэтому часто обходятся лишь 24 буквами (без X и Y).

Испанский язык содержит некоторые особые буквы: CH, LL, N, которые можно заменить эквивалентами: C,H; L,L; N. Как и во французском языке, буквы K и W исключительно редки, и поэтому часто используется 24-буквенный алфавит [Алферов, 2005].

Все это соответственно учитывалось при составлении шифров на данных языках.

Проводил Маттео Ардженти и анализ возможностей криптоаналитиков различных стран, в которых приходилось работать папским послам. В частности он отмечал в одной записке, что для

папских шифров имеется мало опасностей в Польше, Швеции и Швейцарии, а немцы настолько малообразованны в области криптографии, что предпочитают сжигать перехваченные криптограммы, вместо того чтобы попытаться прочесть их. Ардженти рекомендовал папским представителям применять в этих странах только простые криптосистемы. Что и происходило на практике.

Гораздо более сложные шифры рекомендовалось использовать папским представителям в Англии, Венеции, Флоренции и Франции. М. Ардженти был восхищен уровнем развития криптографии в этих государствах [Алферов, 2005], [Бабаш, 2002], [Жельников, 1996], [Kahn, 1967].

Об успехах венецианских и флорентийских криптоаналитиков мы уже рассказали, о том, что происходило в Англии и Франции далее. А пока же рассмотрим деятельность одного из выдающихся криптографов своего времени итальянца Джованни Батиста Порты (в некоторых источниках де ла Порты).

Воскресить смешанные алфавиты, которые применял Альберти, и объединить идеи Альберти с идеями Тритемия и Белазо в современную концепцию многоалфавитной замены выпало на долю итальянца Джованни де ла Порты. Ему было 28 лет, когда он в 1563 г. опубликовал книгу «О тайной переписке». По сути, эта книга являлась учебником по криптографии, содержащим криптографические познания того времени.

Порта предложил использовать квадратную таблицу с периодически сдвигаемым смешанным алфавитом и паролем. Он советовал выбирать длинный ключ. Впервые им был предложен шифр простой биграммной замены, в котором пары букв представлялись одним специальным графическим символом. Они заполняли квадратную таблицу размеров 20×20, строки и столбцы которой занумерованы буквами алфавита:

A B C D E F G H I L M N O P Q R S T U Z

Например, биграмма ЕА заменялась символом



LF — символом и т. д. В своей книге Порта ввел многоалфавитный шифр, в соответствии с таблицей на Рис.3.10

A	a	b	c	d	e	f	g	h	i	k	l	m
B	n	o	p	q	r	s	t	u	x	y	z	w
C	a	b	c	d	e	f	g	h	i	k	l	m
D	o	p	q	r	s	t	u	x	y	z	w	n
E	a	b	c	d	e	f	g	h	i	k	l	m
F	p	q	r	s	t	u	x	y	z	w	n	o
G	a	b	c	d	e	f	g	h	i	k	l	m
H	q	r	s	t	u	x	y	z	w	n	o	p
I	a	b	c	d	e	f	g	h	i	k	l	m
K	r	s	t	u	x	y	z	w	n	o	p	q
L	a	b	c	d	e	f	g	h	i	k	l	m
M	s	t	u	x	y	z	w	n	o	p	q	r
N	a	b	c	d	e	f	g	h	i	k	l	m
O	t	u	x	y	z	w	n	o	p	q	r	s
P	a	b	c	d	e	f	g	h	i	k	l	m
Q	u	x	y	z	w	n	o	p	q	r	s	t
R	a	b	c	d	e	f	g	h	i	k	l	m
S	x	y	z	w	n	o	p	q	r	s	t	u
T	a	b	c	d	e	f	g	h	i	k	l	m
U	y	z	w	n	o	p	q	r	s	t	u	x
X	a	b	c	d	e	f	g	h	i	k	l	m
Y	z	w	n	o	p	q	r	s	t	u	x	y
Z	a	b	c	d	e	f	g	h	i	k	l	m
W	w	n	o	p	q	r	s	t	u	x	y	z

Рис. 3.10 Таблица Порты

Шифрование осуществляется при помощи лозунга, который пишется над открытым текстом. Буква лозунга определяет алфавит (заглавные буквы первого столбца), расположенная под ней буква открытого текста ищется в верхнем или нижнем полуалфавите и заменяется соответствующей ей буквой второго полуалфавита. Например, фраза, начинающаяся словами HUNC CAVETO VIRUM...,

будет зашифрована при помощи лозунга DE LA PORTA в XFHP YTMOGA FQEAS.

Хотя в те времена криптография была уделом государственных служб, использовали шифры и многие ученые. Так что великий итальянский ученый и художник эпохи Возрождения Леонардо да Винчи (1452-1519) владел криптографией и пользовался ею, в частности, в своих рукописях. В частности он использовал запись слов задом наперед при помощи зеркала. Известны и более сложные шифры, которые использовал да Винчи, кстати, некоторые его записи до сих пор не дешифрованы. [Носов, 2003].

Известны примеры использования шифров учеными-астрономами для утверждения приоритета своих открытий. Астрономы использовали так называемые анаграммы — слово или словосочетание, образованное перестановкой букв другого слова или словосочетания. Например, выдающийся итальянский ученый Галилео Галилей (1564-1642) свое открытие колец Сатурна в 1610 году зашифровал с помощью такой анаграммы:

SMAISMRMIELMEPOETALEUMIBUVNENUGTTAVIRAS.

Число вариантов различных перестановок крайне велико, оно определяется числом из 35 цифр, поэтому вероятность того, что подобное сообщение будет прочитано научной общественностью верно, ничтожна мала. При правильном расшифровании получался такой текст:

Altissimum planetam tergeminum observavi (Высочайшую планету тройную наблюдал). “Высочайшую” значит “самую далекую”.

Зрительная труба ученого была настолько несовершенна, что не давала достаточно четкого изображения. Это не позволило Галилею рассмотреть кольцо Сатурна. Но по бокам от диска планеты он увидел неясные объекты, неподдающиеся четкому описанию. Он посчитал их спутниками Сатурна, по аналогии с уже открытыми им спутниками Юпитера. Однако Галилей не был авантюристом. Расплывчатый вид наблюдавшихся им объектов не позволял ему утверждать об открытии наверняка. Чтобы закрепить за собой первенство и в то же время не попасть в неловкое положение ошибившегося, Галилей прибегнул к шифрованию информации об открытии, правильность и достоверность которого вызывали сомнения. Если открытие подтверждалось дальнейшими

исследованиями, сообщение об открытии расшифровывалось, и весь мир видел, кто же был первый.

Но подобный способ оповещения мира об открытиях приводил к курьезам. Анаграмма Галилея, состоявшая из 37 латинских букв, очень заинтересовала немецкого астронома Иоганна Кеплера (1571-1630). Выбросив две буквы, он составил из оставшихся фразу:

Salve, umbistintum gemaum martia proles (Привет вам, близнецы, Марса порождение). Кеплер решил, что Галилей открыл спутники Марса, о возможности существования которых, Кеплер сам высказывал предположения. Спутники Марса действительно открыты два с половиной века спустя.

Что касается колец Сатурна, то их спустя почти полвека открыл голландский ученый Христиан Гюйгенс (Huygens) (1629-1695) и тоже зашифровал свою догадку анаграммой из латинских букв.

AAAAAAA, CCCCC, D, EEEEE, G, H, IIII, LLLL, MM, NNNNNNNN, OOOO, PP, Q, S, TTTT, UUUUU.

Если переставить их в нужном порядке, то получится фраза:

Annulo cingitur, tenui, plano, nusquam cohaerente, ad eclipticam inclinato, что означало: “кольцом окружен тонким, плоским, нигде не прикасающимся, к эклиптике наклоненным”. Это произошло в 1658-м году. Чтобы расшифровать эту криптограмму, нужно было бы сделать примерно 1060 перестановок.

В год опубликования анаграммы Гюйгенс открывает также и первый самый большой спутник Сатурна – Титан, определив, что время его обращения вокруг планеты равно 15 суткам, и составил по этому поводу анаграмму, которую послал своим коллегам. Один из них был выдающийся английский математик и главный на тот момент дешифровальщик Британии Джон Валлис (1616-1703) (с ним мы еще встретимся на страницах данной книги). Он расшифровал анаграмму Гюйгенса и ответил ему собственной анаграммой.

Напомним, что Гюйгенс был универсальным ученым. Он занимался астрономией, физикой, математикой. Установил законы колебаний физического маятника, заложил основы теории удара, создал волновую теорию света, усовершенствовал телескоп, сконструировал окуляр названный его именем. Гюйгенс является автором одного из первых трудов по теории вероятности. Вероятностные методы с давних времен активно используются в криптоанализе [Алферов, 2005], [Бабаш, 2002], [Бутырский, 2008], [Kahn, 1967].

Первым французским криптоаналитиком был Филибер Бабу, занимавший пост первого государственного секретаря при короле Франциске I (годы правления 1494-1547) вскрыл шифры ряда германских государств, а также сумел дешифровать испанскую и итальянскую шифрпереписку. При этом следует отметить, что Бабу работал «не имея алфавита, часто дешифровывал многие перехваченные депеши на испанском, итальянском и немецком языках, хотя он не знал ни одного из этих языков или знал очень плохо, причем он упорно работал над сообщением дни и ночи напролет в течение трех недель, прежде чем разгадывал одно слово. После того как брешь была проделана, остальное происходило очень быстро и напоминало разрушение стен» [Кан, 2004, с. 129]. Как утверждает американский историк Д. Кан «дешифровать криптограмму на «неизвестном» языке можно при условии, что «незнание» означает только то, что человек не понимает смысла слов, как это имеет место в данном случае. Чтобы добиться вскрытия, у криптоаналитика должно быть общее представление об образовании и структуре слов языка. Очевидно, что чем лучше он знает язык, тем легче ему дешифровать криптограммы, открытый текст которых написан на этом языке. Если криптоаналитик никогда не виде ни одного предложения на данном языке, то чтение криптограммы почти невозможно, хотя чередование гласных и согласных, общее для всех языков, все же может подсказать некоторые пути к решению задачи» [Kahn, 1967]. При этом отметим, что в то время как Бабу не покладая рук работал на короля и Францию, король с удовольствием принимал у себя любовницу – очаровательную жену Бабу. Бабу получал много милостей от короля, но сложно сказать, за что он их удостоился – за успехи в дешифровании или за позволение наставлять рога [Бабаш, 2002, с. 103], [Кан, 2004, с. 129].

Существенные успех в области криптоанализа во второй половине XVI века были достигнуты в Нидерландах, при этом следует отметить, что криптографическая деятельность здесь началась еще до формального образования голландского государства. Первым известным голландским криптографом был Филипп ван Марникс, лорд Сент-Альдегонде (Philips van Marnix, Lord of Sint-Aldegonde, 1540-1598): политический деятель, дипломат, публицист времен буржуазной революции, автор современного национального гимна Нидерландов, соратник Вильгельма Оранского, руководившего борьбой голландских колоний за независимость от Испании. Ван

Марникс был одним из организаторов в 1565 году антииспанского "Союза дворян". С конца 1577 года член государственного совета, в 1583-85 годах бургомистр Антверпена. Сдача Антверпена испанцам (в 1585 году) навлекла на Марникса подозрения в измене, и он был отстранён от государственных дел. Его книга "Улей святой римской церкви" (1569) - острая пародия на труды католических священников. Написанная около 1568 года в честь принца Оранского и изданная анонимно песня "Wilhelmus van Nassouwe" стала боевым гимном нидерландских гёзов (голландских партизан) с мелодией, основанной на песне французских солдат. Полный текст содержал 15 куплетов, а много позднее более торжественная и медленная музыка в стиле церковного пения была написана известным голландским композитором Адрианом Валериусом (1575-1625). Интерес ван Марникса к криптографии отражается и в этом гимне, написанном в форме акrostиха, где первые буквы 15-ти куплетов образуют имя "W-I-L-L-E-M V-A-N N-A-S-S-O-V", или в английской переводной версии акrostиха "WILLIAM OF NASSAU" - имя принца Оранского. Этот гимн является старейшим в мире. После 1932 года он стал официальным национальным гимном Нидерландов, в настоящее время исполняется только первый и шестой из куплетов. Один из современников охарактеризовал ван Марникса как «благородного, умного, доброго, проникательного и красноречивого человека, обладающего большим опытом, очень острым чутьем и незаурядным умением обращаться с людьми. Он знает греческий, древнееврейский и латинский языки; очень легко понимает и пишет – по-испански, итальянски, немецки, французски, фламандски, английски, шотландски и на других языках – лучше, чем любой другой человек в нашей стране» [Kahn, 1967]. Благодаря своим способностям ван Марникс добился существенных успехов в дешифровании испанской шифрпереписки. Прежде чем рассказать о них, несколько слов о политической обстановке, сложившейся в Западной Европе в конце XVI века.

Против Испании, престол которой занимал король Филипп II, сложилась коалиция из Англии, Франции и восставших голландских провинций Испании. При этом Англия враждовала с Францией, но руководители этих стран вынуждены были пойти на союз против общего врага. На стороне Испании сражалась «Священная лига», возглавляемая герцогом Майенским (это были французы-католики,

недовольные тем, что на французском престоле находится бывший гугенот – король Генрих IV).

В 1577 году голландскими провинциями Испании управлял губернатор дон Хуан Австрийский, единокровный брат короля Филиппа. Честолюбивые замыслы дона Хуана простирались далеко за рамки управляемой им территории. Он мечтал о разгроме протестантской Англии – главного врага католической Испании. В его планы входила высадка испанских войск на территории Англии, разгром ее вооруженных сил и свержение королевы Елизаветы. Далее он хотел жениться на претендентке на английский престол католичке королеве Шотландии Марии Стюарт и получить английскую корону. Таким образом, дон Хуан хотел вернуть Англию под влияние «его католического величества», как тогда называли Филиппа II. Все эти планы он изложил в письмах королю и его советникам. Филипп согласился с этими планами. Правда, разрешил их осуществление лишь после того, как дон Хуан восстановит мир и спокойствие в Голландии.

Англичанам через своих агентов на Европейском континенте удалось узнать о том, что испанцы замышляют что-то недоброе, но конкретной информации не было. Помощь пришла от союзников. В конце июня 1577 года в Гаскони во Франции агентами Генриха IV были перехвачены несколько зашифрованных писем дона Хуана. Французы предположили, что содержание писем может касаться событий, происходивших в Нидерландах, поэтому их отправили туда. Письма попали к ван Марниксу, который через месяц вскрыл испанский шифр, которым они были зашифрованы. Особенность этого шифра заключалась в том, что каждая гласная открытого текста помимо буквенной и цифровой замен имела еще одно обозначение в виде завитушки. Если в открытом тексте согласная предшествовала гласной, то эту завитушку писали вместе с зашифрованным знаком согласной, так что получался комбинированный символ, представлявший обе эти буквы.

Из содержащийся в письмах информации голландцы узнали о планах дона Хуана. Вильгельм Оранский 11 июля сообщил содержание писем дешифрованным ван Марниксом, Даниэлю Роджерсу, одному из агентов главы английской разведки Френсиса Уолсингема. Роджерс так написал об этом в своем докладе Уолсингему:

Рис. 3.11. Номенклатор дона Хуана дешифрованный Ф. ван Марниксом. [Kahn, 1967]. Нет ссылки в тексте на этот рисунок стр 113

Таким образом, англичане получили информацию о возможных действиях испанцев против их страны и приняли соответствующие меры по укреплению обороноспособности, активизации разведки и т.д. В том числе были приняты меры к созданию собственной дешифровальной службы. С этой целью в Париж для обучения к знаменитому французскому криптоаналитику Франсуа Виету (подробнее о котором будет рассказано ниже) был направлен талантливый молодой человек, который уже имел некоторый практический опыт дешифровальной работы. Это был Томас Фелиппес, первый знаменитый криптоаналитик Англии.

Хотя в 1577 году вторжение испанцев не произошло, так как дону Хуану не удалось победить восставших голландцев. Однако принятые меры принесли результаты позже, когда в 1588 году Филипп II, направил к берегам Англии «Непобедимую армаду». Разгрому испанцев способствовала и успешная работа английских дешифровальщиков.

Кроме намерений испанцев из писем, дешифрованных ван Марниксом, англичане получили еще одну важную информацию, о том, что королева Шотландии Мария Стюарт может быть связана с испанцами. Долгое время между Марией и английской королевой Елизаветой шла непримиримая борьба за английский престол. Этот исторический конфликт послужил основой для создания трагедий и пьес (см., например, произведения У. Шекспира) и стал классическим в литературе. В Шотландии сложились две противостоящие партии сторонников и противников Марии. Вооруженный конфликт сложился не в пользу Марии. Она была вынуждена бежать в Англию и сдаться на милость Елизаветы. Елизавета приняла Марию как «почетную узницу». Узнице предоставили покои в Виндзорском замке, но находилась она под стражей. В то же время Елизавета, естественно, была заинтересована в физическом устранении своей соперницы, тем более, потому что королева Шотландии имела в Англии многочисленных сторонников. Но решение о казни лица королевской крови мог принять только высший суд Англии — «Звездная палата». Для такого вердикта необходимо было предоставить неопровержимое свидетельство участия Марии в

заговоре против Елизаветы. Полученная информация дала возможность организации английскими спецслужбами операции по компрометации Марии. Важную роль в ней сыграл криптоаналитик Т. Фелиппес. Подробнее об этой операции можно прочитать, в частности в книге [Гольев, 2008]. Здесь же заметим, что в 8 часов утра 8 февраля 1587 года Мария Стюарт была казнена путем отсечения головы. Так успех голландского криптографа стал началом пути на плаху королевы Шотландии.

Пока дешифровальная служба Англии находилась в стадии становления, Уолсингем продолжал пользоваться услугами ван Марникса по дешифрованию интересующей англичан переписки, это сотрудничество продолжалось более 10 лет. Так 20 марта 1587 года он писал одному из своих агентов в Нидерландах: «Для службы ее величества очень важно, чтобы это письмо португальского посла было быстро дешифровано. Поэтому я прошу незамедлительно договориться ради этого дела с Сент-Алдегонде. Шифр настолько прост, что не потребует больших усилий» [Kahn, 1967]. Однако на этот раз Уолсингема ждало некоторое разочарование, его агент ответил: «Сент-Алдегонде сегодня уехал в Вормс... Его отдыха перед отъездом не хватило на то, чтобы дешифровать те письма, которые вы прислали мне в последний раз, но зато он передал мне другое прочитанное письмо. Я прилагаю его при сем...» [Kahn, 1967]. В дешифрованном письме португальский посол жаловался на то, что королева Елизавета отказала ему в аудиенции, сказавшись больной.

Ван Марникс оказывал криптографическую помощь и другому союзнику Нидерландов – Франции. Над дешифрованием испанских шифров ван Марникс работал вместе с упомянутом выше Франсуа Виетом. В 1589-1590 годах Виет и ван Марникс примерно за год работы сумели вскрыть общий шифр Филиппа II, который до этого времени считали неуязвимым не только в Испании, но и в Ватикане (как мы уже знаем лишь до 1557 года, но шифр продолжал действовать) – одним из крупнейших криптографических центров того времени. Два года французы и голландцы перехватывали и читали шифрованную переписку испанцев. Эта информация помогла нанести ряд поражений испанской армии.

С одним из дешифрованных ван Марниксом писем связана неудачная операция по дискредитации одного из испанских военачальников Хуана Морео. Шифрованное письмо испанцев, прочитанное Марниксом, было перехвачено агентами Генриха IV во

время осады Парижа. Отправителем письма был Морео, а его адресатом – король Филипп II.

Французский король лично передал эту испанскую криптограмму голландскому криптографу. Ван Марникс дешифровал ее и обнаружил, что в ней содержатся оскорбительные выпады против герцога Пармы, который в это время был испанским губернатором Нидерландов. В августе 1590 года Генрих велел ван Марниксу отправить герцогу Пармы как саму криптограмму Морео, так и ее открытый текст, надеясь тем самым испортить отношения между испанскими сановниками. Однако герцог посчитал ниже своего достоинства отвечать на клеветнические выпады военачальника и не предпринял никаких ожидавшихся Генрихом действий против Морео [Кан, 2004, с. 132].

Еще одним голландским государственным деятелем, который использовал криптографические методы защиты информации, был Гроций (Гуго де Гроот) (Grotius, Hugo de Groot) (1583-1645) голландский юрист, социолог, государственный деятель, один из основоположников теории естественного права и современной науки международного права. Он родился в городе Делфте и в детстве отличался удивительными способностями. В 15 лет Гуго поразил французский двор умом и эрудицией; король Генрих IV назвал его “голландским чудом”. В 16 лет Орлеанский университет удостоил Гроция степени доктора права и он занимал в Голландии ответственные посты до 1618 года, когда был осужден на пожизненное заключение. В 1621 году бежал во Францию, где написал несколько книг о христианской религии и праве. Еще в 1609 году Гроций издал работу «Свободное море», которая заложила основы современного морского права. Его теория международного права, изложенная в великом труде “О праве войны и мира” (1625) имела огромный успех. Так к 1775 году появилось 77 изданий этой работы на латыни, голландском, французском, немецком, английском и испанском языках. По свидетельству современников Гроций, являясь крупным государственным деятелем, проявлял большой интерес и познания в тайнописи. К сожалению подробностей криптографической деятельности Гроция авторам пока найти не удалось.

В XVII веке Нидерланды являлись одной из самых передовых европейских держав с развитыми промышленностью, торговлей и мореплаванием. Голландцы начали процесс колонизации ряда

территорий в Центральной Америке и Юго-восточной Азии. В это время Нидерланды участвовали в ряде войн и военных конфликтов с другими европейскими странами. Разумеется, активная дипломатическая и военная деятельность требовали обеспечения защиты информации. Голландцы использовали, традиционные для того времени номенклатуры и шифры многоалфавитной замены. Последние хотя и были изобретены еще в XV веке, широко применяться стали лишь во второй половине XIX века. Так же активно использовались жаргонные коды. В жаргонных кодах словам придается иной смысл, например на жаргоне многих разведок слово БОЛЕТЬ означает «арест» или «заключение под стражу»; БОЛЬНИЦА - тюрьма; ДОКТОР - контрразведка. Тогда сообщение «Майкл арестован контрразведкой. Ему грозит заключение в тюрьму», принимает следующий «невинный» вид: Майкл заболел. Вчера был доктор и посоветовал ему лечиться в больнице» [Гольев, 2008]. [Kahn, 1967], [Соболева, 2002].

Вместе с Ван Марниксом работал Франсуа Виет (1540-1603) великий французский математик, отец современной алгебры. Алгебра получает развитие у Ф. Виета, который установил связь коэффициентов алгебраических уравнений и корней (формула Виета). Он же начал использовать буквенные обозначения для коэффициентов уравнений, до него это использовалось лишь для корней.

В качестве курьеза можно указать, что Виет не признавал отрицательных чисел. Виет, служил секретарем по шифрам при французском короле Генрихе IV, был членом тайного совета, занимался адвокатской практикой.

Ф. Виет привлекался к дешифровальной работе при дворе Генриха IV и успешно дешифровал переписку испанского короля Филиппа II.

Из-за успехов Виета в криптоанализе, испанский король Филипп II жаловался Папе Римскому на применение французами черной магии и обвинял их в том, что они состоят в сношениях с дьяволом. Однако в папской курии давно знали о возможностях криптоанализа и только посмеялись над обвинениями испанского короля.

Примерно в то же время французский посол в Риме Блез Виженер, познакомившись с трудами по криптографии, пишет книгу «Трактат о шифрах» (1585 год), в которой он предлагает в качестве

ключа применять открытый или шифрованный текст и высказывает мысль о том, что «все вещи в мире представляют собой шифр. Вся природа является просто шифром и секретным письмом».

В книге Виженера «Трактат о шифрах» самоключ представлен следующим образом. В простейшем случае за основу бралась таблица Тритемия с добавленными к ней в качестве первой строки и первого столбца алфавитами в их естественном порядке. Позже такая таблица стала называться таблицей Виженера. Подчеркнем, что в общем случае таблица Виженера состоит из циклически сдвигаемых алфавитов, причем первая строка может быть произвольным смешанным алфавитом.

Первая строка служит алфавитом открытого текста, а первый столбец - алфавитом ключа (см. [рис.3.12](#)). Для зашифрования открытого сообщения Виженер предлагал в качестве ключевой последовательности использовать само сообщение с добавленной к нему в качестве первой буквы известной отправителю и получателю. Последовательности букв подписывались друг под другом.

	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W
A	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W
B	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A
C	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B
D	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C
E	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D
F	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E
G	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F
H	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G
I	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H
K	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I
L	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K
M	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L
N	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M
O	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N
P	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O
Q	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P
R	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q
S	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R
T	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S
U	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T
X	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U
Y	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X
Z	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y
W	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z

Рис. 3.12 Таблица Виженера **Нет ссылки в тексте на этот рис стр 118**

При этом пара букв, стоящих друг под другом, указывала, соответственно, номера строк и столбцов таблицы, на пересечении которых находится знак шифрованного текста. Самоключ Виженера был незаслуженно забыт на долгое время, а под шифром Виженера до сих пор понимают самый простой вариант с коротким ключевым словом и с таблицей, состоящей из обычных алфавитов.

Криптография в эпоху «черных кабинетов»

XVII, XVIII и первая половина XIX веков вошли в историю криптографии как эра «чёрных кабинетов» - специальных государственных органов по перехвату и дешифрованию переписки. В штат «чёрных кабинетов» входили криптографы-дешифровальщики,

агенты по перехвату почты, специалисты по вскрытию пакетов, писцы-копировальщики, переводчики, граверы, специализировавшиеся на подделке печатей, химики, их наличие было необходимо из-за активного использования стеганографических методов защиты информации, так называемых невидимых чернил, специалисты по имитации почерков и так далее. Таким образом, чёрные кабинеты состояли из высококвалифицированных специалистов в различных областях деятельности.

Начнем рассказ об их деятельности с одного интересного эпизода. Город Реальмон был осажден. Армия французского короля под командованием принца Конде окружила его на рассвете 19 апреля 1628 года. Однако гугеноты, укрывшиеся за зубчатыми стенами этого небольшого города на юге Франции, оказывали упорное сопротивление. Они с презрением отвергали все требования о капитуляции, заявляя, что скорее умрут, чем сдадутся.

Вскоре королевские солдаты захватили городского жителя, который пытался доставить зашифрованное сообщение войскам гугенотов за пределами Реальмона. Никто в окружении принца не сумел его прочесть. Только через неделю выяснилось, что перехваченное сообщение гугенотов может дешифровать юный отпрыск влиятельной семьи в городе Альби в десяти милях от Реальмона. Этот молодой человек, по слухам, интересовался шифрами.

Криптограмма была отвезена в Альби. Молодой человек прочитал ее сразу же. Выяснилось, что защитники Реальмона отчаянно нуждались в боеприпасах и что, не получив их, они будут вынуждены в скором времени капитулировать. Это была важная новость, потому что город по-прежнему отважно сопротивлялся, не показывая никаких признаков грядущей капитуляции. Осада города была продолжена, и 30 апреля 1628 года Реальмон сдался. Так было положено начало карьеры человека, которому суждено было стать первым профессиональным криптоаналитиком во Франции. Это был Антуан Россиньоля.

Когда весть о роли Россиньоля в покорении Реальмона дошла до хитрого и предприимчивого кардинала Франции Ришелье, он немедленно присоединил Россиньоля к своей свите. Как раз вовремя. Армия католиков под командованием Ришелье, окружившая главный бастион гугенотов – крепость Ла-Рошель, перехватила несколько зашифрованных писем. Их легко прочитал молодой дешифровальщик

из Альби. Его высокопреосвященству было доложено, что голодающие горожане с нетерпением ожидают помощи, которую англичане обещали прислать морем. Когда английский флот с продовольствием прибыл, он был настолько напуган превосходившими его по силе французскими кораблями, охранявшими подходы к Ла-Рошели, что даже не предпринял попытки пробиться к осажденным силой. Через месяц город капитулировал. Так был заложен фундамент великой традиции во французском криптоанализе.

Очень скоро Россиньолю перешел на королевскую службу. К 1630 году его работа принесла ему капитал, достаточный для того, чтобы выстроить себе эlegantный особняк с очаровательным садом. Здесь для встреч с молодым криптоаналитиком неоднократно останавливался сам король Людовик XIII, когда возвращался в Париж из загородной резиденции.

Россиньолю необычайно плодотворно служил на поприще криптоанализа как при дворе этого монарха, так и в свите Людовика XIV. Например, взятие крепости Эден королевской армией было ускорено благодаря тому, что Россиньолю прочитал зашифрованную просьбу ее защитников о помощи, а после этого тем же шифром составил ответ, в котором жители города извещались о тщетности их надежд. Он тогда не рассказывал о том, сколько других городов вынудил сложить оружие и сколько предательств раскрыл среди высшей знати. Из-за этой скрытности некоторые придворные утверждали, что на самом деле Россиньолю не вскрыл ни одного шифра и что кардинал распространяет слухи о его способностях с целью отбить охоту у потенциальных заговорщиков. На смертном одре Людовик XIII охарактеризовал Россиньоля как человека, от которого зависит благополучие его подданных. Неудивительно, что через два года, 18 февраля 1645 года, преемник Ришелье кардинал Мазарини назначил Россиньоля государственным советником. Как и Ришелье, Мазарини пересылал ему перехваченные шифрсообщения. Например, в 1656 года он направил зашифрованное письмо кардинала Реца с указанием Россиньолю прочесть его. При Людовике XIV Россиньолю часто работал в комнате, непосредственно прилегающей к кабинету короля в Версальском дворце. Отсюда шел поток дешифрованных сообщений, которые помогали королю определять политику Франции.

Одним из лучших друзей Россиньоля был поэт Буаробер, инициатор идеи создания Французской академии. Когда Буаробер попал в немилость при дворе, он пожаловался на свалившееся на него несчастье в стихотворении, адресованном своему влиятельному другу - криптоаналитику. Россиньоля показал это стихотворение Мазарини, который во время следующей аудиенции во всеуслышание похвалил Буаробера. Позже из чувства благодарности Буаробер написал 66 - строчное стихотворение, в котором воспел Россиньоля. Это первая стихотворная ода, посвященная криптоаналитику. Некоторые ее строки звучат так:

Под небом нет ничего,
Что может скрыться от твоих глаз;
Эти глаза Линса, которые, я думаю,
Проникают в наши самые сокровенные мысли.
Как изумительно твое искусство и ярко.
И как важна сила твоего мастерства!
Ибо с его помощью приобретаются провинции,
Раскрываются секреты всех королей,
И с малыми усилиями оно
Вынуждает сдаваться города и форты
...
Действительно, твое мастерство
выше моего понимания,
И я никогда не постигну
Твой секрет; но я сейчас могу сказать,
60 Что оно служит тебе очень хорошо,
Что ты заслуживаешь этого. Не опасайся,
Твое мастерство будет благоприятствовать тебе годами
И судьба будет тебе улыбаться,
Пока войны омрачают землю.

ОБЫЧНО УКАЗЫВАЮТ, ЧЕЙ ПЕРЕВОД уже трудно
восстановить оставим так

Примечание: Линс – аргонавт, взгляд которого был настолько пронзителен, что проникал в недра земли.

Работа Россиньоля сделала его видной фигурой при дворе Людовика XIV. Россиньоля стал первым человеком, прославившимся исключительно благодаря своим криптоаналитическим способностям. Шарль Перро, который больше известен как автор сказок, включил

краткую биографию Россиньоля в свою книгу «Знаменитые люди, появившиеся во Франции в нынешнем веке», наряду с жизнеописанием Ришелье. Возникла даже легенда о том, что успехи Россиньоля во вскрытии шифров были настолько непостижимы для современников, что приспособление, с помощью которого открывают замок, когда ключ утерян, до сих пор называют во Франции «россиньолем». Хотя сам факт такого употребления слова «россиньоля» имеет место, приписываемое ему происхождение ложно. В данном конкретном значении «россиньоля» появился в уголовном жаргоне почти за два века до рождения знаменитого криптоаналитика. Поскольку это слово также означает «соловей», не исключено, что взломщики приспособили его вместо слова «отмычка», поскольку шелканье и дребезжание воровского инструмента звучали для их ушей подобно пению птицы.

Власть, богатство и королевская благосклонность, которые окружали Россиньоля при дворе, совершенно вскружили голову этому выходцу из провинции. Ведь это что-то значит – расхаживать по галереям королевского дворца с надменными принцами Франции, носить дорогие кружевные костюмы с огромными манжетами и чулки из самого белого шелка, играть в бильярд с самим королем и видеть это запечатленным на гравюре, а потом возвращаться домой во всем блеске своей славы. «Монсиньор, – сказал он однажды Ришелье о своих соседях с плохо скрываемой радостью, – они не смеют приближаться ко мне. Они считают меня фаворитом, меня, который живет с ними так же, как и раньше. Они изумляются моей любезности» [Кан, 2004, с. 150-151].

Тем не менее, достижения Россиньоля действительно неоспоримы. С предельной ясностью он показал правителям Франции важность дешифрованных депеш для формирования их политики. Его работа демонстрировала это настолько эффективно, что королевский военный министр Лувуа энергично поощрял каждого, кто мог предоставить полученную таким образом информацию. Сохранилось письмо Лувуа, в котором он выражает благодарность за добытый шифр неприятеля, заверяя, что человеку, который может помочь прочесть несколько зашифрованных писем, «его величество пожалуется все, что он попросит» [Кан, 2004, с. 151].

Россиньоля занимался и созданием шифров для французских королей. Так, в частности им был создан «великий шифр» -

номенклатор на 600 кодвеличин, который долгое время был основным французским шифром.

Будучи в курсе успехов собственных дешифровальщиков, французские правители прекрасно осознавали необходимость повышения надежности своих шифрсистем. Их осмотрительность была нелишней. В 1774 году Людовику XV был доставлен пакет из Вены. Когда французский король вскрыл его, он обнаружил там копии открытых текстов своей зашифрованной корреспонденции. Людовику сообщили, что пакет прибыл от аббата Жоржеля, секретаря французского посла в Австрии. В Вене Жоржель встретился в полночь с человеком в маске, который в обмен на тысячу дукатов передал ему этот пакет и за дополнительное щедрое вознаграждение пообещал два раза в неделю передавать аббату все находки так называемого «черного кабинета» в Вене, в котором тайно вскрывалась и дешифровалась корреспонденция других стран.

В XVIII веке в Англии также функционировал свой «черный кабинет». В отличие от венского, он не имел собственного помещения. Поэтому его небольшой штат экспертов работал большей частью дома, получая материалы через посыльных. У английского «черного кабинета» отсутствовала четкая организационная структура, старший дешифровальщик был в нем просто первым среди равных. Финансирование «черного кабинета» осуществлялось за счет денег, отпускавшихся министерству почт Англии из дополнительных доходов парламента. Во всей стране только около тридцати человек знали о том, что «черный кабинет» читает иностранную дипломатическую переписку. С ней знакомились только король и несколько его главных министров. Однако несмотря на соблюдаемую секретность, большинство деловых людей в Англии предусмотрительно шифровало свою корреспонденцию или доверяло ее частным посыльным. И немудрено – ведь английский закон о почте от 1711 года давал правительственным служащим право вскрывать любые почтовые отправления на основании ордеров, которые они же себе и выдавали.

Английский «черный кабинет» прочитывал в среднем две или три зашифрованные депеши за неделю. Его криптоаналитики успешно вскрывали шифры Австрии, Греции, России, Саксонии, Турции, Франции, а также Неаполя, Сардинии и других итальянских государств. Позднее к этим странам присоединились и Соединенные Штаты Америки. В нем собраны сообщения, перехваченные

англичанами с 1719-го по 1839 годы. Не все испанские шифровки были прочитаны непосредственно после того, как были перехвачены. Многие ждали своей очереди до тех пор, когда их накапливалось достаточно много для успешного дешифрования или когда появлялась необходимость в их чтении.

В 1723 года два криптоаналитика английского «черного кабинета» выступили в качестве свидетелей в палате лордов, где судили епископа Фрэнсиса Эттербери по обвинению в заговоре. Поскольку главные изобличающие Эттербери улики были найдены в дешифровках Эдварда Уиллеса и Энтони Корбире, лорды «сочли уместным вызвать в суд этих дешифровальщиков, дабы убедиться в достоверности их дешифрования» [Кан, 2004, с. 156]. Уиллес и Корбире показали под присягой, что переписка Эттербери была дешифрована ими независимо друг от друга, поскольку один из них находился в провинции, а другой – в столице, и тем не менее результаты дешифрования совпали.

Эттербери попытался поставить под сомнение достоверность открытых текстов, представленных Уиллесом и Корбире. Подсудимый поднял такой шум, что ему и его адвокату было приказано удалиться, а лорды проголосовали за предложение о том, «что, по мнению палаты, любые вопросы **дешифровальщику** все правильно кому чему **дешифровальщику** **ОПЯТЬ ПО-РАЗНОМУ: ВСТРЕЧАЕТСЯ ДЕШИФРОВЩИК. НУЖНО ОДИНАКОВО, ОДНООБРАЗНО** , которые могут привести к раскрытию способов или тайн дешифрования, противоречат общественной безопасности» [Кан, 2004, с. 156]. Голосование было положительным, и дешифрованные тексты были приняты в качестве доказательства виновности Эттербери. Он был отрешен от должности и изгнан из королевства.

За океаном не было ни «черных кабинетов», ни платных криптоаналитиков. Тем не менее, и там криптоанализ сыграл положительную роль – помог американским колониям занять достойное место среди других стран мира.

Эта история началась в августе 1775 года. Булочника Годфри Венвуда навестила в Ньюпорте его бывшая любовница. Она попросила Венвуда помочь передать одно письмо английским офицерам. У патриота-повстанца Венвуда зародилось сомнение. Он уговорил любовницу отдать письмо для доставки по назначению и уехать, прежде чем его невеста узнает о ее посещении. Но Венвуд не отослал письмо, а вскрыл его и обнаружил три страницы,

заполненные странными символами и цифрами. Это укрепило его подозрения.

В конце сентября Венвуд прибыл в штаб генерала Джорджа Вашингтона, чтобы показать ему письмо. Главнокомандующий повстанческими войсками не сумел прочитать криптограмму и распорядился допросить бывшую любовницу Венвуда. Она призналась, что письмо ей передал ее очередной любовник – доктор Бенджамин Черч. Вашингтон был поражен. Черч являлся генеральным инспектором госпиталей. Процветающий бостонский врач, он только накануне просил об отставке с поста директора госпиталей. Вашингтон отклонил эту просьбу из-за своего нежелания расстаться с хорошим инспектором. Мог ли такой известный человек состоять в тайной и, возможно, предательской переписке?

Когда Черча допросили, он с готовностью признался, что письмо принадлежит ему и адресовано брату Флемингу, который находится в Бостоне. Если письмо расшифровать, то обнаружится, что в нем нет ничего криминального. И хотя Черч неоднократно торжественно заверял в своей преданности делу освобождения из-под английского колониального гнета, он не изъявил готовности дословно изложить содержание письма.

Вашингтон занялся поисками людей, которые смогли бы прочесть письмо Черча. Когда стало известно, что Вашингтону нужны криптоаналитики, несколько человек с готовностью предложили свои услуги. 3 октября Вашингтон получил от них открытый текст письма. В нем Черч доносил английскому главнокомандующему о снабжении американцев боеприпасами, их продовольственных запасах и численности войск. Письмо заканчивалось словами: «Соблюдайте всяческую предосторожность, не то я погиб» [Кан, 2004, с. 158].

Черча заключили в тюрьму, а затем в 1780 году выслали в Вест-Индию. Небольшая шхуна, на которой он плыл, пропала без вести. Так первый американец, лишившийся свободы в результате умелого использования криптоанализа, потерял вдобавок и жизнь.

В то время как в ходе американской революции появлялись все новые и новые шифровальные системы, криптоанализ переживал период застоя. Главная причина крылась в том, что за редким исключением, как, например, в случае с Черчем, криптограммы не удавалось перехватить. И лишь когда война с англичанами близилась к своему завершению, было захвачено достаточное количество сообщений для криптоанализа. Большинство из них было

дешифровано Джеймсом Ловеллом, которого можно по праву назвать отцом американского криптоанализа.

Ловелл родился 31 октября 1737 года в Бостоне. В 1756 году он окончил Гарвардский университет и в течение 18 лет преподавал в средней школе. В 1777 году Ловелл был избран депутатом конгресса и вскоре стал известен благодаря своему рвению и трудолюбию.

Криптоаналитические успехи Ловелла пришлись очень кстати. Осенью 1781 года заместитель английского главнокомандующего в Америке Чарльз Корнуоллис перебросил свои войска на север – из Каролины в Вирджинию. Будучи убежден, что для того, чтобы удержать южные земли, сначала нужно овладеть севером, он выступил по направлению к побережью в надежде получить подкрепления по морю от своего шефа, генерала Генри Клинтона, находившегося в Нью-Йорке. Корнуоллис планировал подчинить себе Вирджинию, затем покорить Каролину и известить его величество, короля Георга III, о том, что с восстанием в Америке покончено.

Именно в это время американский командующий на юге Натаниэль Грин направил конгрессу несколько перехваченных английских криптограмм, которые в его штабе никто не мог прочитать, присовокупив их к своему общему донесению. Эта зашифрованная английская корреспонденция оказалась перепиской между Корнуоллисом и некоторыми из его подчиненных.

Донесение Грина было зачитано в конгрессе 17 сентября. Четырьмя днями позже Ловелл расшифровал приложения к донесению. К сожалению, из-за быстрого развития событий добытая Ловеллом информация не принесла много пользы. Но найденные Ловеллом ключи вполне могли пригодиться когда-нибудь в будущем. В своем письме Вашингтону Ловелл написал: «Не исключено, что противник намерен и далее зашифровывать свою переписку... Если это так, то Ваше превосходительство, возможно пожелает извлечь для себя пользу, дав Вашему секретарю указание снять копию ключей и замечаний, которые я через Вас направляю...» [Кан, 2004, с. 159].

Более проницательным Ловелл быть не мог. Вскрытый им шифр действительно служил также и для связи между Корнуоллисом и Клинтонем. К тому времени Корнуоллис отошел к Йорктауну, чтобы дожидаться подкреплений от Клинтона. Но Вашингтон с 16-тысячным войском окружил город, а французский адмирал граф де Грасс с 24 кораблями блокировал помощь англичанам с моря. 6 октября Вашингтон писал Ловеллу: «Мой секретарь снял копии с

шифров и с помощью одного из алфавитов сумел расшифровать параграф недавно перехваченного письма лорда Корнуоллиса сэру Клинтону» [Кан, 2004, с. 159-160].

Эта информация помогла Вашингтону оценить реальное положение дел в английском лагере. Тем временем для связи с Корнуоллисом Клинтон снарядил два небольших судна, которые он отправил из Нью-Йорка 26 сентября и 3 октября. Оба они были захвачены повстанцами. При этом одно из них прибило к берегу, где англичанин, который вез пачку зашифрованных депеш, спрятал их под большим камнем, прежде чем его захватили в плен. Потом, как выразился один американец, «в результате непродолжительной беседы и пообещав прощение» [Кан, 2004, с. 160], повстанцы уговорили англичанина отыскать спрятанные депеши. Поиски заняли около двух дней.

Ловелл получил эти депеши 14 октября и тотчас же принялся за дело. Успех не заставил себя долго ждать, так как к своей радости Ловелл обнаружил, что они зашифрованы тем же шифром, что и остальная переписка Корнуоллиса. В одной из прочитанных Ловеллом депеш, в частности, говорилось: «Милостивый государь! Ваша светлость может быть уверена, что я делаю все, что в моих силах, чтобы оказать вам помощь непосредственными действиями, а полученные мной сегодня от адмирала Грейвса (командующий английским флотом у берегов Америки) заверения дают мне основание полагать, что к 12 октября мы сумеем преодолеть трудности, если позволит ветер и не произойдет ничего непредвиденного. Это, безусловно, не исключает неудачного исхода, а посему, если я получу от вас известие, ваши пожелания будут для меня руководящими, и я буду настойчиво придерживаться своей идеи непосредственного действия...» [Кан, 2004, с. 160].

Через пять дней после того, как Ловелл закончил дешифрование, Корнуоллис капитулировал. Но победа повстанцев была не совсем полной. Вашингтон понял это, когда на следующий день он наконец получил от Ловелла копии дешифрованных депеш. Не теряя ни минуты, Вашингтон переправил их де Грассу, корабли которого должны были воспрепятствовать попытке оказания помощи Корнуоллису Грейвсом и Клинтоном. Будучи предупрежден, французский адмирал основательно подготовился к нападению англичан. 30 октября он заставил английский флот отступить и тем

самым приблизил окончательную победу американцев в Войне за независимость.

Теперь рассмотрим криптографическую деятельность в разных странах в эпоху наполеоновских войн. Напомним, что Наполеон Бонапарт родился в 1769 году на острове Корсика (см. рис 4.1). Начал службу во французской армии в 1785 году в чине младшего лейтенанта артиллерии. Наполеон проявил себя в качестве талантливого полководца во время Французской революции (получил чин бригадного генерала) и Директории (стал командующим армией). В ноябре 1799 года совершил государственный переворот и стал первым консулом, фактически сосредоточив в своих руках всю полноту власти. В 1804 году провозгласил себя Императором Франции Наполеоном I. В период своего правления практически непрерывно вел войны. К 1812 году территория империи, включала в себя большую часть Западной и Восточной Европы, а также ряд территорий в Азии и Северной Африке. Летом 1812 года Наполеон начал войну против России, которая закончилась для него тяжелым поражением. В 1814 году войска антифранцузской коалиции вступили в Париж. Наполеон отрекся от престола и был сослан на остров Эльба. В марте 1815 года вновь занял французский престол. Период возвращения Наполеона к власти получил название «сто дней». После поражения в битве при Ватерлоо он вновь отрекся от престола и был сослан на остров Святой Елены, где и умер в 1821 году. По числу участвовавших в боевых действиях стран и количеству задействованных войск наполеоновские войны являются одним из крупнейших конфликтов в Европе до начала XX века.



Рис. 4.1 Наполеон Бонапарт

Нет ссылки в тексте на этот рис стр 129

Наполеон существенно реорганизовал французскую разведку. Еще в мае 1796 года взамен прежних разведывательных организаций, которые имелись при главной квартире и при штабах отдельных генералов, было создано "Секретное бюро". Его возглавил Жан Ландре. Бюро было разделено на два отдела: общий и политический; в задачи последнего входили наблюдение за оккупированной территорией, подавление народных волнений и другие обязанности. Глава политического отдела Гальди набирал массу агентов. Агентура Бюро проникла в Неаполь, Рим, Флоренцию, Турин, Венецию и австрийскую армию, наконец, даже в Вену. Часто "Секретное бюро" составляло для Наполеона по нескольку отчетов в день. Помимо командующего доклады бюро имел право читать только начальник штаба Бертье. Таким образом, "Секретное бюро" занималось и разведкой, и контршпионажем. Ландре имел своих агентов и в Париже - в их обязанность входило наблюдение за теми,

кого Директория направляла на различные должности во французскую армию, сражавшуюся в Италии.

"Секретное бюро" было обильно снабжено средствами, некоторым агентам за доставлявшиеся ими сведения платили большие суммы (по несколько десятков тысяч франков). Иногда информация, содержащаяся в докладах "Секретного бюро", оказывалась настолько неожиданной, что Наполеон отказывался ей верить, угрожая Ландре смещением с должности. Однако почти всегда сообщенные известия оказывались правильными.

Еще одним способом получения информации о противнике, к которому с самого начала своей полководческой карьеры прибегал Наполеон, был опрос пленных и вербовка среди них агентов. Взятым в плен офицерам обещали большое вознаграждение, если они привлекут к сотрудничеству с французами более высокие чины.

После того как в 1799 году Наполеон сосредоточил всю полноту власти в своих руках, он провел новую реорганизацию разведывательной и контрразведывательной служб. Разведывательные и контрразведывательные задачи были возложены на министерство полиции, возглавляемое Фуше, на бюро независимого от него префекта парижской полиции Дюбуа, на персональных агентов Наполеона, создававших свои особые организации (в их число входили такие видные военные, как Дюрок, Даву, Ланн, Жюно, Савари - будущие маршалы и министры наполеоновской империи). Этой личной разведкой Наполеон управлял через своего секретаря Бурьена. Военной разведкой занималось специальное разведывательное бюро, образованное в военном министерстве. Отдельное разведывательное бюро было создано в армии, предназначавшейся для десанта в Англии в 1804 году. Впоследствии наполеоновская разведка имела агентов во всех столицах и во многих крупных городах большинства европейских государств (кроме России). Обычно это были хорошо оплачиваемые резиденты. Когда район деятельности того или иного агента выдвигался в центр событий, этому разведчику выдавались очень большие суммы денег для добывания информации [Черняк 1991].

Наполеон считал крайне важным организацию информационно-психологического давления на противника, доведения до него нужной (при этом иногда ложной информации). Для этого в армии Бонапарта имелась походная типография производительностью около 10000 листовок в сутки. Вот как сам

Наполеон оценивал силу печатного слова: «Четыре газеты могут причинить больше зла, чем стотысячная армия» [Белоус 2006]. Справедливости ради следует отметить, что французская армия в этот период подвергалась успешным информационным атакам. Во время Итальянского похода генералиссимуса А.В. Суворова (1799 год), его обращение к противнику с разъяснением тяжелого положения, в котором оказались французы привело к осязательному эффекту. Солдаты французской Пьемонтской армии сдавались целыми частями и подразделениями.

Спецслужбы Франции активно использовали в своей деятельности дезинформирование противника. Для этого часто использовали агентов-двойников, одним из таких агентов была графиня Палестрина. Через нее австрийцев снабжали фальшивыми сведениями. В игру включился сам Наполеон. Не раз в присутствии графини он "проговаривался" о важных вещах, симулируя то припадок гнева, то, напротив, порыв радости. Для защиты информации Наполеон применял цензуру прессы. Так, например, когда в 1804 году французская армия из булонского лагеря, где она была сосредоточена для предполагавшегося (но не осуществленного) десанта в Англию, была ускоренным маршем двинута на Рейн против Австрии, Наполеон писал министру полиции: "Запретите газетам говорить об армии, как будто ее вовсе не существует" [Черняк 1991, с. 434]. При этом сам Наполеон демонстративно оставался в Булони, а потом перебрался в Париж, где устраивал пышные празднества. Все делалось для дезориентации неприятеля.

Значительно укрепился «черный кабинет» Франции. Его возглавлял директор почт Лаваллет. Он фактически превратился во второго министра полиции и одного из руководителей наполеоновской контрразведки. Между прочим, при содействии Лаваллета Наполеон завел ряд высокооплачиваемых агентов, которые представляли ему тайные доклады о настроениях различных кругов французской буржуазии и бюрократии. В 1811 году Наполеон создал филиалы «черного кабинета» по всей своей огромной империи: в Турине, Генуе, Флоренции и Риме, Амстердаме и Гамбурге. Эти кабинеты работали весьма эффективно. Перлюстрация дипломатической переписки приняла огромные размеры. Эта деятельность находилась под контролем министра иностранных дел Талейрана. Не обходилось здесь и без курьезов. Так, один из иностранных послов пожаловался министру: «Черный кабинет»

Франции перлюстрирует мою корреспонденцию». Тайлеран скромно ответил: «Господин посол! Я уверен только в одном: ваши депеши вскрывает кто-то, интересующийся тем, что содержится внутри пакетов» [Черняк 1991, с. 433]. Другими словами, прямых улик против «черного кабинета» нет. Отметим, что в основном речь здесь идет лишь о перехвате и перлюстрации сообщений. Успехи в дешифровании были гораздо скромнее.

Примером успехов криптографической службы Франции может служить следующий эпизод. 26 сентября 1812 года американский посланник в Париже в письме президенту США Мэдисону тщательно зашифровал имена двух французских чиновников, которые поддерживали претензии США к Наполеону и особо просили, чтобы этот факт оставался в секрете, но французская дешифровальная служба прочитала послание и выяснилось, что это были Камбасере и Талейран [Kahn 1967] (см. рис.4.2).



Рис. 4.2 Шарль Морис Талейран

Нет ссылки в тексте на этот рис стр 133

Талейран долгое время находился на высоких должностях в правительстве Наполеона (вплоть до министра иностранных дел). В 1808 году Талейран при личной встрече предложил себя в качестве платного информатора русскому императору Александру I. Им

двигали меркантильные соображения и обида на Наполеона. Отношения между Императором Франции и его министром иностранных дел были далеки от идеала. Нередко при большом скоплении людей Наполеон называл Талейрана вором, мерзавцем и другими оскорбительными словами, а иногда обещал и вовсе повесить. После недолгих раздумий о том, не является ли предложение Талейрана провокацией, российский император принял предложение о сотрудничестве и стал весьма щедро оплачивать поставляемую информацию. Так Талейран стал платным агентом русской разведки. Предоставляемая им информация являлась весьма важной для российского двора. Он сообщал сведения о состоянии французской армии, внешнеполитических инициативах Франции, внутривластной обстановке. Одним из важнейших сообщений Талейрана была дата вторжения Наполеона в Россию. Поскольку Талейран имел прямое отношение к деятельности французского «черного кабинета», то вполне возможно, что он продавал и криптографические секреты Франции. Александр I очень ценил этот источник информации и тщательно оберегал его от разоблачения. Все сообщения, передаваемые от Талейрана российским послом в Париже К.В. Нессельроде, тщательно зашифровывались. При этом Талейран сам нередко высказывал весьма конструктивные предложения по организации конспирации и обеспечению секретности переписки. Для защиты информации, в частности использовались жаргонные коды, сам Талейран имел несколько псевдонимов: «Мой кузен Анри», «Анна Ивановна», «Красавец Леандр», «наш книготорговец», «юрисконсульт». Министр полиции Франции Фуше фигурировал как «Наташа», «Бержён», «президент», положение во Франции обозначалось как «английское земледелие» или «любовные шашни Бутягина (фамилия секретаря русского посольства в Париже) и т.д. Так, когда Наполеон отправил Фуше в отставку, Нессельроде 6 июня 1810 года отправил в Санкт-Петербург следующее сообщение: «Уход президента очень мне мешает, именно от него наш юрисконсульт почерпнул сведения, которые я вам пересылал» [Примаков 1997, с. 107]. Интересно отметить, что Талейран предложил подобные услуги и Австрии. Его предложение было принято, о чем агентурных источников узнал Александр I. Это привело к постепенному сворачиванию контактов с Талейраном, который к тому же стал требовать за свои услуги огромные суммы. Таким образом, Талейран одновременно укреплял безопасность Франции, фактически руководя

дешифровальной службой, и наносил ей ощутимый вред. Моральный облик Талейрана очень хорошо характеризует его фраза: «Главное качество денег – это их количество» [Примаков 1997, с. 108].

Активно использовали агентурно-оперативные методы добычи криптографических секретов наполеоновской Франции и англичане, при этом они достигли весьма серьезных успехов в дешифровании французской переписки.

После победы французской революции англичане создали во Франции и оккупированных ей странах большую агентурную сеть. В качестве агентов вербовались как «идейные» роялисты (сторонники восстановления монархии), так и обычные наемники, работавшие исключительно за деньги. Для передачи сообщений агенты прибегали к различным уловкам, посылали их на «явки» в нейтральных странах, использовали коды в сочетании со стеганографией. Кодобозначения были в виде нотных значков, специальных терминов из области музыки, ботаники, кулинарии и даже часового дела. Сами сообщения зашивались в одежду, подошвы ботинок, прятались в укромные места лодок, повозок и т.д. В случае угрозы ареста курьеры съедали компрометирующие документы. Известен случай, когда женщина-агент умудрилась проглотить целую пачку писем. Занимались разведывательной работой и английские дипломаты в нейтральных странах. Так, полномочный представитель Великобритании при баварском дворе в Мюнхене Дрэйк сумел подкупить директора баварской почты и получил доступ ко всей французской корреспонденции, проходящей через мюнхенский почтамт [Дамаскин, 2004].

Наполеон уделял большое внимание техническому прогрессу организации информационного обмена. С конца XVIII века на французы для передачи информации на расстояния использовали семафорный оптический телеграф, станциями которого была покрыта почти вся территория страны. При этом во время осложнений военно-политической обстановки частных лиц временно лишали права пользоваться этим видом связи.

Вопросам криптографической защиты информации французский император уделял недостаточное внимание. Несмотря на некоторые успехи в дешифровании чужих шифров, защита собственной информации, особенно в действующей французской армии, осуществлялась при помощи весьма простых шифров. Во время походов у императора было две основных шифра. «Большой

шифр» Наполеон использовал для связи со своими командующими. Эта система была подобна «великому шифру» Россиньоля, однако представляла собой номенклатор на 200 величин вместо 600. Это делалось для простоты шифрования и расшифрования в полевых условиях. «Малый шифр» был предназначен для связи с небольшими воинскими подразделениями.

Малый шифр Наполеона (Petit Chiffre).

A—15, ar—25, al—39
B—37, bu—3, bo—35, bi—29
C—6, ca—32, ce—20
D—23, de—52
E—53, es—82, et—50, en—68
F—55, fa—69, fe—58, fo—71
G—81, ga—51
H—85, hi—77
I—119,
J—87, jai—123
K—?
L—96, lu—103, le—117, la—106
M—114, ma—107
N—115, ne—94, ni—116
O—90, ot—153
P—137, po—152
Q—173, que—136
R—169, ra—146, re—126, ri—148
S—167, sa—171, se—177, si—134, so—168, su—174
T—176, ti—145, to—157
U—138
V—164, ve—132, vi—161, vo—175
W, X, Y — ?
Z—166

Приведенная выше таблица замены была восстановлена известным французским криптографом Этьеном Базери в конце XIX века. В имевшихся в его распоряжении криптограммах некоторые буквы (K, W, X и Y) не встречались, поэтому он не смог определить соответствующие им шифробозначения.

«Малый шифр» содержит числовые эквиваленты для всех букв алфавита, а также для часто встречающихся биграмм (двухбуквенных сочетаний) и некоторых триграмм (трехбуквенных сочетаний). С помощью этого шифра, слово NAPOLEON, например, может быть зашифровано по-разному:

N	A	P	O	L	E	O	N
115	15	137	90	96	53	90	115
или							
N	A	PO	LE	O	N		
115	15	152	117	90	115		

Использование подобных приемов сильно усложняет задачу криптоаналитика. Свой шифр был и у начальника штаба Бертье [Соболева 2002], [Черняк 1991], [Kahn 1967], [agentura].

Наполеон и его генералы также использовали книжные шифры, шифры простой замены, в том числе и шифры типа «масонский ключ», который был переименован в «алфавит Наполеона». О последнем способе шифрования расскажем подробнее. Из самого названия следует, что данные шифрсистемы активно использовали члены "Братства Франк-масонов", или "Вольных каменщиков". По современным понятиям и вопреки расхожему мнению этот шифр совершенно не стоек, но представляет определенный интерес. Приведем небольшой пример (применительно к английскому языку). Нарисуем три фигуры следующего вида [Бабаш 2002]:

A:	B:	C:	J.	K.	L.	S	T	U
D:	E:	F:	M.	N.	O.	V	W	X
G:	H:	I:	P.	Q.	R.	Y	Z	

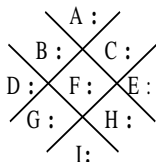
В соответствии с этими фигурами буквы получают следующее геометрическое представление:




A= $\begin{array}{|c|} \hline : \\ \hline \end{array}$, B= $\begin{array}{|c|} \hline : \\ \hline \end{array}$, C= $\begin{array}{|c|} \hline : \\ \hline \end{array}$, J= $\begin{array}{|c|} \hline . \\ \hline \end{array}$, R= $\begin{array}{|c|} \hline . \\ \hline \end{array}$, S= $\begin{array}{|c|} \hline . \\ \hline \end{array}$ и т. д.

Фраза "We talk about" при зашифровании принимает вид:



Геометрическое представление может меняться, например:



Тогда A = , D = , I =  и т. д.

Но даже эти не очень стойкие шифры использовались с серьезными ошибками. Ключи не менялись длительное время, в шифртекстах сохранялось разбиение на слова (в соответствии с открытым текстом), использовались стандартные обращения и подписи, значительная часть сообщения не шифровалась (она считалась несекретной) и т.д. Все это, безусловно, облегчало дешифрование. Кроме того, в экстренных случаях секретные сообщения вообще не шифровались и в открытом виде попадали к противнику.

Следует отметить, что криптография во Франции отнюдь не находилась в застое. В начале XIX века была издана Французская Энциклопедия. В ней были описаны все известные к тому времени исторические шифры и способы их дешифрования. Это способствовало широкому распространению криптографических знаний в Европе. Энциклопедия сыграла роль учебника по криптографии для широкого круга заинтересованных лиц в различных странах (в том числе и в России). Особенно это относится к революционным подпольным организациям, которые не имели доступа к секретам государственных криптографических служб.

При Наполеоне не были изобретены новые специальные шифры. Французская армия пользовалась известными к тому времени

способами шифрования. Поэтому противники Наполеона достигли весьма серьезных успехов в дешифровании его переписки.

Одним из первых добился успехов Джордж Сковелл (George Scovell) (см. рис. 4.3). Он был шефом шифровальщиков при командующем английской армией герцоге Веллингтоне. Во время кампании против французов в Испании (1808-1814) он создал систему сбора развединформации, с помощью которой осуществлялся перехват почты и фронтовых донесений французов и производил их дешифрование.



Рис. 4.3 Джордж Сковелл

Нет ссылки в тексте на этот рис стр 139

В 1808 году внимание Наполеона привлекли Португалия и Испания. Его войска заняли Лиссабон и Мадрид. Наполеон посадил своего брата Жозефа на испанский трон. Не смилившиеся с поражением португальцы и испанцы стали вести партизанскую войну против оккупантов. Они попросили помощи у англичан. Первые подразделения британцев высадились в Португалии летом 1808 года. Следующие шесть лет португальцы и испанцы сражались против врага вместе с англичанами.

В этой войне и отличилась команда дешифровальщиков и агентов по сбору развединформации, работу которой контролировал Дж. Сковелл. По мнению англичан, она сыграла огромную роль в

состоял из комбинаций 150 чисел. Сковелл взломал этот код за два дня. В 1811 году Джордж Сковелл получил книгу «Криптография, или искусство расшифровки», написанную Дэвидом Арнольдом Конрадусом. В книге излагались правила и принципы создания и дешифрования кодов и шифров. Она также описывала особенности английских, немецких, датских, французских и итальянских шифров. Эксперименты Сковелла с различными методами шифрования и кодирования информации основывались на принципах, изложенных в этой книге. Он придумал принцип, гарантирующий, что общий для Британии шифр, защищавший донесения, не будет взломан. По этой системе, обозначение 56C2 направляет получателя к странице 56 некоторой книги, колонке С, второму слову снизу. Это был хоть и очень простой, но довольно надежный код. Вопрос был в том, чтобы узнать, в какой именно книге надо искать нужную страницу. Фактически, это был один из вариантов книжного шифра (см. рис 4.5).

	100	200	300	400
1	et arm	l'homme	l'homme	et arm
2	et arm	l'homme	l'homme	et arm
3	et arm	l'homme	l'homme	et arm
4	et arm	l'homme	l'homme	et arm
5	et arm	l'homme	l'homme	et arm
6	et arm	l'homme	l'homme	et arm
7	et arm	l'homme	l'homme	et arm
8	et arm	l'homme	l'homme	et arm
9	et arm	l'homme	l'homme	et arm
10	et arm	l'homme	l'homme	et arm
11	et arm	l'homme	l'homme	et arm
12	et arm	l'homme	l'homme	et arm
13	et arm	l'homme	l'homme	et arm
14	et arm	l'homme	l'homme	et arm
15	et arm	l'homme	l'homme	et arm
16	et arm	l'homme	l'homme	et arm
17	et arm	l'homme	l'homme	et arm
18	et arm	l'homme	l'homme	et arm
19	et arm	l'homme	l'homme	et arm
20	et arm	l'homme	l'homme	et arm
21	et arm	l'homme	l'homme	et arm
22	et arm	l'homme	l'homme	et arm
23	et arm	l'homme	l'homme	et arm
24	et arm	l'homme	l'homme	et arm
25	et arm	l'homme	l'homme	et arm
26	et arm	l'homme	l'homme	et arm
27	et arm	l'homme	l'homme	et arm
28	et arm	l'homme	l'homme	et arm
29	et arm	l'homme	l'homme	et arm
30	et arm	l'homme	l'homme	et arm
31	et arm	l'homme	l'homme	et arm
32	et arm	l'homme	l'homme	et arm
33	et arm	l'homme	l'homme	et arm
34	et arm	l'homme	l'homme	et arm
35	et arm	l'homme	l'homme	et arm
36	et arm	l'homme	l'homme	et arm
37	et arm	l'homme	l'homme	et arm
38	et arm	l'homme	l'homme	et arm
39	et arm	l'homme	l'homme	et arm
40	et arm	l'homme	l'homme	et arm
41	et arm	l'homme	l'homme	et arm
42	et arm	l'homme	l'homme	et arm
43	et arm	l'homme	l'homme	et arm
44	et arm	l'homme	l'homme	et arm
45	et arm	l'homme	l'homme	et arm
46	et arm	l'homme	l'homme	et arm
47	et arm	l'homme	l'homme	et arm
48	et arm	l'homme	l'homme	et arm
49	et arm	l'homme	l'homme	et arm
50	et arm	l'homme	l'homme	et arm

Рис. 4.5. Большой шифр Наполеона со следами работы английских дешифровальщиков (1812 год). **Нет ссылки в тексте на этот рис стр 141**

В конце 1811 года новые таблицы кодов были разосланы из Парижа всем ведущим французским военным. Они были основаны на дипломатическом коде середины XVIII века, и в них использовалось 1400 кодов величин. Такие таблицы отправлялись вместе с инструкциями по их использованию, призванными устранить некоторые недостатки в использовании шифров, описанные выше. Например, в конце сообщения рекомендовалось приписывать цифры, лишённые всякого смысла. Это было сделано для того, чтобы затруднить работу дешифровальщика, так как была высока вероятность наличия в конце сообщения стандартных фраз, которыми обычно заканчивается корреспонденция (например, звание и фамилия лица отправившего документ). Знание отрывка и зашифрованного текста, разумеется, облегчает дешифрование.

В течение следующего года Сковелл изучал перехваченные документы французов. Он добился успеха, работая с сообщениями, которые содержали незакодированные слова и фразы (как уже упоминалось, для ускорения процесса **шифрования/расшифрования** все правильно оставить **БЫЛО РАСШИФРОВАНИЕ, ДЕШИФРОВАНИЕ** французы часто шифровали не все сообщение, а только «наиболее секретные» его части). В таких сообщениях значение зашифрованных кусков текста становилось ясным из контекста. Информация о передвижениях войск, собранная «армией проводников» Сковелла помогала идентифицировать конкретных людей и определять населённые пункты, упоминаемые в зашифрованных письмах.

В 1812 году в руках Сковелла оказалось перехваченное письмо Жозефа, адресованное его брату – Наполеону Бонапарту. Сковеллу удалось расшифровать большую часть закодированной информации, касающейся плана военной операции. Это позволило Веллингтону подготовиться к битве, от исхода которой зависело, будут ли французы контролировать Испанию (битва при Витториа 21 июня 1813 года). Той ночью британские отряды захватили экипаж Жозефа Бонапарта и завладели копией Великого французского шифра. В результате этот код был раскрыт окончательно [Гольев 2008], [Черняк 1991], [Kahn 1967], [agentura].

Читали англичане и французскую дипломатическую переписку. Достаточно отметить, что в архиве английского «черного кабинета» хранится 5 томов (более 2000 страниц), перехваченной и прочитанной в XVIII – XIX веках, французской корреспонденции, а также три тома (872 страницы) с вскрытыми за это время ключами к шифрам Франции [Kahn 1967].

Еще одной страной, специалисты которой, смогли вскрыть французские шифры была Австрия. Австрийцы активно читали дипломатическую переписку Франции, в том числе Наполеона, Талейрана и других министров, послов и т.д.

Рассмотрим деятельность австрийской дешифровальной службы в XVIII – XIX веках более подробно. Американский историк Дэвид Кан [Kahn 1967] (русские переводы [Кан 2000], [Кан 2004]) детально описывает работу этой организации. Она была очень эффективной. Мешки с корреспонденцией, которая должна была доставляться утром иностранным посольствам, находящимся в Вене, в 7 часов утра ежедневно привозили в помещение «черного кабинета». Там письма аккуратно вскрывали, растапливая печати над свечой, отмечали порядок расположения страниц в конверте и передавали их помощнику директора. Он читал их и давал указания о снятии копий с самых важных документов. Длинные письма для экономии времени копировались под диктовку с использованием до четырех стенографистов одновременно. Если письмо было на незнакомом помощнику директора языке, он передавал его служащему кабинета, знавшему этот язык. Имелись переводчики со всех европейских языков, а когда появлялась потребность в новом языке, один из служащих получал задачу срочно выучить его. После копирования письма укладывались обратно в конверты, которые запечатывались при помощи поддельных печатей и возвращались на почту не позже 9.30 утра.

Через полчаса в «черный кабинет» прибывала новая почта. Она обрабатывалась таким же образом, хотя и с меньшей поспешностью, поскольку была транзитной. Через Вену, находящуюся в центре Европы шел огромный поток переписки между различными державами. Писали правители, дипломаты, военные, торговцы и т.д. Как правило, эта корреспонденция возвращалась на почтовую станцию к 14.00, хотя иногда ее задерживали и до 19 часов. В 11 часов утра прибывали сообщения, перехваченные полицией. А в 16.00 курьеры привозили письма, которые отправляли иностранные

дипломаты. Эти письма снова вливались в поток отправляемой из Вены почтовой корреспонденции к 18.30. Скопированный материал попадал на стол к директору «черного кабинета», который отбирал особо интересную информацию и направлял ее заинтересованным лицам – руководству страны, министрам, дипломатам, военачальникам, полицейским чиновникам и т.п. Таким образом, австрийский «черный кабинет» со штатом всего в десять человек обрабатывал в среднем 100 писем ежедневно, обеспечивая сбор важной информации для всех ветвей государственной власти Австрии. При этом сотрудники венского «кабинета» работали крайне аккуратно, ошибки, когда вкладывали письма в чужие конверты, были крайне редки. Но все же иногда случались, однажды перехваченное письмо для герцога Моденского было ошибочно опечатано очень похожей печатью правителя Пармы. Когда герцог заметил подлог, он отправил его в Парму с ироничной пометкой: «Не совсем мне, но и не вам». Оба государства заявили протест, но Вена отреагировала на него проявлением полнейшего недоумения. Тем не менее, многие представители зарубежных стран при австрийском дворе знали о существовании в Вене «черного кабинета». Его наличие косвенно признали даже сами австрийцы. Когда английский посол с юмором пожаловался, что он получает копии вместо оригинальной корреспонденции, австрийский канцлер холодно заметил: «Как неловки эти люди!» [Кан 2004, с. 153].

Перехваченная зашифрованная корреспонденция подвергалась криптоанализу. В нем австрийцы весьма преуспели. Успех был достигнут в том числе и за счет, того, что сейчас бы назвали «научной организации труда». Были разработаны «нормативные акты», регулирующие работу дешифровальщиков. Они имели следующие положения.

недопускать переутомления сотрудников от интенсивной умственной нагрузки, за исключением чрезвычайных случаев, австрийские криптоаналитики одну неделю работали, а другую – отдыхали;

необходимость материального стимулирования успехов, хотя их заработная плата была невысокой, за вскрытие шифров выдавались значительные премии. Несколько меньшая премия полагалась за дешифрование по украденным ключам. Например, в 1833 году криптоаналитики получили 3/5 суммы, предназначенной для премий, за чтение шифровок французского посланника. В течение одной ночи

ключ к его шифру был тайно изъят, скопирован и снова водворен в шкаф в спальном комнате секретаря французской дипломатической миссии в Вене;

предусмотреть денежную компенсацию дешифровальщикам за вынужденную безработицу, иногда ключи некоторых шифров подолгу не менялись и вскрыв их, дешифровальщики оказывались в вынужденном простое.

Помимо материальных стимулов существовали и моральные. Главным из них было особое внимание монаршей семьи к работе австрийских криптоаналитиков. Император Карл VI вручал им премии лично, а эрцгерцогиня (жена наследника престола) Мария-Терезия часто беседовала с сотрудниками «черного кабинета» о надежности используемых шифров и о достижениях других стран в криптоанализе.

Важное значение придавалось вопросам подготовки специалистов-криптографов. Вся система работы с перспективными кадрами была нацелена на получение от них максимальной отдачи. Были созданы специальные курсы, на которые направлялись юноши двадцатилетнего возраста. К абитуриентам предъявлялись особые требования: высокие моральные качества, знание иностранных языков (в частности французского и итальянского) и математики. Сначала им не раскрывали всех подробностей предстоящей работы и обучали созданию надежных шифров, а затем подвергали испытанию – смогут ли они вскрыть разработанные ими же шифры. Неспособным подыскивали другую государственную службу, а остальных посвящали в секреты криптоаналитического мастерства. В процессе обучения предусматривались особые тесты, предназначенные для определения способностей обучаемого к деятельности в области криптографии. К преподаванию на курсах привлекались криптографы, находящиеся на государственной службе. После завершения обучения выпускников посылали в другие страны для лингвистической практики. После вскрытия первого шифра их жалование удваивалось. Кроме того, для молодого человека открывалась перспектива стать квалифицированным специалистом, который за достигнутые успехи получает аудиенцию у монарха со всеми вытекающими отсюда привилегиями.

Хорошую возможность взглянуть на достижения венского «черного кабинета» дают воспоминания барона Игнаца Коха, который руководил им с 1749-го по 1763 годы. Например, 4 сентября 1751 года

он послал австрийскому послу во Франции некую дешифрованную корреспонденцию, позволявшую, по его словам, «гораздо лучше понять основные политические принципы, которыми руководствуется правительственный кабинет во Франции». А еще через две недели он написал: «Это восемнадцатый шифр, который мы вскрыли в течение года... К сожалению, нас считают чересчур способными в этом искусстве, и мысль о том, что мы можем вторгнуться в их корреспонденцию, побуждает иностранные дворы непрерывно менять ключи, иначе говоря, посылать каждый раз более трудные в смысле дешифрования сообщения» [Кан 2004, с. 153]. К достижениям австрийской дешифровальной службы относится чтение шифрованной переписки множества зарубежных правителей, политических деятелей и дипломатов.

В 1812 году Наполеон начал войну против России. Русские дешифровальщики сыграли значительную роль в разгроме его армии. В России достойное внимание службам перехвата и дешифрования уделял еще Петр I, были заметные успехи во времена Елизаветы и Екатерины II. Регулярное чтение французской дипломатической переписки началось с середины XVIII века. В конце XVIII – начале XIX века российские спецслужбы активно проводили мероприятия по добыванию шифров противника и защите своих собственных секретов. Вот несколько примеров.

В конце XVIII века секретарь российского посольства в Париже Мешков завербовал одного из чиновников МИД Франции. Были получены шифры и ключи к ним, которыми пользовался министр иностранных дел Франции граф Монморси и французский поверенный в делах в России Жене. В результате Россия получала секретную информацию длительное время.

Большое внимание уделялось вопросам защиты собственной информации. Так, в январе 1800 года канцлер России граф И.Остерман приказал русскому послу в Берлине вывести из действия шифр («генеральную цифирь») 1799 года, поскольку возникло подозрение в его компрометации. Этот шифр мог быть утрачен вместе с багажом одного русского генерала во время революции во Франции. Аналогичное подозрение вынудило вывести из действия шифры послов России в Мадриде и Лиссабоне. Одновременно были высланы новые шифры [Кан 2004], [Соболева 2002].

В том же году русская разведка продемонстрировала возможность использования контролируемых каналов связи не только

для «пассивного дешифрования» но и для активного навязывания сообщений, содержащих нужную руководству страны информацию. В марте 1800 года министр иностранных дел Панин писал из Петербурга русскому послу в Берлине: «В нашем распоряжении есть шифры, с помощью которых переписывается король Пруссии со своим поверенным в делах в России. В случае, если у Вас возникнут подозрения в вероломстве министра иностранных дел Пруссии графа Кристиана фон Хаунвитца, то ваша задача будет состоять в том, чтобы под каким-то предлогом заставить его написать сюда письмо по интересующему нас вопросу. И сразу же как только будет дешифровано его письмо или письмо его короля, я проинформирую Вас о содержании» [Кан 2004, с.199].

Теперь рассмотрим организацию криптографической службы Российской империи накануне Отечественной войны 1812 года. В начале XIX века в России была произведена реорганизация органов управления страной. Манифестом императора Александра I от 8 сентября 1802 года вместо коллегий (созданных еще Петром I) учреждались министерства. Были учреждены и новые высшие органы управления страной - Государственный совет и Комитет министров. В частности, было организовано министерство иностранных дел (МИД), руководителем которого был назначен граф А.Р. Воронцов (одновременно он был назначен государственным канцлером, т.е. премьер-министром по-современному). Канцелярия МИД содержала четыре основные экспедиции и три секретные. Первая секретная – цифирная (шифровальная), вторая – цифирная (дешифровальная), третья – газетная (служба перлюстрации). Позднее экспедиции стали называться отделениями. Управляющий канцелярией МИД фактически руководил криптографической службой, он «назидает вообще, ко всем экспедициям; за порядком архива и регистрацией; ему поручается хранение цифирных ключей и весь внутренний порядок канцелярии, а также сношение с директором почт, переписка с нашими министрами вне государства» [Соболева 2002, с.185]. С 1808 года канцелярией МИД руководит А.А. Жерве. Шифровальным отделением руководит Х.И. Миллер, дешифровальное отделение возглавляет Христиан Бек. Напряженная политическая обстановка требовала составления и ввода в действие новых шифров и такая работа проводилась. Вот письмо управляющего канцелярией начальнику первого цифирного отделения от 8 марта 1812 года [Соболева 2002, с. 187]:

«Г. Канцлеру угодно, чтобы Вы, милостливый государь мой, Христиан Иванович, немедленно занялись составлением двух совершенно полных лексиконов как для шифрования, равно как и дешифрования (в данном случае правильно применять термин «расшифрование» - авт.) на русском и французском языках, и чтобы Вы снеслись по сему предмету с Александром Федоровичем Крейдеманом, стараясь соединенными силами работу сию к скорейшему и успешнейшему окончанию.

А. Жерве».

Речь в письме идет о требовании составления двух новых кодов. Этой работой занимались в отделении, кроме упомянутых в письме Х.И. Миллера и А.Ф. Крейдемана занимались еще ряд сотрудников. В XIX веке российская шифровальная служба использовала достижения технического прогресса. Составленные специалистами шифры не переписывались как ранее, а печатались, для чего в первом цифрном отделении имелась литография. Обычно шифры классифицировались на общие и индивидуальные. Общие шифры предназначались для нескольких корреспондентов, как правило, расположенных в одном географическом регионе. Они обеспечивали им связь между собой и с «центром». Индивидуальный шифр предназначался исключительно для связи с центром. Идея такого разделения получилась еще при Екатерине II. Несколько позже в МИД был организован цифрный комитет, в состав которого вошли наиболее опытные и квалифицированные специалисты-криптографы. В задачи комитета входили разработка, анализ стойкости и введение новых систем шифрования, контроль за правильным использованием и хранением криптографических документов; вывод из действия устаревших или скомпрометированных шифров; составление заключений, отчетов и докладных для руководителей МИД и императора по вопросам деятельности шифровальной и дешифровальной служб. Комитет подчинялся непосредственно министру, а возглавлял его "главный член цифрного комитета" [Соболева 2002, с.189].

Большое значение руководство Российской Империи придавало организации быстрой и надежной связи. В 1781 году управление всей внутригосударственной почтой России сосредоточилось в одном ведомстве - Санкт-Петербургском почтамте, или почтовом департаменте, подчинявшемся Коллегии иностранных дел, а в 1802 году, причисленном к Министерству внутренних дел.

Передача информации осуществлялась по почтовым трактам (к концу XVIII века их общая протяженность составляла 33 тысячи верст). При этом правительственная корреспонденция перевозилась специальными курьерами, а ведомственная и частная - почтальонами. Для повышения эффективности доставки правительственной, дипломатической и военной корреспонденции 17 декабря 1796 года указом императора Павла I был создан Фельдъегерский корпус. Корпус стал специальной воинской частью, предназначенной для несения службы связи и выполнения особых поручений императора.

Штат корпуса в соответствии с императорским указом состоял из 1 офицера и 13 фельдъегерей. В дальнейшем он неоднократно увеличивался. Учитывая особенности выполняемых задач (доставка наиболее важных и срочных документов, исходящих от императора, членам правительства, военачальникам и другим должностным лицам в столице и на регионах и от них - в его адрес; сопровождение при поездках по стране и за границу императора, членов императорской фамилии и их зарубежных гостей; перевозка денежных сумм и государственных ценностей и т.д.), Фельдъегерский корпус был укомплектован в основном за счет личного состава особой кавалерийской части придворного назначения - кавалергардов, а также унтер-офицеров гвардейских Измайловского, Преображенского и Семеновского полков. При первом комплектовании корпуса особое внимание уделялось внешнему виду и физическим данным зачисляемых на фельдъегерские должности, а впоследствии от них стали требовать также знания иностранных языков [Астрахан, 1996], [Трифанов 1994].

К началу XIX века корпус состоял из 4 офицеров и 80 фельдъегерей. Все они подчинялись дежурному генералу Главного штаба. Благодаря высокой скорости передвижения (по хорошим дорогам 400 верст в сутки) доставка документов при помощи фельдъегерской связи была наиболее быстрой и надежной. Для охраны фельдъегерей обычно назначался один солдат, а при доставке особо важных депеш и грузов - специальный конвой [Астрахан, 1996].

26 января 1808 года Фельдъегерский корпус, указом императора Александра I был переведен в подчинение военному министру. Это способствовало более четкой организации его служебной деятельности, установлению воинского порядка и укреплению дисциплины среди личного состава. Передача корпуса в Военное ведомство сыграла положительную роль в установлении

единообразия требований при работе с корреспонденцией и исполнения служебных обязанностей фельдъегерями в поездках за границу. Именно фельдъегери выезжали с различными поручениями императора и правительства во многие страны не только к российским дипломатам, но и к главам иностранных государств. Фельдъегери обеспечивали доставку правительственной корреспонденции и внутри страны. Для обеспечения оперативности связи чины корпуса несли дежурство в резиденции императора - Зимнем дворце, в Военном министерстве, Главном штабе, Министерстве иностранных дел, Кабинете его императорского величества, Государственном совете, Сенате, Комитете министров. Чтобы правительство своевременно получало информацию о положении в армии, широко практиковалось прикрепление офицеров и фельдъегерей корпуса к командующим войсками во время военных действий. Особо важные документы, адресованные в Действующую армию, срочно доставляли фельдъегери, которые постоянно дежурили в Главной квартире императора. Так, перед войной 1812 года фельдъегери из Санкт-Петербурга преодолевали расстояние до Вильно за трое суток, доставляя пакеты фельдмаршалу М.Б. Барклаю-де-Толли и от него с такой же скоростью в столицу. [Астрахан, 1996], [Трифанов 1994].

27 января 1812 года было введено в действие "Учреждение для управления большой действующей армией". Это был первый в истории отечественного военного искусства устав для управления армиями в военное время, утверждавший схему полевого управления русской армии. Согласно этому документу фельдъегери подчинялись лично главнокомандующему, им предписывалось действовать совместно с генеральскими адыютантами в случаях передачи важнейших приказаний (о выступлении, движении или передислокации и т.п.). Чины корпуса также осуществляли связь со столицей. В сложных условиях войны фельдъегери, прикомандированные к М.И. Кутузову, доставляли исходящую от него корреспонденцию командующим армиями (П.И. Багратиону и М.Б. Барклаю-де-Толли), командирам корпусов, начальникам партизанских отрядов, губернаторам Московской, Калужской, Смоленской и других губерний, министрам и другим корреспондентам, обеспечивая тем самым связь в оперативно-стратегическом звене руководства действующей армии [Астрахан, 1996].

Специальные поручения, которые возлагались на офицеров и фельдъегерей корпуса в период войны и первые послевоенные годы, носили самый разносторонний характер. Так, именно русскому фельдъегерю И.В. Лицынскому было поручено сопровождать Наполеона в ссылку. После доставки бывшего императора Франции на остров Эльба был Лицынский послан с известием об этом к Александру I и к монархам ряда европейских государств [Астрахан, 1996], [Трифанов 1994].

В описываемый период времени активно велась дешифровальная работа. «Черный кабинет» России, сосредоточенный в МИД, совершенствовал методы, технику перехвата и перлюстрации сообщений иностранных государств. На почтамтах были созданы профессиональные службы по перехвату и перлюстрации дипломатической переписки, разрабатывались методы быстрого копирования, перлюстрации без улик (подделка печатей и т.д.), оперативного ознакомления с содержанием сообщений и передачи их дешифровальным органам.

Можно сказать, что русская криптографическая служба была готова к войне, и с ее началом появились значительные успехи. В ходе военных действий русские дешифровальщики вскрыли не только простейшие шифры для связи с небольшими подразделениями, но и Большой и Малый шифры Наполеона. Несмотря на то, что эти шифры являлись недостаточно стойкими, французы им полностью доверяли. Они не верили в интеллектуальные способности российских дешифровальщиков и считали, что в России даже слабые шифры будут обеспечивать тайну переписки. История показала, что они сильно ошиблись.

Российский император Александр I (см.рис. 4.6) обильно цитировал переписку Наполеона и его генералов. В частности, в одной из своих работ американский историк Флетчер Пратт приводит выдержку из разговора, состоявшегося между Александром I и командующим одного из корпусов армии Наполеона – маршалом Макдональдом: «Конечно, – сказал император России Александр, – нам очень много помогало то, что мы всегда знали намерения вашего императора из его собственных депеш. Во время последних операций в стране были большие недовольства, и нам удалось захватить много депеш». «Я считаю очень странным, что Вы смогли их прочесть, – заметил Макдональд, – кто-нибудь, наверное, выдал вам ключ?» Александр возмутился: «Отнюдь нет! Я даю вам честное слово, что

ничего подобного не имело места. Мы дешифровали их» [Пратт, 39, с.51-52]. Наши криптоаналитики могли гордиться тем, что их достижения пропагандировал сам император.



Рис. 4.6. Александр I **Нет ссылки в тексте на этот рис стр 151**

Ни в коей мере не умаляя заслуг отечественных дешифровальщиков, следует отметить, что в некоторых случаях в их руки действительно могли попадать ключевые документы. Такая возможность объясняется тем, что в тылу у французов шла широкомасштабная партизанская война. В боевых действиях в тылу противника принимали участие не только отряды вооружившегося гражданского населения, но и регулярные воинские подразделения, состоящие из гусар (здесь, безусловно, следует упомянуть

легендарного партизана и знаменитого поэта Дениса Давыдова) и казаков (см. рис.4.7). Эти подразделения, фактически, явились предшественниками современного спецназа. Они нападали не только на фуражиров и небольшие отряды противника, но и совершали лихие рейды по тылам французов. Нередко они захватывали высокопоставленных офицеров и даже целые штабы и добывали таким образом ключи к французским шифрам.



Рис. 4.7 Денис Давыдов

Нет ссылки в тексте на этот рис стр 153

Нельзя не отметить еще один крайне важный аспект деятельности партизан, оказавший существенную помощь российским криптоаналитикам. Именно «эскадроны гусар летучих» занимались перехватом курьеров, осуществлявших связь между подразделениями наполеоновской армии, и поставляли материал для работы дешифровальщиков.

Великий русский полководец М.И. Кутузов (см.рис. 4.8) отдавал должное перехвату и криптоанализу сообщений противника еще до нападения Наполеона на Россию. Так, находясь вместе с русской армией, действующей за пределами России (ноябрь 1805 года), Кутузов получил перехваченные и дешифрованные письма Наполеона и его маршала Л.Бертье к австрийскому императору Францу I. В это время Австрия, напуганная победой Наполеона под Аустерлицем, пыталась тайно войти в сговор с Францией. Если бы это случилось, то Россия лишилась бы мощного союзника и должна была пересмотреть свою стратегию в войне. Но были нужны доказательства

тайного сговора. Изучив полученные письма, Кутузов сообщал Александру I: «Теперь я имею все основания считать, что существуют переговоры между Австрией и Францией» [Жилин 1974, с. 59]. Факт предательства Австрии был подтвержден.



Рис. 4.8. М.И. Кутузов **Нет ссылки в тексте на этот рис стр 153**

О важности перехваченной и дешифрованной переписки французов указывает следующее сообщение М.Кутузова к командующему одной из русских армий адмиралу П. Чичагову (от 30 октября 1812 года): «Господин адмирал! Для большей уверенности посылаю еще раз вашему превосходительству достоверные подробности, почерпнутые из переписки, вплоть до писем самого Наполеона, копии с которых я вам уже отослал. Из этих выдержек Вы увидите, господин адмирал, как в действительности ничтожны те средства, коими располагает противник в своем тылу в части продовольствия и обмундирования...» [Кутузов 1989, с.403].

Приведем еще один пример важности перехваченной депеши противника. 5 октября 1812 года отряд полковника М.Кудашева во время боя у Тарутино захватил предписание маршала Франции Бертье одному из французских генералов. В нем говорилось об отправлении всего тяжелого снаряжения французской армии на Можайскую дорогу. Это позволило Кутузову принять правильное решение. Он отказался от преследования разбитого авангарда

маршала Мюрата и сосредоточил основные силы на Калужской дороге, перекрыв тем самым путь французов на юг. Французы были вынуждены отступать по Смоленской дороге, местность вокруг которой была разграблена ими ранее. Тем самым, французы были лишены продовольственного снабжения в ходе отступления.

Действие российских конных отрядов в тылу французов очень беспокоили Наполеона. Французский генерал А. Коленкур, постоянно находившийся рядом с Наполеоном, вспоминал: «Император был очень озабочен и начинал, без сомнения, сознавать затруднительность положения, тогда как до сих пор он старался скрыть это даже от себя. Ни потери, понесенные в бою, ни состояние кавалерии и ничего вообще не беспокоило его в такой мере, как появление казаков в нашем тылу» [Кудрявцев 2002, с. 467].

Сам Наполеон неоднократно высказывал сожаление о том, что ему не удастся создать разведывательную сеть в тылу русской армии. Конные французские отряды в тылу у русских были бы мгновенно выявлены и уничтожены. Поэтому нужно было вербовать русских на службу Наполеона, что было связано с большими трудностями. Приведем один из примеров неудачной вербовки. В период пребывания Наполеона в Москве был захвачен купец Жданов, не успевший выехать из Москвы. Под угрозой смертной казни ему предложили проникнуть в расположение Русской армии и собрать нужные французам сведения. За выполнение задания Жданову было обещано большое вознаграждение, он «согласился». Прибыв в расположение русских войск, Жданов обратился к генералу М. Милорадовичу и передал ему список вопросов, на которые французы хотели бы получить ответы. Этот список содержал существенную военно-тактическую информацию, и Кутузов, узнав об этом, наградил Жданова медалью. Таких примеров было немало.

Рассмотрим теперь вопрос об эффективности криптографических усилий наполеоновской Франции против России. Использувавшиеся в военных сетях связи российские шифры по сложности их дешифрования были аналогичны французским, однако российское руководство уделяло гораздо большее внимание правильному их использованию. Значительные усилия были направлены на развитие службы перехвата и дешифрования. Полученные из дешифрованных сообщений сведения своевременно передавались командованию армии и высшему политическому руководству, включая царя. Наполеон же находился на захваченной

территории и не имел возможности «партизанского» перехвата сообщений российских военачальников. Вообще, как отмечает Д. Кан, французский полководец определенно не придавал большого значения криптографии. Он целиком полагался на мощь своей «непобедимой» армии и не имел дешифровальной службы в войсках. Она казалась ему бесполезной. Поэтому сведения об эффективном дешифровании французами российских военных депеш в истории отсутствуют. Таким образом, можно утверждать, что российская криптография победила в борьбе с французской.

В заключение данного раздела отметим, что в середине XIX века под давлением общественности были официально запрещены «чёрные кабинеты» в ведущих странах Европы. Бурные политические события середины XIX века привели к ограничению абсолютной власти европейских монархов и их полицейских ведомств. Провозглашенные принципы свободы и равенства были несовместимы с цензурой переписки. Подглядывание и подслушивание якобы противоречили нравственным нормам поведения государств в отношении друг с другом. И эти «кабинеты» везде были закрыты. В июне 1844 года волна протестов со стороны общественности по поводу перлюстрации писем вынудила английское правительство прекратить перехват дипломатической переписки. В Австрии двери венского «черного кабинета» закрылись в 1848 году. А во Франции «черный кабинет», который уже со времен Великой французской революции дышал на ладан, в этот год также прекратил свое существование. Но это была только видимость. Очень скоро руководители государств поняли, что отказ от информационно-криптографической поддержки наносит серьёзный ущерб в плане принятия и реализации эффективных государственных решений. «Чёрные кабинеты» ушли в «подполье» и получили ещё большее распространение. Хотя они действовали неофициально, но очень скоро получили полную, хотя и секретную моральную и материальную поддержку со стороны государства.

Научно-технический прогресс в XIX веке и криптография

До XIX века криптография развивалась скорее как искусство, чем наука. И лишь в XIX веке она начала приобретать качество точной математической науки. XIX век вошел в историю криптографии как пример серьёзного влияния научно-технического

прогресса на развитие криптографии. Во второй половине XIX – начале XX века произошел революционный прорыв в области передачи информации на дальние расстояния. В этот период были изобретены и внедрены в эксплуатацию телеграф, телефон и радио, также были изобретены фотография и возможность записи акустических сигналов (прежде всего речи) на магнитные носители. Эти изобретения оказали огромное влияние на развитие криптографии в данную историческую эпоху. Рассмотрим этот вопрос подробнее.

Телеграф. Люди всегда хотели иметь возможности непосредственного живого общения или передачи важных срочных сведений на значительные расстояния. Самым надежным средством связи долгое время оставались гонцы. Однако изобретались и другие способы передачи информации. Корни современной связи, возможно, находятся в начале истории человечества и при желании можно историю современных телекоммуникационных технологий вывести от первобытного тамтама (Африка), дымовых сигналов (такой способ передачи информации в частности использовали казаки Степана Разина), огня костров и т.д. Такие способы передачи информации уже требовали использования соответствующих кодов. Эти коды позволяли предоставлять информацию в виде, пригодном для передачи по линии связи.

Первое упоминание о неудачном опыте передачи информации на расстояние встречается в древнегреческом мифе о Тесее. Царь Эгей, провожая сына на битву с Минотавром, просил в случае успеха поднять на корабле белый парус, а в случае поражения - черный. Тесей Минотавра убил, но паруса на радостях перепутал, и несчастный отец, увидев на горизонте черный цвет, бросился в море, которое с тех пор зовется Эгейским.

То, что может быть явно отнесено именно к системам передачи сигналов (неэлектрическим) появилось более 2000 лет тому назад. Знаменитый греческий историк Полибий (201 – 120 годы до нашей эры) в своей девятой книге «Всеобщая история» указал способ передачи сведений на расстояние при помощи световой факельной сигнализации из 10 факелов о котором было рассказано выше. Еще ранее в 1200 году до нашей эры Гомер в поэме Илиада сообщает об использовании греками сигнальных костров. Римские войска строили сигнальные пункты, используя некоторые принципы семафорной связи, у них действовали более 3000 вышек для передачи световых сигналов по территории империи. В разных странах для передачи

сигнала между удалёнными местами использовались в пределах визуальной видимости горящие костры (в частности в 1588 году английские передовые наблюдатели сигнальными кострами передали в Англию сообщение о приближении испанской «непобедимой армады»), костровые дымы, зеркала, отражавшие солнечные лучи, семафоры, а при наличии только звуковой связи – сигнальные барабаны, гонги, колокольчики, деревянные и костяные свистки, трубы и даже свистовые языки.

Свистовые языки и сегодня используются мексиканскими индейцами, обитателями островков Канарского архипелага, деревень Северо-Западной Турции, Французских Пиренеев. Свистовые языки, являющиеся “запасными языками”, используются, когда обычная речь не может быть услышана из-за большого расстояния или в присутствии посторонних. При этом выполняется имитация тонального и ритмического рисунка обычной речи с помощью свистов нескольких (чаще всего четырёх) разных тональностей. Дальность акустической связи при этом особенно при использовании слуховых трубок была весьма значительной.

Ещё дальше могла обеспечиваться передача почтовых сообщений голубями. Отметим, что лучшие почтовые голуби в конце XIX – начале XX века летали со скоростью 70-80 км/ч, что для тех времен было очень неплохо. С 700 года до нашей эры передавались сообщения, посылаемые с ручными голубями во время Олимпийских игр в древней Греции. Широко использовалась возможность передачи сообщений голубями в Киевской Руси. Во время русско-турецкой войны 1877-1878 годов с помощью голубей осуществлялась связь между представителями русского командования и болгарскими разведчиками, действовавшими в турецком тылу [Абадшиев, 2006]. В частности, таким образом, была передана информация о наиболее удобном для русских войск месте форсирования Дуная. Голубиная почта активно применялась и в XX веке. Такой способ связи использовали буры во время англо-бурской войны. Активно использовалась связь с помощью голубей во время Первой мировой войны. Использовали голубиную почту не только военные. Так, например, владелец известного английского телеграфного агентства «Рейтер» в 1849 году для получения сообщений из Берлина организовал линию голубиной почты между городами Ахеном и Брюсселем (телеграфной связи между этими городами тогда еще не было) [Виргинский 1984].

Наиболее массовый характер использование голубиной почты приняло во время Второй мировой войны. Голуби имелись на борту многих бомбардировщиков и разведчиков британских ВВС, использовались они в британском военно-морском флоте и сухопутных войсках. Главным же театром боевых действий для английских голубей стали оккупированные немцами страны Европы. Голубиная почта применялась английскими агентами и силами сопротивления для связи с Англией. Для этих целей в годы войны было использовано около 200 тысяч птиц. Немцы высоко оценивали эффективность такого способа связи, для борьбы с голубями создавались специальные команды снайперов, которые отстреливали птиц. Вскоре немцы пошли еще дальше, в странах, где активно действовали силы сопротивления (прежде всего Франции), были созданы подразделения, главным оружием которых были специально обученные ястребы, которые выступали в роли истребителей английских голубей-связников. В годы Второй мировой войны в Великобритании для животных отличившихся в боевых действиях была учреждена специальная медаль всего ей были награждены 60 «братьев наших меньших», более половины из них были именно голуби. Последнее регулярное армейское подразделение голубиной почты было расформировано в одной из европейских стран лишь во второй половине XX века [Гладыш, 2005].

Другими животными, которых использовали для передачи сообщений, были собаки. В русской армии начало применения собак для связи было положено Петром I. Во время военных походов первого российского императора при нем состояла специально обученная собака, которая доставляла на поле боя приказы Петра командирам русской армии и приносила императору ответные донесения. В 1912 году были созданы специальные питомники для обучения собак-связников в лейб-гвардии Измайловском полку (Санкт-Петербург) и лейб-гвардии Гусарском полку (Царское село). В советской армии собаки-связники применялись очень активно, в частности они участвовали в боях на реке Халхин-Гол (1939 год) и Великой Отечественной войне. В период ВОВ собаками было доставлено около 200000 донесений. Во время этой войны собаки использовались и для прокладки проводных линий связи, они размотали 7883 км телефонного кабеля. Весьма широко собаки-связники использовались и в армиях других стран [Гладыш, 2005].

В 1854 году в Лондоне был опробован еще один вид связи – пневматическая почта. Корреспонденция закупоривалась в специальные алюминиевые гильзы, которые перемещались по металлическим трубам, обычно проложенным под землей, при помощи силы воздушной струи. Вот как описывает функционирование подобной системы советский историк В.С. Виргинский: «Воздушные насосы, приводимые в движение паровыми машинами, производили либо сжатие, либо разрежение воздуха в специальных камерах. Последние были соединены с системой подземных труб пневматической почты. Движение гильз по трубам обеспечивалось либо давлением струи сжатого воздуха сзади, либо разрежением воздуха впереди» [Виргинский 1984, с. 218]. Вскоре подобные системы появились в Париже и Вене. В XX веке пневматическая почта получила широкое распространение в разных странах, в основном в различных учреждениях. В 1920-30 годах использовалась пневмопочта и в авиации для передачи сообщений между членами экипажей больших многоместных самолетов (средства голосовой связи были в то время еще очень несовершенны). Кстати в это же время сила сжатого воздуха стала использоваться для шифрования. Известны механические шифраторы, части которых приводились в движение от пневмопривода, принцип действия этих аппаратов был таким же как в пневматических ружьях и пистолетах.

Некоторые простые способы передачи сигналов на расстояние сохранились и в наше время. Так во время боевых действий в Афганистане (1979-1989 годы), воевавшие против советских войск душманы, несмотря на наличие у них современных средств связи, активно применяли для передачи информации дым, зеркала (солнечные «зайчики») и выложенные на холмах и дорогах знаки из камней. Другой пример: сигнализация флажным семафором, до сих пор используется на флоте. Здесь каждое положение рук сигнальщика соответствует одной букве. Таким способом передаётся определённое высказывание (полный аналог текста) с помощью элементарных визуальных сигналов. Но какого бы совершенства не достигли сигнальщики в быстроте передачи и чтении семафорного текста, этим способом невозможно передать более, чем 60-70 знаков в минуту, что примерно в 25 раз медленнее скорости речевого общения собеседников.

Во всех флотах мира используется ещё одно средство оптической сигнализации на расстоянии – флажный код. Существует

и международный код этого типа, в котором помимо нескольких флагов с особыми специальными значениями содержится 26 “буквенных” флагов. Каждой букве латинского алфавита соответствует флаг определённой формы и расцветки. Принципиально таким образом можно составить комбинацию флагов соответствующую любому сложному высказыванию.

Однако этот способ также не обеспечивает необходимой скорости передачи и декодирования сообщений. Поэтому в большинстве случаев используются сигналы из одного, двух или трёх флагов, но при этом каждый флаг или их комбинация соответствуют целой фразе. Для шифровки и расшифровки используются специальные кодовые книги – своды сигналов. Например, сочетание трёх буквенных флагов Р, С и I расшифровывается так: “Вы столкнётесь с большими трудностями при проходе через льды в районе мыса” (для географических названий существуют свои комбинации). Передача текста “по буквам” производится только для совершенно необычных сообщений, и это обстоятельство сигнализируется особым вымпелом над комбинацией флагов.

Однако решающую роль в появлении систем передачи информации на большие расстояния сыграло открытие электричества. В 1729 году английский химик Стефен Грей осуществил передачу постоянного электрического тока по медным проводам на расстояние около 300 футов (≈ 100 м). В 1753 году английский физик Чарльз Моррисон опубликовал в журнале “The Scot’s Magazine” описание по видимому первой системы электрического телеграфа для передачи письменных сообщений с использованием 26 отдельных проводов (для каждой из 26-ти букв), подвешенных на изоляторах с интервалом 20 м. Передатчиком служил электростатический генератор, а на приёме к каждому проводу на нити подвешивался лёгкий шарик из бузины, под которым располагалась полоска бумаги с изображением буквы. При подключении генератора к любой из проволок соответствующая бумажная полоска притягивалась к шарiku. Во втором варианте этой системы предлагался акустический приёмник с колокольчиками, возбуждавшимися искровым разрядом с концов проводов.

Но все же время практического применения электрического телеграфа еще не пришло, в XVIII веке продолжали совершенствоваться оптические методы передачи информации.

Известный английский естествоиспытатель Роберт Гук (1635-1703), автор закона упругости для твердых тел, названного его именем, выдвинул идею визуального телеграфирования. В своем докладе Лондонскому королевскому обществу в 1684 году он предложил вывешивать большие буквы на высоких помостах и разглядывать их в изобретенную к тому времени подзорную трубу. Но идея Гука не была воплощена в жизнь. Во Франции в 1690-х годах пробовали прикреплять буквы к медленно вращающимся крыльям ветряных мельниц, однако успеха эти попытки не имели.

Апофеозом доэлектрических средств связи стал оптический, или семафорный, телеграф. Изобрел его французский механик Клод Шапп (1763-1805). В 1790-91 годах во Франции юные братья Шапп, которые учились в удалённых друг от друга школах, изобрели для визуального общения между собою сигнальную семафорную систему. Первоначально они занялись экспериментами с электростатическим телеграфом, которые оказались неудачными из-за отсутствия в то время линий передач с изоляцией, пригодной для высоковольтной работы слабыми токами.

Уже в 1793 году они установили вблизи Парижа первую коммерческую семафорную систему визуальной сигнализации. Летом 1793 года комиссии Конвента Французской республики была успешно продемонстрирована опытная линия телеграфа длиной 6,5 км с тремя станциями - двумя оконечными и одной промежуточной. Побуквенная передача сообщений обеспечивалась различными механическими движениями "рук" - рычагов на вышке. В 1794 году К. Шапп построил «воздушный телеграф» между Парижем и Лиллем. Первая в мире действующая линия семафорного телеграфа имела длину 225 км, она состояла из 22 станций. По ней 15 августа 1794 года в менее чем за час было передано первое сообщение о том, что республиканскими войсками освобожден город Ле Кенуа. Через две недели, 30 августа, телеграф принес в Париж другую радостную весть о взятии крепости Конде. Новое средство связи сразу же приобрело исключительное значение для республики, вынужденной сражаться с объединенными силами интервентов.

Станция семафорного телеграфа представляла собой следующую конструкцию. Над крышей башни возвышался металлический шест, к которому крепились вращающаяся на оси горизонтальная перекладина длиной 3-4 м. Сооружение напоминало современную телевизионную антенну, только, в отличие от нее, к

обоим концам длинной перекладины были шарнирно прикреплены короткие (1 - 1,3 м) также вращающиеся вокруг своих осей перекладины - линейки. От перекладин в комнату, где сидел телеграфист, были протянуты тяги. Посредством рычагов и блочного приводного механизма телеграфист приводил в движение перекладины. Изменяя положение длинной перекладины и линеек на ее концах, можно было составить ряд фигур. Перекладины, окрашенные в черный цвет, были хорошо видны днем на фоне неба (конечно, не в туманную погоду). Ночью к ним подвешивали зажженные лампы, но вскоре от ночных передач отказались из-за большого количества ошибок. Между городами устанавливали ряд башен на расстоянии 8-12 км одна от другой. Для передачи телеграммы ее надо было сначала закодировать, то есть изобразить ее текст в виде условных положений перекладины и линеек. Эта работа выполнялась специальным кодировщиком. Затем телеграмма передавалась сигнальщику, или, иначе говоря, телеграфисту, который последовательно в соответствии с кодом устанавливал на передающей башне перекладину и линейки в требуемые положения. Телеграфисты всех последующих промежуточных башен повторяли эти комбинации. На каждой станции дежурили двое: наблюдатель с подзорной трубой и телеграфист. На последней (приемной) башне комбинацию записывали и, пользуясь кодом, расшифровывали, после чего телеграмму доставляли адресату. Длинной перекладине придавалось одно из четырех фиксированных положений: горизонтальное, вертикальное, правый или левый наклон под углом 45° . Каждая линейка - правая и левая - могла занимать одно из восьми различающихся на 45° положений относительно перекладины - под углом 45° , 90° , 135° и т.д. В результате получалось $4 \times 8 \times 8 = 256$ фигур, из которых Шапп отобрал 92 наиболее отчетливых. Они обеспечивали возможность передавать двумя сигналами любое из отобранных им 8464 наиболее употребительных слов. Эти слова были записаны в тетради на 92 пронумерованных страницах по 92 пронумерованных слова на каждой. Первый поданный сигнал означал номер страницы, второй - номер слова на указанной странице. При использовании секретной кодовой книги происходило шифрование сообщения. Известно, что Наполеон по достоинству оценил изобретение Шаппа, широко и успешно использовал семафорный телеграф для передачи различных военных приказов. Правда, если верить А. Дюма отцу, то и цифровой код не давал полной гарантии от постороннего

вмешательства. Граф Монте-Кристо за 25000 франков подкупил служащего одной из промежуточных станций семафорного телеграфа и послал фальшивую депешу, в результате чего его злейший враг Данглар потерял миллион франков. Подкупленный служащий передал на последующую станцию не те сигналы, которые появились на предыдущей, а те, что написал ему граф. Главу третьей части четвертой своего знаменитого романа А. Дюма так и назвал "Телеграф".

Изобретение Шаппа назвал "телеграфом", впервые применив это слово к средству связи, в 1793 году один из его ближайших помощников: по одной версии французский офицер Миотт. по другой - брат Клода Игнаций.

Довольно скоро семафорные станции, по виду похожие на большие ветряные мельницы, появились в главных городах Франции, а вскоре распространились по другим странам. В 1795 году оптический телеграф появился в Швеции, в 1802 году в Дании. За ними последовали Италия, Испания, затем Алжир и Египет. На Британских островах в 1796 году был сооружен оптический телеграф по проекту лорда Джорджа Муррея (он во многом уступал телеграфу Шаппа). Интересно отметить, что Англии из-за частых туманов и промышленного смога передачу сигналов нередко приходилось откладывать. В Азии была построена линия в Индии между Калькуттой и Ченором. В Германии вступила в действие правительственная линия семафорного телеграфа Берлин-Потсдам-Магдебург-Кельн-Кобленц-Трир. На трассе протяженностью 750 км была расположена 61 станция. В одной только Франции к 1852 году было сооружено около 5000 км линий оптического телеграфа с 550 башнями для соединения столицы с 28 наиболее крупными городами. Самая длинная из них Париж-Лион-Марсель-Тулон протяженностью свыше 1000 км имела 100 станций. Тысячи людей обслуживали работу станций, которые могли обеспечить передачу сообщений в пределах визуальной видимости (с применением подзорных труб дальность связи составляла до нескольких десятков километров) со скоростью ~15 символов в минуту. При этом стали широко использоваться кодовые книги, построенные таким образом, что целые предложения могли быть представлены всего несколькими буквами-знаками.

Семафорные системы успешно применялись и в Соединённых Штатах в районах Бостона, Нью-Йорка, Сан-Франциско, в том числе и

для контроля движений морских судов. Первая линия длиной 104 км была сооружена в 1800 году между Бостоном и островом Мартас-Вильярд. Любопытно, что в 1840 году конгресс США потребовал обеспечить финансирование семафорной системы от Нью-Йорка до Нового Орлеана, но против этого резко возражал С.Морзе, разрабатывавший систему электрического телеграфа (об этом ниже).

Независимо от братьев Шапп в 1794 году гениальный русский изобретатель И.П. Кулибин сконструировал семафорный (оптический) телеграф и разработал код к нему. Записанный в виде одной таблицы код упрощал работу по передаче сообщений. Это позволяло быстрее передавать нужную информацию. Оптический телеграф широко применялся в России всю первую половину XIX века.

В 1808 году офицер русского военно-морского флота А. Бутаков разработал свою систему семафорного телеграфа. Она успешно была применена в 1810 году и русскими моряками эскадры, действовавшей на Средиземном море под флагом вице-адмирала Д.Н. Сенявина.

В 1824 году между Санкт-Петербургом и Шлиссельбургом была проложена опытная линия семафорной связи (в ту пору их в России называли "горизонтными") по проекту генерал-майора П.А. Козена. Линия проработала до 1836 года. Она служила для передачи сообщений о движении судов по Ладожскому озеру.

Первая правительственная линия оптического телеграфа между Санкт-Петербургом и Кронштадтом (Зимний Дворец-Стрельна-Ораниенбаум-Кронштадт) протяженностью 30 км была оборудована французским инженером Жаком Шато в 1833 году. Интересно отметить, что Шато сумел существенно упростить телеграфный код.

Зимний дворец в 1835 году получил прямую оптическую телеграфную связь с Царским Селом и Гатчиной. Тогда же международные события побудили русское правительство выделить средства для строительства линии оптического телеграфа от Санкт-Петербурга до Варшавы. В течение 1835-1838 годов была сооружена самая длинная в мире линия семафорного телеграфа. Еще год ушел на ее испытания. Официальное открытие линии круглосуточного действия состоялось 20 декабря 1839 года. На линии длиной 1200 км было 149 промежуточных станций в виде типовых башен высотой 21,5 м. с металлическим шестом высотой 3 м., через которые сигнал проходил за 15 минут. Правительственная шифрованная депеша,

состоявшая из 45 знаков, передавалась из Санкт-Петербурга в Варшаву за 22 минуты. В штате линии числилось 1908 человек.

В зависимости от числа промежуточных станций и погодных условий на передачу сигнала по российским линиям оптического телеграфа затрачивалось от двух до 15 минут. По линиям длиной 1000-1200 км депеша из 45-100 знаков передавалась за 22-35 минут.

Оптический телеграф просуществовал в России около полувека примерно до середины 1850-х годов. Он сыграл значительную роль в развитии внутренних коммуникаций как средство оперативного управления исполнительными органами государства в мирное и военное время.

Визуальные семафорные системы по всему миру использовались в течение нескольких десятилетий, одна из последних была выведена из эксплуатации в Алжире в 1860 году. Судьба же самого изобретателя сложилась трагически. В 1805 году Клод Шапп покончил самоубийством, не выдержав организованной против него травли. Его обвиняли в том, что он украл идею своего изобретения у английского министра Эджуорта, якобы уже в 1763 году построившего оптический телеграф для личных нужд между Лондоном и Ньюмаркетом.

Тем временем открытия в области электричества продолжались. В 1800 году итальянец Александр Вольта изобретает первую химическую батарею для генерирования постоянного напряжения и тока. В 1809 году состоялась первая демонстрация электрической телеграфной системы С.Т.Зёммеринга на конкурсе Баварской академии наук с передачей на расстояние 600 м. Использовалась низковольтная система с числом проводов 35 для того, чтобы включить помимо букв цифры. Источником электрических сигналов на передаче служила химическая батарея, а приёмником являлся резервуар с водой, в который погружались золотые электроды. Поступление сигнала сопровождалось появлением пузырьков на соответствующем электроде.

В 1820 году датский физик Христиан Эрстед открывает новые, связанные между собою явления электрического тока и магнетизма. В следующем году английский физик Майкл Фарадей (1791-1867) строит первый электрический генератор (динамомашину) с преобразованием механической энергии в электрическую. Менее чем через 10 лет (1830 год) американский профессор Джозеф Генри демонстрирует действие изобретённого им электромагнита на

железные предметы (примитивный телеграф); из его работ следует понимание им возможностей использования явления электромагнетизма для целей дальней связи.

Первый практически пригодный электромагнитный телеграф был создан российским подданным бароном Павлом Львовичем Шиллингом фон Канштадтом (П.Л. Шиллинг (1786-1837) в течении ряд лет возглавлял цифирную экспедицию (шифровальную службу) МИД Российской империи. Он является изобретателем оригинального биграммного шифра, который более 80 лет использовался для защиты российских государственных секретов), выдающимся ученым и изобретателем. Этот аппарат он публично продемонстрировал в 1832 году. В основе действия этого аппарата находился эффект отклонения магнитной стрелки в результате воздействия электромагнитного поля от электрических проводов. При этом передающий и приемный аппараты соединялись кабелем, состоящим из восьми проводов. Каждый провод при передаче включался своей клавишей. При этом приходилось для передачи одной буквы нажимать по три – четыре клавиши одновременно. На приеме каждый проводник подсоединялся к своему электромагниту с висящей над ним магнитной стрелкой. Если по проводу проходил ток, то стрелка поворачивалась. По набору состояний стрелок восстанавливалась переданная буква. Таким образом, каждая буква кодировалась своим набором нажимаемых клавиш.

В 1828 году прообраз будущего электромагнитного телеграфа был готов и испытан (см. рис. 5.1). Он представлял собой двухпроводный однострелочный телеграф. Аппарат содержал все основные узлы, необходимые для телеграфирования: источник питания — вольтов столб (или столбец, как его называл сам Шиллинг); передатчик, подключавший к каждому из двух линейных проводов то один, то другой полюс батареи; двухпроводную линию; коммутатор, производящий переключение с приема на ожидание передачи; и, наконец, приемник.

Основной частью приемника являлась так называемая астатическая пара стрелок, предложенная французским физиком А.М. Ампером в 1821 году для устранения влияния земного магнетизма. Две магнитные стрелки укреплялись на общей медной оси и располагались параллельно одна другой. Полюса были обращены в противоположные стороны. Спаренные стрелки подвешивались так, что могли вращаться в горизонтальной плоскости,

причем одна располагалась внутри катушки, состоящей из нескольких сот витков изолированного провода, а другая — вне ее. К шелковой нити, на которой подвешивались стрелки, был прикреплен небольшой диск диаметром около 40 мм. Одна его сторона окрашивалась в черную краску, другая — в белую. В зависимости от направления тока в катушке магнитная стрелка поворачивалась в ту или иную сторону (правую П и левую Л), и телеграфист, принимающий депешу, видел либо черный, либо белый диск. Если ток в катушку не поступал, то диск был виден ребром. Внизу располагался сосуд с ртутью, гасящий колебания астатических стрелок и приводящий их в первоначальное положение по окончании действия электрического тока.

Для передачи латинского алфавита и цифр Шиллингом был разработан специальный код из комбинаций разного числа (от одного до пяти) последовательных сигналов, посылаемых током разного направления. Однако подобный код оказался чересчур неудобным: для распознавания каждой буквы требовалось запоминание всей комбинации обозначающих ее последовательных сигналов. Например: для буквы А — П, Л; для буквы М — Л, П, Л; для цифры 5 — Л, П, П, Л, Л и т.д. Процесс телеграфирования происходил очень медленно.

Решение проблемы принес шестистрелочный телеграф в сочетании с более рациональным кодом. Передача всех букв русского алфавита обеспечивалась отклонением в разные стороны одной или двух стрелок из шести. Цифры обозначались отклонением трех стрелок из шести. Были разработаны единый передатчик с восемью парами белых и черных клавиш (одна пара служила для посылки вызова и одна пара являлась общей) и единый приемник с семью стрелками, смонтированными на общей раме (одна стрелка обозначала наличие вызова). Линейная часть устройства состояла из восьми проводов, включая вызывной и общий обратный. Для передачи латинского алфавита достаточно было пяти стрелок и пятизначного кода.

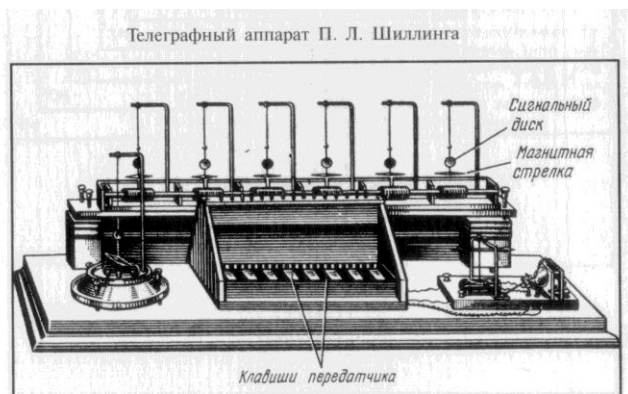


Рис. 5.1 Телеграф Шиллинга **Нет ссылки в тексте на этот рис стр 167**

Первая публичная демонстрация телеграфа Шиллинга происходила 9(21) октября 1832 года. Передатчик был установлен на одном конце этажа, а приемник — на другом, в рабочем кабинете Шиллинга, на расстоянии немногим более 100 м. Первая телеграмма, состоящая из десяти слов, на глазах у присутствующих была принята по электромагнитному телеграфу лично П.Л. Шиллингом моментально и верно.

Несмотря на большой интерес общественности к новому изобретению, правительство не торопилось с его внедрением. Только в 1836 году в России был, наконец, образован под председательством морского министра "Комитет для рассмотрения электромагнитического телеграфа", предложивший Шиллингу установить телеграф в здании Главного Адмиралтейства с целью длительных испытаний его в условиях, близких к эксплуатационным. Аппараты располагались в противоположных концах длинного здания, провода были проложены частично под землей, частично под водой. Но из-за неполадок линия так и не была введена в действие. В мае 1837 года комитет предписал Шиллингу устроить телеграфное сообщение между Петергофом и Кронштадтом, для чего составить проект и смету. Выполнить задачу ученый не успел, так как летом 1837 года П.Л. Шиллинг скончался.

В 1837 году была продемонстрирована телеграфная установка Гаусса-Вебера-Штейнхайля, использовавшая всего лишь 2 провода. Буквы представлялись последовательным кодом из положительных и

отрицательных электрических сигналов, причём ноль обозначал пробел между символами. Длинный пробел из нулей указывал на разрыв между кодовыми словами.

В 1838 году американским инженер и художник Сэмюэль Ф.Б.Морзе (1791-1872) получил свой первый патент на работоспособный электрический телеграф; ему принадлежат идеи применения ручного ключа для прерывания тока и передачи сообщений по проводам посредством последовательной кодовой системы, использующей в роли элементарных символов коротких и длительных посылок тока.

В 1843 году был предложен эффективный последовательный код переменной длины Вейла-Морзе, в котором ускорение передачи обеспечивалось согласованием длины кодовых слов с частотой появления соответствующих букв в английском языке, т.е. самые короткие кодовые символы присваиваются наиболее часто используемым буквам (например, наиболее частой букве “Е” соответствует символ “точка”, букве “Т” – “тире”, букве “А” – “точка-тире”, букве “І” – “точка-точка”, а редким буквам “Х” и “Z” соответственно “тире-точка-точка-тире” и “тире-тире-точка-точка”. Математическая теория связи, разработанная спустя 100 лет, установила, что код Морзе не более, чем на 15% отличается от теоретически достижимого предела.

В 1844 году С. Морзе передал первую телеграмму по проводному телеграфу, своей конструкции: «Вот что сотворил Бог!». При этом Морзе использовал специальную азбуку для кодирования букв, получившую название «азбуки Морзе». Многие «старые» шифры стали непригодными для использования на телеграфных линиях связи. Так, например, экзотические замены букв на замысловатые знаки (например, пляшущих человечков из знаменитого рассказа А. Конан-Дойля) оказались принципиально неприемлемыми.

Уже в 1845 году **С. Морзе** **исправилНЕ ЧИТАЕТСЯ** опубликовал коммерческий код под названием «Словарь для тайной корреспонденции; приспособлен для применения на электромагнитном телеграфе Морзе». Для обеспечения безопасности предлагалось применять код с перешифровкой, легко реализуемый на телеграфных линиях связи. В последующем развитие шифровального дела и создание механических шифровальных устройств шло с учетом использования их в телеграфной связи.

Хотя П.Л. Шиллинг опередил Морзе в создании телеграфа на 12 лет, электромагнитный телеграф Морзе оказался более удобным в практической реализации и именно он получил широкое распространение.

В 1850 году российский инженер Б.С. Якоби буквопечатающий телеграф. Однако, как и в случае с телеграфом Шиллинга всемирное распространение получил другой аппарат – буквопечатающий телеграф англичанина Д.З. Юза, созданный им в 1855 году. В 1875 году появился телеграфный аппарат Бодо с использованием 5-значного кода фиксированной длины. Операторы работают на передатчике с пятью клавишами, комбинация которых нажимается после получения синхронизирующего акустического сигнала от аппарата.

Примерно с 1848 года телеграфия становится большим бизнесом и занимает центральное положение в технике электрической связи. Поскольку телеграфные передачи стоили недёшево, и эта стоимость определялась количеством букв передаваемого сообщения, то сразу же были предложены эффективные методы «сжатия» информации — несекретные телеграфные коды, в которых буквы, слова, фразы «сжимались» до коротких буквенно-цифровых единиц передаваемого текста. Однако при передаче секретных сообщений помимо такого несекретного кодирования по необходимости должны были использоваться шифры (шифрование кодированного сообщения). Особенно остро вопросы стоимости телеграфного послания встали в 1866 году после прокладки трансатлантического кабеля (США - Европа).

Телеграфная передача сопряжена с неизбежными искажениями сообщения в линии связи. Поэтому появилось новое направление в кодировании - помехоустойчивое кодирование. За счет избыточности, вводимой в передаваемое сообщение, на приемном конце появлялась возможность устранить эти искажения. Одновременно увеличилось внимание к такому свойству шифров, как помехоустойчивость. Одной из самых неприятных ситуаций, связанных с искажениями, является ситуация, когда на приемной стороне воспринимается текст иного содержания. Приведем исторические примеры, связанные с использованием «азбуки Морзе».

Выпадение одной точки в сообщении, соответствующей букве «Е» (Е=.) превращает французский глагол *citerons* («мы укажем») в слово *citrons* («лимоны»). Увеличенный пробел в букве М (М= - -)

превращается в биграмму ТТ (Т= -). При таких искажениях получаются слова, по смыслу далекие от оригинала. Например, слово baneful («губительный»), имеющее в азбуке Морзе вид: -.-... .---.-...-.-.. может превратиться в слово dutiful («обязательный»): -.. ..-.-.. ..-.-.-.-.. Такие искажения приводили к дезинформации приемной стороны и порождали серьезные негативные последствия. Так, в 1887 году один торговец шерстью в США направил своему агенту телеграмму с указанием продать большой объем шерсти и затем ждать дальнейших указаний. Обмен посланиями был защищен разработанным торговцем собственным секретным кодом, в котором шифробозначения букв также имели вид азбуки Морзе. В процессе обмена сведениями в результате искажения слово «продай» превратилось в слово «купи»; такое указание получил агент и выполнил его. В результате торговец потерял несколько десятков тысяч долларов. Он подал в суд на телеграфную компанию. Его иск был удовлетворен своеобразным образом: компанию обязали выплатить торговцу стоимость искаженной телеграммы (чуть больше одного доллара).

Из-за искажений иногда при передаче сообщений по телеграфу возникали почти непреодолимые трудности. Для иллюстрации приведем один эпизод, имевший место в конце русско-турецкой войны 1877-1878 годов.

25 января 1878 года передовой отряд русской армии под командованием генерала Чернушова вошел в город Гюмюрджина (в Западной Фракии на территории современной Греции). Начальником штаба этого отряда был подполковник Сухомлинов, будущий министр обороны Российской Империи. В тот же день он отправился на телеграф.

Турецкая сторона была обеспокоена тем, что русские взяли Гюмюрджину. В частности, турки боялись, что русские уничтожат телеграфную станцию. Они стали присылать на телеграфную станцию занятого русским отрядом города сообщения о заключении перемирия. Однако Сухомлинов потребовал подтверждения. Уже глубокой ночью удалось установить связь с городом Чорлу, занятым русскими войсками. Тогда Сухомлинов сделал запрос: «Кто из русских генералов находится в Чорлу?» Ответ был: «Двое русских пашей, одного называют Скобелев. Однако утром Скобелев уехал вперед, а есть другой паша с очень трудной фамилией». Вопрос: «Нельзя ли сообщить ее?» Отвечают: «Невозможно».

- «Почему невозможно»?
- «Слишком много непроизносимых шипящих звуков».
- «Неужели даже и для турецкого языка невозможно!»
- «Невозможно».

После такого ответа возникло подозрение, что турки врут. Сухомлинов попросил сообщить, какой частью командует этот генерал. Был получен ответ: «Он командует какою-то частью с номером 30-м на погонах». Тогда, наконец, стало ясно, что это генерал Шнитников. Передовой русский отряд провел ночь в довольно опасных условиях в двухстах верстах от ближайших частей своей армии и, фактически, в окружении превосходящих сил противника. С генералом Шнитниковым удалось связаться только утром 26 января. От него пришло подтверждение о перемирии, которое было заключено 19 января [Крестовский, 1879].

Такого рода искажения приводили к необходимости принимать меры защиты. Наиболее важные места сообщений дублировались, что приводило к увеличению расходов на связь. Использовали так называемый «двухбуквенный дифференциал»: ключевые слова должны были отличаться друг от друга не менее, чем двумя буквами. Это приводило к появлению большого числа неологизмов — слов, не являющихся общепринятыми в данном языке (т.е. вырабатывался телеграфно-кодовый язык, имеющий вид жаргонных кодов). Наконец, начали применяться помехоустойчивые коды, позволявшие обнаруживать и устранять искажения. Но это опять привело к удорожанию связи.

Учитывая повышенные требования к точности передачи шифрованных телеграмм, телеграфные компании повысили цену за их передачу. Телеграфисты утверждали, что они вынуждены тщательно и побуквенно передавать нечитаемые тексты, что существенно снижало эффективность их работы по сравнению с передачей обычных «осмысленных» сообщений. В ответ пользователи шифров попытались придать шифрованному (кодированному) сообщению «осмысленный вид» (хотя бы на уровне имеющихся в шифртексте «слов»). Поэтому в 1889 году в Лондоне была проведена специальная конференция, посвященная толкованию понятия «шифрованная телеграмма». Наконец, в 1890 году конференция в Париже ввела в обращение официальный словарь кодового языка, содержащий лишь «читаемые слова». Этот словарь вызвал бурю протестов, поскольку, по существу, запрещал передачу секретных (шифрованных)

сообщений. Участники конференции в Лондоне в 1903 году отказались от единого словаря. Было разрешено применять искусственные слова, но при условии, что они будут состоять из «читаемых и произносимых слов» и их длина не будет превышать 10 букв. И все же в 1932 году на конференции в Мадриде все ограничения по кодированию и шифрованию были сняты.

В 1904 году в Англии появился словарь Уайтло для кодобозначений; по утверждению автора, он содержал 400 миллионов произносимых слов. Слова имели вид FREAN, LUFFA, LOZOI, FORAB и т.д., т.е. все слова были пятибуквенными. Уайтло допускал соединение слов для обозначения нового словообразования. Идею Уайтло уже в 1905 году поддержал и развил Э. Бентли, создавший универсальный 5-буквенный код для телеграфных сообщений. Разбиение шифртекстов на пятибуквенные сочетания дошло до наших дней. Также «нормированные» по длине коды вытеснили коды, полностью основанные на использовании словарных величин.

Почти каждая промышленная или коммерческая компания разрабатывала секретные коды для собственных нужд. Появились коды торговцев автомобилями, коды банкиров, биржевых маклеров и т.д., что вызвало создание специальных профессиональных «криптографических групп», которые «по заказу» составляли секретные коды для пользователей с учётом их профессионального языка. Такие коды стоили достаточно дорого, они стали обычным рыночным товаром. Составляемые ими кодовые книги по объему были сравнимы со словарем английского языка. Появился рынок торговли кодами. При этом возникли и разноязычные коды, т.е. коды, предназначенные для корреспондентов, говорящих на разных языках. Были созданы и многоязычные кодовые книги. Эти коды дошли до наших дней. Сигнал «SOS» (Спасите наши души) во всех странах сегодня воспринимается как просьба о помощи. Современные коды «сжимают» информацию более чем в 10 раз (этот эффект зависит, естественно, от богатства лексики открытого языка). Сжатие передаваемой по техническим каналам связи информации и в наши дни является актуальной задачей. При этом имеются в виду не только экономические аспекты передачи, но и скорость (оперативность) обмена сообщениями. Проблемы наиболее эффективного «сжатия» информации породили новое научное направление в теории связи — математическую теорию кодирования. Сегодня это научное

направление исследований занимает одно из первых мест в теории связи.

Вернёмся к проблемам, порождённым в криптографии появлением телеграфа. Сопряжение аппаратуры шифрования с техникой передающей телеграфные сообщения существенно повысило требования к быстродействию процесса шифрования. Шифрование при непосредственной передаче сообщения должно производиться в том темпе, который диктует телеграфный аппарат.

Телеграфная связь значительно увеличила объем передаваемых сообщений (в том числе и секретных). Потребовалась разработка новых шифров с легкой сменой ключей. Это также стимулировало развитие криптографии. Одновременно, телеграфная связь существенно затруднила перехват сообщений. Оказалось, что перехватить сообщение стало гораздо сложнее (в техническом смысле), чем перехватить гонца с документами или получить документы через почтамты. Конечно, можно было завербовать телеграфиста, но этот путь получения посланий оказался недостаточно эффективным. Поэтому начала создаваться техника тайного съёма информации с телеграфных линий связи. Одновременно возникла проблема обнаружения такого тайного съёма. Однако именно телеграф стал эффективным методом обеспечения оперативной связи между удалёнными друг от друга абонентами в XIX веке. Скорее всего, впервые электрический проводной телеграф для связи в ходе боевых действий был применен русскими войсками во время Крымской войны 1853 – 1856 годов, а первые факты перехвата и дешифрования телеграфной информации имели место в 1861 году во время гражданской войны в США 1861-1865 годов.

В XIX веке применялось, в основном, так называемое, предварительное шифрование сообщений. В этом случае отправитель зашифровывал передаваемое сообщение (в котором шифртекст удовлетворял требованиям телеграфной передачи), а после этого относил зашифрованное сообщение на телеграф. В XX веке такое замедление в передаче сообщений часто оказывалось неприемлемым. Потребовалось разработать методы, так называемой, линейной передачи зашифрованных сообщений; здесь аппарат шифрования (шифратор) встраивался непосредственно в аппаратуру передачи сообщений, так что передача зашифрованного сообщения, в принципе (в техническом смысле) не отличалась от передачи незашифрованного сообщения. В целом, прав американский историк Дэвид Кан,

утверждая, что «свой современный вид шифровальное дело получило благодаря телеграфу» [Kahn, 1967].

Телефон. Попытки передачи речи на дальние расстояния предпринимались еще в глубокой древности. Голосовой акустический телеграф использовался за сотни лет до нашей эры вплоть до сегодняшнего дня на Канарских островах.

В конце XVI века итальянский ученый Джованни Батиста Порта (1538-1615) предложил проложить по всей Италии переговорные трубы вроде тех, что используются на кораблях для связи капитана с машинным отделением. Но современники идею не поддержали.

Такую же идею в 1627 году выдвинул крупнейший английский ученый и философ Фрэнсис Бэкон. В своей книге “Новая Утопия” он предсказал о возможность удалённой голосовой связи по длинным акустическим трубам. Отметим, что Ф.Бэкон будучи лордом-канцлером Англии уделял серьезное внимание шифрам. Он выдвинул ряд требований к ним, остающихся актуальными и сегодня: «Они (шифры – авт.) не должны поддаваться дешифрованию, не должны требовать много времени для написания и чтения и не должны вызывать никаких подозрений» [Бабаш, 2002, с. 73]. Он также предложил оригинальную идею стеганографической защиты информации, опирающуюся на двоичном кодировании букв алфавита и использовании в открытом тексте двух мало отличающихся шрифтов. Бэкон предупреждал о возможных негативных последствиях ошибок в использовании даже весьма надежных шифров. Он писал: «В результате неловкости и не искусности тех рук, через которые проходят величайшие секреты, эти секреты во многих случаях оказывались облеченными слабейшими шифрами». Другими словами, даже сильный шифр в плохих руках не обеспечивает надежной защиты секретов.

В начале 2001 года в Свердловской области была обследована интересная церковь, построенная в XVIII веке. Построил церковь известный промышленник А. Демидов. Церковь высотой более 50 метров напоминает знаменитую Пизанскую башню: отклонение вершины куполов от вертикальной оси составляет более двух метров. Выяснилось, что именно так она и была построена. При детальном ее обследовании была обнаружена так называемая “слуховая камера”, предназначенная для проведения конфиденциальных разговоров. Одновременно был обнаружен замаскированный акустический ход в

соседнюю камеру. Находясь в ней, каждый мог легко прослушивать переговоры в “слуховой камере”, ведущиеся даже шепотом. Возможно, А. Демидов и подслушивал эти переговоры.

Термин “телефон”, составленный из греческих слов “теле” (далеко) и “фон” (звук), употреблялся ещё в XVIII веке. Первые телефоны механического действия передавали речь в её естественной акустической форме по, шнурам, проволоке, трубам, рельсам, с использованием мегафонов и звуководов, но результаты чаще всего были малоприемлемыми.

Так, например, по утверждению газеты “Петербургский листок” опыты с прототипом телефона, носившего название “телелог”, происходили 2 января 1799 года. Изобретатель, имя которого не сохранилось для истории, обратился в муниципальный совет Парижа и заявил о создании аппарата, позволяющего услышать человеческий голос на расстоянии от Марсова поля до Люксембургского сада. Администраторы города сочли это невозможным и поместили изобретателя в дом для сумасшедших. Друзья «умалишенного» всё-таки устроили пробу аппарата, но с плачевными результатами. Когда на Марсовом поле говорили в трубу аппарата, в Люксембургском саду вместо отдельных слов был слышен только пульсирующий шум.

В этом механистическом, доэлектрическом периоде дальней связи оставил заметный след исключительно разносторонний английский изобретатель и учёный Чарльз Уитстон. Он занимался речевой акустикой, музыкальными инструментами, электрическим телеграфом, стереографией, криптографией, электрическими измерениями и другой обширной тематикой. По видимому Чарльз Уитстон первый стал использовать такие термины, как «телефон», “микрофон” и «криптофон». Однако в качестве телефона он предлагал систему звуковой передачи по стальным рельсам со скоростью 200 миль в секунду. А микрофоном он назвал прибор для механического усиления слабых звуков, передававших акустические вибрации на оба уха. Ещё юный Ч. Уитстон шокировал английскую общественность, утверждая, что изобретенный им «эконкриптофон» будет способен в будущем транслировать музыку (т.е. доставлять в любой дом подобно газовому снабжению) по всему Лондону, используя тонкие стальные провода в качестве звукопровода.

Один из изобретателей, делавших первые шаги в передаче речи в форме электрических сигналов швейцарец Чарльз Бурсель, был

инженером на французской военной телеграфной станции и занимался усовершенствованием системы передачи, изобретенной Морзе.

Фундаментальная идея об электрической передаче звуковых колебаний по двум проводам с помощью сконструированных им приборов передающего и принимающего была опубликована Ч. Бурселем в 1854 году в журнале “Иллюстрированный Париж”. Предлагавшаяся конструкция устройства, воспринимающего звуковые волны, во многом была подобна будущему микрофону, но прибор для обратного воспроизведения электрического тока в человеческий голос не оправдывал надежд изобретателя. Официальное признание оригинальности его идеи наступило лишь в 1878 году после опубликования результатов, достигнутых в разработке телефонных систем, немецким самоучкой Д.Ф. Рейссом (1834-1874) и американским инженером Александром Грехэмом Беллом (1847-1922), которому и приписана честь первого изобретателя телефона благодаря своевременной подаче патентной заявки совместно со своими партнерами Г.Г.Хаббардом и Т.Сандерсом. Это трио и получило патент США №174465 на “Усовершенствования в телеграфии”, опубликованный 3 марта 1876 года.

В 1861 году школьный учитель Джон Филипп Рейс закончил свою модель телефона, в передатчике и приёмнике которого использовались пробка, вязальная игла, оболочка от сосисок, кусочек платины. Колебания диафрагмы или мембраны передатчика в некотором соответствии с изменениями звукового давления прерывали контакт в электрической цепи, чем напоминали работу электрического телеграфа. Хотя телефон Д.Ф.Рейса с большими искажениями и воспроизводил некоторые звуки на приёме, но по существу дела был неработоспособным. С акустических позиций этот прибор был способен передавать только низкочастотные пульсации звукового давления, которые передают так называемый основной тон речи. В дальнейшем изобретатель уже не пытался его усовершенствовать.

Александр Белл родился в Эдинбурге (Шотландия) и получил образование в университетах Эдинбурга и Лондона. В 1870-71 годах он последовательно эмигрировал в Канаду и США. Его ранний интерес к исследованиям речи и слуха возможно стимулировался тем фактом, что его мать Элиза была практически полностью глухой.

А. Белл так же, как и его отец был учителем в школе для глухонемых детей и искал средства, которые позволяли бы сделать

звуковые волны видимыми. Интересно, что он тщательно изучал препараты внутреннего уха человека теми же методами, как и Д.Ф. Рейс несколькими годами ранее. Случайно А. Беллу пришла мысль соединить проволочную катушку, размещенную вокруг магнитного стержня с гибкой мембраной. По словам изобретателя у него ушло много времени на создание работоспособной телефонной системы, содержащей два главных элемента – микрофона и воспроизводящего телефона, которые имели похожую конструкцию. В колеблющейся вдоль магнитного сердечника проволочной катушке, воспринимавшей через гибкую мембрану звуковые колебания, индуцировался переменный по амплитуде и частоте электрический ток, который намного быстрее и легче передавался на дальнейшее расстояние в сравнении со звуковыми волнами.

А. Белл видел главное преимущество телефона перед другими электрическими аппаратами в том, что “...все другие телеграфные машины создают сигналы, для трансляции которых необходимы эксперты, и такие инструменты могут иметь лишь ограниченное распространение в то время, как по телефону можно разговаривать любому, кто владеет речью”.

А. Белл столкнулся с такими же проблемами, как и большинство изобретателей средств дальней электросвязи. Несмотря на сенсационную демонстрацию телефона на мировой выставке в Филадельфии в 1876 году в октябре 1877 года в журнале “Scientific American” публикуется описание системы А. Белла с предсказанием не столь быстрого её практического применения. На предложение А.Белла в 1877 году о покупке его патента за 100 тысяч долларов специалисты американской компании Western Telegraph ответили нижеследующим заключением (в кратком переложении).

”Цель изобретения состоит в передаче разговорного голоса по телеграфным проводам. Мы нашли, что передаваемый голос очень слаб и невнятен особенно с увеличением расстояния между передатчиком и приёмником. Мы не видим технической возможности передавать с помощью телефона разборчивую речь на расстояние более нескольких миль.

Господа Г.Г.Хаббард (финансовый спонсор изобретателя) и А.Г.Белл желают установить свои “телефонные приборы” в каждом городе и эта идея представляется идиотской. Зачем некто пожелает воспользоваться этим неуклюжим и непрактичным прибором, когда он может посетить телеграфный офис и послать безупречное

письменное сообщение в любой крупный город Соединенных Штатов?

Электрики нашей компании уже создали все необходимые к настоящему времени улучшения телеграфа и мы не видим причины для поддержки группы аутсайдеров с их экстравагантной и непрактичной идеей. Розовые фантазии мистера Г.Г.Хаббарда основываются на богатом воображении и счастье непонимания реальных технических и экономических фактов ситуации, а также желании игнорировать серьёзнейшие недостатки прибора, являющегося не более, чем игрушкой” [Kahn, 1967].

В 1876 году телеграфные проводные линии в Соединённых Штатах для деловых, коммерческих, правительственных кругов, полиции, противопожарной службы, частной связи составляли 214000 миль, а количество телеграфных офисов достигло 8500. Поэтому для телеграфных компаний “игрушка” А.Г. Белла казалась забавным музыкальным прибором. **ВСЕ ТАК? Все нормально**

Но Белл твердо верил в возможность коммерческого использования его системы. И действительно, несколькими годами позже та же самая компания сделала предложение изобретателю уже 25-ти миллионов долларов за его патент, которое он отверг. Хотя А. Белл известен прежде всего своим телефоном, он был исключительно разносторонним учёным и изобретателем, и даже талантливым пианистом. Также Белл был большим энтузиастом авиации, в начале XX века занимался конструированием самолётов и вертолётов, а в возрасте 75 лет получил патент на самый быстрый в мире гидроплан HD-4. Считается, что в записных книжках А. Белла содержатся полезные идеи, которые и сейчас представляют интерес для современных конструкторов и изобретателей будущей техники.

Более 600 патентов по телефонной тематике было зарегистрировано в последующие 11 лет и многие изобретатели пытались оспаривать первенство Белла. Так, всего лишь с опозданием на три часа запатентовал свой микрофон американский изобретатель Элише Грей. Конструктивно этот микрофон состоял из металлической полоски, одна сторона которой прикреплялась к мембране, а другая погружалась в жидкость. А. Белл использовал оба изобретения и основал “Белл Телефон Компани”, которая за три года изготовила и установила оборудование для пятидесяти тысяч абонентов (телефонная сеть США в 1880 году), а впоследствии стала

крупнейшей в мире телефонной компанией, известной сейчас, как AT&T или “American Telephone and Telegraph Company”.

Большую роль сыграло изобретение Дэвидом Эдвардом Хьюзом угольного микрофона с угольными стержнями и питанием от батарей в 1878 году, который был намного чувствительнее прототипов. Годом позже русский инженер М. Михальский предложил более совершенный угольный порошковый микрофон. Такие микрофоны успешно используется до настоящего времени.

Для вызова телефонных абонентов в 1877 году американский изобретатель Ваден применил электрический звонок, цепь которого замыкалась телеграфным ключом. Позднее Гилеланд предложил использовать индуктор – магнитоэлектрическую машину, вырабатывающую при вращении её приводной ручки переменный электрический ток, достаточный для срабатывания звонка в проводной линии длиной в несколько десятков километров.

В 1880 году А.Г. Белл делает патентную заявку на фотофон – первое устройство защищённой от перехвата скрытной беспроводной передачи речи остро сфокусированным оптическим лучом. В передатчике модуляцию яркости луча осуществляла звуковая мембрана, колеблющаяся вместе с маленьким приклеенным к ней зеркальцем, а отраженный луч от него проходил через специальную частично прозрачную решетку. В приёмнике модулированный луч фокусировался на светочувствительном селеновом элементе, выходной ток которого подавался на звуковую катушку телефона.

Следующий важнейший шаг в 1889 году сделал англичанин Элмон Строуджер. До этого времени все проводные подключения абонентов между собою осуществлялись посредством вызова операторов (обычно “барышень-телефонисток”) на центральной станции, которые вручную через коммутационные доски выполняли требуемые соединения. Изобретение Э.Б.Строуджера, основавшего в 1892 году свою “Strowger Automatic Telephone Exchange Company”, позволило перейти на автоматическое индивидуальное соединение абонентов благодаря применению дисковых номеронабирателей на телефонных аппаратах и декадно-шаговому коммутационному оборудованию на телефонных станциях.

Нелишне отметить, что именно телефонные аппараты компании Э.Б. Строуджера благодаря высокому качеству и громкости звучания предпочитались абонентами правительственной связи СССР на протяжении многих десятилетий.

Начиная примерно с 1880 года, когда все основные элементы телефона были изобретены, он стал доминировать, как средство связи. Телефон обеспечивал быстроту, удобство и живой контакт между абонентами и был доступен широкой публике, не требуя подготовки в применении телеграфных кодов.

Телефонная связь основывалась на передаче непрерывно изменяющихся по амплитуде (аналоговых) сигналов. После 1880 года развивающиеся сети связи создавались в расчёте на осуществление передачи в аналоговой форме, тем более, что появившиеся после около 1920 года усилительные приборы на основе электровакуумных ламп были пригодны для обработки именно аналоговых сигналов.

Цифровая передача (телеграфия) вынуждена была приспособляться под характеристики именно этих сетей. К 1950 годам системы связи в мире были почти полностью аналоговыми, за исключением телеграфных систем, работающих на магистральные подводные кабели, и некоторых специальных систем радиосвязи.

Однако сразу же возникла проблема передачи по телефону конфиденциальной информации. Считается, что первая патентная заявка на телефонный шифратор была сделана главным электротехником Капитолия Джеймсом Роджерсом в конце 1881 года. Он писал: «Мое изобретение состоит в том, что сообщение ... посылается по двум (или более) цепям поочередными импульсами в быстрой последовательности..., так, что тот, кто подключается лишь к одной из цепей, может принимать лишь отдельные неразборчивые сигналы... Две (или более) линии, по которым передаются сигналы речи, могут быть проведены к оконечной станции на значительном расстоянии друг от друга, что таким образом исключает возможность для пытающегося подслушать ... подключиться одновременно к обеим линиям» [Kahn, 1967]. По чисто техническим причинам это изобретение не получило широкого распространения. Однако уже в XX веке аналогичная идея воплотилась в так называемых СИЧ (скачкообразное изменение частоты) передачах, в которых несущая частота быстро меняется в широком диапазоне по некоторому сложному закону.

Вскоре начал использоваться такой метод передачи сообщений, как предварительное шифрование текста с последующей передачей шифрованного текста по телефону. Для борьбы с неизбежными помехами предлагался «классический способ»: буквы передавались в виде коротких слов (чаще – имен): А=Анна, Б=Борис и

т.д. Поскольку у абонентов часто не было возможности использования какой либо аппаратуры или приборов шифрования, то использовались обычно достаточно простые шифры, например, типа квадрата Полибия. Однако здесь появился существенный недостаток: значительно снизилась оперативность связи. Поэтому чаще всего в сообщениях шифровались только отдельные, особо «секретные» слова. Остальной текст передавался открытой речью. Нередко вместо шифрования использовались коды, но указанный недостаток оставался. Достаточно широко использовался «условный язык», жаргонные выражения, иносказания и т.д. При этом защита информации строилась на том предположении, что «условный язык», жаргон, намеки и иносказания будут правильно поняты абонентом связи и останутся непонятными для противника. Приведем пример. В жаргонных кодах, специально разработанных для агентурной связи, были такие слова: БОЛЕТЬ означает «арест» или «заключение под стражу»; БОЛЬНИЦА - тюрьма; ДОКТОР - контрразведка. Тогда сообщение «Майкл арестован контрразведкой. Ему грозит заключение в тюрьму», принимает следующий «невинный» вид: Майкл заболел. Вчера был доктор и посоветовал ему лечиться в больнице». Так же использовались словарные (принцип тот же только зашифрованный текст не является осмысленным) и цифровые коды. Эти способы активно использовались даже во время Второй мировой войны. К тому времени шифраторы для защиты речевого сигнала уже были созданы, но имели большие габариты и массу, поэтому в авиации, передовых подразделениях сухопутных войск, при проведении агентурных операций по-прежнему использовались коды. Так в конце Второй мировой войны американцы связывались со своей агентурой на территории Германии с помощью портативных радиотелефонов, такие системы связи тогда только появились и их небольшие размеры были очень удобны для использования в тайных операциях. Связь осуществлялась в определенное, заранее оговоренное время, через специальный самолет-ретранслятор, так как дальность действия новой аппаратуры была небольшой. Для защиты информации использовался специальный цифровой код, который разведчик должен был выучить наизусть [Кочик, 2006].

Ранее упоминалось, что иногда собеседники прибегали к известному им, но предположительно неизвестному противнику, языку. Например, американцы в обеих мировых войнах XX века использовали практически неизвестные в воюющих странах языки

некоторых малочисленных индейских племен. С этой целью на этих узлах связи работали специально подготовленные представители этих племен. Аналогичным образом поступили ирландские военнослужащие, входившие в 1960 году в миротворческий контингент в Конго – они вели радиопереговоры на гэльском языке (язык малочисленной народности – потомков древнего кельтского населения, проживающих на территории Великобритании и Ирландии) **УЖЕ БЫЛО поправил.** Нередко средством защиты конфиденциальной информации становился такой прием как отказ передачи ее по телефону. К этому средству прибегают и сейчас. Вспомним часто используемые фразы: «Это не телефонный разговор. Поговорим при встрече». Естественно такие способы защиты речевой информации имели существенные недостатки: низкую стойкость, снижение оперативности связи, невозможность массового применения. Поэтому в начале XX века начались исследования по созданию аппаратуры автоматического засекречивания речевого сигнала. Например, было предложено инвертировать частотный спектр: низкие частоты инвертировались и заменялись на высокие; аналогично высокие частоты речи заменялись на низкие. Таким образом, предлагалась реализация шифра инверсной перестановки частот речевой передачи. Технические проблемы такой инверсии были решены достаточно просто. Особо подчеркнем, что в данном случае засекречивается не сам сигнал, а акустический способ его передачи. Такое засекречивание не является стойким, но на заре развития телефонной связи оно казалось достаточно надёжным. Затем появилось предложение о засекречивании частот по принципу шифра Цезаря. Все частоты смещались на расстояние, определяемой ключом. Наконец, появилась идея разбиения частотного диапазона речевого сигнала на интервалы, которые переставлялись по ключевому закону. Эта идея реализуется и сегодня, Однако по современным меркам такая защита не является достаточно надёжной.

Был предложен и другой способ защиты телефонных переговоров. Он заключался в «забивании» сигнала посторонним шумом. Это мог быть просто шум, помеха речевого характера или, например, передача сопровождалась одновременно передаваемой «защищающей» музыкальной мелодией. Зная передаваемую мелодию, приёмная сторона «снимала» музыкальный шум и получала секретную передачу. Способ «зашумления» передачи так же дошёл до наших дней.

В 1893 году сотрудник датской телефонной компании Вальдемар Паульсен (другая транскрипция Поульсен) изобрел магнитную запись. Возможность записи акустического сигнала продемонстрировал еще в 1877 году знаменитый американский изобретатель Томас Эдисон, который изобрел фонограф. Однако аппарат Паульсена имел перед изобретением Эдисона существенное преимущество – на носитель (стальную проволоку) можно было многократно записывать и стирать информацию. В 1898 году Паульсен запатентовал свое изобретение под названием «телеграфон» и на его основе разработал еще один прибор – автоответчик. В мире изобретение Паульсена более известно под названием магнитофон, в разных странах этот прибор подвергался различным улучшениям, с целью повышения качества звучания, уменьшения габаритов и веса (так в начале 1930-х годов вместо проволоки стали использовать пластмассовые магнитные ленты). Практически сразу изобретение Паульсена стало использоваться в криптографической деятельности, в частности для записи перехваченной зашифрованной информации, а также при разработке новых методов защиты речевого сигнала.

В 1900 году сам Паульсен предложил разбивать речь на сегменты, записывать их на магнитофон и воспроизводить их в обратном направлении при передаче (временная инверсия). В 1918 году датский инженер Тигерстедт предложил разбивать речь на временные сегменты и переставлять их во времени (временные перестановки). Суть этого предложения проста. Представим себе, что ваша речь записана на магнитную ленту. Эта лента разрезается на мелкие фрагменты, которые затем «склеиваются» по заранее заданному закону перестановки «отрезков». В этом склеенном виде информация поступает в канал телефонной связи. На приёмном конце, зная правило перестановки, восстанавливается исходное сообщение. В 1920 году русский ученый М.А. Бонч-Бруевич усовершенствовал временную перестановку, введя кадровую структуру преобразований (каждые N сегментов переставлялись по-своему). В 1922 году англичанин Хоу-Гольд предложил применять синхронное изменение несущей частоты передатчика и настройки приемника (для засекречивания радиотелефонной связи). В этот период были сделаны и другие изобретения в области методов засекречивания речевого сигнала, однако серийное производство и применение аппаратуры автоматического засекречивания речевых сообщений началось лишь в 20 - 30-х годах XX века.

В связи с развитием проводной телеграфной и телефонной связи возникла проблема эффективного снятия информации с линий связи. Дело состояло в том, что непосредственное подключение к линии не всегда можно было реализовать тайно. В 1904 году японские спецслужбы впервые в практике радиотехнической разведки реализовали схему дистанционного съёма информации, передаваемой по каналам электросвязи. В 1915 году английский капитан Р. Стэнли (в прошлом профессор Белфастского университета) создал аппарат, который позволял индуктивным способом перехватывать информацию с проводов с расстояния до 100 метров от них. Вскоре удалось создать приемник, «снимающий» эту информацию с расстояния до трех километров. Позднее и немцы, в свою очередь, сконструировали аналогичные аппараты.

Радио. 7 мая 1895 года русский ученый А.С. Попов выступил с публичным докладом на заседании физического отделения русского физико-химического общества, в ходе которого продемонстрировал первый в мире радиоприемник. Уже первые испытания беспроволочного телеграфа на флоте доказали превосходство радио над другими средствами связи. Одновременно с опытами по радиосвязи на флоте подобные работы стали проводиться и в армии. Началом таких опытов нужно считать 1898 год. Именно с этого времени в них участвовал целый ряд армейских телеграфных специалистов.

После испытания в 1900 году сконструированных А.С. Поповым переносных полевых радиостанций на маневрах был сделан вывод, что при помощи радио можно установить связь между высшими штабами на расстоянии 50 верст и более. В 1901 году Попову удалось добиться дальности связи 150 км. Дальнейшие работы по созданию полевых радиостанций в русской армии были продолжены специалистами Офицерской электротехнической школы.

В 1897 радиоприемник запатентовал итальянский изобретатель Гульельмо Маркони (1874-1937). В 1901 году он впервые осуществил успешную передачу радиосигнала через Атлантический океан. В 1906 году также считающийся на Западе “отцом радио” американский инженер Ли де Форест (1873-1961) совершил революционное изобретение, он изобрел электровакуумную усилительную трёхэлектродную лампу, которая на долгие годы стала одним из основных элементов радиоаппаратуры. В 1912-13 годах американец Эдвин Армстронг (1890-1954) усовершенствовал усилительные

возможности радиоаппаратуры (до ~1000 раз) с помощью регенеративной схемы. В 1933 году этот же человек изобрел радио с широкополосной частотной модуляцией.

Итак, человечество получило новый способ связи - радио. Появление радио оказало огромное влияние на криптографию. Многократно увеличались объемы передаваемых сообщений (в том числе и секретных). Потребовалась разработка всё новых и новых шифров для защиты информации. Стали создаваться значительные по числу абонентов сети засекреченной связи, что породило проблему эффективного распределения и смены ключей между абонентами связи. Возник повышенный риск компрометации абонентов (тайного изъятия у них ключевой информации, что, в случае удачи, могло поставить всю сеть под контроль противника).

Вопрос перехвата радиосообщений в техническом смысле уже не представлял принципиальных проблем. Впервые перехват иностранных радиোগрам был организован российскими военными моряками примерно с 1903 года. Во время русско-японской войны 1904-05 годов впервые в мире начала применяться радиоразведка (наблюдение за радиосетями противника, перехват и дешифрование вражеских радиোগрам) и радиоэлектронная борьба (постановка помех с целью срыва радиосвязи противника). Приоритет в использовании этих новых видов боевых действий принадлежит российскому военно-морскому флоту. Теперь работа дешифровальщиков облегчилась, так как информацию, передаваемую по радио, защитить физически не представлялось возможным. Защищаемая сторона, естественно осведомленная о таком положении дел, иногда отказывалась от эффективной радиосвязи и использовала проводной телеграф, а нередко и отправку специальных курьеров. Резко возросли требования к помехоустойчивости шифров, поскольку радиоканал порождал значительно более серьёзные искажения, чем проводная связь. Значительно более актуальным стал вопрос об имитостойкости сети засекреченной связи. Большое количество абонентов сети не исключало возможности внедрения агента в качестве абонента сети; этот агент от имени других абонентов мог давать зашифрованные распоряжения, указания и т.д. другим абонентам сети. Это предположение в дальнейшем подтвердилось и приводило к серьёзным негативным последствиям для «лояльных» абонентов сети связи. Радиосвязь дала импульс к развитию стеганографических методов защиты информации. На фоне

«невинной» передачи (например, музыкального произведения) оказалось возможным передавать секретные послания. Наконец, широкое развитие радиосвязи привело к так называемой «радиоэлектронной войне». Противник, например, мог нанести ущерб сети связи путем постановки мощных радиопомех (для чего нужно было разработать соответствующую технику зашумления). К помехоустойчивости шифров в этих условиях возникли новые повышенные требования. Появилась возможность лёгкого создания «псевдосетей» (ложных сетей связи), отвлекающих силы и средства противника на перехват и анализ «псевдосообщений». Был дан толчок к организации так называемых «радиоигр», когда противнику под видом ценных сведений поставлялась дезинформация.

Радиосвязь оказалась дешевле и мобильнее проводной. Появилась возможность активизировать связь между военными подразделениями, устанавливать связь с подвижными объектами (автомобили, самолёты, корабли).

Резкое расширение объёмов секретных зашифрованных передач и сравнительная простота радио перехвата сообщений подтолкнуло криптографов-дешифровальщиков к мысли о том, что исследование отдельной перехваченной криптограммы необходимо связать с анализом всего массива перехвата, в котором появилась эта криптограмма. Этот путь оказался весьма плодотворным. Как справедливо отмечает Д. Кан, «телеграф создал современное шифровальное дело, радио — современный криптоанализ» [Kahn, 1967].

Скачкообразный рост количества абонентов сетей засекреченной связи привёл к росту количества технических работников шифрслужб, в частности, шифровальщиков. Раньше, при единичных корреспондентах сети секретной связи, шифрование осуществлял обычно сам абонент. Когда же его связи значительно расширились, а шифры усложнились, появилась необходимость «прикреплять» к секретному абоненту операторов-шифровальщиков. Они справлялись с задачами подготовки и передачи секретных посланий значительно лучше, чем абонент, специально не подготовленный для этой работы. Да и отвлекать этого абонента для выполнения сложных для него технических функций передачи информации стало нецелесообразным. Таким образом, появилась массовая подготовка технических сотрудников спецслужб - шифровальщиков. Массовый характер приняли разработка и

внедрение различных механических, (позднее и электро-механических) приборов для шифрования и расшифрования сообщений – шифраторов.

Лавинообразный рост количества секретных сообщений, передаваемых по каналам связи, привёл к значительному росту количества ошибок, допускаемых при шифровании. Дешифровальщики быстро научились их находить и использовать. Родилось новое направление в криптографии (в области дешифрования) - поиск ошибок шифровальщиков с целью их использования при дешифровании. Типичные ошибки - повторное использование ключа шифра, повторное зашифрование открытого текста на другом ключе и т.д. Это привело к разработке «сверхнадёжных» шифраторов и создания технических приспособлений, «блокирующих» ошибки шифровальщика.

Аналогичный вывод относится и к проблеме ненадёжности техники шифрования (шифраторов). Как было отмечено выше, эта техника неизбежно начала возникать одновременно с требованиями обеспечения массовости и оперативности секретной связи. Технический отказ аппаратуры приводил к передаче «слабо зашифрованного» сообщения, что, естественно, немедленно использовалось противной стороной. Кроме того, эти отказы, которые случались нередко, приводили порой к дезорганизации самой системы закрытой связи и вызывали недовольство у пользователей «машинными системами» по сравнению с традиционным шифрованием с помощью бумаги и карандаша. Однако «машинный» век криптографии, естественно наступил.

Одновременно с развитием радиосвязи появилась возможность идентификации абонента. Техническими приёмами можно было достаточно точно определять источник передачи информации. Даже без раскрытия секретной информации этот факт позволял определить источник секретной передачи. Таким образом, установление самих абонентов сети засекреченной связи и их иерархии, даже без дешифрования, позволяло получить весьма полезную информацию. Это породило интересное исследование сетей защищённой связи — анализ интенсивности, адресации, длин передаваемых сообщений и т.д. для извлечения разведывательной информации. Такого рода анализ состояния сетей засекреченной связи с динамикой их изменения во времени дошёл до наших дней. Например, немцы, во время Второй мировой войны, прослушивая передачи английской

радиостанции Би-би-си и других радиостанций союзников по резкому нарастанию количества шифрованных сообщений на континент, смогли определить начало высадки десанта союзных войск во Франции («второй фронт»). Правда, они серьёзно ошиблись в вопросе о предполагаемом месте высадки.

Телеграф и радио начали постепенно вытеснять кодирование с целью защиты информации в пользу применения шифров. Громоздкие, малоудобные при использовании секретные кодовые книги могли стать и становились добычей противника, а их смена порождала серьёзные проблемы. Шифры оказались гораздо мобильнее и дешевле. Секретное кодирование пошло на убыль, но не исчезло совершенно. Коды стали применяться совместно с шифрами. Такое сочетание оказалось весьма эффективным и дошло до наших дней. Подчёркнём, что при компрометации шифра достаточно лишь сменить его ключи, а не все кодовые книги. Отметим также, что коды очень чувствительны к лексике, словарному запасу языка общения. Появление новых терминов и понятий приводило к необходимости обновлять кодовые книги. Шифры в этом плане гораздо предпочтительнее, ибо их применение не связано со смысловым содержанием открытого текста.

Появились специальные военные шифры, так называемые «полевые шифры». К ним предъявлялись специальные требования: максимальная простота применения; не требовалось серьёзной подготовки шифровальщиков; надёжность защиты уже определялась требованием краткой временной сохранности тайны (приказы на поле боя утрачивают свою ценность для противника по их исполнению). Среди первых полевых систем шифрования начали использоваться шифры Виженера с коротким повторяющимся лозунгом. Затем появились и другие системы, возрождающие, в частности, шифры перестановки (в том числе и маршрутной). Например, открытый текст выписывался повторно в таблицу заданного размера, а затем считывался по колонкам по легко запоминаемому маршруту. Появились выписки по диагоналям и другим путям.

Применялись и книжные шифры, причём в качестве ключевой книги иногда использовались различного рода энциклопедические словари, которые позволяли вести замену на уровне слов. Это облегчало и ускоряло процесс шифрования (по сравнению с побуквенным шифрованием), но одновременно порождало очевидные слабости шифра. Самых ключей (словарей) в то время было немного, и

они были общедоступны. Внешние признаки такой замены вполне очевидны. К такому же результату приводило использование перестановки на уровне слов. Такая перестановка не устраняет осмысленности переставляемых единиц текста, что успешно используется при дешифровании (особенно при повторном использовании одного и того же ключа перестановки; в этом случае варианты возможной перестановки по первой телеграмме легко перепроверяются на периодичность осмысленным прочтением второй телеграммы).

Фотография. Даже такое, мирное, на первый взгляд, изобретение, как фотография стало использоваться в военном деле, в агентурной разведке (в том числе и копирования открытых и зашифрованных текстов, ключевой информации, а в последствии конструктивных элементов, инструкций по эксплуатации и ремонту шифрмашин) и для тайной передачи информации (стеганография). Основоположниками фотографии стали французы Л.Ж.М. Дагер и Ж.Н. Ньепс, которые в 1839 году продемонстрировали возможность получения видимого изображения на специальных светочувствительных материалах. В 1840-1841 годах их идеи развил англичанин У.Г.Ф. Толбот. Цветные фотоизображения впервые получил француз Л. Дюко дю Орон в 1868-1869 годах. Во Франции в 1870 году с целью компактного хранения информации был разработан метод «миниатюрного фотографирования». Текст из нескольких сотен тысяч букв умещался на фотографии небольшого размера. В XX веке немцы довели размер микрофотографии до 1 кв. мм. Она представляла собой крошечный негатив фотопленки размером не более типографской точки (!), которая при увеличении давала четкое изображение печатной страницы стандартного размера. Негатив таких размеров мог содержать чертежи и тексты, и при этом его можно было вклеить как точку в обычное письмо, которое затем пересылалось по нужному адресу. Впервые в военном деле этот метод был использован во время франко-прусской войны 1870-1871 годов. Кстати, депеши в виде микрофотографий на особой пленке пересылались в осажденный немцами Париж со специально организованных станций голубиной почты. Во время этой войны активно использовались и другие способы незаметной транспортировки сообщений. Вот что пишет по этому поводу английский историк Р. Роуан: «Были задержаны курьеры, зашивавшие важные французские депеши в подкладку или прятавшие их в тросточках и палках. Документы прятали также в

подошвах, в козырьках кепок, в искусственных зубах и даже в десятисантиметровых монетах, распаянных, выдолбленных и снова запаянных, причем шов заглаживался действием уксусной кислоты. Некоторые особо важные сообщения, были найдены в покрытых резиной пилюлях, которые их владельцы проглатывали в случае опасности. Французов, заподозренных в том, что они являются агентами связи, немцы обыскивали, раздевали догола, давали им сильнодействующие слабительные и держали под постоянным наблюдением» [Роуан, 1992].

Особенности развития криптографии в XIX веке. В заключение подведем некоторые итоги. В качестве особенностей развития криптографии в XIX веке можно отметить следующие.

1. Шифры начали вытеснять коды. До этого коды имели существенный приоритет. В конечном счете, именно шифры оказались наиболее эффективным средством защиты информации, передаваемой при помощи новых видов связи. Это привело к необходимости разработки новых шифров. Кроме того, выяснилось, что в ходе боевых действий в многочисленных войнах XIX века значительное количество кодов было скомпрометировано (оказались в руках противника). Напомним, что замена кода - весьма трудоемкая операция. Код это целая книга, ее замена приводит к необходимости написания новой книги и рассылки ее по многочисленным абонентам связи. В этом смысле шифр более устойчив к компрометации: абонентам достаточно разослать компактные новые ключи. Получило широкое распространение совместное использование кодов и шифров. Эти обстоятельства привели к необходимости разработки новых шифров, хорошо «согласующихся» с новыми каналами связи.

2. Начали активно разрабатываться механические шифровальные устройства - шифраторы, которые заметно облегчали и убыстряли процессы зашифрования и расшифрования. Оперативные характеристики связи повысились. Кроме этого, работе на несложных шифраторах можно было обучить большое количество операторов - шифровальщиков, далеких от понимания сущности криптографической защиты. В связи с активным ростом числа абонентов засекреченной связи потребность в таких специалистах резко возросла. Операторы - шифровальщики стали необходимой составной частью военных штабов и отдельных подразделений.

3. Началось осмысление криптографии как самостоятельной науки, а не только как искусства, доступного лишь «избранным».

Появились точные определения, правила разработки шифров и требования к ним, первые математические модели шифров. Развитие этого направления привело к тому, что в середине XX века криптография стала уникальной математической наукой. Ее начинают изучать в военных академиях, здесь следует отметить роль французской военной академии Сен-Сир, у нас в России криптографические методы защиты информации и основы криптоанализа изучались в Академии Генерального штаба.

4. Морально – этическое восприятие криптографической деятельности привело к новому осмыслению криптографии. В это время криптография уже стала известной общественности различных стран. Право на защиту секретов не оспаривалось. Но «криптографический взлом» чужих секретов вызывал негативное отношение общества. К середине XIX века «черные кабинеты» в ведущих странах Европы были официально закрыты. Но спустя некоторое время они возродились под повышенным покровом секретности. Правительства разных стран прекрасно понимали, что лишаться информации, добытой путем дешифрования, было бы, мягко говоря, нецелесообразно.

5. Криптография стала известной общественности и начала активно использоваться в художественных произведениях (Эдгар По, Конан Дойл и др.). Уже в XX веке Д. Кан отметил, что криптография является царицей головоломок (кроссвордов и т.д.). Не редко это имело вид игры, в которой авторы скрывали свое имя. Не избежал этого увлечения в молодости и наш великий поэт А.С. Пушкин. В юные годы он использовал для подписи следующие «криптографические» преобразования. Одна из подписей: НКШП, что означало инвертированную фамилию с пропуском гласных букв: НиКШуП. Другая подпись: 1...14...16. Здесь буквы имени заменены на номера букв в естественном русском алфавите: 1=А, 14=Н, 16=П. Подпись АНП — Александр НикшуП. Ему нравились загадочные и ложные имена в тетрадях отцовского бюро. В них автор прятался за буквами, цифрами, анаграммами. Ему казалось, что, приобретая новое имя, он сам приобретал новый вид [Тынянов, 1988]. Криптография как самостоятельная научная дисциплина начала привлекать внимание ученых, которые ранее с ней не были связаны. Криптография вышла в «открытый мир». Ее начали активно применять антиправительственные организации (оппозиционеры, диссиденты, революционеры), а также уголовный мир (террористы, бандиты,

контрабандисты). В частности в России, помимо государственных организаций в России в XIX веке и начале XX века шифрование активно использовали различные подпольные организации, оппозиционные власти, такие как «Народная воля», РСДРП, БУНД (еврейская подпольная организация), эсеры, анархисты и т.д. Интересно отметить, что помимо криптографических методов защиты информации подпольщики активно использовали стеганографию (невидимые чернила, на основе природных и специально синтезированных химических компонентов). Криптографические методы начали применять и историки, занимающиеся раскрытием тайн «умерших языков».

6. В связи с усилением стойкости шифров заметно возросла агентурная деятельность разведок в интересах дешифрования информации (кража шифров и ключей, подкуп и т.д.). В связи с этим талантливый голландский криптограф О. Керкгоффс сформулировал следующее правило. Шифр должен надёжно защищать информацию даже в том случае, когда он становится известным противнику. Стойкость засекречивания должна обеспечиваться только секретным ключом.

В заключении этого раздела отметим, что XIX век вошёл в историю криптографии как пример серьёзного влияния научно-технического прогресса на разрешение проблем криптографии, на морально-нравственное осмысление самой криптографической деятельности. Так же следует отметить, что криптография не только опиралась на достижения научно-технического прогресса, но и ставила перед учеными новые проблемы (в частности, организация перехвата). Естественно, что эта сторона деятельности спецслужб не афишировалась.

Машинная криптография

Первым шифровальным прибором (шифратором) является древнегреческая сцитала. Как уже упоминалось выше в XV веке Л. Альберти предложил идею шифровального диска, его идеи (с некоторой модификацией) развили Белазо, Порта и др. На рисунке 6.1 представлен шифровальный диск немца Гаспара Шота (XVII век).

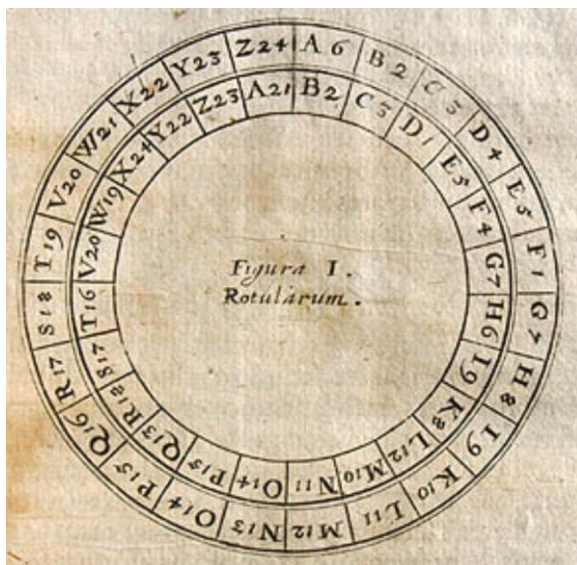


Рис. 6.1 «Ротариум» Г. Шота.

Однако в то время идеи механизации шифрования в то время не нашли понимания среди криптографов. Объяснялось это довольно просто – скорость передачи сообщений (с помощью гонцов) занимала априори значительно больше времени, чем процессы шифрования/расшифрования, и на протяжении многих веков главным «оружием» криптографов всего мира были карандаш и бумага. Как было отмечено выше ситуация радикально изменилась в середине XIX века. Изобретение электросвязи потребовало резкого увеличения скорости осуществления криптографических преобразований, к тому же это надо было делать без ошибок. Именно в это время появились первые механические «протошифраторы». В основном они реализовывали различные варианты шифра многоалфавитной замены.

Еще одним фактором начала активного применения шифраторов стал успех криптоаналитиков по дешифрованию одного из основных шифров того времени – шифра Виженера. Усилиями французов Базери и де Виари, англичанина Бэббиджа, голландца Кергоффа и немца Казиски были разработаны методы вскрытия данного шифра. Срочно нужна была замена, альтернативой стал шифр многоалфавитной замены, однако процессы шифрования/расшифрования были весьма сложны, к тому же ошибка при шифровании хотя бы одного знака приводило к невозможности

расшифрования остального текста, следовавшего за ним. Вот тут-то и вспомнили о шифровальных приборах.

Одним из величайших изобретений «доэлектрической» эпохи криптографии стал шифратор Джефферсона (см. рис. 6.2). В начале XIX века криптография обогатилась замечательным изобретением. Его автор – государственный деятель, первый государственный секретарь, а затем и президент Америки Томас Джефферсон. Свою систему шифрования он назвал «дисковым шифром». Этот шифр реализовался с помощью специального устройства, которое впоследствии назвали шифратором Джефферсона. Конструкция шифратора может быть вкратце описана следующим образом. Деревянный цилиндр разрезается на 36 дисков (в принципе, общее количество дисков может быть и иным). Эти диски насаживаются на одну общую ось таким образом, чтобы они могли независимо вращаться на ней. На боковых поверхностях каждого из дисков выписывались все буквы английского алфавита в произвольном порядке. Порядок следования букв на различных дисках – различный. На поверхности цилиндра выделялась линия, параллельная его оси. При шифровании открытый текст разбивался на группы по 36 знаков, затем первая буква группы фиксировалась положением первого диска по выделенной линии, вторая – положением второго диска и т. д. Шифрованный текст образовывался путем считывания последовательности букв с любой линии параллельной выделенной. При расшифровании на аналогичном шифраторе полученный шифртекст выписывался путем поворота дисков по выделенной линии, а открытый текст отыскивался среди параллельных ей линий путем прочтения осмысленного возможного варианта. При таком расшифровании принципиально возможно появление различных вариантов открытого сообщения, но как показал накопившийся к тому времени опыт, это событие весьма маловероятно: осмысленный текст читался только по одной из возможных линий. Шифратор Джефферсона реализует ранее известный шифр многоалфавитной замены. Частями его ключа являются: порядок расположения букв на каждом диске, порядок расположения этих дисков на общей оси.

Общее количество ключей огромно: оно равно $(26!)^{36}$ – это примерно 10 в степени 936 ТАК?



Рис. 6.2 Шифратор Джефферсона стр 196

Однако при жизни Джефферсона судьба его изобретения сложилась неудачно. Будучи госсекретарем, сам Джефферсон продолжал использовать традиционные коды (номенклатуры) и шифры типа шифра Виженера. Он очень осторожно относился к своему изобретению и считал, что его нужно основательно проанализировать. С этой целью он длительное время поддерживал связь с математиком Р. Паттерсоном. В результате обмена информацией Паттерсон предложил свой собственный шифр, который, по его мнению, являлся более надежным, чем шифр Джефферсона. Этот шифр представлял собой шифр вертикальной перестановки с введением «пустышек». По стойкости он значительно уступал шифру Джефферсона, однако Джефферсон принял доводы своего оппонента и признал его шифр более приемлемым для использования. Таким образом, Джефферсон сам не оценил всей глубины своего собственного изобретения. В XX веке криптоаналитики США признали высокую стойкость шифра Джефферсона. Они даже назвали его автора «отцом американского шифровального дела». В связи с указанным эпизодом можно особо выделить два момента. С одной стороны, уже будучи президентом Джефферсон не навязывал употребление изобретенного им шифра. С другой стороны, поскольку его изобретение попало в архив, оно неизбежно повторилось в будущем. До обнаружения «архивного шифра» Джефферсона другие криптографы самостоятельно изобрели аналогичные шифры. В истории криптографии имеются многочисленные примеры, иллюстрирующие забвение старых идей и попытки изобретения «нового колеса». И в наши дни дилетанты в криптографии изобретают свои собственные «недешифруемые» шифры, которые на самом деле оказываются легко раскрываемыми.

Это изобретение стало предвестником появления так называемых дисковых шифраторов, нашедших широкое распространение в развитых странах в XX веке. Шифратор, совершенно аналогичный шифратору Джефферсона, использовался в армии США во время Второй мировой войны (об этом ниже).

Как и многие другие изобретения в истории человечества, идея такого шифратора пришла в голову нескольким людям одновременно. В 1786 году шведский специалист Фредерик Грипенстерна (Fredrik Gripenstierna) преподнес королю Густаву III свое изобретение. В XVIII веке оно получило у шведов название «шифрмашина». В Швеции считается, что это был первый в мире шифратор, хотя как отмечалось выше первым шифратором все же была считала.

Машина состояла из 57 колец, которые в сменяемом порядке располагались на общей оси. Эта конструкция помещалась в цилиндрический корпус. На одной стороне каждого колеса были нанесены буквы шведского алфавита в их естественном порядке. На другой стороне наносились числа из множества $\{00, 01, \dots, 99\}$. На каждом колесе имелось 29 чисел (по числу букв шведского алфавита). Эти числа являлись независимой (без повторений) выборкой из описанного множества. На разных колесах выборки были независимыми, то есть одно и то же число могло появиться на разных колесах. На каждой стороне вдоль оси цилиндра прорезалась щель, через которую можно было видеть строку из 57 символов. Одна сторона цилиндра использовалась для набора открытого текста – другая для считывания шифрованного.

Перед началом работы колеса (которые могли вращаться на оси независимо друг от друга) устанавливались в исходное состояние, так что буквы алфавита и числа шифробозначений находились каждые на своей стороне. Каждую сторону машины обслуживал свой оператор. При шифровании один оператор путем вращения колес набирал открытый текст (57 букв). После чего второй оператор на своей стороне считывал 57 соответствующих чисел шифрованного текста. При расшифровании роли менялись: один оператор набирал строку из чисел шифртекста, а другой считывал открытый текст. Следующие 57 букв шифровались по тому же принципу и так далее [Бутырский, 2007].



Reconstruction of Gripenstierna's cipher machine.

Рис. 6.3 Шифратор Грипенстерна

В очередной раз изобретение Джефферсона в конце XIX века повторил француз Этьен Базери. Однако и его устройство - «цилиндр Базери» было отвергнуто из-за «чрезвычайной сложности» как в изготовлении, так и в применении. Базери упростил свою систему, объявив порядок расположения букв на дисках несекретным. Ключом шифра являлся лишь порядок расположения дисков. Порядок же расположения букв алфавита для удобства запоминания образовывался из легко запоминаемых лозунгов – фраз для каждого диска. Однако при таком упрощении шифр значительно утратил свою стойкость. Маркиз де Виари показал пример дешифрования этого шифра. Упрощенный вариант опять был отвергнут, а сам шифр вторично забыт.

В начале XX века трудами Паркера Хитта (США) идея дискового шифратора была еще раз повторена. При этом она приняла вид «полоскового шифра», значительно более простого в изготовлении. Диски заменялись на полоски с нанесенным на них удвоенным произвольным алфавитом.

Полоски с удвоенным алфавитом, закрепленные в рамку, гораздо более технологичны, чем деревянные диски с алфавитом. Смысл шифрования и расшифрования остался тем же, что и в изобретении Джефферсона, однако сложные диски были заменены на легко воспроизводимые «полоски» из твердого материала (картона, металла и т. д.). Значимость этого изобретения заключается не в

появлении новых криптографических идей, а в технологической простоте их воплощения.

В 20-х годах XX века шифр Джеффферсона-Хита наконец-то получил признание. Американские криптоаналитики, пришли к выводу о достаточной стойкости и простоте этого шифра, и армия США приняла его на вооружение. Но самое главное последствие изобретения Джеффферсона – это появление в XX веке первых сложных электромеханических устройств. Однако для их появления понадобились новые изобретения, о которых будет сказано позднее.

Ручной дисковый цилиндрический шифратор модели М-94 (см. [рис.6.4](#)) , позволяющий реализовать **любую из 26! перестановок** 26 букв посредством вращения 26 дисков, начал использоваться на тактическом уровне в Армии США начиная с 1921 года. Следующая “флотская” модификация CSP-488 с 1928 года и модель CSP-493 для морской пограничной службы с 1939 года применялись военными вплоть до 1945 года. Примечательно, что вся история криптографии вплоть до настоящего времени показывает, что практически применяемые устройства и методы шифрования с временной стойкостью были, есть и по видимому будут.

Конструктивно плоские и более удобные в эксплуатации версии М-94, называвшиеся М-138 (CSP-845) ([см.рис. 6.5](#)), также широко применялись в вооруженных силах США во время Второй мировой войны. Версии CSP-845, изготавливались из полированного алюминия и могли иметь 25 или 30 передвигаемых вручную полос с двукратно повторяющимся алфавитом. **Версия CSP-1756 представлена на рис. 6.6**



Рис. 6.4. Ручная дисковая криптомашинка вооруженных сил США модели М-94

Нет ссылки в тексте на этот рис стр 200

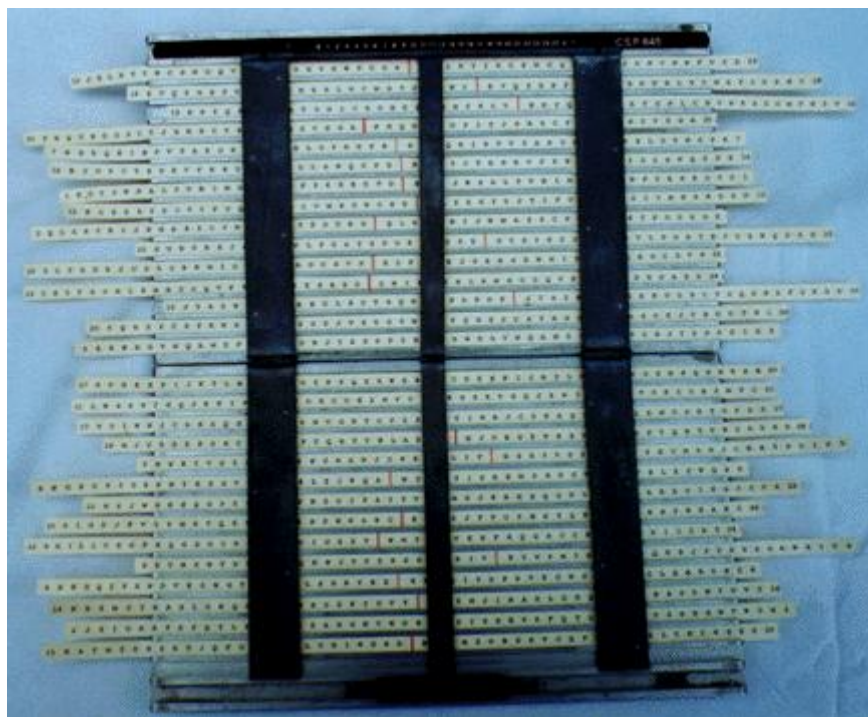


Рис. 6.5 Полосковый шифратор вооруженных сил США модели М-138 (CSP-845). Нет ссылки в тексте стр200

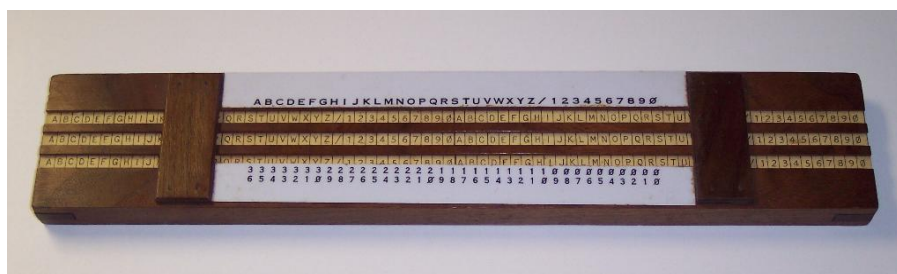


Рис. 6.6 Ручная шифратор-линейка модели CSP-1756. Нет ссылки в тексте на этот рис

Полосковые шифраторы CSP-1750 и CSP-1756 широко применялись в послевоенное время в армиях США и стран НАТО, а гриф секретности на них был снят в 1980-м году.

Идея Джефферсона возродилась в России. В 1916 году подпоручиком Попазовым было изготовлено шифровальное устройство, впоследствии названное «Прибор Вави». Устройство по своей идее было адекватно «цилиндру Джефферсона», но вместо дисков на оси имелись 20 колец, надетых на цилиндр вплотную друг к другу, которые могли вращаться на нем. На ребрах (цилиндрических поверхностях) колец были нанесены смешанные алфавиты (30 букв), а на первом и последнем - 20-м кольцах были нанесены упорядоченно цифры от 1 до 30. При заданном расположении колец на цилиндре ключом шифра являлись: цифра, например, 5 и буква, например Б, и также «ключ шага» – две буквы, например, АГ. Сообщение делилось на части по 17 букв. Для зашифрования фразы «Прибор Вави Попазова ...» на первом кольце отыскивалось ключевая цифра – 5. Напротив этой цифры поворотом второго кольца ставилась ключевая буква - Б. А затем напротив них поворотами остальных колец выставлялась фраза из 17 букв «Прибор Вави Попазов...» (см. [поясняющую таблицу](#)). Эта часть текста заменялась на другие буквы с параллельных строк ключа шага –АГ. А – строка соответствующая букве А на втором кольце. Вторая аналогичная строка начиналась с буквы Г второго кольца. Буква П заменялась буквой Ж 3-го кольца на строке А, р - заменялась буквой Э стоящей в 3 кольце на строке Г. Таким образом зашифрованные буквы брались поочередно, то со строки А, то со строки Г.

Поясняющая таблица

5	Б	П	Р	И	Б	О	Р	В	А	В	И	П	О	П	А	З	О	В	5
6	Я	И	А	Ж	Т	Р	Э	П	В	У	Р	О	Б	А	З	В	Ф	Ш	6
7	Л	З	Б	Р	Л	О	Д	Ф	Ч	К	Б	Л	Т	Б	Х	Э	Д	Ч	7
8	А	Ж	Я	У	А	В	Л	О	Б	Г	Т	К	А	Ф	Н	Ч	Ш	И	8
9	Г	Т	Э	А	Ф	Ж	Ю	Д	Ш	Р	Е	Ж	Ы	Т	Д	Х	Г	Ю	9

Шифртекст имел вид: ЖЭУФВЮОШГЕКЫФДЧГИ. Процесс расшифрования очевиден. Заметим, что принципиальное отличие «Прибора Вави» от шифра Джефферсона заключалось в единственности выбора шифртекста (по шагу ключа). Прибор не нашел широкого применения. Пока еще предпочтение отдавалось ручным шифрам.

Еще одним типичным прибором для шифрования стали различные линейки. В конце XIX века криптография начинает приобретать черты точной науки, а не только искусства как это было ранее. Ее начинают изучать военных академиях, здесь следует отметить роль французской военной академии Сен-Сир. К этому времени в академии был разработан свой собственный военно-полевой шифр, получивший название «Линейка Сен-Сира» (см. рис. 6.7). Линейка представляет собой длинный кусок картона с напечатанными на нем буквами алфавита. Эта последовательность букв называется «неподвижной шкалой». Снизу, под неподвижной шкалой, в линейке были сделаны вырезы, через которые легко перемещался «движок» - узкая полоска из картона с нанесенным на него (с двойным повторением) тем же самым алфавитом. Алгоритм шифрования заключался в следующем. Полоска (движок) перемещается в положение, когда буква ключа-лозунга окажется под буквой «А» неподвижной шкалы. Образуется простая замена первой буквы открытого текста (буквы движка образуют нижнюю строку подстановки-замены). При шифровании второй буквы открытого текста вторая буква ключа-лозунга путем передвижения движка встает под буквой «А» неподвижной шкалы и т.д. Лозунг повторяется периодически по шифруемым буквам открытого текста. Таким образом, линейка Сен-Сира является простым механическим воплощением шифра Виженера - короткопериодического гаммирования. Она позволила существенно повысить эффективность труда шифровальщика, облегчить алгоритм реализации шифра Виженера. Именно в этой механизации процессов зашифрования-дешифрования и заключается вклад авторов линейки в практическую криптографию. По сути дела этот «шифратор» технологически простым путем реализовывал идеи Альберти («дисковый шифратор»), Тритемия и Виженера («таблица шифрования») и Беллазо («лозунговый выбор строк шифрования»). Однако в силу этой простоты линейка Сен-Сира получила определенное распространение.

Слабость этого «шифратора» заключалась в короткопериодическом продолжении ключа-лозунга.

Развитием идеи линейки Сен-Сира явилось произвольное расположение букв алфавита на движке. Секретное (ключевое) расположение этих букв существенно усилило криптографическую стойкость шифра. Однако основная слабость - короткопериодическое продолжение ключа-лозунга сохранилось, и это предопределило в последующем успехи дешифровальщиков. В заключение исторического эпизода с линейкой Сен-Сира отметим, что эта линейка является простейшей технологической реализацией диска Альберти. Реализация шифра Виженера на уровне картонных полосок значительно «дешевле», чем создание оригинальных устройств типа дискового шифратора Альберти. Поэтому «линейка» получила достаточно широкое распространение.

В Германии также применяли линейку Сен-Сира, однако она была усовершенствована. В частности ей был придан округлый вид, по сути дела повторяющий диск Альберти на новой технологической основе.



Рис. 6.7 Линейка Сен-Сира

Нет ссылки в тексте на этот рис стр 204

Еще одним интересным изобретением XIX века в области шифраторостроения стали приборы Уодсворта и Уитсона.

В 1817 году полковник американской армии, начальник артиллерийско-технической службы армии США Д. Уодсворт предложил оригинальное устройство — механический шифратор. Схема шифратора приведено на рисунке 6.8.



Рис. 6.8. Шифратор Уодсворта

Основной элемент устройства — два шифровальных диска. На торце первого диска (2), реализующего алфавит открытого текста, в алфавитном порядке расположены 26 букв английского алфавита. Второй диск, на котором располагается алфавит шифрованного текста, в произвольном порядке располагались эти же буквы и цифры от 2 до 8. Таким образом, он содержал 33 знака. Литеры на диске — съемные, что позволяет менять алфавит шифрованного текста. Диски соединены между собой шестеренчатой передачей с числом зубьев 26×33 . При перемещении первого диска (с помощью кнопки) на один шаг второй диск перемещается также на один шаг в другую сторону. Поскольку числа 26 и 33 взаимно просты, то при пошаговом вращении первого диска оба диска приходят в исходное состояние через $26 \cdot 33 = 858$ шагов. Диск открытого текста вращался только в одну сторону. Диски помещались в футляр, в котором были прорезаны окна (5). С помощью специальной кнопки (6) шестерни разъединялись, что позволяло независимо друг от друга перемещать диски в начальное для шифрования положение (с помощью кнопок 7 и 8). Долговременным ключом являлось расположение букв алфавита на втором диске (их количество 33!) исправил ВСЁ ТАК?; разовый

ключ состоял из двух букв (верхнего и нижнего диска) и устанавливался в окнах при независимом повороте дисков. Количество разовых ключей - $26 \cdot 33 = 858$. На **рисунке 6.8 КАКОМ?** изображен разовый ключ LB. Шифрование производилось следующим образом. Перед началом шифрования диски ставились в начальные условные положения (LB). Затем шестерни соединялись, и с помощью кнопки 2 диск поворачивался до тех пор, пока в верхнем окне не появлялась первая буква открытого текста. С окна под ним списывалась первая буква шифрованного текста. Остальные буквы шифровались аналогичным образом. Если буквы повторялись (например, AA), то диск совершал полный оборот, поэтому в шифртексте этой паре соответствовала пара из различных знаков (например, 8B).

Расшифрование производилось очевидным образом. При этом буквы шифрованного текста устанавливались по нижнему окну, а с верхнего списывалась соответствующая буква открытого текста.

Отметим следующие особенности данного шифра.

1. Количество знаков в алфавите шифрованного текста (33) больше количества букв в алфавите открытого текста (26);

2. Шифрование буквы открытого текста зависит от того, какой была предшествующая ей шифруемая буква.

В предложении Уодсворта просматриваются идеи Энея (замена букв на расстояние), Альберти (2 диска), Тритемия и Виженера (но при достаточно сложном выборе строк шифруемого алфавита).

Формализованное представление процесса шифрования можно представить следующим образом. Выпишем алфавиты открытого и шифрованного текста в две строки.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z							
F	Z	G	T	W	B	P	V	U	A	Y	S	C	4	E	D	Q	8	X	Z	R	L	S	M	H	N	O	I	3	J	6	7	K

Диски вращаются в противоположных направлениях, которые отмечены стрелками. Зашифруем слово THE APPLE при начальном угловом положении дисков (разовом ключе) LB. Буква T открытого текста отстоит от буквы L на 8 шагов. На восьмом шаге от буквы B (в алфавите шифрованного текста) находится соответствующий знак шифрованного текста 6 (циклическое отсчитывание). Вторая буква

открытого текста Н отстоит от буквы Т на 14 шагов. На 14 месте после знака 6 (по стрелке движения) в алфавите шифрованного текста находится буква Q; она и является буквой шифрованного текста. Продолжая этот процесс дальше, получим шифрованный текст: 6QOWS3PR.

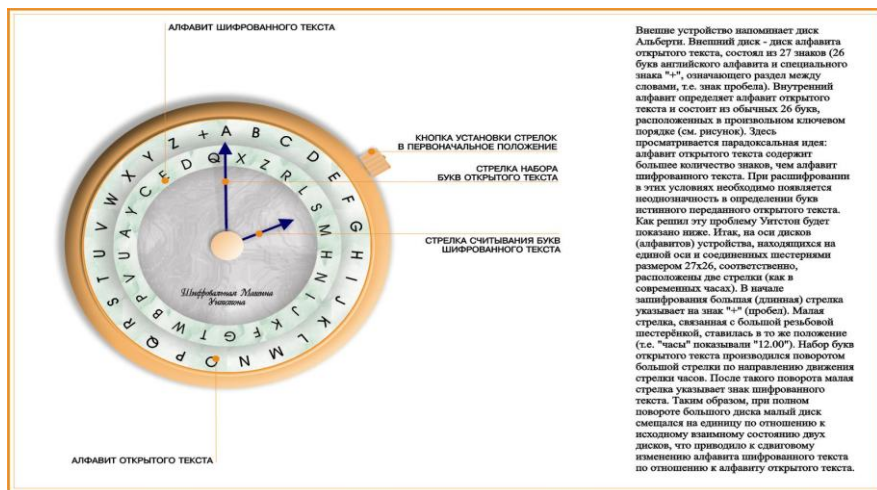
Расшифрование производится в обратном порядке. Первый знак шифрованного текста (6) отстоит от буквы разового ключа В (в алфавите шифрованного текста) на 8 шагов. В алфавите открытого текста 8-й буквой после L является буква Т, и т.д.

Предложение Уодсворта заслуживало внимания. Недостатком шифра является его особая чувствительность к неточностям (типа замены и пропуска знаков в шифрованном тексте). Искаженная или пропущенная буква делала весь последующий текст при расшифровании нечитаемым. Однако представляется, что исторический отказ от предложенной системы шифрования связан с другими обстоятельствами. В эти годы господствовали так называемые «ручные шифры», применение которых не требовало специальных приспособлений; эти шифры были хорошо освоены, им верили и их хорошо знали. Предложение Уодсворта порождало лишние «хлопоты».

Следующее интересное предложение по созданию механических устройств шифрования сделал англичанин Ч. Уитстон во второй половине XIX века. Современным специалистам это имя знакомо его достижениями в области применения электричества. Уитстон создал первый макет электрического телеграфа (до изобретений Морзе и Шиллинга), изобрел концертино, усовершенствовал динамо машину, изготовил несколько стереоскопических рисунков, изучил подводный телеграф, опубликовал ряд работ по акустике и фонетике, в том числе по проблеме «говорящих машин». Он создал известный электрикам «мостик Уитстона» для точного измерения сопротивления и т.д. За свои работы Уитстон был избран членом королевского научного общества и удостоен звания пэра.

Среди увлечений Уитстона была и криптография. Когда ему уже было далеко за 50 лет, он дешифровал архивное, длинное шифрованное письмо короля Карла I (как оказалось, весьма слабо зашифрованное небольшим по объёму кодом). Впервые Уитстон продемонстрировал своё шифровальное устройство (см. рис.6.9) на Всемирной выставке в Париже в 1876 году. Смысл этого устройства

закljučается в следующем. В нем, так же, как и в шифраторе Уодсворта, просматривается влияние идей Альберти, а так же и самого Уодсворта.



Шифробалльная Машина Уитсона

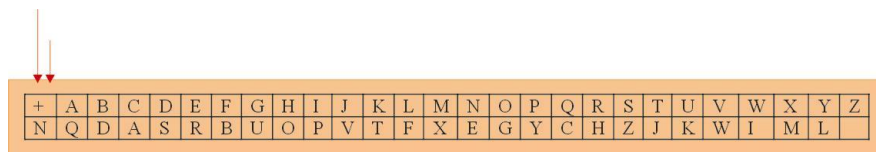
Рис. 6.9. Шифратор Уитсона. Нет ссылки в тексте на этот рис стр 208

Внешне устройство напоминает диск Альберти. Внешний диск — диск алфавита открытого текста, состоял из 27 знаков (26 букв английского алфавита и специального знака «+», означающего раздел между словами, т.е. знак пробела). Внутренний алфавит определяет алфавит открытого текста и состоит из обычных 26 букв, расположенных в произвольном ключевом порядке (см. **рисунок 6.9 КАКОЙ?**). Здесь просматривается парадоксальная идея: алфавит открытого текста содержит большее количество знаков, чем алфавит шифрованного текста. При расшифровании в этих условиях необходимо появляется неоднозначность в определении букв истинного переданного открытого текста. Как решил эту проблему Уитстон будет показано ниже.

Итак, на оси дисков (алфавитов) устройства, находящихся на единой оси и соединенных шестернями размером 27x26, соответственно, расположены две стрелки как в современных часах. В начале зашифрования большая (длинная) стрелка указывает на знак

«+» (пробел). Малая стрелка, связанная с большой резьбовой шестерёнкой, ставилась в то же положение, т.е. «часы» показывали «12.00». Набор букв открытого текста производился поворотом большой стрелки по направлению движения стрелки часов. После такого поворота малая стрелка указывает знак шифрованного текста. Таким образом, при полном повороте большого диска малый диск смещался на единицу по отношению к исходному взаимному состоянию двух дисков, что приводило к сдвиговому изменению алфавита шифрованного текста по отношению к алфавиту открытого текста. По окончании каждого слова большая стрелка становилась на знак раздела (+), буква, на которую при этом указывала короткая стрелка, записывалась как знак шифрованного текста. Во избежание неоднозначности расшифрования, удвоение букв в открытом тексте не допускается. Повторную букву следует либо пропустить, либо ставить вместо нее какую-нибудь редкую букву, например Q. Таким образом, слово THE APPLE при шифровании записывается так: +THE+APLE+ или +THE+APQLE+.

Ключом шифра является порядок расположения букв на внутреннем диске ($26! \approx 4 \cdot 10^{26}$). Приведем формализованный пример шифрования на устройстве Уитстона. Выпишем алфавиты в две строки:



+	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N	Q	D	A	S	R	B	U	O	P	V	T	F	X	E	G	Y	C	H	Z	J	K	W	I	M	L	

Фраза THE APPLE шифруется следующим образом. Под буквой Т стоит соответствующая шифрованная буква J; буква Н отстоит от Т на 15 шагов; на этом расстоянии от буквы J находится вторая буква шифрованного текста Р, и т.д. Окончательно получим шифрованный текст JPUASZYVB. Расшифрование производится в обратном порядке. Над буквой J шифрованного текста открытая буква Т. От J до Р 15 шагов. За буквой Т на этом расстоянии располагается буква Н и т.д.

Заметим, что если допускалось удвоение букв (например АА), то шифртекст имел бы вид QD. Однако, такой же шифртекст соответствует и биграмме АВ, т.е. расшифрование неоднозначно.

Шифр Уитстона обладает одним существенным недостатком. Так, если в шифртексте появляется удвоенная буква (например ВВ), то это означает, что в открытом тексте стоят буквы, стоящие в алфавите рядом, но в обратном порядке (FE). Это уже является существенной слабостью шифра и может быть эффективно использовано при дешифровании.

Изобретение Уитстона, как и Уодсворта, не нашло широкого применения. Однако, у второго предложения Уитстона в области криптографии судьба сложилась лучше, хотя и исторически несправедливо получила имя другого автора. Уитстон изобрел шифр для обеспечения секретности телеграфной переписки, но этот шифр в истории получил имя его друга барона Плейфера. Заметим, что сам Плейфер вел себя весьма корректно: популяризируя изобретение, он всегда указывал имя автора - Уитстона. Однако, к сожалению, история распорядилась иначе: шифру было присвоено имя не изобретателя, а популяризатора. Это изобретение повторяет предложение Дж. Порты о шифровании не отдельных букв, а двухбуквенных сочетаний (биграмм), однако уже на новом уровне. Шифр Порты не мог быть использован при применении телеграфной передачи сообщений, поскольку экзотические обозначения биграмм в шифрованном тексте недоступны телеграфу. Смысл предложения Уитстона заключается в следующем. В квадрат размером 5х5 выписывались в произвольном порядке буквы английского алфавита (буквы I и J не различались). Для облегчения запоминания такой выписки Уитстон предложил использовать идею создания «хаотического» набора букв из ключевого слова (лозунга). Пусть этим словом является слово MAGNETIC. Составим табличку по этому слову, дополняя ее буквами алфавита, не вошедшими в это слово, в их естественном порядке расположения в алфавите. Получаем следующий результат:

M	A	G	N	E	T	I	C
B	D	F	H	K	L	O	P
Q	R	S	U	V	W	X	Y
Z							

Выпишем буквы по столбцам:

MBQZADRGFSNHUEKVTLWIOXCPY

Эта последовательность располагается в квадрат 5х5:

М	В	Q	Z	А
D	R	G	F	S
N	H	U	E	K
V	T	L	W	I
O	X	C	P	Y

Правило (алгоритм) шифрования поясним на примере. Пусть требуется зашифровать слово THE APPLE. Удвоенные буквы разделяются буквой X; получим THE APXPLE. Поскольку получилось нечетное число букв, добавим произвольно выбранную букву (Z): THEAPXPLEZ. Этот текст разбивается на пары:

TH.EA.PX.PL.EZ.

Буквы TH стоят в одном столбце. Они заменяются буквами, стоящими под ними в том же столбце (при циклическом сдвиге). Таким образом, TH заменяется на XT. Биграмма EA соответствует буквам, стоящим в разных строках и столбцах. Она заменяется на биграмму ZK, стоящую в противоположных углах соответствующего прямоугольника.

Биграмма PX, расположенная в одной строке, шифруется циклическим сдвигом нижней строки, получаем YC.

Биграмма PL заменяется по правилу прямоугольника на WC.

Наконец, биграмма EZ по правилу шифрования столбцов заменяется на WF.

Окончательно получаем зашифрованный текст:

XTZKYCWCWF

Расшифрование определяется очевидным образом.

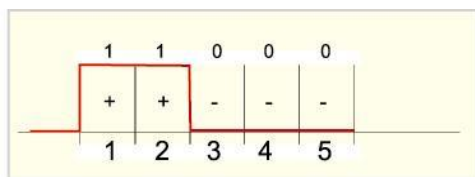
Уитстон и Плейфер доложили новую идею шифрования заместителю министра иностранных дел Англии. Он, признав достоинства системы шифрования, нашел ее слишком сложной. В ответ на это Уитстон заявил, что берется за 15 минут обучить ее использованию учеников ближайшей начальной школы. Представляет интерес ответ английского чиновника: «Это вполне возможно, но вам никогда не удастся обучить этому наших атташе».

Однако достоинство шифра, заключающееся в переходе от зашифрования отдельных букв к зашифрованию биграмм, было вполне очевидно. Этот шифр не был забыт. Он был принят английскими вооруженными силами. Некоторые последователи даже посчитали этот шифр недешифруемым, что является ошибочным мнением (с одной существенной оговоркой: с современных позиций, на которых находится криптография сегодня).

Значительный вклад в развитие криптографии сделал американец Г. Вернам. В 1917 году он, будучи сотрудником телеграфной компании, предложил идею автоматического шифрования телеграфных сообщений. Суть этой идеи заключается в следующем. Открытый текст представляется в коде Бодо (в виде пятизначных «импульсных комбинаций»). В этом коде, например, буква «А» имела вид (+ + — — —). На бумажной ленте эта буква получала следующий вид:

1	●	(+)
2	●	(+)
3	•	(-)
4	•	(-)
5	•	(-)

Знак (+) означал отверстие, а знак (—) его отсутствие. При считывании с ленты пятерка металлических щупов «опознавала» отверстия (где было отверстие щуп замыкал электрическую цепь). В линию связи посылались импульсы тока:



Вернам предложил электромеханически покоординатно складировать импульсы знаков секретного текста с импульсами гаммы. Гамма это секретный ключ, представляющий из себя хаотический набор букв того же самого алфавита. Сложение, по современной терминологии, осуществлялось «по модулю 2»: $0+0=0$, $0+1=1$, $1+0=1$, $1+1=0$ (здесь «0» означает знак — «кода Бодо», «+» -

знак 1). Пусть, например, знак гаммы имеет вид: + — + — — (10100). Тогда буква «А» при шифровании переходит в двоичную комбинацию: 01100 (— + + — —).

При расшифровании ту же операцию необходимо повторить (по координатно):

$$(01100) \oplus (10100) = (11000) = (A)$$

Вернам создал устройство, производящее указанные операции автоматически, без участия шифровальщика. Тем самым было положено начало так называемому «линейному шифрованию». В этом случае процессы шифрования и передачи сообщения происходят в одно и то же время. До сих пор шифрование было предварительным, т.е. сообщение сначала зашифровывалось, а уже потом передавалось в линию связи. Линейное шифрование существенно повысило оперативность связи.

Отметим одну важную особенность шифра Вернама. Эта особенность послужила в последующем обоснованию теории совершенного шифра, предложенную американским классиком криптографии К. Шенноном. Дело в том, что при применении шифра Вернама за перехваченным шифрованным текстом вида b_1, b_2, \dots, b_n может скрываться любой открытый текст a_1, a_2, \dots, a_n . Любому открытому тексту можно подобрать гамму, которая порождает данный шифрованный текст. Поскольку гамма является ключом, то по перехвату шифрованного сообщения невозможно отвергнуть ни одного открытого текста той же длины. Усилия дешифровальщиков сводятся «на нет». Шифр обладает исключительной криптографической стойкостью. В то же время становится ясным и недостаток этой системы шифрования. Хаотическая гамма (ключ) должна иметь ту же длину, что и открытый текст. Для расшифрования на приемном конце связи ему нужно передать (по тайным, защищенным каналам) гамму достаточной длины. При практической реализации это порождает существенные проблемы. Эти проблемы оказались весьма существенными, что и предопределило весьма скромное распространение шифров Вернама. Был предложен простой выход. Гамма шифра записывалась на ленту, склеенную в кольцо. Таким образом, она становилась не случайной, а периодической (как в шифре Виженера). Шифр становился нестойким. Вернам предложил делать гамму шифра составной. При этом имеется в виду, что гамма шифрования получается путем сложения гамм, имеющих взаимно простые периоды. В этом случае общий период равняется

произведению периодов исходных гамм. Это существенно усиливало шифр. Сам Вернам не был математиком-криптографом. Тем не менее, он настаивал на том, что гамма шифра не должна повторяться при шифровании. И здесь он был прав. Его идеи породили новые подходы к надёжной защите информации при передаче больших объемов сообщений.

Наиболее распространенными в первой половине XX века стали электро-механические дисковые шифраторы. В начале XX века революцию в криптографии произвело изобретение шифровального диска, что позволило реализовать шифры многоалфавитной замены в механических и электромеханических шифраторах. Концепция механического дискового (роторного) шифратора встречается у нескольких независимо работавших в одно время изобретателей. Ранее первенство в изобретении дисковой шифрмашины приписывалось четырем изобретателям, работавшим независимо друг от друга в один и тот же период времени: американцу Эдварду Хеберну (Edward Hugh Hebern), шведу Арвиду Дамму (Arvid Gerhard Damm), голландцу Хьюго Александру Коху (Hugo Alexander Koch) и немцу Артуру Шербиусу (Arthur Scherbius).

Однако в 2003 году в журнале “Cryptologia” была опубликована статья Карла де Лееува [Leeuw, 2003], в которой доказывалось, что первыми изобретателями дискового шифратора были два голландских морских офицера, Тео А. ван Хенгель (Theo A. van Hengel, 1875-1939) и Р.П.Ц. Спенглер (R.P.C. Spengler, 1875-1955). Они сделали это в 1915 году. Действующий прототип был построен инженером-механиком В.К. Мауритсом (W.K. Maurits) и испытан летом того же года на борту флагманского корабля военно-морского флота Нидерландов в Голландской Ост-Индии (ныне Индонезия), которым командовал адмирал Ф. Баудуин (F. Bauduin).

Дисковые шифрмашины продолжали успешно использоваться даже в электронную компьютерную эпоху. Так 8-ми дисковая машина KL7 (ADONIS) широко применялась в США и других странах с 1950-х по 1980-ые годы. Последнее канадское сообщение, шифрованное KL-7 было получено 30 июня 1983 года [en.wikipedia].

В 2002-м году уникальная дисковая машина была сконструирована в Нидерландах Татьяной ван Варк (Tatjana van Vark). Эта необычная шифрмашинa (см. рис. 6.10 и 6.11) использовала диски с 40 контактами (буквы, цифры, знаки пунктуации), причем каждый диск состоял из 509 деталей.



Рис. 6.10. Дисквая шифрмашина Татъяны Ван Варк **Нет**
 ссылки в тексте на этот рис стр 215

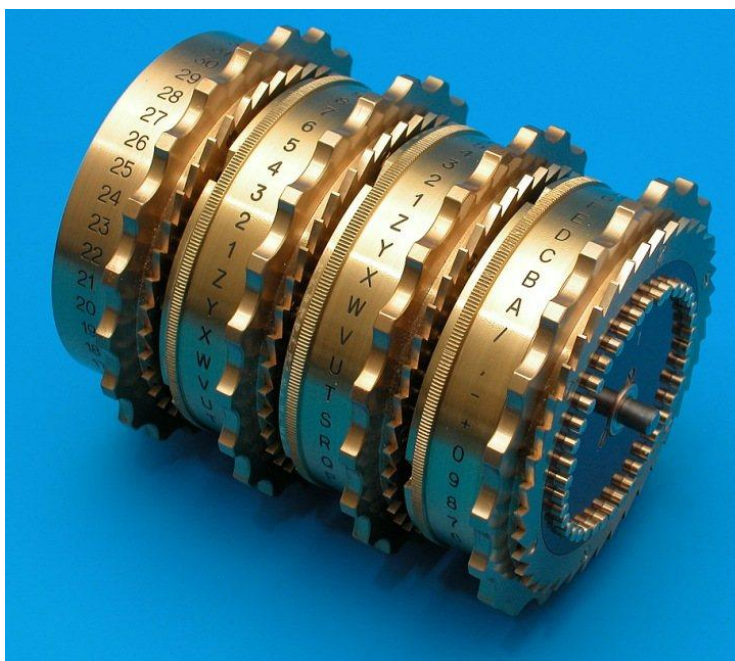


Рис. 6.11. Диски к машине Т. ван Варк. **Нет ссылки в тексте на этот рис стр 215**

В США Э. Хеберн, начиная с 1917 года, разработал серию шифрмашин с числом дисков от одного до пяти. Хеберн заинтересовался криптографией сидя в тюрьме за кражу На деньги инвесторов Хеберн организовал компанию Hebern Electric Code и в течение ряда лет пытался продавать свои криптомашины (см. рис. 6.12) коммерческим банкам, флоту и армии США. Ещё в 1920-х годах компания сконструировала первые в мире 5-тидисковые шифрмашин. У возможных потребителей, однако, не было большого интереса к защите информации, партнеры Хеберна вышли из игры, а флот США в 1931 году закупил несколько систем. **Таким образом, ТАК? БЕЗ ЗАПАЯТОЙ?** дальнейшего коммерческого успеха не было.



Нет ссылки в тексте на этот рис

Рис. 6.12 Трехдисковая механическая криптомашина конструкции
Э.Хеберна **стр 217**

Другой дисковый шифратор с возможностью печати шифртекста изобрел голландец Х. Кох (1870-1928), получив патент 7 октября 1919 года. Шифратор (Geheimschrijfmachine (секретную пишущую машинку) – codeermachine) состоял из 3-х подвижных дисков и штепсельного коммутатора. Кох основал небольшую фирму **Наамлозе Венотшап инженерсбюро** не могу, надо оставить **НЕЛЬЗЯ ЛИ НА ЯЗЫКЕ ОРИГИНАЛА?** «Секуритас». В патенте Кох отметил, что «стальные проволоочки на шкивах, рычаги, лучи света, воздух, вода или масло, протекающие по трубкам, могут передавать шифрующий импульс так же хорошо, как и электричество». Так же Кох отметил, что «этот импульс не обязательно должен протекать через диск, а может проходить по трубкам, просверленным в болванках, скользящих между неподвижными пластинами, или от внутреннего диска в окружающее его кольцо» [Kahn, 1967]. Однако реализовать свои замыслы «в металле» изобретатель не смог.

Наибольшую известность получила дисковая машина А. Шербиуса, который получил патент 23 февраля 1918 года, в этом же году была создана фирма Шербиус & Риттер. Корпорация Chiffriermaschinen AG позднее развернула производство и продажу шифрмашин, которая получила название “Энигма”. В 1926 году эта машина была принята на вооружение в Германии и массово эксплуатировалась до 1945 года. Всего было выпущено около 200000 «Энигм». При разработке “Энигмы” А. Шербиус использовал свой патент 1923 года, идеи немца А. Кирха и Х. Коха, который в 1927 году передал ему права на свой патент. Историки предполагают - Шербиус купил патент Коха (голландский патент №10700, эквивалентный патент в США №165336252), чтобы дополнительно защитить свой приоритет от 1918 года.

«Энигма» в переводе с греческого языка означает «загадка». В течении Второй мировой войны это был наиболее распространенный шифратор, который использовался в Германии (и в странах-союзниках Германии, например, в Италии и Японии), а так же в нейтральной Швейцарии.

Первоначально «Энигма» была коммерческим шифратором. С начала 1920-х годов немцы начали активно рекламировать коммерческий вариант «Энигмы». Шербиус развернул энергичную деятельность с целью повышения спроса на «Энигму». В 1923 и 1924

годах он выставлял «Энигму» на съезде Международного почтового союза. «Энигма» стала широко рекламироваться на радио и в прессе. Однако, несмотря на активную рекламную кампанию, дела у Шербиуса шли неважно. Потенциальных покупателей отпугивала слишком высокая цена «Энигмы». Считанные экземпляры шифратора были приобретены армиями различных государств и компаниями связи, но с массовыми закупками никто не спешил.

Английские криптоаналитики ознакомились с устройством «Энигмы» в июне 1924 года. Германская компания Chiffriermaschinen AG, производившая этот шифратор, предложила британскому правительству закупить партию аппаратов по цене около 200 долларов за штуку. В ответ правительство Великобритании предложило немцам зарегистрировать сначала аппарат в Британском патентном бюро. Лишь при таком условии рассмотрение сделки полагалось возможным. Германская компания согласилась и предоставила в Бюро полную документацию с описанием работы шифратора. В результате криптографическая спецслужба Британии получила доступ к криптосхеме коммерческой версии «Энигмы».

В середине 1920-х годов немецкие военные пришли к выводу о необходимости принятия мер по усилению безопасности своих линий связи. Было решено использовать для этого «Энигму». В 1925 году Шербиус приступил к массовому производству своего шифратора. Начиная со следующего года им стали оснащаться вооруженные силы и спецслужбы Германии. Наиболее востребованными «Энигмы» стали после прихода Гитлера к власти в Германии в 1933 году, когда началось серьезное перевооружение армии. До Второй мировой войны и во время нее было выпущено около двухсот тысяч экземпляров шифратора «Энигма», они применялись во всех видах германских вооруженных сил, в Абвере (немецкая военная разведка) и в службе безопасности.

Кратко опишем устройство шифратора. В начале он представлял собой три вращающихся на одной оси барабана – диска (позже их стало четыре). На каждой стороне диска, представлявшего собой зубчатое колесо, по окружности имелось двадцать шесть электрических контактов – столько же, сколько букв в латинском алфавите. Контакты с обеих сторон соединялись внутри диска случайным образом двадцатью шестью проводами, формировавшими замену символов. Диска складывались вместе и их контакты, касаясь друг друга, обеспечивали прохождение электрических импульсов

сквозь весь набор дисков на регистрирующее устройство. На боковой поверхности дисков был нанесен алфавит. Перед началом работы диски поворачивались так, чтобы установилось кодовое слово. При нажатии клавиши происходило шифрование очередного знака открытого текста. При этом электрический импульс поступал с клавиатуры и проходил через систему дисков, после чего левый диск поворачивался на один шаг. Движение дисков происходило как в счетчике электроэнергии. После того, как первый диск делал полный оборот, на один шаг поворачивался второй диск. После полного поворота второго диска сдвигался на один шаг третий диск.

После прохождения трех дисков электрический сигнал поступал на рефлектор. Рефлектор представлял собой тринадцать проводников, соединявших пары различных контактов на задней стороне третьего диска. С его помощью сигнал шел обратно через диски, но уже по другому пути. Когда сигнал выходил из системы дисков, он поступал на лампочку-индикатор, которая указывала на букву шифрованного текста.

Как правило, с «Энигмой» работали три человека (см. рис. 6.13 и 6.14). Один зачитывал открытый текст, другой набирал его на клавиатуре, третий считывал шифртекст с ламп и записывал его. «Энигма» была портативной (размером с пишущую машинку), работала от батареи, имела деревянный футляр. Одним из недостатков шифратора было то, что он не печатал шифртекст. Впоследствии появились модификации «Энигмы», дающие такую возможность.



Рис. 6.13 «Классический» снимок – немецкие солдаты работают с «Энигмой»





Рис. 6.14. Еще два снимка немецких солдат работающих с «Энигмой»

В 1930 году «Энигма» была модернизирована. В ее конструкцию включили штепсельную (коммутационную) панель из двадцати шести пар розеток и штепселей. С помощью этой панели осуществлялась дополнительная замена знаков перед тем, как знаки открытого текста в виде электрических сигналов поступали с клавиатуры на систему дисков и после того, как они ее покидали. У коммерческих вариантов шифратора такая панель отсутствовала.

Ключами шифратора являлись следующие элементы.

Коммутации дисков. Они формировали долговременный ключ шифратора. Заметим, что количество возможных коммутаций для одного диска равно числу $26! = 26 \cdot 25 \cdot \dots \cdot 2 \cdot 1$ различных перестановок двадцати шести элементов, что составляет приблизительно $4 \cdot 10^{26}$ вариантов. Выбор дисков из комплекта и взаимное расположение их в шифраторе. Всего в комплекте имелось 5 дисков, в шифратор устанавливались три диска. Количество различных вариантов выбора этих трех дисков равно 10. Три диска можно переставить шестью различными способами. Поэтому всего получается 60 вариантов. Выбор дисков также был элементом долговременного ключа. Начальное положение дисков. Для каждого диска – 26 вариантов, для трех дисков – $26^3 = 17\,576$ НЕПОНЯТНО. Это был разовый ключ.

Коммутация штепсельной панели (менялась достаточно часто).
 Электрическая схема шифратора «Энигма» дана на рис. 6.15. Фото
 четырехдискового варианта «Энигмы» показано на рис. 6.16.

Отметим, что для перебора начального положения дисков
 «Энигмы» во время Второй мировой войны в Великобритании была
 создана «бабушка» современных компьютеров вычислительная
 машина под названием «Бомба» (см. рис.6.17).

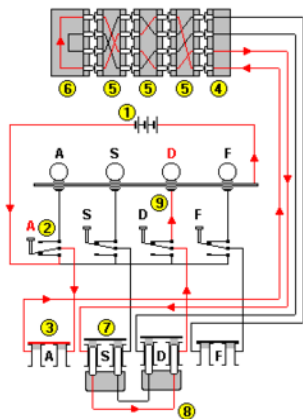


Рис. 6.15. Схема немецкого шифратора «Энигма» **Нет
 ссылки в тексте на этот рис стр 223**



Рис. 6.16. Четырехдисковый вариант «Энигмы» **Нет ссылки в тексте на этот рис стр 223**



Рис. 6.17. Электронно-вычислительная машина «Бомба»
Нет ссылки в тексте на этот рис стр 223

Первая модификация «Энигмы» обозначалась литерой А. Машина была тяжёлой и очень большой и напоминала печатную машину. Её размеры были $65 \times 45 \times 35$ см, и весила она около 50 кг. Потом была представлена модель «В» подобной же конструкции. Первые две модели «А» и «В» были совсем не похожи на более поздние версии. Были разработаны четыре варианта близких по конструкции машин, но коммерческого интереса к ним проявлено не было, вероятно потому, что машины были дорогими и сложными в обслуживании.

Ни ВМФ, ни МИД не приняли предложений изобретателя, поэтому он попробовал предложить свою шифровальную машину в гражданские секторы экономики. В армии и МИДе продолжали пользоваться шифрованием по кодовым книгам.

В 1923 году вышли воспоминания Черчилля, в которых он рассказал о криптоаналитических успехах англичан во время Первой мировой войны. Это вызвало шок у руководства немецкой армии. Немецкие офицеры узнали, что большая часть их военных и дипломатических сообщений была расшифрована британскими и французскими экспертами! И что этот успех во многом определялся слабостью немецких систем шифрования. Естественно, они начали искать надежные способы шифрования для военных сообщений. Поэтому у них возник интерес к Энигме. Естественно, они начали искать надежные способы шифрования для военных сообщений. Поэтому у них возник интерес к Энигме.

Массовое производство 3-х дисковых машин Энигма началось только в 1925 году и они использовались в коммерческих целях, а также в военных и государственных службах многих стран мира. Как и другие роторные машины этого периода, Энигма состояла из комбинации механических и электрических систем, которые позволяли реализовать многоалфавитный шифр подстановки, что давало высокую стойкость шифра для того времени. Ключ к шифру на определенный период, например сутки, определялся положениями каждого из 3-х роторов, которые легко менялись. При нажатии клавиши и кодировании очередного символа крайний ротор поворачивался на один шаг. После того, как он делал оборот, на один шаг поворачивался следующий ротор. Таким образом длина ключевой шифрпоследовательности имела период $26 \times 26 \times 26 = 17576$ и, так как сообщения обычно не превышали нескольких сотен символов, не было риска повтора позиции роторов при шифровании одного сообщения. Для повышения стойкости позднее был использован специальный коммутатор - "рефлектор", а тяжелая буквопечатающая машинка заменена на панель сигнальных лампочек, что привело к созданию компактной модели под названием - "ламповая Энигма-С". Трехдисковая Энигма предназначалась для сухопутных и военно-воздушных сил. В военно-морских силах эксплуатировалась как 3-х, так и 4-х роторные Энигмы – модели М3 и М4.

Чтобы сообщение было правильно зашифровано и расшифровано, машины отправителя и получателя должны были быть одинаково настроены, конкретно идентичными должны были быть: выбор роторов, начальные позиции роторов и соединения коммутационной панели. Эти настройки оговаривались заранее и записывались в специальных шифровальных книгах.

Семейство шифровальных машин Энигма насчитывает огромное количество моделей и вариаций дизайна. Ранние модели были коммерческими, начиная с 1920-х годов. Начиная с середины 1920-х годов, различные немецкие военные службы стали использовать эти машины, внося большое количество собственных изменений для повышения безопасности. Кроме того, другие страны использовали чертежи «Энигмы» для создания своих собственных шифровальных машин. Своеобразные клоны «Энигмы» были разработаны в ряде стран, например: Великобритания – TYPEX, США – M-325 (SIGFOY), Японии – “GREEN/JADE”, Швеции – B-21, Польше – “Lacida”.

Новая модель Энигма-D была выпущена в 1927 году и широко использовалась в Нидерландах, Великобритании, Японии, Италии, Испании, США, Польше, Швейцарии. В 1928 году немецкая армия внедрила собственную 4-хроторную модель Энигма-G («Энигма» абвера), модифицированную в 1930 году в модель Энигма-I (Энигма вермахта – размеры 28x34x15 см, вес около 12 кг). Существовала также большая 8-ми роторная печатающая модель Энигма II, которая использовалась для связи высших армейских структур, но вскоре Германия прекратила её использование из-за ненадежности. По приблизительным оценкам было выпущено более 100000 машин типа «Энигма» (а с учетом зарубежных клонов более 200000), из которых до конца войны вермахт закупил более 30000 машин. А. Шербиус никогда не узнал о беспрецедентном успехе своего шифратора Энигмы так как погиб в ДТП в 1929 году. По окончании Второй мировой войны союзнические силы продали трофейные машины, по прежнему считавшиеся на тот момент надёжными, в различные развивающиеся страны. Следует отметить, что сами немцы допускали возможность взлома шифра Энигмы. Ещё в 1930 году ведущий немецкий криптоаналитик Георг Шредер продемонстрировал такую возможность, вполне по-немецки заметив при этом: «Энигма – дерьмо!» Однако из-за постоянного усложнения моделей были периоды, когда английские криптографы из Блетчли-Парка не могли с ней справиться. Так, в Германии считали абсолютно надёжным шифрование 4-х дисковой Энигмой M4 поскольку возможен был выбор из огромного числа способов кодирования текстовых сообщений – 2x10¹⁴5(!)

Семейство моделей знаменитой немецкой криптографической машины под кодовым наименованием “Энигма”, предназначавшихся

для шифрования текстовых сообщений, отличилось завидным долголетием практического применения от эксплуатации первых образцов в середине 1920-х годов до краха гитлеровского рейха в 1945 году. История создания “Энигмы” и беспрецедентной тайной войны за добычу её образцов и разработки подходов к дешифрованию отражена в сотнях публикаций, а также в ряде документальных и художественных фильмов. На рис. 6.18 и 6.19 предстволнены фото некоторых разновидностей шифратора «Энигма».



Рис. 6.18. Фронтальная 3-дисконная «ламповая» «Энигма»
Нет ссылки в тексте на этот рис стр 227



Рис. 6.19. Японский клон 4-дискowej «Энигмы» [Нет ссылки в тексте на этот рис стр 227](#)

Другие немецкие шифрмашины довоенного и военного периода не получили и тысячной доли популярности в сравнении с «Энигмой». Ниже приблизительно в хронологическом порядке излагаются краткие сведения о некоторых немецких шифрмашинах, применявшихся до 1945 года.

Ручные механические машины предварительного шифрования текстовых сообщений широко применялись в Германии, Великобритании, США и ряде других стран, начиная с 1920-х годов и примерно до 1950-х. В истории немецкой криптографии к таким шифрмашинам относились, например, модели семейства Круга ([см. рис. 6.20](#)). Это была ручная полностью механическая двухдисксовая шифрмашинa (изобретатель Александр Круга, родившийся в 1891 году в Харькове на Украине) весьма своеобразного конструктивного оформления. Во время Второй мировой войны А. Круга был офицером Вермахта и разработал несколько версий своей машины, которая применялась в войсках и дипломатическом корпусе Германии. Стандартная машина была весом около 5 кг, но позднее была

сконструирована портативная модель под названием “Лилипут”. Шифраторы Крюга применялись республиканцами во время гражданской войны в Испании (были закуплены в Германии, как коммерческие шифраторы). Армия США проявляла интерес к этой машине и впоследствии группа криптографов, возглавляемая Вильямом Фридманом дешифровала зашифрованное сообщение длиной 1135 символов от ослабленной (с фиксированным приводом) модели за 2 часа 41 минуту [wiki.kryha.com].



Рис. 6.20. Немецкая механическая шифрмашинa Крюга.
Нет ссылки в тексте на этот рис стр 228

Таким образом, несмотря на свою популярность Крюга была криптографически слабой. Кроме того, насущная необходимость в буквопечатающих аппаратах, обеспечивающих автоматическое шифрование набираемого на клавиатуре текста с одновременной его передачей была очевидной из-за лавинообразного роста объемов секретной переписки. Немецкая также полностью механическая криптомашина с двумя дисками появилась в 1920 году, а её

электрифицированная версия использовалась дипломатами Германии и Англии. Применение таких машин, постоянно подключенных к линии связи, позволяло бы существенно повысить скорость передачи и приема шифрованных сообщений по сравнению с обычными методами ручного предварительного шифрования. Телеграфные аппараты того времени каждый символ кодировали кодом Бодо (был взят за основу при создании международного кода №1 в 1931 году) или МТК-2 (двух регистровый международный телеграфный код 1932 года). Код Бодо кодирует буквы в виде 5 - значной импульсной комбинации в линии связи, “1” или “0”. Т.о. $2^5=32$ таких комбинаций достаточно для кодирования 26 букв и 6-ти дополнительных служебных и управляющих знаков: “пробел”, “останов передачи”, “возврат каретки”, “сдвиг на строку”, “включение буквенного регистра”, “включение регистра с цифрами и символами”. При использовании в качестве носителя информации телетайпной ленты двоичным знакам соответствовали круглые отверстия « 1 » в ней или их отсутствие « 0 ».

Стандартная скорость передачи информации по радио составляла 50 импульсов в секунду (скорость 50 бод). Возможны 2 режима работы шифратора. В реальном масштабе времени открытый текст вводится с клавиатуры и шифруется машиной, которая передает шифрованные комбинации вместо букв открытого текста в линию связи. В режиме предварительного шифрования шифртекст создается на перфоленте для последующей передачи в канал связи. Засекречивание осуществляется суммированием по модулю 2 пятиразрядных двоичных комбинаций, соответствующих буквам открытого текста и случайной гамме, зафиксированной на другой бумажной перфоленте. В канал связи передаются посылки из 7-ми импульсов. Первый из них является стартовым, заставляя приемник принять следующие за ним 6 импульсов. Из них 5 импульсов передают информацию о кодированной букве, а последний является стоповым сигналом.

Одна из крупнейших электротехнических немецких фирм Siemens & Halske в 1929-1932 годах разработала первый вариант “Der Geheimfernsehrreiber” (патент под наименованием “Anordnung zur Nachrichtenübermittlung in Geheimschrift über Telegraphenanlagen” - устройство для передачи шифрованных сообщений по телеграфу). Общим наименованием для целой серии подобных механических секретных буквопечатающих телеграфных аппаратов впоследствии

стало “Geheimfernschreiber” или “Schlüssel fernschreibmaschine” (SFM). Алгоритмы формирования шифрующей гаммы реализовывались механически с помощью вращающихся кодирующих элементов, имевших одинаковое или различное число возможных положений.

Так, если 3-х-дисковая (число возможных положений каждого диска - 26) модель “Энигмы” тактического применения имела общее число возможных ключей $26 \times 26 \times 26 = 17576$, то 10 дисков наиболее секретной версии «Geheimschreiber» (русский перевод - “личный секретарь”) вращались с периодами 47, 53, 59, 61, 64, 65, 67, 69, 71 и 73, генерируя шифрующую гамму с периодом $47 \times 53 \times 59 \times 61 \times 64 \times 65 \times 67 \times 69 \times 71 \times 73 = 893622318929520960$. Таким образом общее число ключей было значительно больше.

Geheimschreiber постепенно развивался, и нашли применение различные его модели. Первой машиной, которую начала использовать криптографическая служба, была модель T52A/B (разработка 1937 года под наименованием “Geheimzusatz”). Позже были введены в эксплуатацию T52C, D и E. Существовали также разновидности каждой модели. Последняя разработанная модель этого семейства шифраторов таинственная T52Y (ясности с Y-машиной нет; возможно, что это была машина фирмы “Siemens & Halske” типа T-43 с одноразовой лентой). Тем не менее, все они основывались на схожих принципах. После войны, для своей секретной переписки модернизированные захваченные машины использовала полиция Норвегии.

В шифраторах T52 a/b (см. рис. 6.21) имеется коммутационная панель, которая позволяет менять местами выходные данные колес (место пробивки каждого элемента кода), то есть осуществляется операция перестановки. Для этого использовались 5 колес, а оставшиеся другие 5 колес использовались для создания гаммы и дальнейшего суммирования. Полученные десять значений помечались "1", "3", "5", "7", "9", и I, II, III, IV, и V, с помощью этой последовательности открытый текст и преобразовывался в шифрованный. Значения на колесах I - V складывались по модулю 2 с символами открытого текста в коде Бодо. Затем элементы кода в символе переставлялись: "1" вызывала перестановку знаков 1 и 5; "3", "5", "7", и "9" переставляли знаки 4 и 5, 3 и 4, 2 и 3, и наконец 1 и 2. Нуль на соответствующем по порядку колесе разрешал перестановку, а единица запрещала.

После зашифровывания каждого символа все десять колес перемещались вперед на одну позицию (надо помнить, что периоды вращения колес имели разную величину), и формировалась новая гамма для суммирования с открытым текстом и новая перестановка. Поскольку периоды колес были взаимно просты, битовая последовательность начинала повторяться только после зашифровывания текста длиной $47 \times 53 \times \dots \times 71 \times 73 = 893\,622\,318\,929\,520\,960$ символов. Это же значение соответствовало и числу возможных начальных ключевых установок колес.

Операции суммирования и перестановки осуществлялись с использованием электромеханических реле. Изменение (наложение гаммы) осуществлялась пятью реле, а пять других отвечали за перестановку. Реле управлялись кодирующими колесами, которые, через набор штифтов и пазов, могли соединять реле случайным образом.

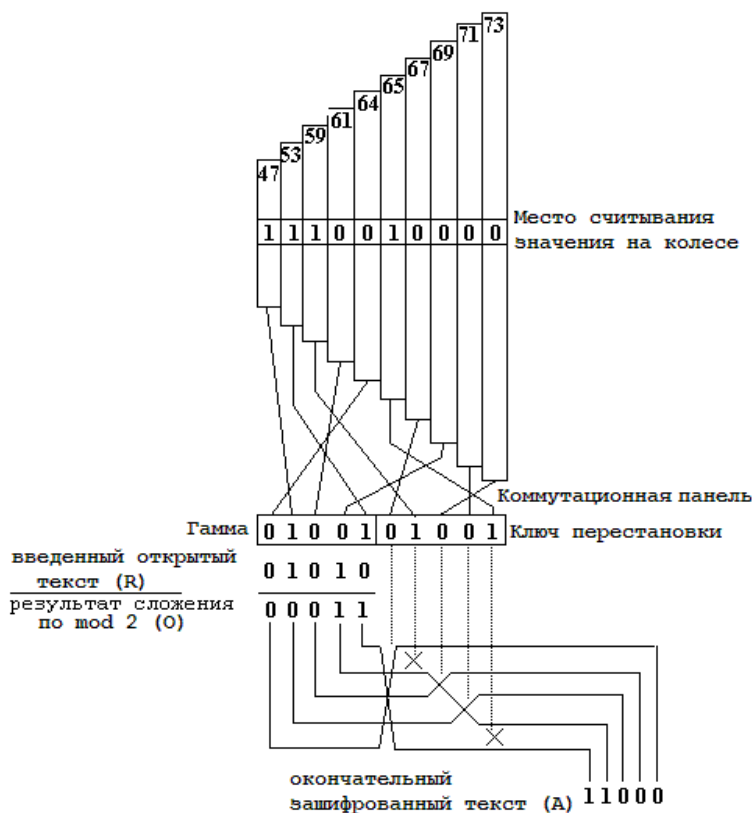


Рис. 6.21. Схема блока шифрования T52a/b. **Нет ссылки в тексте на этот рис стр 231**

В T52c (см. рис. 6.22) был реализован более сложный алгоритм выработки ключевой последовательности. В начале формируется десять комбинаций по четыре колеса в каждой. Каждое колесо участвует в четырех комбинациях. Во время каждого такта значения, снимаемые с четырех колес входящих в комбинацию, складывались по модулю 2. В результате получалось десять знаков, которые подвергались перестановке с помощью коммутационной панели. Полученная десяти битная комбинация использовалась для шифрования очередного знака открытого текста. Считывание с колес последовательностей, отвечавших за образование гаммы и перестановку, в T52c выполнял механизм, называвшийся

«пятиугольник». Таким образом, основными элементами ключа являются, начальные угловые положения 10 колес и коммутационная панель. **10 КОЛЕС ИЛИ 10-ЗУБЧАТЫХ КОЛЕС?**

T52c-схематический рисунок

выходные данные 10 зубчатых колес

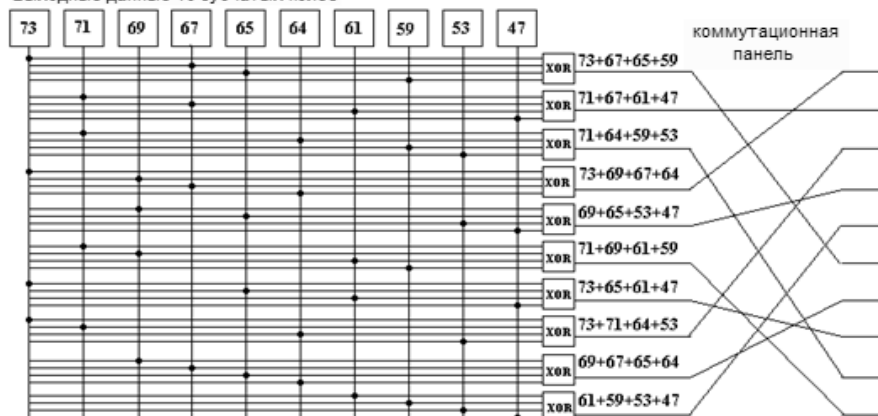


Рис. 6.22. Схема устройства телеграфного шифровального аппарата T52c.

Разработчики «Geheimschreiber» T52 полагали, что применение шифра гаммирования и шифра перестановки при использовании ключевой последовательности большой длины приведет к тому, что в линии связи будет передаваться нечитаемая криптограмма с гарантированной стойкостью. Количество возможных коммутаций колес и их начальных положений до изобретения компьютеров считалось чрезвычайно большим числом. Однако T52a/b и T52c оказались криптографически нестойкими и их место заняла модель T52d (см. рис.6.23).

В отличие от модели T52c, в T52d, не было «пятиугольника», использовалась не сумма показаний нескольких колес, а значение на каждом отдельном колесе. Движение колес стало нерегулярным. Сдвигать или не сдвигать каждое конкретное колесо после зашифровывания символа, определялось по двум другим колесам, но таким образом, чтобы все одновременно никогда не простаивали. Кроме считывания показаний колес в основной (шифрующей) точке вывода, их показания также снимались в точке на 25, 24, 23, 23, 22, 22, 20, 20, 18, и 16 позиций раньше, соответственно. И эта дополнительная информация управляла перемещением колес.

Все операции суммирования и перестановки осуществлялись с использованием электромеханических реле. Смена полярностей при наложении гаммы осуществлялась пятью реле, а пять других реле отвечали за перестановку. Реле управлялись кодирующими колесами, которые, через набор штифтов и пазов, могли соединять реле случайным образом.

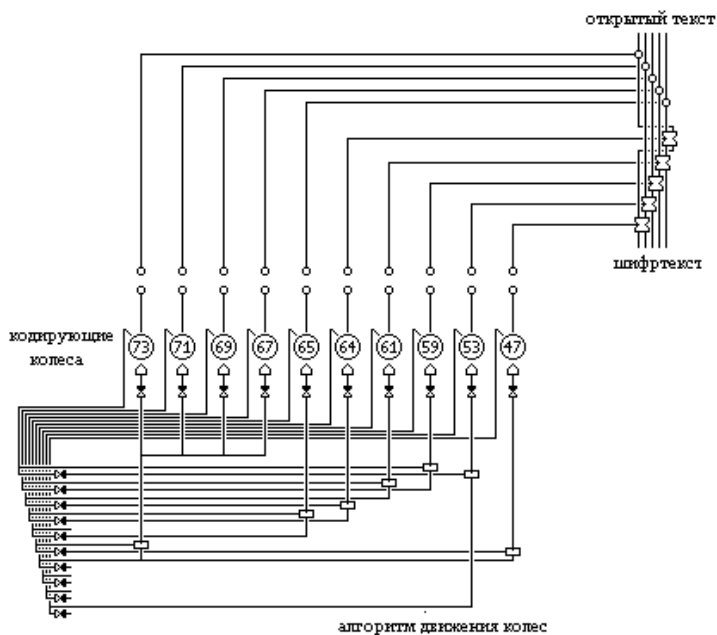


Рис. 6.23. Схема устройства телеграфного шифровального аппарата T52d. Нет ссылки в тексте на этот рис стр 234

Окончательная версия машины, T52e (см.рис. 6.24), включила в себя все улучшения, которые прежде появлялись отдельно в других моделях шифратора, однако, в ней остались и прежние недостатки. Например, невозможность изменять положения штифтов.

Машине T52 предшествовала экспериментальная модель “Schlüsselgeraet 39” (SG-39), созданная в 3-х экземплярах. Эту 3-хдисковую полностью автоматическую шифрмашину с электромоторным приводом изобрел Фриц Мензер из контрразведки Абвера в 1939 году. Предполагалось, что она заменит “Энигму” т.к. период шифграммы новой машины более, чем в 15000 раз ($2,7 \times 10^8$

символов) превышал количество возможных ключей “Энигмы”. По словам оператора, работавшего на одной из них, военные не сочли её приемлемой из-за несоответствия специальным эксплуатационным требованиям.

К середине войны количество шифраторов “Энигма”, использовавшихся немцами было весьма велико. Однако, определенные сомнения в гарантированной стойкости засекречивания сообщений этим дисковым шифратором появились у немецких ученых-криптографов ещё в конце 1930-х годов. В 1941 году в компании Wanderwerke, специализировавшейся на пишущих машинках, Ф.Мензер начал разработку шифрмашины SG-41,

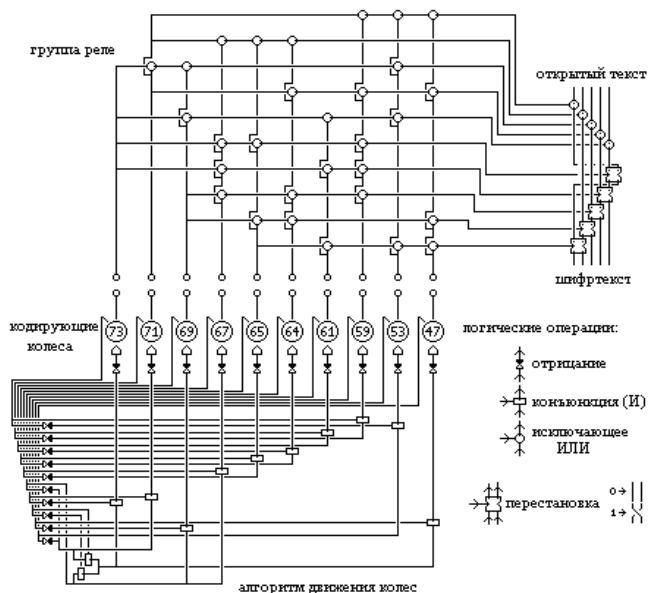


Рис. 6.24. Схема устройства телеграфного шифровального аппарата T52e. **Нет ссылки в тексте на этот рис стр 235**

получившей впоследствии жаргонное кодовое наименование “Hitlermuhle” (мельница Гитлера, т.к. сленговым словом для пишущих машинок в немецком языке было именно “muhle”). Функционально и конструктивно SG-41 имела некоторое сходство с американской машиной M-209 и швейцарской BC-38, “прародителем” которых был Борис Хагелин (о нем ниже). Фирма Хагелина не имела патентов в Германии и поэтому его недовольство осталось неудовлетворенным.

И хотя отдельные удачные конструктивные решения действительно были скопированы с BC-38 в целом SG-41 была новой конструкцией с рядом преимуществ по сравнению с шифраторами Хагелина. В середине 1944 году германское Верховное командование заказало 11000 машин SG-41 для армии и ещё 2000 машин SG-41Z для шифрования сводок метеорологической службы BBC Германии. Но из-за нехватки цветных металлов таких, как магний и алюминий и победного шествия советских войск к границам Германии к концу войны было поставлено по разным данным от 500 до 1000 экземпляров и использовалась Абвером и немецкими дипломатами с 1944 года. В настоящее время криптографическое превосходство SG-41 в сравнении с машинами Хагелина не доказано, хотя сохранилось 2 музейных работоспособных экземпляра этого шифратора.

Первая шифрмашинка из семейства SZ-40/SZ-42/SZ-43 (см. рис. 6.25 и 6.26) была разработана в конце 1930-х годов фирмой “Standard Elektrik Lorenz”, а обозначение “SZ” означало “SchlüsselZusatz” (шифрующая приставка), поскольку наиболее секретный механизм шифратора помещался в блоке, который мог извлекаться из машины в случае опасности.

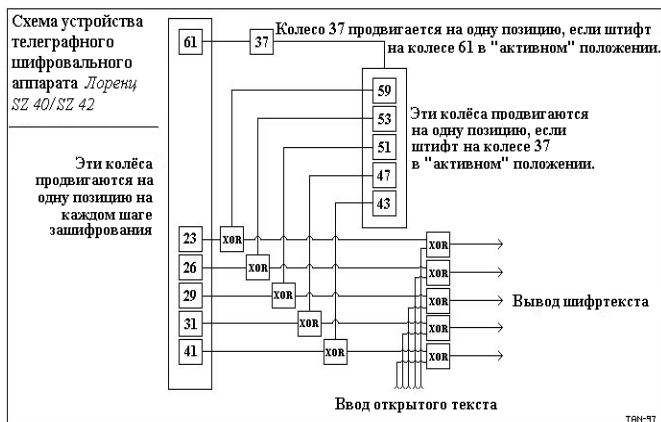


Рис. 6.25 Схема шифратора семейства SZ-40/SZ-42/SZ-43

Нет ссылки в тексте на этот рис стр 237

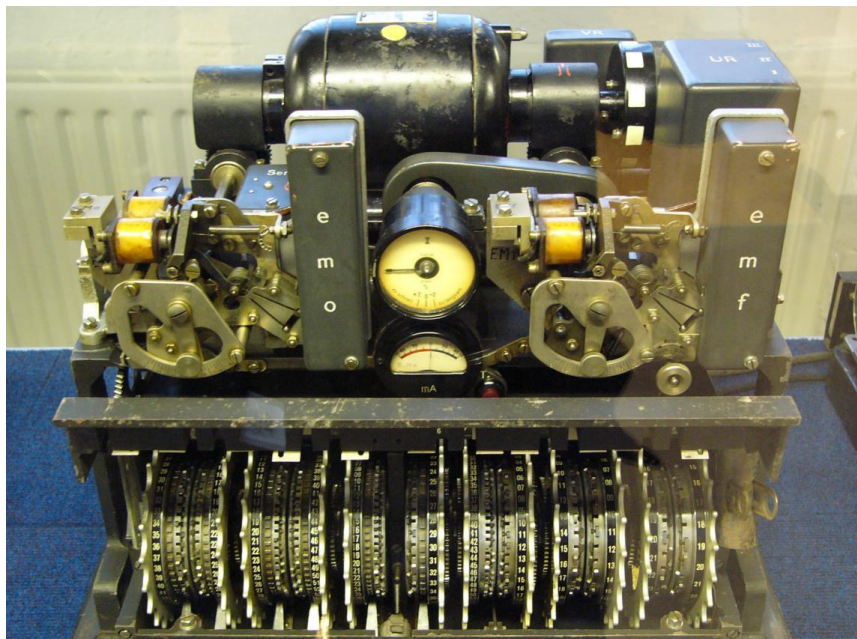


Рис. 6.26. Шифратор Lorenz SZ-42 **Нет ссылки в тексте на этот рис стр 237**

К отдельному классу принадлежала шифрмашинa T-37 ICA, разработанная “Siemens & Halske ” во второй половине 1930-х годов. По существу к стандартному коммерческому телетайпу T-37 был добавлен внешний шифрблок с механическим приводом от T-37, представлявший собою считыватель информации с бумажной “ключевой” перфолентой, содержавшей гамму шифрования в коде Бодо. Принцип шифрования - суммирование по модулю 2 (исключающее или) ключа и открытого текста. На левой стороне T-37 ICA загорались большие сигнальные лампы красного или зеленого цвета при нажатии кнопок соответственно режимам работы - “открытая” или “шифрованная” передача.

Аппарат T-37 ICA не являлся секретным. Однако это не относилось к ключевой перфоленте, которая была секретной. Перфолента находилась в специальной кассете, правила хранения которой, передачи её двум операторам, осуществлявшим установку и извлечение кассеты из шифрмашины перед и по окончании работы.

На ключевых лентах имелись специальные маркеры, позволявшие операторам на передаче и приеме осуществить строго одинаковую установку лент в считывающие устройства и обеспечить синхронную работу 2-х шифрмашин. Ключевые ленты использовались однократно и затем уничтожались. Машины T-37 ICA располагались в рабочих бункерах. Эти шифраторы были очень шумными, причем вплоть до того, что операторы боялись оглохнуть, т.к. звуки работающей аппаратуры напоминали стрельбу из пулеметов по стальным бочкам. Кроме этого, шифрмашины устанавливались на мягкие маты, в середине которых размещалось 100 грамм мощной взрывчатки, предназначенной для уничтожения машины в случае внезапного нападения или экстренной эвакуации, что дополнительно создавало весьма нервную обстановку для обслуживающего персонала. T-37 ICA были выведены из эксплуатации в 1980 годах.

В конце войны по рекомендации немецких операторов была создана новая шифровальная машина, конструктивно похожая на T-37 ICA. Об этом шифраторе ничего не было известно вплоть до ноября 1944 года, когда упоминание о нем появилось в перехваченном сообщении к немецкому воздушному аташе в Стокгольме.

Это была поздняя модель “Siemens & Halske ” T-43 использовавшая одноразовую ключевую перфоленту. После того как очередной знак гаммы был считан, для уничтожения использованной одноразовой ключевой перфоленты, на ней пробивались пять отверстий немного большего диаметра чем у стандартного телеграфного оборудования.

При использовании “хорошего” генератора случайных импульсных последовательностей в производстве ключевых перфолент и соблюдении всех установленных нормативных правил эксплуатации криптографической техники шифрмашин T-37 ICA и T-43 могли считаться стойкими.

В заключении несколько слов о судьбе немецких криптографов в послевоенное время. По заданию TICOM (“Target Intelligence Committee ” – “Комитет по целевой разведке”) в последние месяцы войны две сотни ведущих криптографов Германии были тайно переброшены в Великобританию. В марте 1945 года шесть специально подготовленных англо-американских групп были отправлены в Германию, с первоначальной задачей найти и захватить немецкие криптографические центры, местоположение которых было установлено, главным образом, благодаря дешифровавшейся в Блечли

Парк "Энигме". Главная задача групп ТИСОМ состояла в том, чтобы захватить столько германского криптооборудования, сколько будет возможно и вывести его вместе с обслуживающим персоналом. Одна из групп была послана для захвата замка в Саксонии, где находился архив радиоразведки министерства иностранных дел. В результате успешной операции весь этот объект, включая и штатных сотрудников, был переправлен в Британию.

Эта же группа ТИСОМ захватила конвой грузовиков, в котором перевозили четыре германских шифратора "Fish", группу техников-шифровальщиков и командовавшего ими офицера. Всю эту технику вместе с людьми также отправили в Англию. Добытые в Германии материалы дали англо-американским союзникам информацию о том, какие из их собственных шифров были вскрыты немцами. В частности, оказалось, что Германия успешно читала "Шифр ВМС №3", использовавшийся британскими и американскими конвоями в Атлантическом океане. Именно по этой причине конвои столь часто становились жертвой атак немецких подводных лодок. Собранные ТИСОМ данные позволили впоследствии читать секретную переписку, по крайней мере 35 стран, включая Францию, Италию, Японию, Испанию, Швейцарию и Ирландию.

В начале XX века в Швеции разработкой шифраторов занимался Арвид Герхард Дамм (Arvid Gerhard Damm). Свою карьеру Дамм начал в качестве инженера в текстильной промышленности. С юных лет Дамм очень увлекался механикой и изобретательством. Интерес к шифровальному делу пробудился у Дамма под влиянием его брата, криптоаналитика-любителя, преподававшего математику в средней школе в шведском городе Евле.

Дамм разработал шифрмашину, и ему удалось передать информацию о своем изобретении одному своему знакомому, работавшему в шведском посольстве в Берлине, который и организовал встречу Дамма с капитаном 3-го ранга Олафом Гюльденом, начальником Королевского морского училища в Стокгольме. В 1915 (по другим данным в 1916) году Гюльден и Дамм основали свою фирму «Aktiebolaget Cryptograph». Компаньоны собирались продавать ряд шифровальных машин, спроектированных Даммом после Первой мировой войны. Шифровальное устройство, изобретенное Даммом (патент #52,279 от 10 октября 1919 года), было двухдисковым: два шифрдиска вращались над и под горизонтальной неподвижной пластиной. Движением шифрдисков управляли

зубчатые колеса, которые позволяли поворачивать их на различное количество позиций для каждой буквы открытого текста. Придуманый Даммом шифрующий механизм оказался громоздким и сложным и никогда не был построен.

Огромный вклад в мировую криптографию внес Борис Цезарь Вильгельм Хагелин. Он родился 2 июля 1892 года на Кавказе, где некоторое время работал его отец, который был управляющим российским отделением нефтедобывающей компании Альфреда Нобеля, того самого Нобеля, кто изобрел динамит и является учредителем знаменитой Нобелевской премии. В течение нескольких лет Борис учился в Санкт-Петербурге, а затем отправился в Швецию и в 1914 году окончил Королевский технологический институт в Стокгольме, получив диплом инженера-механика. Затем шесть лет работал в шведском филиале американской компании «Дженерал Электрик», а потом около года провел в США на службе в компании «Стандарт Ойл».

Борис проявлял тягу к изобретательству, увлекался техникой. В круг интересов молодого Хагелина входила и криптография, Последнему он уделял повышенное внимание. В 1920 году Б. Хагелин сумел создать первый в мире электромеханический шифратор. В нем имелись клавиатура и индикаторные лампы для набора и вывода открытых и шифрованных текстов.

Шифратор А-22 «Cryptograph» – достаточно простой механический шифратор многозначной замены, состоящий из:

- барабана, содержащего 29 переставленных букв алфавита шифрованного текста;
- линейки, содержащей буквы открытого текста в алфавитном порядке, находящейся в 2-х возможных позициях – верхней и нижней;
- штифтового колеса с 25-тью угловыми положениями, управляющим положением линейки.

Шифратор имеет окошко, открывающее два перемешанных алфавита барабана. Линейка с алфавитом открытого текста, находясь в верхнем или нижнем положении, в каждый такт работы шифратора (зашифрования каждой буквы открытого текста) закрывает один из видимых в окошко алфавитов барабана - либо верхний, либо нижний, соответственно. Таким образом, формируется замена: открытая буква считывается с линейки и заменяется на соответствующую букву шифрованного текста, находящуюся на барабане (располагающуюся под или над буквой открытого текста в

зависимости от расположения линейки). После процесса зашифрования одной буквы (одного такта шифрования), барабан с перемешанными алфавитами сдвигается на две угловые позиции, штифтовое колесо – на одну и определяется новое расположение линейки, исходя от текущего расположения “активных” штифтов колеса.

Отметим, что описанный шифратор не является стойким. Действительно, разбив шифрованный текст на группы по 29 символов в каждой и подписав группы одна под другой, получим, что при формировании букв шифрованного текста каждого столбца участвовало только 2 алфавита, что естественным образом позволяет найти открытый текст. Правда инструкция по использованию данного шифратора предполагает после шифрования определенного числа букв, несколько тактов шифрования осуществлять в “холостую”, что естественным образом увеличивает стойкость рассмотренного шифратора [Бутырский, 2007], [Бутырский, 2007-2].

В 1921 (по другим сведениям в 1922) году отец Бориса Цезарь Хагелин и племянник Альфреда Нобеля Эммануэль устроили его в фирму «AB Cryptoteknik», основателем которой, как было сказано выше, был А. Дамм, а Ц. Хагелин и Э. Нобель были основными акционерами этой фирмы. Борис, фактически, представлял интересы главных акционеров предприятия. Придя на фирму Дамма, Б. Хагелин активно включился в работу по созданию новых шифрмашин с приемлемыми для потенциальных потребителей размерами, ценой и криптографической стойкостью.

Первым крупным успехом Б. Хагелина стала модификация одного из дисковых шифраторов, разработанных Даммом. В 1925 году он узнал, что Генеральный штаб Швеции решил ознакомиться с немецким шифратором «Энигма». К этой шифрмашине внимание шведских вооруженных сил привлекла одна немецкая компания, которая собиралась заняться поставками их в Швецию при условии одобрения шведской стороны. Хагелин сообщил штабу, что фирма, в которой он работает, готова разработать и предложить более подходящую шифрмашину шведского производства. Для выполнения этой работы Хагелину было выделено 6 месяцев. Изготовление опытного образца этого шифратора, который получил название В-21, обошлось фирме АВ Сгуртограф в 500 шведских крон (примерно 110 долларов в то время). Дамм весьма критически отнесся к работе своего коллеги, а вот шведские военные остались довольны В-21 и в

1926 году сделали крупный заказ на ее поставку. Хагелин выиграл соревнование с «Энигмой», и для последней путь в Швецию был закрыт. После смерти в начале 1927 года Дама, Б. Хагелин возглавил фирму, которая получила название «Aktibolaget Cryptoteknik». Он сосредоточил свои усилия на создание шифраторов с возможностью печати шифртекста. В В-21 (см. рис. 6.27), как и в шифраторе «Энигма», использовались электрические лампочки, которые загорались, отмечая текущую зашифрованную букву при наборе буквы открытого текста на клавиатуре. Для стационарного использования была создана модификация В-22, которая предусматривала возможность подключения к стандартным электромеханическим пишущим машинкам, так что шифрованный и расшифрованный тексты автоматически распечатывались. Однако получившееся в результате шифровальное устройство оказалось слишком громоздким. Поэтому вскоре Хагелин решил объединить в одной машине и печатающий, и шифрующий механизмы.



Рис. 6.27. Шифратор В-21 **Нет ссылки в тексте на этот рис стр 243**

Позднее, в 1932 году армия Франции объявила конкурс на шифратор для французской армии. Эта система должна была быть настолько компактной, что могла бы помещаться в карман армейской шинели и применяться непосредственно на поле боя. Кроме того, шифратор должен снабжаться независимым печатающим устройством. Шифраторы В-21, В-22 не отвечали этим требованиям. Хагелин принял и это предложение и создал компактный шифратор В-211.

Рассмотрим криптографические принципы работы шифратора. Предварительно буквы алфавита открытого текста записываются в таблицу размером 5x5 (одна буква с наименьшей частотой встречаемости выбрасывается, для шведского языка - буква «W»). Порядок записи алфавита в таблицу может быть различным и являться дополнительным ключевым параметром. Каждая буква открытого текста представляется парой чисел, задающих положение буквы в соответствующей таблице, по горизонтали и вертикали.

Процесс **зашифрования** **все правильно** **ЕЩЕ ОДИН ТЕРМИН** буквы заключается в шифровании каждой координаты в отдельности, осуществляемый двумя роторами, реализующими преобразования коммутации. Угловые положения роторов отмечаются соответствующей буквой латинского алфавита от А до К (без J), всего 10 позиций. Роторы шифратора В-211 отличаются от роторов в шифраторе «Энигма». Вместо 26 входов и 26 выходов (как в «Энигме») в шифраторе В-211 каждый ротор содержит 5 входных контактов и 10 выходных контактов. Таким образом, формируется одна из 2 – х возможных коммутаций для каждого ротора при текущем угловом положении в зависимости от четности такта шифрования. Вращением роторов управляют 4 штифтовых колеса, имеющих различное число угловых положений: 23, 21, 19 и 17.

Угловым положениям колес соответствуют буквы латинского алфавита:

- для 1-го - от А до Х,
- для 2-го - от А до V,
- для 3-го - от А до Т,
- для 4-го - от А до R.

На каждом колесе имеются штифты (стержни), соответствующие каждому угловому положению колеса, которые могут находиться либо в рабочем, либо в нерабочем положении. В текущем такте шифрования правильно штифты всех колес, влияющих на движение роторов формируют текущую штифтовую комбинацию.

Первые два колеса (с периодом обращения 23 и 21) управляют движением 1 – го ротора по следующему принципу: если один из двух, или оба штифта в текущей штифтовой комбинации 1- го и 2- го колеса находятся в рабочем положении, то 1-й ротор после зашифрования буквы открытого текста сдвигается на один шаг, иначе простаивает.

Аналогичным образом, движением второго ротора управляет 3 – е и 4 – е колеса. В результате движение роторов становится нерегулярным, в отличие от регулярного, последовательного движения соответствующих роторов в «Энигме». После шифрования каждой буквы, колеса сдвигаются на одну позицию. Полный период колес равен $23 \times 21 \times 19 \times 17 = 156009$, что на порядок выше, чем у Энигмы.

Начальное положение роторов и колес является сеансовым ключом и определяется набором из шести букв латинского текста : первые две буквы – для определения начальных угловых положений роторов, остальные - для положений колес.

Процесс расшифрования правильно является обратным процессу зашифрования правильно. При этом специальная ручка на шифраторе переводится в положение «расшифрование».

Этот шифратор весил около 17 килограммов, работал со скоростью 200 знаков в минуту и помещался в деревянном футляре размером с большой портфель. Конечно до «карманных размеров» было еще далеко, но тем не менее, в первой половине 1930-х годов это был самый компактный печатающий шифратор [Бутырский, 2007].

Этот шифратор в то время удовлетворял потребностям французской армии и был поставлен ими на вооружение. Возможно некоторое количество этих машин было продано в СССР или хотя бы предложено для ознакомления.

В 1934 году французский генеральный штаб уточнил задачу. Хагелина попросили создать «карманную» шифрмашину для нужд французской армии. Хагелину удалось разработать компактный механический печатающий шифратор, который мог использоваться

одним человеком и пригодный для использования в полевых условиях. В результате появился шифратор, названный С-35.

Механическую схему шифратора С-35 можно условно разделить на 3 блока:

- наборно-печатающего блока;
- блока вращающихся колес;
- барабана с линейками.

Наборно-печатающий блок позволяет выставлять букву открытого текста и считывать её зашифрованный эквивалент с возможностью печати его на бумажную ленту.

Блок вращающихся колес представляет из себя 5 колес с различным периодами обращения, соответствующими числу их угловых положений, помеченных буквами латинского алфавита:

- 25 для 1-ого: A B C D E F G H I J K L M N O P Q R S T U V X Y Z;

- 23 для 2-ого: A B C D E F G H I J K L M N O P Q R S T U V X;

- 21 для 3-ого: A B C D E F G H I J K L M N O P Q R S T U;

- 19 для 4-ого: A B C D E F G H I J K L M N O P Q R S;

- 17 для 5-ого: A B C D E F G H I J K L M N O P Q

(буква W удалена из алфавита).

После каждого такта шифрования все колеса сдвигаются на одну позицию. В связи с тем, что периоды обращения колес попарно взаимно простые числа, полный период обращения всех колес равен $17 \times 19 \times 21 \times 23 \times 25 = 3\,900\,225$.

То есть, если при начале процесса шифрования угловым положениям колес соответствовало AAAAA, то данная комбинация впервые появится снова через 3900225 тактов работы шифратора.

На каждом колесе имеются специальные штифты, количество которых соответствует числу угловых положений колеса. Каждый штифт может быть выдвинут либо вправо и являться “нерабочим” (считаем, что при этом значение данного штифта равно “0”), либо влево и являться “рабочим” (значение штифта соответствует “1”). Расположение штифтов на колесах образует долговременный ключ шифратора.

Штифты колес, находящиеся в верхней позиции, образуют так называемую текущую штифтовую комбинацию, представляющуюся двоичным вектором, например (10101). Над каждым штифтовым колесом с левой стороны располагаются специальные рычажки. Если

на данном колесе в текущей штифтовой комбинации штифт находится в рабочем положении (значение штифта равно “1”), то соответствующий рычажок выдвигается вверх.

Барабан с линейками представляет из себя два диска, соединенных стальными прутьями – линейками. Всего линеек 25. На каждой линейке напротив колес находятся неподвижные зажимы – рейторы. Расположение рейторов на линейках в шифраторе С-35 строго фиксированы. Рейторы расположены:

- на 1-ой линейке – напротив 1-ого колеса (всего 1 рейтор);
- на 2, 3-ей линейке – напротив 2-ого колеса (всего 2 рейтора);
- на 4–7-ой линейке – напротив 3-ого колеса (4 рейтора);
- на 8–15-ой линейке – напротив 4-ого колеса (8 рейторов);
- на 16–25-ой линейке – напротив 5-ого колеса (10 рейторов).

Нажатие рукоятки шифратора с правой стороны приводит к вращению барабана с линейками. При этом рейторы, имеющие специальные скосы, соприкасаются с выдвинутыми рычажками и выдвигают свою линейку (на которой они располагаются) влево. Выдвинутые таким образом линейки образуют шестеренку с переменным числом зубьев, которая, в свою очередь, через шестереночно-передаточный механизм приводит к вращению колеса наборно-печатающего блока на определенное, произвольное число угловых положений. Таким образом, рассматриваемый шифратор – пример механического шифра гаммирования. Так как число рейторов фиксировано (1 – напротив 1-ого колеса, 2 – напротив 2-ого, 4 – 3-его, 8 – 4-его, 10 – 5-ого), то сдвиг колеса может изменяться от 0 (если текущая штифтовая комбинация является нулевым вектором) до 25 (при единичном штифтовом векторе). После такта шифрования все колеса блока штифтовых колес сдвигаются на 1 угловую позицию и появившаяся новая штифтовая комбинация выдвигает соответствующие рычажки.

Инициализация шифратора заключается в установке “рабочих” и “нерабочих” штифтов на колесах (долговременного ключа) и выставлению начальных их угловых положений, которым соответствует 5-ти грамма букв латинского алфавита, расположенных на колесах (разовый ключ, как правило, свой при шифровании каждой телеграммы).

Для демонстрации и лучшего понимания функционирования шифратора обратимся к рисунку 6.28, на котором в каждом такте шифрования телеграммы с содержанием

"Enemy of battalion strength advancing along eastern railway"

показаны: текущие штифтовые комбинации, угловые положения штифтовых колес, сдвиг (знак гаммы), буква, подлежащая шифрованию и её значение при зашифровании. Заметим, что начальное расположение штифтовых колес соответствует положению ААААА, а знаки пробелов между словами заменяются на литеру "Z" и также подлежат зашифрованию [Бутырский, 2007].

1	2	4	8	10	Положение колес	Сдвиг	О.Т.	Ш.Т.	1	2	4	8	10	Положение колес	Сдвиг	О.Т.	Ш.Т.
0	1	0	1	0	A A A A A	10	E	F	1	0	1	1	1	F H J L N	23	V	B
1	1	1	1	1	B B B B B	25	N	L	0	0	0	0	0	G I K M O	0	A	Z
1	1	0	0	0	C C C C C	3	E	Y	1	1	0	1	1	H J L N P	21	N	H
0	0	1	1	0	D D D D D	12	M	Z	0	0	1	0	1	I K M O Q	14	C	L
1	1	1	0	1	E E E E E	17	Y	S	1	1	0	1	0	J L N P A	11	I	C
1	1	0	1	0	F F F F F	11	Z	L	0	0	0	0	1	K M O Q B	10	N	W
0	1	1	1	1	G G G G G	24	O	J	1	1	1	0	0	L N P R C	7	G	A
1	0	0	0	0	H H H H H	1	F	V	1	1	1	1	0	M O Q S D	15	Z	P
0	0	1	0	0	I I I I I	4	Z	E	0	0	1	1	1	N P R A E	22	A	V
1	1	1	1	0	J J J J J	15	B	N	1	0	1	1	0	O Q S B F	13	L	B
0	0	0	1	1	K K K K K	18	A	R	1	1	0	0	1	P R T C G	13	O	Y
1	1	0	1	0	L L L L L	11	T	R	1	0	0	1	0	Q S U D H	9	N	V
1	0	1	0	1	M M M M M	15	T	V	0	0	0	0	0	R T A E I	0	G	T
0	1	0	1	1	N N N N N	20	A	T	1	1	1	1	0	S U B F J	15	Z	P
1	1	0	0	0	O O O O O	3	L	R	0	1	0	1	1	T V C G K	20	E	P
1	0	1	1	1	P P P P P	23	I	O	0	0	1	0	0	U X D H L	4	A	D
1	0	1	0	1	Q Q Q Q Q	15	O	A	0	1	1	0	1	V A E I M	16	S	X
0	1	1	0	0	R R R R A	6	N	S	0	1	0	1	1	X B F J N	20	T	A
1	0	1	1	1	S S S S B	23	Z	X	1	1	1	1	0	Y C G K O	15	E	K
0	0	0	1	0	T T T A C	8	S	P	0	0	0	1	1	Z D H L P	18	R	A
0	1	0	1	0	U U U B D	10	T	Q	0	1	1	0	1	A E I M Q	16	N	C
0	1	0	0	1	V V A C E	12	R	U	1	1	1	1	0	B F J N A	15	Z	P
0	0	1	1	0	X X B D F	12	E	H	1	1	0	0	1	C G K O B	13	R	V
1	1	0	0	1	Y A C E G	13	N	Z	0	0	0	1	0	D H L P C	8	A	H
0	1	1	1	0	Z B D F H	14	G	H	1	0	1	0	0	E I M Q D	5	I	W
0	1	1	1	0	A C E G I	14	T	U	1	1	0	0	1	F J N R E	13	L	B
1	0	0	0	0	B D F H J	1	H	T	0	0	0	1	0	G K O S F	8	W	L
1	1	1	0	1	C E G I K	17	Z	R	1	1	1	1	1	H L P A G	25	A	Y
0	1	0	1	0	D F H J L	10	A	J	0	0	1	1	0	I M Q B H	12	Y	N
1	1	1	1	1	E G I K M	25	D	V	1	1	1	0	0	J N R C I	7	Z	H

Рис. 6.28. Иллюстрация процесса шифрования шифратором С-35

В октябре 1937 года французы одобрили шифрмашину, шесть экземпляров слегка модифицированного шифратора, названного С-36 были переданы шведским военно-морским силам для испытаний. Фактически шифратор С-36 тот же С-35, но с двумя весьма существенными дополнениями: наличием дополнительной крышки, 248

закрывающей шифратор на ключ и подвижных рейторов, расположение которых теперь не фиксировано, а является ещё одним ключевым параметром (долговременным ключом). Этот аппарат реализовывал шифр гаммирования и отличался небольшими габаритами ($83 \times 140 \times 178$ мм) и массой. Хагелин даже добился, чтобы «С-36» распечатывал шифртекст с разбиением на пятизначные группы, а открытый текст – в виде обычных слов. Скорость работы «С-36» составляла в среднем 25 букв в минуту. С-36 получил высокие оценки французских специалистов и в итоге Франция заказала сразу пять тысяч шифраторов. Это принесло фирме Хагелина существенную прибыль. Примерно в это же время Хагелин создал для французской полиции миниатюрные шифраторы. Это была карманная аппаратура. Она приводилась в движение большим пальцем левой руки, правой рукой можно было записывать шифртекст. Некоторое количество этих аппаратов так же было закуплено Францией. После войны идея портативного карманного шифратора нашла свое развитие в моделях CD-55 и CD-57 [Бутырский, 2007], [Бутырский, 2007-2].

В предвоенные годы машины типа С-36 кроме Франции закупили для использования на линиях связи: Великобритания, Италия, Германия (по некоторым данным немцы даже организовали у себя «пиратское производство» шифрмашин и выпустили около 1000 экземпляров, которые использовались Абвером и МИД) и некоторые другие европейские страны.

В 1936 году Ив Гюльден (Yves Gylden), сын одного из основателей фирмы, проанализировал стойкость шифратора С-36 и порекомендовал внести в него некоторые изменения, которые были одобрены самим Хагелином. В результате добавилось еще одно, шестое колесо, а число линеек увеличилось до 29-ти. Новый шифратор получил название С-38 и был принят на вооружение шведской армии. В 1939 году Хагелин создал шифратор ВС-543 - электромеханическую реализацию С-36.

Но главный успех ждал Б. Хагелина в США. Еще в 1936 году он начал переписку с американцами относительно возможных закупок С-36, а в 1937-м и 1939 годах совершил длительные деловые поездки за океан. США выразили большую заинтересованность и решили закупить модернизированный шифратор (С-38).

Однако вскоре стало ясно, что организация массового производства шифраторов в Европе и отправка их в Америку будут

крайне затруднительны из-за начавшейся Второй мировой войны. Хагелин решил уехать в США и организовать производство С-38 непосредственно в Америке. Однако выехать из воюющей Европы было непросто. Б. Хагелин вспоминал: «Обычную визу получить было невозможно, поэтому я убедил шведское министерство иностранных дел послать меня в Америку в качестве дипломатического курьера. Мы с женой отправили наш багаж заранее и сели в поезд, следовавший в Стокгольм. Там мы узнали, что стокгольмские бюро путешествий отменили все поездки в США. Тогда мы решили попытаться отплыть из Италии. С чертежами в портфеле и двумя разобранными шифраторами в сумке мы сели в экспресс Стокгольм – Берлин. Нам сопутствовала удача. Мы с грохотом промчались через самое сердце Германии и через три дня благополучно прибыли в Геную. В ту ночь стекла в окнах отеля, в котором мы остановились, были побиты – мы совершенно случайно решили расположиться в отеле «Лондон», а Италия уже находилась в состоянии войны с Англией. Но мы все же сумели отправиться в Нью-Йорк с последним рейсом парохода, отплывавшего из Генуи» [Кан, 2004, с. 329].

Несмотря на трудности, Хагелин добрался до США. С-38 американцам очень понравился, и они развернули его массовое производство. В 1942 году в США создали компанию, выпускающую до 400 аппаратов в день. Всего было выпущено более 140 000 шифраторов. Шифратор получил название Converter M-209 (эта версия имела небольшие конструктивные отличия от С-38, в частности число линеек американского “Хагелина” было равно 27), и массово использовался в армии США (в звене от батальона до дивизии) и на флоте в период Второй мировой войны и после нее. Довольно широко использовались М-209 американцами и их союзниками во время войны в Корее 1950-53 годов. После окончания Второй мировой войны множество стран в различных регионах мира закупили и длительное время использовали на своих линиях связи значительное количество шифраторов типа С-36/38 и их модификаций.

Отчисления Хагелину, как владельцу патента на изобретение шифратора, составили миллионы долларов. Он стал первым человеком, нажившим многомиллионное состояние благодаря криптографии [Бутырский, 2007], [Кан, 2004], [Kahn, 1967]. Рассмотрим конструкцию М-209 подробнее (см. рис. 6.29).

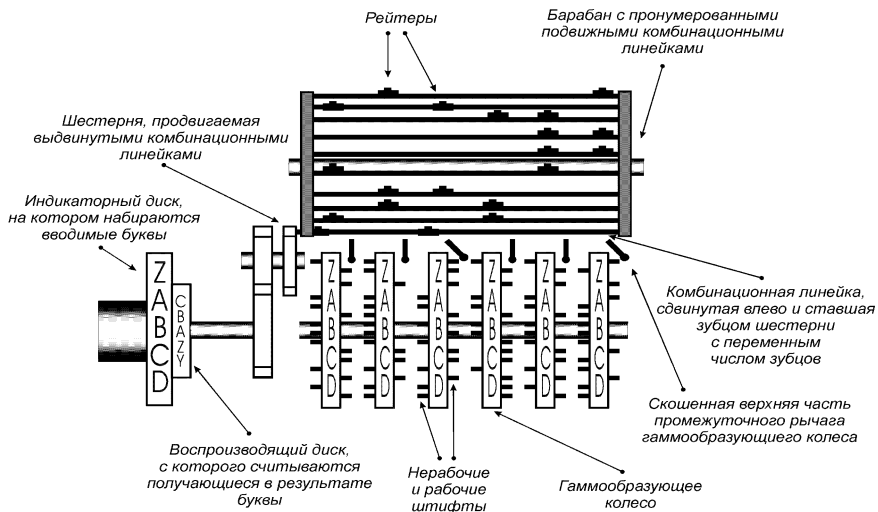


Рис. 6.29 Схема шифратора М-209

Шифратор реализовывает шифр модульного гаммирования (модуль шифрования 26). Устройство шифратора и схема его функционирования повторяет принципы, заложенные в шифраторе С-35, но имеется ряд особенностей. Также как и С-35, машина М-209 состоит из трех основных частей:

наборно-печатающего блока;

блока ключевых колес.

барабана с комбинационными линейками;

Наборно-печатающий блок предназначен для установки (набора) букв открытого текста на индикаторном диске и печати соответствующих букв шифртекста на бумажной ленте. Буквы открытого текста набираются напротив специально нанесенной риски, другая риска позволяет считать букву шифртекста с воспроизводящего диска. Кинематически наборно-печатный блок расположен целиком на отдельной оси, связанной путем шестереночной передачи с барабаном, несущим комбинационные линейки. Нумерации букв на индикаторном и воспроизводящем дисках являются взаимно-обратными, что позволяет реализовать шифр Бофора:

$$\beta = \gamma - \alpha + 1,$$

где α - буква открытого текста, β - буква открытого текста, а γ - выработанный сдвиг, то есть знак гаммы.

Шифрмашина приводится в действие мускульной силой человека путем проворачивания специально предназначенной для этих целей рукоятки на один оборот. Рукоятка находится на одной оси с барабаном, с расположенными на нём запрограммированными подвижными комбинационными линейками, который при зашифровании одной буквы совершает полный оборот. Во время вращения барабана специальный зуб приводит к вращению блока ключевых колес на одну позицию.

Блок ключевых колес состоит из 6 колес с **периодами обращения** приведенными ниже: **ГДЕ ОНИ?**:

- 26 символов, с угловыми положениями, соответствующими буквам латинского алфавита от A до Z;

- 25 символов, от A до Z, за исключением W;

- 23 символа, от A до X, за исключением W;

- 21 символ, от A до U;

- 19 символов, от A до S;

- 17 символов, от A до Q.

Так же как и в предыдущих моделях, на каждом колесе располагаются штифты. Но в отличие от C-35 и C-36, если штифт выдвинут вправо – то является “рабочим”, соответственно, если влево – то “нерабочим”.

Барабан с линейками состоит из 27 линеек с 2-мя рейторами на каждой линейке. Так же как и в шифраторе C-38 (модификации C-36), рейторы подвижны и могут быть либо “рабочими”, либо “нерабочими”.

Функционирование шифратора М-209 повторяет логику работы C-35.

Пусть в начале процесса шифрования в шести окошках выставлены буквы ВВВВВВ, соответствующие начальному положению колес (см. рис. 6.29). Тогда текущая штифтовая комбинация будет соответствовать двоичному вектору (001001). При повороте барабана с линейками на 1 оборот, “рабочие” рейторы напротив 3-его и 6-ого колес (если они имеются) будут выдвигать соответствующие линейки, число которых и будет формировать сдвиг, то есть знак гаммы γ . После зашифрования 1-ой буквы, каждое колесо повернется на одну позицию и в окошках будут видны

буквы СССССС. Тем самым формируется новая шифтовая комбинация: (101110), которая будет участвовать в формировании 2-ого знака шифрованного текста и так далее.

Краткие сведения о некоторых шифраторах, разработанных Б. Хагелином в 1930-е годы приведены в таблице.

	В-211	С-35	С-36	С-38	М-209
Примерный год разработки шифратора	1932	1934-35	1937	1938-39	1940
Расположение рейторов	-	фикс.	произв.	произв.	произв.
Число линеек	-	25	25	29	27
Число колес	4	5	5	6	6
Периоды обращения колес	17,19,21,23	17,19,21,23,25		17,19,21,23,25,26	

В 1944 году Хагелин, уже будучи мультимиллионером, вернулся в Швецию. После начала «холодной войны» и развала старых колониальных империй сформировался новый, еще более ёмкий рынок для шифраторов. Фирма Хагелина стала получать многочисленные заказы, как от «старых заказчиков», так и от только что образовавшихся на карте мира государств. Вскоре к ним присоединились и негосударственные организации (в первую очередь банки и крупные корпорации, закупавшие шифроборудование для защиты своих коммерческих тайн).

Впервые послевоенные годы Б. Хагелин сосредоточил все свои научно-исследовательские подразделения и производственные мощности в Стокгольме. Однако шведское законодательство позволяло правительству реквизи́ровать изобретения, в которых оно нуждалось для целей национальной обороны, и это вынудило Хагелина перенести в 1947 году свою научно-исследовательскую работу в швейцарский город Цуг. Цуг оказался настолько привлекательным для предпринимательской деятельности Хагелина (в

немалой степени из-за своих льгот по налогам), что в 1959 году он перевел туда и остальные части своей фирмы.

В конструктивном отношении разработки этого блестящего шведского инженера, как правило, были коммерчески успешными на протяжении десятилетий, начиная с 1925 года. Отвечая требованиям времени, Хагелин, наряду с механическими шифраторами типа С-35, С-36, С-38 конструировал и первые электромеханические модели В-21 и В-211. В 1945 году появилась модель С-446А, в которой открытый и зашифрованный тексты печатались на двух отдельных бумажных лентах. Версии С-38, оснащенные клавиатурой, назывались ВС-38, ВС-543. Многочисленные версии машин С- типа продавались по всему миру. В эру холодной войны С-52 и СХ-52 поставлялись во многие страны и получили широкое распространение. Версия ВС-52 с электрической клавиатурой имела исключительный коммерческий успех и продавалась более чем в 60-ти странах. Так, например, после Второй мировой войны в Германии не допускалась разработка своих собственных кодов и шифрсистем. Поэтому были куплены права на изготовление криптомашин Хагелина. Таким образом, шифратор CD-57 с некоторыми небольшими отличиями и усовершенствованиями стал в 1961 году моделью STG61, а С-52 – моделью фирмы Hell: Hell 54 (1954 год). Единственная роторная шифрмашинка, созданная Хагелином – НХ-63, имела беспрецедентную мощность ключевого множества: 10600.

До настоящего времени в честь Хагелина шифраторы основанной им известнейшей швейцарской фирмы Crypto AG имеют буквенно-цифровое обозначение - “НС-xxxx” (Hagelin Cipher). В настоящее время продукция фирмы Crypto AG поставляется правительственным, военным и коммерческим структурам, а также частным лицам в 130 странах мира [Бутырский, 2007-2]. Умер гениальный изобретатель в 1983 году. Разработки Бориса Хагелина в период 1927-1970-х годов в фирмах Swiss Hagelin/Crypto AG составили целую эпоху в криптографии и некоторые из них отражены ниже на диаграмме представленной на рис. 6.30.

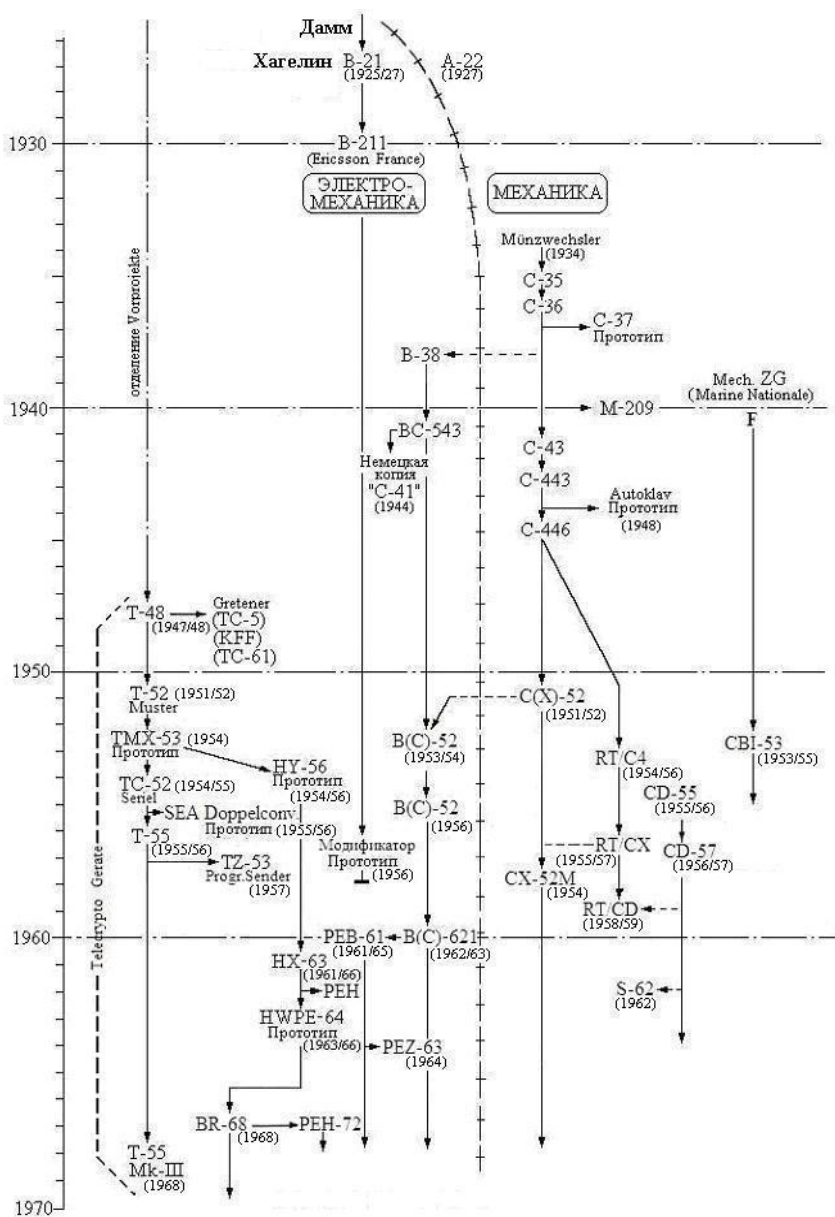


Рис. 6.30 Эволюция развития шифраторов конструкции Б. Хагелина

Отметим, что в первой половине XX века шифровальные приборы использовали не только государственные службы, но и криминальные структуры, в качестве примера на рис. 6.31 представлена шифрмашинка, ныне экспонируемая в Пражском музее в Чехии.



Рис. 6.31 «Прибор, используемый для шифрования сообщений Мафии».

Охота за «Энигмой»

Одним из центральных моментов криптографической истории Второй мировой войны, а может быть и вообще мировой истории криптографии стала операция «Ультра» (дешифрование союзниками немецкого шифратора «Энигма» в годы Второй мировой войны). Об этой операции написано очень много, в качестве наиболее доступных источников укажем [Гольев, 2008, с. 167-219], [Лайнер, 2004], [Ларин, 2007], снят ряд документальных и художественных фильмов. Об устройстве шифратора «Энигма» рассказано в предыдущей лекции.

Несмотря на довольно сложное устройство шифратора и большое число возможных ключей, вначале польским, а впоследствии

английским и американским специалистам удавалось в массовом порядке вскрывать шифруемые с помощью «Энигмы» сообщения. Это был один из крупнейших успехов криптоанализа времен Второй мировой войны. Соответствующая операция получила название «Ультра». Информация, полученная в результате операции «Ультра», существенно повлияла на ход боевых операций, проводимых вооруженными силами Англии и США во время Второй мировой войны.

До Второй мировой войны и во время нее было выпущено по разным данным от тридцати до двухсот тысяч экземпляров шифратора «Энигма», они применялись во всех видах германских вооруженных сил, в Абвере (немецкая военная разведка) и в службе безопасности. Успех англичан был во многом достигнут, благодаря самоотверженной работе криптоаналитиков, а также серии агентурных и боевых операций союзников. Интересно, что благодаря агентурным операциям советских разведчиков некоторые сведения из дешифрованной англичанами переписки немцев получал и СССР. Официально информация операции «Ультра» в Советский Союз практически не передавалась. Об этом подробнее будет сказано в конце параграфа.

Летом 1931 года сотрудник шифрбюро министерства обороны Германии Ганс-Тило Шмидт через французское посольство в Берлине предложил продать правительству Франции имевшиеся у него секретные документы. Среди них Шмидт особо выделил руководства по эксплуатации новейшей немецкой шифровальной машины «Энигма». Осенью того же года Шмидт несколько раз встретился с представителями Второго бюро – разведывательной спецслужбы Франции.

В контакт со Шмидтом вступили агент Второго бюро немец по национальности Рудольф Лемуан (настоящая фамилия Шталлман) и начальник шифровального отдела Второго бюро Густав Бертран. Шмидт передал им справочное руководство по «Энигме» и обещал добыть действующие ключевые установки для шифратора. Лемуан и Бертран поняли, что им достался кладезь ценнейшей информации, которая может оказать большую помощь в обеспечении безопасности Франции.

Вернувшись в Париж, Бертран познакомил своих подчиненных с материалами, купленными у Шмидта. Французские криптографы выяснили, что из этих материалов становится ясно, как

шифровать сообщения при помощи «Энигмы», однако они не позволяют читать немецкие шифрсообщения. Бертран был очень разочарован этим отзывом и решил проконсультироваться с английскими экспертами в области криптографии. Ответ из Лондона совпал с мнением французских криптографов: документы, переданные Шмидтом, не позволяют читать сообщения, зашифрованные с помощью «Энигмы».

Но Бертран не сдавался. Ему было известно, что польские криптографы трудятся над взломом «Энигмы». Он попросил у начальства разрешения встретиться с одним польским специалистом-криптографом.

Тем временем, поляки уже располагали информацией о коммерческой версии «Энигмы». В январе 1929 года на варшавскую таможенную из посольства Германии в Польше пришло уведомление, согласно которому необходимо было как можно скорее передать работникам посольства коробку, попавшую по недоразумению на варшавскую таможенную. Когда заинтригованные поляки вскрыли коробку, то в ней они обнаружили «Энигму». Это был коммерческий вариант шифратора. По другой версии первое знакомство поляков с коммерческим вариантом «Энигмы» произошло на польской таможне еще раньше в 1927 году.

По поручению начальника польского шифрбюро майора Гвидо Лангера на таможенную незамедлительно прибыли инженеры-специалисты фирмы AVA, работавшие в тесном контакте с шифрбюро. Руководил ими Антоний Паллытх. Он был не только инженером и совладельцем фирмы, но и криптоаналитиком. Эти люди тщательно изучили попавший в руки польских таможенников экземпляр «Энигмы». Обследование закончилось только рано утром. Немецкая шифровальная машина была упакована в коробку и передана в посольство Германии. Никаких протестов со стороны работников посольства не последовало. По-видимому, никто из них не заподозрил, что поляки ознакомились с содержимым коробки.

Попытки сотрудников польского шифрбюро прочесть немецкую переписку, засекреченную с помощью «Энигмы», не дали результата. Дело в том, что в министерстве обороны Германии был принят на вооружение шифратор, отличающийся от коммерческого варианта «Энигмы».

В 1928-1929 годах в Познани были созданы курсы по изучению криптографии для студентов-математиков со знанием

немецкого языка. Упор был сделан на углубление математических знаний. Поляки начали активную подготовку специалистов-криптографов. В Познаньском университете прочитал курс лекций по криптологии начальник «немецкого» отдела шифрбюро министерства обороны Польши лейтенант Максимилиан Ченжский. В числе его студентов, были Мариан Режевский (другая транскрипция Раевский), Генрих Зыгальский и Ежи Розицкий. Эти специалисты впоследствии поступили на службу в шифрбюро и первыми получили результаты по дешифрованию «Энигмы». По поводу важности математической подготовки для криптоаналитика М. Режевский с гордостью отметил: «Мы, поляки, поняли это раньше других». Именно поляки разработали первый математический аппарат для дешифрования «Энигмы» и дешифровали некоторые перехваченные криптограммы.

Надо отметить, что в конце 1920-х начале 1930-х годов польские криптографы считались весьма авторитетными специалистами. Так, например, японцы пригласили читать лекции по криптографии специалиста по кодам, капитана польской армии Яна Ковалевского. Позже к нему в Польшу была направлена группа японских студентов, среди которых был Ризобар Ито (впоследствии крупный японский криптограф), занимавшийся разработкой шифров и шифрмашин, а также криптоанализом (в частности, он вскрыл шифрсистему типа «Playfair», которая применялась в 1930-е годы на английских линиях связи) [Соболева, 2002].



Рис. 7.1 М. Режевский

Информация французов о немецком шифраторе оказалась для поляков полезной. Бертран передал фотокопию руководства по использованию «Энигмы» Лангеру. После ее изучения в польском шифрбюро было сделано заключение о том, что немецкие военные адаптировали для собственных нужд коммерческий вариант «Энигмы». Однако сотрудники польского шифрбюро подтвердили вердикт, вынесенный их французскими коллегами. Полученные от Бертрانا материалы не позволяли читать немецкую военную переписку, поэтому Лангер попросил Бертрانا попытаться раздобыть через своего агента ключевые установки для «Энигмы».

Вскоре Шмидт передал Бертрану действующие ключевые установки для «Энигмы». Они были незамедлительно отосланы дипломатической почтой Лангеру. В мае и сентябре 1932 года от Шмидта были получены новые ключевые установки для «Энигмы», которые снова были доведены до сведения Лангера. Но ни в 1931-ом, ни в 1932 году Бертран так и не дождался от поляков данных о том, насколько им удалось продвинуться во взломе «Энигмы».

Надо сказать, что Лемуан и Бертран были не единственными сотрудниками Второго бюро, регулярно встречавшимися со Шмидтом. Вскоре к ним присоединился Андре Перрюш, которого мало интересовали шифры. Он занимался сбором любых сведений, касавшихся франко-германских отношений. Перрюш считал информацию о планах перевооружения Германии, которую поставлял Шмидт, значительно более важной, чем данные о немецких шифрах.

К маю 1932 года Перрюш получил от Ганса Шмидта несколько писем с ценными разведывательными сведениями. Перрюш обратился к руководству Второго бюро с просьбой сократить до минимума число поездок Шмидта за границу для встреч с Лемуаном и Бертраном. Несмотря на возражения последнего, начальство встало на сторону Перрюша и поручило Лемуану проработать вопрос о том, как безопаснее всего организовать контакты со Шмидтом в Берлине. Между тем у французов наметились серьезные проблемы.

История знает много примеров, когда шпионы проваливались из-за несоответствия своих расходов официальному заработку. Не стал исключением и Шмидт. Получаемые от французов весьма значительные суммы Шмидт тратил на дорогую одежду, развлечения и путешествия. Разумеется, такие расходы скромного государственного служащего могли вызвать подозрения начальства. Лемуан посоветовал Шмидту заняться каким-нибудь бизнесом. Тогда

деньги, получаемые от Второго бюро, можно было бы выдать за прибыль. Шмидт приобрел завод по производству жира для мыловарен, однако бизнесмен из него оказался никудышный, и дела его шли отнюдь не лучшим образом. Разрешил проблему все тот же Лемуан, который посоветовал Шмидту распространить слухи о том, что он изобрел новый способ производства мыла, который был куплен крупной французской компанией, и теперь Шмидт получает процент от доходов от использования этого метода.

Бертран, раздосадованный решением своего руководства, отправился в Варшаву, где выразил Лангеру крайнюю обеспокоенность отсутствием результатов в работе по дешифрованию «Энигмы». Лангер попросил Бертрана проявить побольше терпения и пообещал, что он будет первым, кто узнает об успехах польских криптоаналитиков. По словам Лангера, сначала требуется создать действующий образец «Энигмы», и только после этого можно будет приступить непосредственно к чтению немецких шифрованных сообщений. В конце ноября 1932 года Бертран в очередной раз встретился со Шмидтом. На этой встрече Бертран выразил сомнение в точности данных, поставляемых Шмидтом. В ответ Шмидт вспылал. Назревавший скандал удалось замять, и Шмидт продолжал поставлять французам важную информацию. В 1936 году брат Шмидта Рудольф получил чин генерала и был повышен в должности. Он делился с Гансом секретной информацией о планах перевооружения Германии, о новых разработках в области стратегии и тактики и т.д. Во Втором бюро эту информацию считали более важной, чем ключевые установки «Энигмы». Для большей безопасности Шмидту предложили не выезжать за границу, а поддерживать связь через французское посольство в Берлине. При этом при необходимости срочно встретиться с сотрудниками французских спецслужб Шмидт должен был позвонить по определенному телефонному номеру и произнести парольную фразу «Дядюшка Курт скончался» [Лайнер, 2004].

В ноябре 1937 года шпионская карьера Шмидта чуть было не закончилась из-за французского посла в Германии. Ранее Шмидт сообщил, что немцы вскрыли французский дипломатический шифр, и хотя французы его сменили, было ясно, что немцы будут пытаться дешифровать его снова. Все сообщения от Шмидта надо было посылать только дипломатической почтой. Однако, когда Шмидт передал сведения о секретном совещании у Гитлера, на котором было

принято решение присоединить к Германии территории некоторых соседних государств, в первую очередь Австрии и Чехословакии, французский посол отправил сообщение по телеграфу. Видимо, посол посчитал сообщение слишком срочным и поэтому не стал дожидаться диппочты.

Французскую шифртелеграмму прочли в Исследовательском отделе министерства авиации Германии. Эта организация имела неофициальное название «Большое ухо». Она была создана в апреле 1933 года и занималась прослушиванием телефонных переговоров и криптоанализом. У Шмидта в ней были знакомые, которые рассказали ему об этой телеграмме. Поэтому Шмидт не стал передавать послу дополнительные подробности о совещании у Гитлера, полученные от брата. Во время встречи с сотрудниками Второго бюро в Швейцарии Шмидт рассказал об ошибке посла и заявил, что продолжит сотрудничество с французами, если информация будет передаваться без посредничества французского посольства в Германии.

Вскоре Шмидт получил специальные невидимые чернила, которые ему можно было использовать для связи со Вторым бюро. Письма с сообщениями надо было отсылать на ряд адресов, один из которых находился в Швейцарии. Тем временем, Шмидта прикомандировали к Исследовательскому центру, и в начале 1938 года ему удалось получить доступ к стенограмме совещания у шефа Абвера адмирала Канариса, посвященного злополучной телеграмме. Из стенограммы было ясно, что немцы уверены в том, что французский посол сообщил о совещании у Гитлера гораздо меньше, чем знал, потому что ему известно о взломе немцами французского шифра. Немцы собирались продолжить расследование. Шмидт сообщил эти сведения французам, которые порекомендовали ему попытаться перейти на постоянную работу в Исследовательский отдел, чтобы следить за ходом расследования, но в этом случае он терял доступ к ключам «Энигмы». В общем можно сказать, что на этот раз судьба пощадила Шмидта.

В марте 1938 года немецкая контрразведка арестовала Лемуана, участвовавшего в вербовке Шмидта. Но за неимением доказательств вскоре его отпустили. Французы поверили Лемуану, заявившему, что он ничего не рассказал немцам, однако контакты со Шмидтом ему запретили. В 1940 году над Шмидтом снова нависла угроза. После захвата немцами Франции в архивах Генерального штаба и полиции немцы обнаружили сведения об утечке информации

из шифрбюро министерства обороны Германии и Исследовательского отдела министерства авиации. Немцы могли сопоставить, что Шмидт работал в обеих этих организациях. Однако таких служащих было несколько и однозначно идентифицировать Шмидта немцам не удалось. Однако самая большая опасность для Шмидта заключалась в том, что в связи с упомянутой утечкой информации из немецких спецслужб всплыла фамилия Лемуана. Немцы начали активные поиски этого человека.

Вскоре у Шмидта неожиданно появилась еще одна проблема. В начале 1941 года резидент советской разведки Л. Василевский создал сеть нелегалов во Франции. Василевский узнал, что в начале 1930-х годов Шмидт был завербован французской разведкой. Французские коммунисты, помогавшие людям Василевского, установили, что Шмидт также работал на британскую спецслужбу (на самом деле англичане получали информацию от Шмидта через французов). Имя английского агента, который работал с информацией Шмидта во Франции, установил советский разведчик Д. Маклин в 1939 году. Шмидту пришлось поделиться имеющейся у него информацией теперь и с советской разведкой. По характеру материалов, переданных Шмидтом Василевскому, советские спецслужбы поняли, что англичане регулярно перехватывают и дешифруют немецкие радиোগраммы.

В феврале 1943 года везение Шмидта кончилось: немцы нашли и арестовали Лемуана. После захвата Франции Лемуан жил на юге страны. Напомним, что южная часть Франции до осени 1942 года не была оккупирована и управлялась пронемецким правительством Виши. Лемуану не раз предлагали покинуть Францию. Его готовы были вывезти на английском корабле или обеспечить переход франко-испанской границы, но по разным причинам сделать этого не удалось. Даже после полной оккупации Франции Лемуан продолжал оставаться в стране. После ареста Лемуана доставили для допроса в Париж. 17 марта 1943 года он начал давать подробные показания. Он рассказал о Гансе Шмидте, о передаче информации по «Энигме», о генерале Рудольфе Шмидте, через которого Ганс добывал для французов военную информацию. Кстати, во время одного из допросов Лемуан, упомянув о сильной тяге Шмидта к деньгам, высказал предположение, что Шмидт может работать еще на какую-то разведку. После этого Ганс-Тило Шмидт был немедленно арестован. Однако, так как скандал затрагивал высоких руководителей Германии

(по одной из версий, кроме брата за Ганса Шмидта хлопотал сам рейхсмаршал Геринг) дело спустили на тормозах. Осенью 1943 года Г. Шмидт умер в тюрьме. По некоторым сведениям ему позволили покончить с собой. Так сложилась судьба человека, открывшего одну из первых страниц в истории тайных операций, связанных с шифратором «Энигма». Что касается Лемуана, то он пробыл в плену до конца войны и умер в 1946 году.

Г. Шмидт перестал иметь доступ к ключевой информации «Энигмы» примерно за два года до начала войны. С того времени шифратор прошел ряд модернизаций, и много раз менялись его ключи. Поэтому предательство Шмидта не посеяло в немцах сомнений в стойкости своего основного шифратора.

Теперь вернемся в Польшу начала 1930-х годов. Используя полученную от французов информацию, поляки добились значительных успехов в дешифровании «Энигмы». Фактически, они начали читать немецкий шифратор примерно с 1933 года. В начале 1930-х годов польская спецслужба обнаружила завод в Юго-Восточной Германии на границе с Польшей, где немцы производили «Энигму». В 1933 году один поляк-подпольщик начал изучать продукцию завода. Эта дополнительная информация оказалась весьма ценной для польских криптоаналитиков и помогла разобраться в устройстве шифратора. Однако в 1938 году немцы серьезно изменили процедуру использования ключевых установок, в частности были введены «разовые ключевые установки» (начальные положения дисков, менявшиеся при каждом сеансе связи). Это привело к серьезным трудностям для польских криптоаналитиков. Для решения проблемы под руководством М. Режевского на фирме AVA было разработано электромеханическое устройство под названием «Бомба». Оно представляло собой шесть соединенных между собой «Энигм». Этот аппарат позволял находить путем перебора начальное положение дисков за два часа. Для ускорения процесса вскрытия ключевых установок использовалась параллельная работа нескольких «Бомб». Впервые для управления «Бомбой» стали использоваться новые носители информации – перфокарты, их изобрел Г. Зыгальский. Продолжала в Польшу поступать и новая информация от Г. Шмидта, которая была весьма полезна. Однако поляки не торопились делиться своими достижениями с союзниками – французами и англичанами. Это чуть не привело к серьезным последствиям. В 1938 году французские специалисты сделали на основе получаемой от Шмидта

информации категорический вывод: эти материалы не позволяют взломать «Энигму» и читать немецкую военную шифрпереписку. Тогда же во Втором бюро был придуман план операции с целью решить проблему «Энигмы» раз и навсегда. Французские агенты, имевшие контакты с немецкой разведкой, должны были распространить ложные сведения о том, что французам удалось взломать «Энигму». Предполагалось, что немцы, напуганные этим известием, заменят «Энигму» на другую шифровальную машину, которую будет легче взломать.

Доподлинно не известно, получил ли этот план одобрение со стороны руководства Второго бюро. Возможно, оно посчитало, что подобную операцию лучше провести не столько против немцев, сколько против поляков, чтобы вынудить последних раскрыть подробности их работы по дешифрованию «Энигмы». Но каковы бы ни были мотивы, которыми руководствовалось Второе бюро, задумывая свою операцию, начальник польского шифрбюро Лангер, узнав о ней в 1938 году от Бертрана, пришел в ужас. Он убедил Бертрана на некоторое время отложить ее проведение, клятвенно обещая, что вскоре французы будут должным образом информированы об успехах, достигнутых поляками. О том, что польские криптоаналитики уже давно читают «Энигму», Лангер умолчал. Не вспомнил он и о своем прежнем обещании сообщить в первую очередь Бертрану о положительных результатах в работе над «Энигмой».

В 1938-1939 годах немцы внесли в «Энигму» ряд усовершенствований. В частности, вместо трех дисков появилось пять дисков, из которых для установки выбиралось три. Это создало для поляков большие проблемы. К лету 1939 года польские криптоаналитики поняли, что достигли предела своих возможностей и решили поделиться своими достижениями с союзниками. 24-25 июля 1939 года в Варшаве прошло совещание, в котором участвовали английский криптограф Дилли Нокс, директор английской Правительственной криптографической школы Аластер Деннистон, начальник шифровального отдела французского Второго бюро Густав Бертран и французский криптограф Генри Бракени. Они узнали, наконец, от своих польских коллег о дешифровании ими «Энигмы». Присутствовавшие на совещании англичане и французы получили от польской стороны по одной копии «Энигмы» вместе с инструкциями по изготовлению и использованию перфокарт для вскрытия ключевых

установок. И англичане, и французы были глубоко возмущены поведением союзников. Особое недовольство высказал Бертран. Это было вызвано тем, что ценнейший агент Г. Шмидт, рискуя провалиться, в течении нескольких лет добывал все новые и новые ключевые установки. А в это время поляки восстанавливали ключи аналитически.

После оккупации Польши большинство сотрудников польского шифровального бюро бежало во Францию через Румынию. Все копии «Энигмы» были тщательно уничтожены. Немцы так и не узнали о том, что их шифратор был вскрыт поляками. Польские криптографы стали работать вместе с французами и достигли некоторых успехов. В период с октября 1939 года по апрель 1940 года было дешифровано около 15000 немецких документов (приказов, директив и других военных сообщений).

Основные же работы по дешифрованию «Энигмы» развернулись в Великобритании. Полученная от поляков информация позволила англичанам начать операцию «Ультра» по дешифрованию «Энигмы» в Англии. Работы по дешифрованию велись в местечке Блетчли-Парк (см. рис. 7.2) в викторианской усадьбе графства Бэкингемшир. Там был создан центр, в котором собрали лингвистов, криптографов, математиков. Им удалось вскрыть главный немецкий шифратор и практически в течение всей войны поставлять политическому и военному руководству Великобритании ценнейшую информацию. Но эта работа могла оказаться безуспешной, если бы в руки союзников не попало значительное количество экземпляров шифратора и документации к ним.



Рис. 7.2. Блетчли-Парк **Нет ссылки в тексте на этот рис стр 226**

С большой долей уверенности можно утверждать, что первый экземпляр военно-морского варианта «Энигмы» достался англичанам в результате атаки на немецкую подводную лодку «U-33». С этой лодки устанавливались мины у побережья Шотландии, когда она была обнаружена английским патрульным кораблем. Подлодка успела погрузиться, после чего была атакована глубинными бомбами и, получив повреждения, вынуждена была всплыть. Перед сдачей в плен капитан раздал нескольким членам экипажа диски от «Энигмы», приказав при первой же возможности выбросить их в море. Один из членов экипажа забыл это сделать. Так, англичане получили первые 3 диска с коммутациями, используемыми кригсмарине (германскими ВМС). Благодаря этому в Блетчли-Парке серьезно продвинулись в дешифровании морской «Энигмы», однако полученных трофеев было недостаточно. Требовалась дополнительная информация. Добыть новые сведения можно было с помощью захватов немецких судов или подводных лодок, на которых были экземпляры шифраторов с соответствующей ключевой документацией. Англичане с этой целью развернули настоящую охоту за немецкими шифраторами.

Удача чуть было не улыбнулась англичанам 15 апреля 1940 года, когда английские эсминцы после атаки глубинными бомбами заставили всплыть у берегов Норвегии немецкую подводную лодку «U-49». Однако ее экипаж успел уничтожить «Энигму» и всю документацию к ней, а лодку затопить. После этого случая командующий английскими ВМС приказал обстреливать входные люки всплывавших немецких подводных лодок. Такой обстрел не позволял немцам выбраться из лодки и выбросить «Энигму» за борт до прибытия группы захвата — абордажной команды. В такой ситуации капитану субмарины оставалось либо сдаться, либо затопить лодку вместе с экипажем.

Операции по захвату немецких кораблей с целью добычи информации о немецком военно-морском шифраторе нередко специально планировались в английском адмиралтействе. Весной 1940 года несколько подобных операций было проведено у норвежских берегов.

26 апреля английский эсминец «Гриффон» захватил немецкое транспортное судно С-26, маскировавшееся под голландский траулер.

Англичанам досталась ценная документация, в том числе, новые ключевые установки к «Энигме». Один экземпляр «Энигмы» англичане получили в 1940 году, когда у норвежских берегов был сбит немецкий самолет. Среди обломков была обнаружена «Энигма» и полный комплект рабочих ключей. Несколько позднее такое же ценное имущество было захвачено у немецкого подразделения связи одной из танковых групп, которое вместе с танкистами участвовало в наступлении во Франции и оторвалось от главных сил. Хотя эти трофеи были весьма ценными, в Блетчли-Парк хотели большего. Необходимо было получить целую морскую «Энигму» и полный комплект документации к ней. Капитанам английских военных судов была показана фотография шифратора и даны инструкции по поиску шифрмашин на захваченных кораблях противника. В случае успеха предписывалось как можно быстрее доставлять трофеи в Лондон.

Помощник начальника английской военно-морской разведки Я. Флеминг в сентябре 1940 года предложил следующий план. Предполагалось разбить трофейный немецкий бомбардировщик в проливе Ла-Манш и подать сигнал бедствия. «Спасенный экипаж» после подъема на борт подошедшего немецкого судна, должен был расстрелять команду судна и захватить «Энигму». Флеминг уже начал подготовку операции, однако руководство посчитало, что шансы на успех невелики и отменило ее проведение. Интересно заметить, что позднее Флеминг «провел» тайную операцию по добыче криптографических секретов в одном из своих романов про Джеймса Бонда. Агенту 007 удается соблазнить и переманить на свою сторону русскую шифровальщицу и добыть шифрмашину.

4 марта 1941 года опять же у побережья Норвегии, английский эсминец «Сомали» захватил немецкое судно «Краб». Англичанам достались два диска от находившихся на его борту «Энигмы». Англичане использовали любую возможность для добычи материалов, облегчающих дешифрование «Энигмы». Большую пользу английскому командованию оказал в этом специалист Блетчли-Парка Гарри Хинсли. Он занимался анализом трафика переговоров в кригсмарине и научился даже без дешифрования, лишь по интенсивности переговоров и почерку радистов, определять конкретные немецкие корабли. Он предложил захватить одно из немецких судов, направляемых в северные моря для наблюдения за погодой (данные метеонаблюдений крайне необходимы летчикам и морякам). Задача облегчалась тем, что эти суда были легко вооружены

и действовали в одиночку. Это позволяло сохранить операцию в секрете. Для атаки было выбрано метеорологическое судно «Мюнхен». 7 мая 1941 года английский эсминец «Сомали» обстрелял «Мюнхен». Немецкий радист выбросил за борт «Энигму», но не успел уничтожить ключевую документацию, в том числе, ключевые установки для военноморской «Энигмы» на июнь 1941 года. В результате англичане получили очень ценную информацию.

9 мая 1941 года была захвачена подводная лодка «U-110». Подлодка под командованием капитан-лейтенанта Фрица Лемпа атаковала южнее Гренландии конвой, вышедший из Англии. Эсминцы эскорта забросали «U-110» глубинными бомбами. Поврежденная субмарина вынуждена была всплыть. С эсминцев по ней открыли огонь из пулеметов. Один из эсминцев чуть было ее не протаранил. Экипаж вместе с командиром в спешке покинул поврежденную подводную лодку, открыв кингстоны. Немцы надеялись, что лодка утонет до того, как англичане до нее доберутся. «Энигму» и документацию к ней уничтожить не успели. Тем временем, абордажная команда с эсминца «Бульдог» во главе с лейтенантом Дэвидом Балмом сумела проникнуть на лодку и захватить «Энигму» со всеми секретными документами. Лодка затонула на следующий день во время буксировки к берегам Исландии. Думая, что лодка затонула, немецкое командование не проявило особого беспокойства, потому что инструкции, в том числе и шифрматериалы, печатались на растворимой в воде бумаге.

Большой удачей для англичан стал захват на «U-110» так называемых «офицерских» ключевых установок, на которых предварительно шифровались наиболее важные отрывки сообщения. После этого все сообщение перешифровывалось на обычных ключевых установках. Самое главное — на офицерских ключах шифровалась информация об изменениях процедуры шифрования. На лодке также была захвачена документация по флотскому ручному шифру, который использовался немцами для шифрования не столь важных сообщений. Кроме того, на «U-110» были захвачены карты, которые оказались полезными для определения передаваемых в криптограммах координат немецких судов и подводных лодок.

Благодаря полученной документации, флотский ручной шифр был вскрыт в июне 1941 года. Немцы часто шифровали одинаковые сообщения флотским ручным шифром и «Энигмой». Это приводило к слабостям. Получалась пара криптограмм, отвечающих одному

открытому тексту. Дешифровав одну из них, соответствующую более простому ручному шифру, они получали открытый текст, который использовался как подстрочник для второй криптограммы, соответствующей «Энигме». По нему определялись наиболее вероятные слова и фразы открытого текста. Подстрочники применялись затем для определения ключей «Энигмы».

Разумеется, англичане тщательно скрывали факт захвата «U-110». Немалую роль в этом сыграли органы цензуры. Известно, что один из офицеров подлодки, находясь в лагере для военнопленных, в завуалированной форме в письме домой сообщил о захвате лодки, но это письмо было перехвачено. В дальнейшем англичане сумели убедить пленных членов команды, что «U-110» быстро пошла на дно, и англичане не успели ее осмотреть. Захват подводной лодки «U-110» держался в строжайшей тайне вплоть до 1958 года.

На «U-110» и «Мюнхене» были захвачены так называемые «погодные» коды, при помощи которых передавались сводки погоды. Эти сводки затем шифровались «Энигмой». Они стали хорошим источником «подстрочников». «Погодные коды» были сменены немцами лишь в январе 1942 года.

Работая круглосуточно, английские криптоаналитики сумели проникнуть в основной оперативный шифр, имевший кодовое название «Дом». С мая 1941 года англичане получили возможность беспрепятственно читать радиogramмы немецких моряков. Результаты этой работы позволили англичанам вскрывать месячный ключ в течение двух суток.

Однако, вскоре немцы вновь сменили ключевые установки, и англичанам опять понадобились ключи за июль. С помощью Г. Хинсли была выбрана очередная цель захвата – судно метеоразведки «Лауенбург». 28 июня 1941 года четыре английских эсминца перехватили немецкое судно. После первых же предупредительных выстрелов экипаж покинул судно. «Энигму» и большую часть документации немцы успели уничтожить, но кое-что осталось: соединения коммутационной панели и бумага, на которой был указан порядок следования дисков. Эти трофеи существенно помогли английским дешифровальщикам.

Успешная работа англичан была под постоянной угрозой. После капитуляции Франции в июне 1940 года дешифровальный центр, возглавляемый Г. Берграном, переместился в поместье Фузес на юге Франции. Эта местность находилась в неоккупированной

немцами части страны. Здесь же работали и польские криптографы. Хотя центр находился в относительной безопасности, постоянно существовала угроза его захвата немцами. Несмотря на то, что французы и поляки в Фузесе не достигли значительных успехов в дешифровании «Энигмы», они были в курсе некоторых аспектов деятельности Блетчли-Парка. И Бертран, и поляки владели крайне важной информацией по дешифрованию «Энигмы», помимо собственной работы (французы и поляки в Фузесе продолжали работы по дешифрованию «Энигмы»). Они были в курсе некоторых аспектов деятельности Блетчли-Парка. Напомним, что накануне и в первый период Второй мировой войны разведывательные службы Франции и Великобритании (в том числе дешифровальные) очень тесно сотрудничали. По некоторым сведениям, сотрудничество продолжалось и после поражения Франции. Например, поляки передавали своему правительству, находившемуся в эмиграции в Англии, содержание швейцарских шифрсообщений, которые перехватывались и дешифровывались в Фузесе. Причем поляки делали это втайне от Бертрана. Когда тот узнал об этом факте, то был буквально взбешен. В книге [Лайнер, 2004] утверждается, что англичане прекратили делиться с Бертраном ключевыми установками к «Энигме» лишь летом 1941 года. Автор считает, что такая ситуация крайне маловероятна, это должно было произойти гораздо ранее. Дело в том, что Англия и вишистская Франция (во Франции после ее капитуляции пришло к власти пронемецкое правительство во главе с А. Петеном, которое обосновалось в городе Виши на юге страны) с 1940 года фактически находились в состоянии войны. Боевые действия начались уже летом 1940 года. Так, с 3 по 6 июля в ходе операций «Катапульта» и «Восход» английские корабли и самолеты без малейших колебаний уничтожили базировавшийся в Северной Африке французский флот (в том числе 3 линкора). При этом погибли сотни французских моряков. Два дня спустя английские торпедоносцы уничтожили в гавани Дакара (Сенегал) французский линкор «Ришелье». Для того, чтобы французский флот не достался немцам, англичане пошли на значительные жертвы среди моряков недавнего союзника. В последующие месяцы неоднократно происходили стычки между вишистами и англичанами (главным образом, воздушные).

Весьма значительные события произошли в мае 1941 года. 5 мая англичане захватили Мадагаскар (тогда французская колония).

Без выстрелов и здесь не обошлось. Самые активные боевые действия между вишистами и англичанами развернулись в мае – июле 1941 года в Ливане и Сирии, обе стороны понесли серьезные потери в людях и технике. Кампания закончилась в пользу англичан, которые захватили эти территории, ранее принадлежавшие Франции. Кстати, все французы, сражавшиеся против немцев в английских вооруженных силах и в рядах созданной генералом де Голлем «Свободной Франции» (в эти вооруженные формирования входила, в том числе, и сражавшаяся на советско-германском фронте знаменитая эскадрилья (позднее авиаполк) «Нормандия-Неман») и считались правительством Виши изменниками и дезертирами. В случае попадания в плен к вишистам они подвергались самым суровым наказаниям, вплоть до смертной казни. Учитывая эти данные, факт передачи англичанами важнейшей и чрезвычайно секретной информации врагу (пусть его и представляет старый товарищ по оружию Бертран) кажется крайне сомнительным.

Во второй половине 1941 года англичане достигли ряда новых успехов на море. Так, 27 августа в 80 милях к югу от Исландии находилась в надводном положении субмарина «U-570». Она не имела возможности погрузиться, и была атакована английским самолетом. Командир субмарины доложил об этом командованию, но замешкался с приказом экипажу покинуть лодку и затопить ее. Тем временем рядом появились английские корабли, с которых просигналили, что если немцы попытаются затопить лодку, то все спасательные плоты будут расстреляны. Свою угрозу англичане подтвердили предупредительной очередью из пулемета. Немецкому командиру ничего не оставалось, как сдаться. Англичане захватили подлодку, однако немцы успели выбросить «Энигму» и большую часть документации к ней за борт до подхода англичан. Англичанам достались лишь фрагменты списка ключевых установок и обрывки открытых и шифрованных текстов. «U-570» была отбуксирована в Исландию и впоследствии вошла в состав британского флота под названием «Граф».

В конце декабря 1941 года англичане в рамках операций «Лучник» и «Браслет» совершили очередной удачный рейд к побережью Норвегии. 27 декабря английский эсминец обнаружил в одном из фьордов 4 немецких патрульных корабля, покинутых экипажами. После их осмотра англичанам достались ключевые установки, таблицы биграмм и все 5 дисков к «Энигме». Другой

эсминец захватил немецкий траулер «Гром», на котором удалось добыть целый экземпляр «Энигмы» и таблицы биграмм. Спустя менее суток еще один английский эсминец обстрелял очередной траулер «Гриф», после чего его экипаж сдался в плен. При этом радист так испугался обстрела, что выпрыгнул за борт, не уничтожив оборудование и не передав сигнал о захвате судна. Полученные в ходе рейда трофеи были доставлены в Блетчли-Парк и существенно помогли английским криптоаналитикам.

Немцы продолжали совершенствовать свой основной шифратор. С 1 февраля 1942 года в сети связи с подводными лодками, которая называлась «Тритон», стал использоваться четырехдисковый вариант «Энигмы» (см. рис. 7.3). В результате чтение англичанами немецких сообщений прекратилось. Положение казалось безвыходным, более полугода радиogramмы не могли дешифровать. Возникший кризис был разрешен только в октябре.



Рис. 7.3. Четырехдисковый вариант немецкого шифратора «Энигма» **Нет ссылки в тексте на этот рис стр 273**

30 октября 1942 года в Средиземном море неподалеку от египетского берега английский разведывательный самолет засек германскую подводную лодку «U-559». Затем пять британских эсминцев с помощью сонаров обнаружили ее и атаковали. Подводная лодка была повреждена, но ее капитан старался оторваться от преследователей. Охота за ней длилась 16 часов. Лодка всплыла в 70 милях от Порт-Саида. Экипаж стал спешно покидать тонущую субмарину. С одного из эсминцев преследования под названием «Petard» была выслана abordажная команда. Однако еще до ее подхода четыре человека прыгнули за борт, добрались вплавь, и

проникли на борт гибнущей лодки. Это были лейтенант Тони Фассон, матросы Колин Гразье, Кеннет Лакруа и помощник кока 16-летний Томми Браун. Все спустились внутрь лодки. Фассон и Гразье пылись найти «Энигму» и документы, а Браун три раза выносил найденные документы. Ему успели передать только коды, вспомогательную клавиатуру и документы от «Энигмы». Командир прибывшей абордажной команды предупредил, что лодка тонет. Браун позвал остальных, но выбраться удалось только Лакруа. Лодка ушла на дно, унося с собой двух английских моряков.

Найденные документы позволили дешифровывать сообщения, передававшиеся в сети «Акула» – так англичане называли немецкую сеть радиосвязи «Тритон». В частности, удалось получить новый «погодный код». Сводки погоды немцы по-прежнему шифровали на трех дисках, а четвертый фиксировался всегда в одном положении. Используя эту оплошность немцев, англичане начали вновь читать «Энигму». Это позволило британским ВМС оперативно наносить удары по немецким подводным лодкам и сократить потери союзного флота вдвое. В декабре 1942 года Блетчли-Парк снова начал бесперебойную поставку информации. Вследствие этого немцы стали нести значительные потери подводных лодок.

Дениц признал поражение своих подводных сил 24 мая 1943 года, когда «приказал подводным лодкам перейти в район к юго-западу от Азорских островов, соблюдая при этом чрезвычайные меры осторожности». Ежемесячные потери немецких подводных сил в процентном отношении к количеству действовавших в море подлодок стали резко увеличиваться: с 3,9 процента в первой половине 1942 года до 9,2 процента в первой четверти 1943 года. И хотя вскоре немецкие субмарины снова вернулись в Атлантику, до конца войны за любой успех немецким подводникам приходилось платить очень дорого.

Кстати, как и в случае с субмариной «U-110», один из пленных немцев пытался сообщить родственникам о захвате подлодки, но цензура вновь сработала четко. Секретность соблюдалась очень строго. Через 7 месяцев, при награждении орденами, участники захвата «U-559» даже не рассказали об операции самому королю Англии Георгу VI.

Тем временем, над тайной операции «Ультра» нависла опасность. В ноябре 1942 года немцы приняли решение оккупировать оставшуюся часть Франции. Кстати сказать, и ранее немецкие

спецслужбы действовали в вишисткой Франции как у себя дома и в любой момент могли наведаться в дешифровальный центр в Фузесе. При оккупации вероятность такого события значительно увеличивалась. К счастью, французы вовремя узнали о предстоящих событиях. Буквально за несколько дней до немецкого вторжения оборудование и документация были либо уничтожены, либо надежно спрятаны. Персонал центра, включая поляков, перешел на нелегальное положение. Тот факт, что специалисты, имевшие непосредственное отношение к дешифрованию «Энигмы», продолжали находиться на территории, занятой немцами, серьезно беспокоил англичан. Английские спецслужбы вместе с силами французского сопротивления пытались эвакуировать носителей тайны взлома «Энигмы». Несколько таких попыток по разным причинам провалились. Лишь 29 января 1943 года М. Режевскому и Г. Зыгальскому удалось нелегально перейти франко-испанскую границу. Впоследствии этим польским криптоаналитикам удалось добраться через Португалию до Великобритании. Путешествие было трудным и заняло несколько месяцев. Но так повезло не всем.

12 февраля 1943 года немцы арестовали А. Паллътх (напомним, что под его руководством была создана первая копия «Энигмы»), а 12 марта при попытке перейти франко-испанскую границу в руки немцев попала группа поляков, среди которых были Г. Лангер и М. Ченжский. Причем в последнем случае Бертран и англичане узнали об аресте лишь месяц спустя. До этого считали, что группа Лангера благополучно перебралась в Испанию. Однако англичанам фантастически повезло: тайна взлома «Энигмы» так и не была раскрыта. Сами немцы не знали, что А. Паллътх ими арестован (его задержали с документами на чужое имя). Между тем этого человека активно разыскивали немецкие спецслужбы. Они знали, что фирма AVA имела тесные контакты с польским шифрбюро и горели желанием побеседовать с ее совладельцем. Для приманки немцы даже оставили на свободе в Польше жену Паллътх, хотя в ходе обыска в ее доме в Варшаве был найден радиоприемник. По немецким законам, установленным в оккупированной Польше, все радиооборудование надо было сдать в полицию. Неповиновение каралось смертной казнью. Но супругу Паллътх не репрессировали. Немцы ожидали, что муж рано или поздно свяжется с ней и они сумеют выяснить его местонахождение. Ожидания немцев не оправдались: 18 апреля 1944 года А. Паллътх погиб во время авианалета союзников на завод, где

работали заключенные концлагеря Заксенхаузен, в котором он содержался. Вскоре после гибели Паллытха в этом же лагере скончался еще один поляк, причастный к тайне «Энигмы», Э. Фокчиньский. Немцы так и не успели его допросить. Ранее, в начале 1942 года, так и не попав в руки немцев, погиб Е. Розницкий. Однако в одном из немецких концлагерей продолжали находиться Лангер и Ченжский. В марте 1944 года немецкие спецслужбы каким-то образом получили информацию, что в их руках находятся руководители польской криптографической службы (Лангер и Ченжский были задержаны с чужими документами). Тут же начались их допросы. Лангеру и Ченжскому удалось убедить немцев, что хотя работы по криптоанализу немецких шифров в Польше накануне войны велись, и даже были некоторые успехи, но с началом войны немцы ввели новые шифры, которые полякам вскрыть не удалось. К счастью для англичан, немцы поверили польским криптоаналитикам. Действительно, с 1939 года «Энигма» прошла ряд усовершенствований, а ключи менялись несчетное количество раз. Это касалось и других немецких шифров. Г. Лангер и М. Ченжский были освобождены союзными войсками в конце войны и оказались в Великобритании.

17 февраля 1943 года при атаке конвоя союзников у берегов Ливии глубинными бомбами с английского эсминца была повреждена подводная лодка «U-205». На всплывшую лодку была отправлена абордажная партия. Внутри лодки были обнаружены таблицы биграмм и погодный код. Эти материалы доставили в Блетчли-Парк, однако большого интереса они не вызвали, так как были захвачены ранее на «U-559» и в ходе операции «Лучник». Подлодка «U-205» затонула при попытке буксировки в ближайший порт. Самое главное состояло в том, что англичанам опять удалось сохранить факт захвата подводной лодки в тайне.

Но угроза тайне взлома «Энигмы» возникла вновь: во Франции 5 января 1944 года немцами был арестован Г. Бертран. Однако и на этот раз англичанам крупно повезло. Бертрану удалось убедить немцев в готовности работать на них. В частности, он послал шифрсообщение в Англию, в котором просил организовать встречу со связным английской разведки. Немцы собирались устроить засаду и захватить связника. Но Бертран сумел уговорить немцев отпустить его, так как иначе его соратники могли заподозрить, что он арестован и попытка ведения «двойной игры» окончилась бы неудачей. Немцы

пошли на риск и прогадали. 11 января, сразу после освобождения, Бертрону удалось скрыться. Он связался с силами сопротивления и отменил встречу с английским связным. Тайна операции «Ультра» и на этот раз была сохранена, однако англичане прекрасно понимали, что после всех произошедших событий Бертрана надо срочно вывозить из Франции. При этом слишком легкое освобождение французского разведчика вызвало у англичан подозрения в его вербовке. Развееь их можно было, доставив Бертрана в Англию. Ситуация усугублялась тем, что в это время уже готовилось вторжение в Нормандию.

Союзники предприняли грандиозную операцию по дезинформации немцев относительно места открытия второго фронта. Немцев решили убедить, что высадка пройдет в районе порта Кале, а не в Нормандии. Именно в этом районе ширина пролива Ла-Манш наименьшая, и немцы поверили, что десант будет именно здесь. Для внедрения дезинформации использовались самые разные каналы, в том числе, немцам «подставлись ТАК? Да\» шифры, по которым затем передавались ложные сообщения. Для оценки успеха предпринимаемых действий активно использовались материалы, добываемые криптоаналитиками из Блетчли-Парка. Если бы Бертран сообщил немцам о взломе «Энигмы», то немцы могли бы начать свою игру. Сделав вид, что поверили союзникам, и подтвердив это передачей зашифрованных «Энигмой» сообщений, они могли разработать совершенно иной план отражения англо-американского десанта. Вопрос требовал скорейшего прояснения. Сразу вывезти Бертрана не удалось. Тогда англичане пошли на хитрость: центральная английская радиостанция Би-Би-Си в конце января несколько раз передала сообщение о том, что Г. Бертран и его супруга благополучно добрались до Англии. Прошло более 4 месяцев после освобождения прежде чем чета Бертран оказалась в Великобритании. Для связи с силами сопротивления и агентами английской разведки в Германии и оккупированных ею странах очень активно использовали Би-Би-Си. Так, при вывозе Бертрана 31 мая 1944 года Би-Би-Си передало условную фразу «Расцвели белые лилии». Это означало, что Бертран, его супруга и сопровождающие их участники сопротивления, с которыми Бертран заранее вошел в контакт, должны ночью прибыть в заранее условленное место и с определенного времени подавать факелами сигналы, обозначающие место посадки самолета. В эту ночь самолет по каким-то причинам не прилетел. Но 2 июня условная

фраза прозвучала вновь, и на этот раз Бертран с женой улетели в Англию. Вскоре Би-Би-Си передала еще одну условную фразу «Майкл сбрил свои усы». Это означало, что операция по доставке Бертрана на Британские острова завершилась успешно, и стало своеобразной благодарностью обеспечивавшим ее проведение бойцам французского сопротивления. А Бертран мог теперь сбрить усы, которые отрастил для конспирации, когда находился на нелегальном положении. Несмотря на благополучный исход операции, Бертрану все же не до конца доверяли. До конца операции «Оверлорд» (высадка в Нормандии) он был фактически заключен под домашний арест. Позднее подозрения с него были сняты. Бертран пережил войну и вышел в отставку в 1950 году.

Не только англичане захватывали немецкие подводные лодки. 5 марта 1944 года при атаке конвоя союзников в 400 километрах к западу от Ирландии была обнаружена и атакована немецкая подводная лодка «U-744». После того как на лодке разрядились аккумуляторные батареи и подошли к концу запасы кислорода, ее командир Хайнц Блишке отдал команду заминировать подлодку и всплыть. Однако во взрывном устройстве что-то не сработало, и взрыва не произошло. На борт прибыла абордажная команда с канадского корвета. В результате было захвачено много ценных документов, но на обратном пути шлюпка перевернулась, и все находки утонули. В результате канадцам не удалось внести свой вклад в добычу материалов по «Энигме». Лодку добили торпедой, а в газетах написали, что лодка затонула, и канадских моряков на ее борту не было.

Успехи американцев были более значительными. 4 июня 1944 года у островов Зеленого мыса у побережья Западной Африки американский эсминец во время боевого патрулирования обнаружил и атаковал подводную лодку «U-505». Вообще этой субмарине не везло. В 1942 году, действуя в составе «стаи» у берегов Бразилии, не потопив ни одного судна, подводная лодка при всплытии попала под глубинные бомбы атакующего ее американского патрульного самолета. Одна из них угодила в кормовую пушку подлодки и взорвалась у поверхности воды. Лодка получила тяжелые повреждения и с трудом смогла добраться до Франции. Субмарину отремонтировали и вновь отправили в Атлантику. На этот раз на нее наткнулся американский эсминец. После атаки серией глубинных бомб лодка всплыла, хотя ее материальная часть была

неповрежденной. Весь ее экипаж сдался. Американцы на буксире отвели субмарину к Бермудским островам. На лодке было захвачено много ценных документов, «офицерские» и обычные ключевые установки за июнь 1944 года, действующий «погодный» и «адресный» код (с помощью последнего немцы шифровали координаты подводных лодок и кораблей), а также новый «погодный код». Однако командующий американским флотом в Атлантике адмирал Эрнст Кинг пригрозил отдать командира отряда, в который входил эсминец, захвативший лодку, капитана 1 ранга Даниеля Галлери под трибунал. Своими действиями американцы поставили под угрозу операцию «Ультра». Беспокойство по сохранению в тайне факта захвата «U-505» высказал и первый морской лорд Англии (начальник главного штаба английских ВМС) Э. Каннингхем. Американцы приняли меры: все пленные были помещены в лагерь на территории США, к ним не допускали даже представителей Красного Креста, что противоречило нормам международного права. О том, что члены экипажа «U-505» остались в живых, их родственники узнали лишь в 1947 году. Кстати, это один из многих эпизодов, доказывающих, что в случае необходимости поборники защиты прав человека во всем мире с легкостью нарушают нормы международного гуманитарного права. Что касается самой субмарины «U-505», то ныне она демонстрируется на смотровой площадке музея науки и техники в Чикаго. Об этом экспонате говорится: «Немецкая подводная лодка "U-505" является первым трофеем ВМС США, начиная с 1812 года».

В конце войны имели место случаи захвата союзниками «Энигм», которые использовались в сухопутных войсках. Нередко немцы просто не успевали уничтожить шифраторы. За немецкими шифрмами союзники развернули настоящую охоту. За каждый экземпляр шифратора полагался внеочередной отпуск. После войны англичанам и американцам досталось большое количество «Энигм» различных модификаций. Некоторые из них до сих пор демонстрируются в музеях.



Рис. 7.4 Коллекция «Энигм» различных модификаций

Во время Второй мировой войны в ходе операции «Ультра» англичане использовали возможность «навязывания» открытых сообщений, которые затем немцами шифровались «Энигмой». С помощью слабого шифра (который немцы легко разгадывали) английские ВВС передавали «секретные» сообщения. Эти сообщения перешифровывались на «Энигме», и в результате англичане имели открытый текст в дополнение к перехваченному шифрованному. Задача дешифровальщиков при этом существенно упрощалась. Однако иногда таких усилий не требовалось. Немцы сами «помогали» англичанам добыть открытый текст к шифrogramмам. Так, немецкая метеорологическая станция, располагавшаяся в районе Бискайского залива, в течение многих месяцев подряд передавала сообщения, которые начинались примерно так: «Метеопрогноз для Бискайского залива...», далее шли сами прогнозы, не отличавшиеся большим разнообразием в смысле текста: температура – такая-то, ветер такой-то и т.д. Это приводило к слабостям, так как практически один и тот же открытый текст постоянно шифровался на разных ключевых установках. Англичане сумели дешифровать такой прогноз. Они убедились, что он раз от раза почти не меняется и стали весьма эффективно использовать этот факт для вскрытия новых ключевых установок к «Энигме». Кстати, немецкая служба связи предупреждала о недопустимости передачи ежедневно в одно и то же время практически одинаковых прогнозов, немецкие метеорологи не обратили внимание на это предупреждение и продолжили свое «черное дело» [Лайнер, 2004].

Англичане получали из материалов «Ультра» и дезинформацию. Связано это было с легендарным немецким военачальником Эрвином Роммелем. В 1940-1942 годах он командовал немецким Африканским корпусом, который вместе с итальянскими войсками вел боевые действия против англичан в Северной Африке. Однажды из пустыни Роммель доложил Берлину о своем отчаянном положении, в частности, о малых запасах горючего и боеприпасов. Когда же воодушевленная этим известием британская армия попыталась окружить его, то была разбита. Оказалось, что состояние немецких войск было великолепное. Похоже, Роммель пытался привлечь внимание генштаба к своим проблемам, преувеличивая их. Он еще раз разбил англичан при Кассерине. Это произошло благодаря тому, что англичане дешифровали приказ немецкого генштаба о наступлении в одном направлении. Роммель лучше видел сложившуюся ситуацию и стал наступать в другом направлении. Кроме того, Роммель начал наступление раньше указанного ему генштабом в шифровке срока. В результате только за один день американцы потеряли половину бронетанковой дивизии. Читать шифрпереписку врага – не значит читать его мысли! Талантливый полководец и независимый человек, Роммель хорошо доказал этот тезис на деле.



Рис. 7.5. Э. Роммель

Однако английское руководство сделало правильный вывод из этих ошибок: на большой войне случайностей не избежать. Руководители Великобритании продолжали доверять информации «Ультра», несмотря на эти досадные неувязки.

При решении задачи дешифрования большую помощь могут оказать случаи агентурного проникновения в криптографические секреты. Однако не следует забывать и о другой стороне оперативной деятельности – защите собственных криптографических секретов. Спектр деятельности здесь достаточно широк: защита материалов, документов, техники; охрана помещений; выявление каналов утечки информации и принятие соответствующих мер; проверка лиц, допущенных к криптографической работе; защита собственных источников информации, обеспечение их секретности; легендирование мероприятий, при проведении которых используется полученная путем дешифрования информация и т.д. Вот что сказал Ф. Уинтерботэм, один из бывших руководителей службы безопасности Великобритании, отвечающий за сохранение тайны операции «Ультра»: «Я указал, что потребуются очень строгие правила, регламентирующие число людей, которые могут знать о существовании такой информации, и особые правила для тех, кто получает информацию: запрет предпринимать какие-то ни было действия, которые могут вызвать подозрения у противника, либо подтвердить его опасения, что союзному командованию были известны его планы... В известных условиях может оказаться соблазнительным нанести удар, который выдаст тайну...» [Уинтерботэм, 1978]. Премьер-министр Великобритании У. Черчилль, которому докладывались сводки по дешифрованным сообщениям, далеко не всегда знакомил с ними даже членов своего кабинета. Материалы дешифрования поступали только начальникам разведслужб вооруженных сил и главе Интеллидженс сервис (разведывательная служба Великобритании) сэру Стюарту Мензису. В остальные инстанции направлялись только распоряжения, основанные на сведениях, полученных в ходе операции «Ультра». Но и они составлялись так, чтобы немцы не смогли догадаться об источнике информации.



Рис. 7.6. У. Черчилль

По одной из версий само название операции появилось следующим образом: в Великобритании, как и во многих других странах, существуют грифы «Секретно», «Совершенно секретно». Когда встал вопрос о грифе информации, получаемой в результате дешифрования «Энигмы», то был предложен вариант «Ультрасекретно», который потом сократился до «Ультра». При этом следует отметить, что когда объем информации, получаемой в результате дешифрования «Энигмы» был относительно невелик, обеспечение сохранения тайны организовать было относительно несложно. С увеличением объема поступающей информации и числа потенциальных потребителей ситуация осложнилась. Например, руководители английских спецслужб были обеспокоены следующей проблемой. Сообщать большому количеству лиц информацию «Ультра» рискованно. У кого-то из них может появиться желание поделиться информацией со своими подчиненными, которые могут поделиться еще с кем-то и т.д. В результате интенсивность радиообмена англичан из-за передачи данной информации возрастет, и немцы могут заподозрить, что у англичан появился какой-то новый важный источник информации. А тут уже недалеко до подозрений о ненадежности своих шифров, в том числе и «Энигмы».

Ни одному получателю информации «Ультра» не разрешалось передавать кому-либо или копировать радиogramмы «Ультра». Все действия, предпринимаемые на основании информации, полученной

от «Ультра», должны были оформляться боевым приказом, приказанием или решением без ссылок на радиogramмы «Ультра» и с таким расчетом, чтобы не дать противнику повода подозревать, что его радиogramмы читаются. Если приходилось предпринимать действия, которые могли вызвать подозрения у противника (например, постоянное потопление осенью 1942 года в Средиземном море немецких конвоев, которые везли африканскому корпусу Роммеля горючее), то применялись те или иные меры маскировки. Например, английские корабли и самолеты шли в атаку лишь после того, как над конвоем проходил разведывательный самолет, который немцы отлично видели. Нередко при распространении информации «Ультра» делалась ссылка на некоего агента, который якобы имел доступ к совершенно секретным материалам немцев. Так, один из средиземноморских конвоев был уничтожен в сильном тумане. «Фокус» с самолетом-разведчиком провести было невозможно. Тогда начальник английской секретной разведывательной службы С. Мензис послал мифическому агенту в Неаполе телеграмму с благодарностью за ценную информацию и информировал его о повышении жалованья. Разумеется, телеграмма была зашифрована весьма слабым шифром, который немцы легко дешифровали и списали гибель конвоя на деятельность этого агента. По некоторым сведениям, из-за этой телеграммы начальник неаполитанского порта был отстранен от должности по подозрению в шпионаже.

Требование маскировать источник информации при проведении операции «Ультра» исходило от премьер-министра Великобритании У. Черчилля. Он также требовал, чтобы ни один получатель информации «Ультра» не имел права по собственной инициативе ставить себя в такие условия, когда появлялась малейшая опасность попадания в плен к противнику. Некоторым старшим офицерам, получавшим информацию из дешифрованных сообщений, просто запрещали непосредственное участие в боевых действиях. В некоторых случаях англичане сталкивались с непростыми ситуациями, когда для сохранения секретности операции «Ультра» надо было поделиться этой информацией. Например, об операции было сообщено сотрудникам станций радиоперехвата. В Блетчли-Парке опасались, что они могут рассказать кому-либо, что ведут активную работу по перехвату немецких сообщений и что объемы этой работы постоянно возрастают. Узнав об этом, немцы могли сделать правильный вывод о дешифровании «Энигмы». Ведь если

сообщения нельзя прочесть, то зачем их тщательно перехватывать? Зная же для чего нужна их информация, сотрудники станций радиоперехвата свято хранили в тайне сведения о своей работе.

Здесь нельзя не вспомнить один трагический эпизод, связанный с сохранением тайны «Ультра». 15 ноября 1940 года немцы провели против Англии операцию, которую назвали «актом устрашения». В результате массированного налета авиации они почти полностью разрушили английский город Ковентри. В налете участвовало 437 самолетов, которые сбросили на город 56 тонн зажигательных бомб, 394 тонны фугасных и 127 парашютных мин. Имели место значительные человеческие жертвы. Вышли из строя системы водо- и газоснабжения, были разрушены авиазаводы, в результате чего выпуск самолетов в Англии упал на 20%. При этом немцы потеряли всего один самолет. Восхищенный успехом операции Гитлер пообещал «ковентризировать» и другие английские города. Но трагедия заключалась не только в этом.

Англичане в ходе операции «Ультра» заблаговременно получили информацию о готовящемся налете. Можно было предпринять действия для защиты города и его населения: усилить противовоздушную оборону, эвакуировать жителей и т.д. Однако эти меры могли бы насторожить немцев, которые попытались бы выявить причину утечки информации о налете. Английские аналитики пришли к выводу о том, что в этом случае немцы разгадают тайну «Ультра», и операция на этом закончится. Трагическое решение о непринятии мер по защите города принял лично премьер-министр У. Черчилль. Узнав об этом решении, президент США Рузвельт писал Черчиллю: «Война заставляет нас все чаще действовать как Бог. Не знаю, как бы я поступил...» [Лайнер, 2004]. Операция «Ультра» успешно продолжалась до конца войны.

Интересно отметить следующий факт. В апреле – июне 1982 года во время Фолклендской войны между Англией и Аргентиной, американцы (АНБ) перехватывали и дешифровывали аргентинские военные сообщения. Полученной информацией они делились с англичанами. Безусловно, эта информация способствовала победе англичан в конфликте. Но и аргентинцы имели некоторые успехи. Во время боевых действий 25 мая бомбовым ударом аргентинской авиации был потоплен британский эсминец «Ковентри». В некотором смысле он повторил судьбу города, в честь которого был назван,

подтвердив тем самым старинную пословицу: «Как корабль назвать – так он и поплывет».

Приведем еще один трагический эпизод, связанный с обеспечением секретности операции «Ультра». Английский актер Л. Ховард, имевший мировую известность и одновременно являвшийся сотрудником одной из спецслужб Англии, получил задание передать важные секретные документы одному из адресатов разведки. С этой целью он должен был вылететь на гражданском самолете; рейс был ему указан. Немецкая разведка агентурным путем узнала об этой операции англичан. Немцы приняли решение сбить самолет. В свою очередь, англичане, благодаря операции «Ультра», узнали о намерении немцев. Однако они не отменили операцию. Самолет был сбит, и Ховард погиб. Так, англичане защищали источники своих важных разведывательных сведений. Благодаря высокому уровню секретности, операция «Ультра» продолжалась до окончания войны. Ее вклад в дело победы англичане и американцы оценили очень высоко. Премьер-министр Великобритании У. Черчилль отмечал, что «"Ультра" являлась самым важным и самым секретным источником информации. Он также отмечал, что «..."Ультра" – это то, чем мы выиграли войну» [Лайнер, 2004]. Маршал военно-воздушных сил Великобритании Слессор писал: «"Ультра" – невероятно ценный источник разведывательных данных, который оказывал почти сказочное влияние на стратегию, а иногда даже и на тактику союзников». Верховный главнокомандующий западными союзными войсками генерал Д. Эйзенхауэр назвал операцию «Ультра» «решающим фактором победы союзников» [Лайнер, 2004].



Рис. 7.7. Д. Эйзенхауэр

В связи вышесказанным интересен еще один исторический эпизод, имевший место во время Первой мировой войны. У. Черчилль, в то время военно-морской министр Англии, из перехваченной и дешифрованной переписки немцев узнал об их намерении потопить в Атлантическом океане лайнер «Лузитания». Было время для принятия необходимых мер: сообщить капитану «Лузитании» об угрозе и предложить ему изменить курс, выслать корабли прикрытия и т.д. Но ничего сделано не было, и лайнер был потоплен 7 июня 1915 года германской подводной лодкой «U-20». Погибло тысяча сто девяносто восемь человек, в том числе, сто пятнадцать граждан США. Непринятие мер по спасению «Лузитании» Черчилль объяснял опасностью раскрытия немцам успехов английских криптоаналитиков, хотя многие историки считают, что целью Черчилля было склонить Америку на вступление в войну на стороне Антанты.

Тайна операции «Ультра» сохранялась и после окончания войны. Как мы упоминали ранее, У. Черчилль высоко оценил успехи английских дешифровальщиков во время Первой мировой войны. В мемуарах же, посвященных Второй мировой, английский премьер-министр не написал об «Энигме» ни строчки. Официально факт дешифрования «Энигмы» был признан англичанами лишь 12 января 1978 года. Лишь с этого момента сотрудникам Блетчли-Парка разрешалось открыто говорить о своей причастности к вскрытию основного немецкого шифратора второй мировой. Однако им запрещалось раскрывать какие-либо подробности своей работы по криптоанализу. Правда еще до этого вышел ряд книг посвященных «Энигме». В 1973 году опубликовал свою книгу Г. Бертран. В ней он в основном осветил вопросы вербовки и последовавшей работы со Шмидтом. В 1974 году Ф. Уинтерботэм издал свою книгу (русский перевод [Уинтерботэм, 1978]), в которой уделил основное внимание вопросам использования информации «Ультра» при ведении боевых действий союзников против Германии, оценкам того как повлияла получаемая информация на те или иные решения высшего государственного и военного руководства союзников. Большое внимание в этой книге уделено мероприятиям по обеспечению секретности операции «Ультра». Видимо впервые некоторые сведения о криптоаналитической работе англичан по дешифрованию «Энигмы» были освещены в книге бывшего высокопоставленного сотрудника Блетчли-Парка Г. Уэлчмена. В 1983 году он опубликовал книгу, в

которой рассказал некоторые подробности вскрытия «Энигмы» люфтваффе. В 1985 году Уэлчмен более подробно описал некоторые методы, которые англичане использовали при дешифровании «Энигмы». Руководство ШКПС крайне отрицательно отнеслось к этим публикациям, но поскольку к тому времени Г. Уэлчмен уже давно жил в США, помешать опубликованию его работ не удалось. В последующие годы появилось довольно много публикаций посвященных операции «Ультра». Помимо документальных публикаций, эта история нашла отражение в ряде художественных произведений: книг и кинофильмов.

Нередко результаты криптоанализа приводили к провалу агентов. Приведем ряд примеров успехов союзников в годы Второй мировой войны. В разоблачении немецких агентов англичанам и американцам «помогала» «Энигма» и другие вскрытые немецкие шифры.

8 декабря 1941 года в Блетчли-Парке дешифровали первую криптограмму, зашифрованную на специальной модификации «Энигмы», используемой Абвером. Благодаря информации, полученной дешифровальщиками, был разоблачен ряд немецких агентов. Часть из них удалось перевербовать. Была начата радиоигра с немцами в интересах английской контрразведки.

Во время войны англичане выявили немецкого агента Э. Симоеса, португальца по национальности. Это случилось в результате перехвата и дешифрования немецких радиопередач. Было решено позволить Симоесу некоторое время свободно действовать в Англии. Англичане надеялись на то, что он может навести на других немецких агентов. Однако вскоре он был все же арестован. На допросе он объяснил, что его целью был не шпионаж, а желание добраться из Португалии в Англию и там заработать хорошие деньги. Он выдал англичанам все известные ему сведения, включая инструкции, микроточки и т.п., полученные им в Лиссабоне от немцев. Некоторые показания были проверены по другим источникам. Слова Симоеса подтвердились. Несостоявшийся агент был наказан очень мягко.

В середине войны с помощью дешифровальщиков был выявлен другой немецкий агент, клерк МИД Португалии, направленный для работы в Лондон. Сведения о нем были получены в результате вскрытия португальской дипломатической почты. Агентом оказался некто Р. де Менезес. Его имя оказалось на конверте,

спрятанном в дипломатической почте. Арест агента породил серьезную проблему. Ведь основной источник информации о нем содержался в неприкасаемой диппочте. Однако посол Португалии в Англии ограничился лишь сожалением по поводу допущенной англичанами «нескромности». Менезес был осужден.

29 ноября 1944 года на атлантическое побережье США с немецкой подводной лодки «U-1230» были высажены два диверсанта с целью радиокомандного наведения на Нью-Йорк экспериментальной межконтинентальной баллистической ракеты, разрабатываемой знаменитым Вернером фон Брауном. Подозрительных лиц заметили местные жители и сообщили о них в полицию, а оттуда эта информация попала в ФБР. Вообще подобных сообщений во время войны были тысячи, и на него попросту могли не обратить внимание. Однако в ФБР поступила информация из дешифрованных перехватов «Энигмы», что «U-1230» выполняет специальное задание в районе, откуда поступило данное сообщение. В результате было проведено прочесывание местности. И хотя поначалу немецким диверсантам удалось уйти и добраться до Нью-Йорка, ФБР продолжало поиски. В результате диверсанты были задержаны. Эта операция продолжалась несколько недель и стала крупнейшей спецоперацией в США в годы войны.

Как уже отмечалось выше, тайна операции «Ультра» тщательно оберегалась. Однако Великобритания вела войну не в одиночку, и некоторыми криптографическими секретами ей приходилось делиться с союзниками. Хотя США вступили во Вторую мировую войну лишь 7 декабря 1941 года, с самого начала боевых действий они помогали Англии, поставляя вооружения и боевую технику. Обменивались англичане и американцы и разведывательной информацией. Впервые вопрос о предоставлении американцам информации по «Энигме» встал в конце 1940 года, но несмотря на готовность Черчилля предоставить эту информацию, руководители английских спецслужб категорически возражали против этого. В конце концов было принято решение предоставить американцам минимум информации об устройстве «Энигмы» и результатах работы по ее дешифрованию, и не давать никаких сведений о содержании дешифрованных сообщений. Вскоре в Англию на стажировку прибыла группа американских криптографов. Они поделились с англичанами информацией о дешифровании в США японской «пурпурной» шифрмашин. Взамен англичане все же поделились

информацией о дешифровании «Энигмы». При этом с американцев были взяты особые обязательства ни при каких обстоятельствах не разглашать полученную информацию. Полученные сведения было разрешено передать только руководителям дешифровальных служб американских армии и флота. В дальнейшем в 1941-1942 годах англичане крайне неохотно поставляли в США дополнительные сведения по криптоанализу «Энигмы», опасаясь утечки информации, но тем не менее, сотрудничество продолжалось. Вскоре верность союзническому долгу взяла верх, и англичане начали полноценный обмен информацией в сфере криптоанализа с американцами. Здесь оказали влияние два фактора. Во-первых, на тесном сотрудничестве с США настаивал премьер-министр Великобритании У. Черчилль, а во-вторых, американцы сами собирались развернуть работу по криптоанализу «Энигмы». Технические и финансовые возможности у США были гораздо выше, чем у англичан, и в успехе сомневаться не приходилось. Заставлять же союзников решать те проблемы, которые уже были решены в Блетчли-Парке, англичане посчитали неправильным. Примерно с конца 1942 года в США стала передаваться вся имеющаяся у англичан информация о вскрытых ключевых установках «Энигмы». Мало того, англичане поделились своим главным секретом: сведениями об устройстве так называемой «бомбы» – по существу первой электромеханической вычислительной машины, созданной под руководством знаменитого математика Алана Тьюринга для вскрытия ключевых установок «Энигмы». Вскоре американцы наладили производство этих машин у себя и с их помощью смогли вскрывать ключи самостоятельно. Также в США для криптоанализа стали передавать недешифрованные материалы радиоперехвата, так как сами англичане не справлялись с огромными объемами работ по дешифрованию всей перехваченной информации. В дальнейшем английскими и американскими специалистами были созданы более совершенные варианты «бомбы», получившие названия «паук» и «колосс». Кстати, беспокойство англичан о сохранении тайны «Ультры» американцами оказалось напрасным. В США этим вопросом занимались на самом высоком уровне, включая президента Ф. Рузвельта. Так, главнокомандующий союзными войсками на Западе генерал Д. Эйзенхауэр не информировал о получаемых материалах даже своих ближайших соратников. Интересно отметить, что среди прочей информации, полученной из дешифрования «Энигмы», Эйзенхауэр ознакомился с крайне нелестными оценками

немцами способностей ряда американских военачальников. В своих воспоминаниях он сожалел, что из-за необходимости соблюдать секретность, не было возможности ознакомить американских генералов с оценкой их деятельности противником. Правда речь шла о событиях 1943 года, когда американцы воевали в Северной Африке и Италии. Второй фронт в Европе тогда еще не был открыт.



Рис. 7.8. А. Тьюринг

Англо-американское сотрудничество в области криптографии не ограничивалось «Энигмой». Совместная работа шла и в других направлениях. В конце 1942 года А. Тьюринг был командирован в США для консультаций по оценке криптографической стойкости шифратора вокодерных станций SIGSALY (известных также под наименованиями “x-ray”, “project X”, “The Green Hornet”). На их основе в годы Второй мировой войны была создана правительственная система закрытой радиотелефонной связи США, первая в мире обеспечившая гарантированную стойкость шифрования речевого сигнала. Терминалы этой системы связи, начиная с 1943 года, располагались в Вашингтоне, Лондоне, Алжире и Австралии, Калифорнии, Окледских островах, позднее – в Париже (после его освобождения), Северной Африке, Гаваях, Гуаме, Маниле и после войны – в Берлине, Франкфурте и Токио. Один терминал был размещен в Севастополе во время Ялтинской конференции в феврале 1945 года. Интересно отметить, что один из терминалов был размещён

на 250-тонном океанском лихтере «OL-31», обеспечивавшем закрытую связь командующего союзными войсками генерала Дугласа Макартура во время тихоокеанской кампании против Японии.



Рис. 7.9 Терминал аппаратуры SIGSALY

Руководители операции «Ультра» были категорически против предоставления Советскому Союзу информации из дешифрованных сообщений «Энигмы». В качестве одного из аргументов выдвигался тезис о слабости советских шифров (материалы по «Энигме» могли быть зашифрованы на них, перехвачены и дешифрованы немцами; секретность операции «Ультра» таким образом, оказалась бы под угрозой). В Блетчли-Парке имелись тому доказательства, из материалов «Ультра» было известно, что накануне войны немцы читали шифрованные сообщения советских морских судов и одного из авиационных соединений, дислоцированного в районе Ленинграда.

Однако Черчилль распорядился передавать в СССР разведывательные материалы «Ультра». Накануне начала Великой Отечественной войны по распоряжению Черчилля в СССР передали информацию о готовящемся нападении Германии, полученную

англичанами в результате дешифрования «Энигмы». В дальнейшем сообщения «Ультра» шли со ссылкой на агентурные источники, представителей нейтральных стран, показания пленных и т.д. Любые детали, которые могли бы свидетельствовать о том, что информация получена в результате дешифрования, исключались. Приведем в качестве примера начало одного из таких сообщений. У. Черчилль – И.Сталину (30.9.1942): «Из того же самого источника, который был использован мною для того, чтобы предупредить Вас о предстоящем нападении на Россию полтора года тому назад, я получил следующую информацию. Я полагаю, что этот источник, заслуживает абсолютного доверия. Пожалуйста, пусть это будет только для Вашего сведения» [Переписка, 1957]. Далее излагались сведения о планах немцев на Северокавказском фронте. Англичан очень беспокоила возможность проникновения немцев к нефтяным источникам в Баку, и они хотели бы, чтобы советская армия не допустила этого.

Такое сотрудничество продолжалось до конца 1942 года, после чего англичане его почти прекратили. Исключения были во время Сталинградской и Курской битв, когда информация вновь поступала. С 1944 года материалы «Ультра» официальным путем полностью прекратили поступать в СССР.

К сожалению, поступавшие от англичан материалы не всегда оценивались должным образом. Так, весной-летом 1942 года англичане предоставили СССР материалы, свидетельствовавшие о готовящемся наступлении немцев под Харьковом. Однако на них не обратили внимания, и советские войска понесли тяжелые потери. Справедливости ради заметим, что информацией, полученной путем дешифрования «Энигмы» иногда пренебрегали французы и англичане, которые знали источник информации, и, следовательно, могли ему доверять. Приведем примеры.

Летом 1940 года М. Режевский из дешифрованных сообщений люфтваффе узнал о планируемом налете немецкой авиации на Париж. Режевский довел до сведения французов количество самолетов, маршрут и высоту полета, и самое главное, точную дату и время налета. У французов была неделя на принятие мер. Но сделано ничего не было, и 3 июня 1940 года самолеты люфтваффе провели первую бомбардировку Парижа, не встретив никакого сопротивления со стороны французских ВВС и ПВО.

В 1944 году английский фельдмаршал Монтгомери, своевременно предупрежденный о наличии в районе голландского

города Арнем двух германских танковых соединений, все-таки приказал выбросить полки 1-й парашютно-десантной дивизии именно в этом районе, где их почти полностью уничтожили.

Но были и примеры другого рода. В начале февраля 1942 года англичане дешифровали приказ верховного немецкого командования, в котором войскам, отступавшим на Восточном фронте, предписывалось не допустить попадание в руки противника новейшего вооружения, в особенности секретных бронебойных снарядов новой конструкции. Эту информацию передали в СССР. Только что закончилась битва под Москвой, советские войска захватили много немецкой техники и вооружения. Среди трофеев оказались и новые снаряды. Выяснилось, что их сердечник изготовлен из самого прочного в те времена материала – карбида вольфрама. Месторождений вольфрама на территории Германии и ее союзников не было, а значит, он поставлялся из нейтральных стран. Эту информацию сообщили англичанам и американцам, их спецслужбы провели ряд оперативных мероприятий и сумели перекрыть каналы поставки вольфрама в Германию, лишив ее военную промышленность ценного сырья [Васильев, 2004].

А вот как оценивал помощь англичан СССР У. Донован, руководивший во время Второй мировой войны американской военной разведкой в Европе. В своем докладе президенту США Ф. Рузвельту об операции «Ультра» он отметил: «Если бы англичане пересылали в Кремль перехваченные германские военные приказы, Сталин, может быть, уяснил бы истинное положение вещей. Однако англичане считают аппарат Блетчли совершенно секретным. Они используют перехваченную информацию в собственных целях» [Даллес, 1992].

Однако информация из материалов дешифрования «Энигмы» поступала в СССР не только официальным путем. Гораздо более полные материалы поступали по линии разведки. В 1935 году на советскую разведку начал работать сотрудник МИД Англии Джон Кернкросс. Он стал передавать в СССР важные разведывательные материалы. Наиболее ценные среди них – это материалы, связанные с операцией «Ультра», к которым Кернкросс имел доступ с 1942 по 1944 год. Весной 1943 года от Кернкросса поступила информация о намерениях немцев начать наступление в районе Курска (операция «Цитадель»). При этом сообщались подробности предстоящей операции, число и номера дивизий, которые должны принять участие

в операции (номера немецких частей в официальных английских сообщениях не указывались). Эта информация имела особую ценность, так как советское командование предполагало, что немцы нанесут удар в направлении Великих Лук, а не Курска. В дальнейшем информацию Кернкросса подтвердили другие источники советской разведки. Сам Кернкросс особенно гордился тем, что шифры люфтваффе, которые он передал советскому командованию, позволили перед Курской битвой разбомбить значительную часть немецких самолетов на земле, и это стало предпосылкой господства советских ВВС в небе над Курском. Он также информировал о расположении авиабаз частей люфтваффе, нацеленных на действия в операции «Цитадель», и за два месяца до ее начала советская авиация нанесла по ним три упреждающих удара. Было уничтожено 17 аэродромов, немцы потеряли около 500 самолетов.

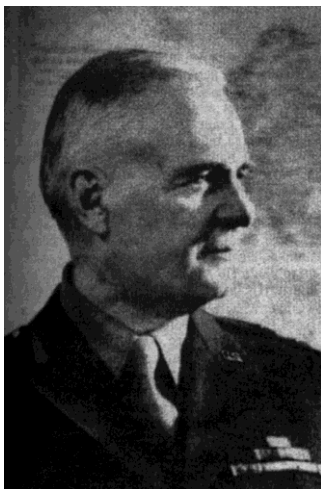


Рис 7.10. У. Донован

Советское руководство получило возможность изучить важные дешифрованные материалы нацистской Германии. По мнению некоторых историков, Кернкросс передавал СССР «копии наиболее секретных документов». За свою работу он был награжден орденом Красного Знамени. Когда передавать информацию стало почти невозможно, Кернкросс ушел из Блетчли-парка. В связи с возникшими у английской спецслужбы подозрениями, в 1944 году Кернкросс покинул Великобританию, куда вернулся только в 1995

296

году. Материалы «Ультра», переданные Кернкроссом, заметно дополнялись сведениями от сотрудника британской разведки Лео Лонга. С декабря 1940 года он работал в британском министерстве обороны в отделе MI-14, в котором занимались сопоставлением и анализом разведывательной информации. Лонг регулярно имел доступ к дешифрованным документам. Через некоторое время Лонг уволился с военной службы и прекратил сотрудничество с советской разведкой. Англичанами он так и не был разоблачен.

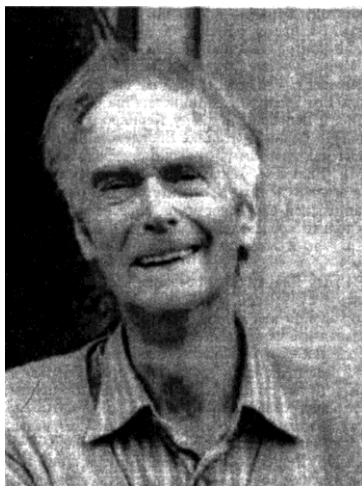


Рис. 7.11. Д. Кернкросс

Примером результативной работы советских агентов может служить следующий факт. В мае 1943 года НКГБ СССР направил в Государственный комитет обороны следующее сообщение: «Наш резидент в Лондоне передал текст телеграммы, отправленной 25 апреля 1943 года из южной группы германских войск за подписью генерал-фельдмаршала фон Вейхса в адрес оперативного отдела Верховного командования армии; в телеграмме говорится о подготовке немцами операции «Цитадель» (прорыв нашего фронта в районе Курск-Белгород)» [РД-5]. Скорее всего, текст этой телеграммы англичане получили в результате дешифрования «Энигмы», и она была передана советской разведке Кернкроссом.

Ценный источник информации в британском военном ведомстве имело и ГРУ. Агент ГРУ имел доступ к материалам дешифровальной службы и передавал их советскому разведчику. В

Москве этот агент имел оперативный псевдоним «Долли». В Лондоне его работой руководил военный разведчик «Билтон». В 1942 году «Долли» передал «Билтону» множество дешифрованных немецких, японских и турецких радиোগрам.

Интересно, что материалы, добытые Кернкроссом и Лонгом, послужили основанием для критики советских криптографов со стороны руководства страны. Им ставилось в вину, что они не дешифруют «Энигму», в то время как англичане умеют это делать. Но это было закономерно, так как наши криптографы не обладали той исходной информацией, которая имелаась у англичан.

Тем не менее, в конце 1942 года научная группа дешифровальной службы ГРУ выявила теоретическую возможность дешифрования немецких телеграмм, зашифрованных «Энигмой». Так сказано в представлении к награждению орденами группы офицеров дешифровальной службы военной разведки, которое было подписано начальником ГРУ генералом И. Ильичевым 29 ноября 1942 года. К наградам были представлены 14 офицеров. Однако следует отметить, что от определения того, можно ли вообще дешифровать шифратор до практических результатов – дистанция огромного размера.

Немцы весьма высоко оценивали возможности советских дешифровальщиков. В январе 1943 года специалисты Управления связи вермахта (немецкие сухопутные войска) пришли к выводу о вскрытии «Энигмы» советскими криптоаналитиками, так как в расположении окруженной под Сталинградом группировки немецких войск находилось 26 шифраторов этого типа, а подтвердить факт их уничтожения в условиях окружения не представлялось возможным и имелаась вероятность попадания «Энигмы» к русским. Кроме этого, среди тысяч пленных, захваченных советскими войсками под Сталинградом, могли оказаться шифровальщики. Действительно, в ходе боевых действий во время Второй мировой войны в руки советских специалистов попадали экземпляры основной шифровальной машины вермахта, а также ключи к ней. Были взяты в плен связисты-шифровальщики. Двое шифровальщиков были захвачены еще в 1941 году, еще три – при ликвидации Сталинградского котла (как видим, подозрения немцев не были напрасными). 30 июля 1944 года советские специалисты получили экземпляр морской «Энигмы» с поднятой со дна Финского залива немецкой подводной лодки U-250. После войны трофейные «Энигмы»

широко использовались в качестве учебных пособий при подготовке советских криптографов.

Однако эффективно воспользоваться этими трофеями нашим специалистам не удалось, в основном, из-за слабого развития «машинных» средств обработки информации и недостаточной математической подготовки. Основное внимание советские криптографы уделяли не «машинным» шифрам, а низовым армейским «ручным» шифрам Германии. Здесь им удалось достичь значительных результатов. Несмотря на это, в дальнейшем немцы применяли усовершенствованный вариант «Энигмы».

Разумеется, встает вопрос о том, предполагали ли немцы, что «Энигма» могла читаться англичанами. Отметим, что некоторые немецкие специалисты допускали возможность ее взлома. Еще в 1930 году один из ведущих немецких криптоаналитиков Георг Шредер, проанализировав шифратор, указал на такую возможность, едко заметив при этом: «Энигма - дерьмо!» [Лайнер, 2004]. Правда, шифратор постоянно усложнялся, появились коммутационная панель, дополнительные диски, от трехдисковой машины перешли к четырехдисковой. Ключевые установки часто менялись. Эти меры немецкие криптографы посчитали достаточными и в стойкости «Энигмы» не сомневались.

Выше мы уже привели примеры, когда тайна взлома «Энигмы» могла быть раскрыта из-за попадания к немцам людей, причастных к работам по криптоанализу немецкого шифратора. Однако здесь союзникам повезло. Теперь же рассмотрим как развивалась ситуация с оценкой стойкости «Энигмы» в самой Германии.

Одним из тех, кто постоянно высказывал подозрения, что англичане читают «Энигму», был командующий немецким подводным флотом гроссадмирал Карл Дениц. Но его все время убеждали, что подобные сомнения не обоснованы. В качестве аргументов ему представляли результаты работы немецких дешифровальщиков.



Рис. 7.12 К. Дениц

Первый раз Дениц поднял тревогу в июне 1940 года после пропажи судна «С-26» и потопления 31 мая 1940 года у берегов Англии подлодки «U-13». Однако специалисты службы связи кriegсмарине заявили, что все документы напечатаны краской, которая быстро растворяется в воде, а команды проинструктированы о необходимости уничтожения шифратора и документов к нему при угрозе захвата. К тому же, ключевые установки были уже сменены. Еще в феврале после потери подводной лодке «U-33» специалисты службы связи анализировали методы обеспечения безопасности связи на флоте, и один из них, капитан Людвиг Стаммель, заявил: «они лучше любого другого метода, в том числе, используемого противником» [Лайнер, 2004]. Главным аргументом стала информация от службы наблюдения – организации, отвечающей в кriegсмарине за криптоанализ. С лета 1940 года служба наблюдения читала шифры английских ВМС, и в дешифрованных сообщениях не было ни намека на то, что англичане читают «Энигму». Дениц на время успокоился.

Следует отметить, что на фоне дешифровальных успехов немцев их уверенность в абсолютной надежности собственных шифров выглядит по меньшей мере странной. Мало того, в практике кriegсмарине были примеры силового захвата английских шифров. 1 ноября 1940 года германский рейдер «Атлантис» атаковал и захватил

британский пароход «Отомедон», перевозивший совершенно секретные документы, в том числе, действующую кодовую книгу. Эти материалы были упакованы в специальный мешок, прикрепленный к грузу, чтобы в случае угрозы захвата немедленно их утопить. Однако англичанам не повезло, первым же залпом с рейдера был убит офицер, отвечавший за эти документы. Таким образом, немцы стали обладателями оперативных планов британского военно-политического руководства на случай войны с Японией. Расшифрованные документы срочно переслали в Токио. Император Хирохито наградил самурайским мечом командира «Атлантика». Такой награды среди немцев удостоились еще лишь Геринг и фельдмаршал Роммель.

В 1942 году другой германский рейдер «Тор» захватил в Индийском океане австралийский лайнер «Нанкин». Капитан успел выбросить за борт все коды и секретные документы корабля. Но 120 мешков с дипломатической почтой, где оказались и оперативные документы британского командования, достались врагу. Там были и сообщения о том, что союзники сумели вскрыть японские шифры. Последовала немедленная реакция: с помощью германских криптографов японская система кодирования была срочно переработана. В сентябре того же года немцы захватили на британском эсминце схему маршрутов своих конвоев. Это породило у немцев новые подозрения о компрометации собственных шифров, но дело ограничилось лишь сменой ключевых установок. «Энигме» все еще доверяли.

Вернемся к адмиралу Деницу. Весной 1941 года он обратил внимание на то, что английские конвои стали обходить места засад немецких подлодок. Стойкость «Энигмы» вновь была поставлена под сомнение. Однако и на этот раз Деница удалось убедить, что с шифратором все в порядке. В это время немецкие криптоаналитики вскрыли английский военно-морской код №3. В прочитанных немцами сообщениях не содержалось никакой информации о дешифровании англичанами немецких шифровок. Все же некоторые меры предосторожности немцами были приняты: ключевые установки на подводных лодках и надводных кораблях отныне стали разными. Кроме того, во избежание утечки информации Дениц предельно ограничил круг людей, которым были известны места засад «волчьих стай».

Вот, что написал сам Дениц в 1941 году по этому поводу: «Читал ли противник наш радиообмен, и если да, то в какой степени, – установить уверенно, несмотря на все наши усилия, нам не удалось. Во многих случаях резкое изменение курса конвоя наводило нас на мысль, что противник делал это. В то же время было много и таких случаев, когда, несмотря на оживленный радиообмен подводных лодок в определенном районе, одиночно следовавшие суда противника и даже конвои шли прямо в тот район, где только что были потоплены суда или даже имел место бой с атаковавшими конвой подводными лодками» [Дениц].

В мае 1941 года в ходе боев на острове Крит в руки немцев попала телеграмма, адресованная командующему английскими войсками генералу Фрейбергу, в которой сообщалось со ссылкой на надежный источник о ближайших планах немецкого командования. Это была информация, полученная в результате дешифрования «Энигмы». Перевод этой телеграммы был отправлен в Берлин, но никакой реакции, к счастью для англичан, не последовало.

4 июня 1941 года английский эсминец захватил немецкое грузовое судно «Гедания». О захвате немцы узнали, взяв в плен двух матросов с этого эсминца. Команда «Гедании» успела уничтожить шифратор и документацию к нему, однако об этом немцам известно не было. Добавил беспокойства и захват подлодки U-570 в августе. Скрыть факт захвата лодки англичанам оказалось невозможно. Дениц был очень обеспокоен возможностью попадания «Энигмы» к англичанам, но начальник службы связи ВМС Германии Эрхард Мартенс убедил Деница в надежности связи. Главным аргументом послужило то, что во время последнего сеанса связи с U-570 поступила информация, что там испытывают трудности с приемом ответных сообщений, Мартенс объяснил это тем, что команда уже начала уничтожение шифрдокументов. Мартенс утверждал, что команда «Гедании», также успела все уничтожить. Даже если к англичанам и попала какая-то информация, то новые ключевые установки, которые вводились с 1 ноября, и которых не было на лодке, обеспечат безопасность связи. На этот раз Мартенс был прав – англичане почти ничего не получили на «Гедании» и U-570, однако, как мог видеть читатель, в других случаях все обстояло для немцев не так благополучно.

Сентябрь 1941 года принес немцам новые сомнения. 11 числа англичане заставили всплыть очередную подводную лодку U-501.

Что-либо найти на ней англичанам не удалось, так как немцы успели уничтожить все необходимое и открыть кингстоны. Английская абордажная партия сама еле успела спастись с тонущей лодки. Но англичанам повезло в другом. Попытка захвата осталась в тайне, несмотря на то, что в этом районе в тот момент было чрезвычайно много немецких подлодок.

В конце сентября командование английскими ВМС преподнесло немцам ценный подарок, которым немцы не воспользовались. Несмотря на то, что тайна операции «Ультра» тщательно охранялась, иногда желание добиться успеха перевешивало соображения безопасности. Узнав из материалов «Ультра» координаты и время встречи в море трех немецких подводных лодок U-67, U-68 и U-111 у западного побережья Африки, Адмиралтейство отправило для их атаки английскую подлодку. Атака прошла крайне неудачно для англичан, им не только не удалось потопить немцев, но они сами попали под удар и английская субмарина получила серьезные повреждения. Самое плохое заключалось в том, что вновь Дениц усомнился в стойкости «Энигмы», так как справедливо посчитал, что английская лодка не могла случайно оказаться в удаленном районе океана в нужное время. А получить нужную информацию можно было только путем дешифрования немецких сообщений. Но Мартенс опять настаивал на стойкости «Энигмы». В противоположном мнении Деница «продолжало убеждать» английское Адмиралтейство. 22 ноября и 1 декабря английские крейсера потопили немецкие суда снабжения подводных лодок «Атлантида» и «Питон» в точках их встречи с подлодками. Последним в обоих случаях удалось уйти. Сразу после этих событий Дениц вновь поднял вопрос о стойкости «Энигмы», но в очередной раз его смогли убедить, что шифратор не читается англичанами. Одним из аргументов был уже упомянутый выше английский военно-морской код №3, вскрытый службой наблюдения. В дешифрованных сообщениях, зашифрованных при помощи этого кода, не было никакой информации по линии «Ультра». Адмирал Курт Фрике, которому поручили заниматься расследованием гибели «Атлантиды» и «Питона», предполагал, что имелась возможность предательства или вскрытия англичанами «Энигмы». Однако последнее предположение Фрике все же ставил под сомнение, так как «ни в одном из многочисленных сообщений, посланных противником с самого начала войны и прочитанных нами, не содержится ни малейшего намека на

то, что «Энигма» им взломана», – писал он [Лайнер, 2004]. Также аргументами в пользу «Энигмы» служили переход в январе 1942 года немецкого линкора «Тирпиц» в Норвегию и прорыв в феврале через Ла-Манш линкоров «Шарнхорст», «Гнейзенау» и крейсера «Принц Ойген» из французского порта Брест в норвежские порты. Появление этих кораблей в данном регионе угрожало проводу конвоев из США в Англию и СССР. Фрике утверждал, что если бы англичане читали «Энигму», то они бы сделали все, чтобы не допустить подобного перебазирования. В отношении «Тирпица» вообще ничего сделано не было, а против кораблей из Бреста меры были приняты с опозданием и не принесли результатов. На самом деле в Блетчли-Парке читали сообщения, зашифрованные «Энигмой», но с опозданием и просто не успели использовать полученную информацию.

В феврале 1942 года немецкие криптоаналитики вскрыли очередной шифр, с помощью которого поддерживалась связь между английскими и американскими судами, входящими в состав конвоев. Немцы стали получать информацию о маршрутах конвоев, в результате чего эффективность атак немецких подводных лодок возросла. Это стало очередным аргументом в пользу стойкости «Энигмы», так как, по мнению службы связи, в случае ее дешифрования англичанами эти успехи были бы невозможны.

Поскольку действиями любой немецкой лодки в Атлантике управляли из центра на берегу и, поскольку сосредоточение лодок для атак конвоев производилось Деницем на основе донесений с этих лодок, постоянно существовала реальная опасность того, что интенсивный радиообмен между субмаринами в море и центром на суше может оказаться доступным для англичан. В штабе Деница группа из шести офицеров непрерывно вела наблюдение за действиями англичан. Отслеживались действия эскортных сил, маневры конвоев, отклонявшихся от ожидавших их «волчьих стай», действия прикрывающей конвой авиации. Немецкая разведка старалась выявить признаки того, что англичанам удастся заблаговременно устанавливать места нахождения немецких кораблей и подводных лодок. Причем эту информацию нельзя было получить путем радиопеленгации, воздушной разведки или при помощи логических расчетов и умозаключений аналитиков английской морской разведки. Результаты этой работы убедили немецкий штаб в надежности своих шифров.

Но сомнения Деница подкрепляла и немецкая разведка. 10 августа 1943 года Дениц получил информацию, добытую немецкими разведчиками в Швейцарии. Со ссылкой на высокопоставленный источник в министерстве обороны США следовало, что союзники читают немецкие военно-морские шифры, при помощи которых шифровались приказы подводным лодкам (т.е. читают «Энигму»). Эта информация подтверждалась и событиями в Атлантике. С 12 июня по 1 августа 1943 года противник пытался помешать около половине встреч немецких подлодок в открытом океане, а с 3 по 11 августа все такие встречи были прерваны противником. Однако Дениц сделал вывод о том, что противнику удалось добыть ключевые установки к «Энигме» оперативным путем.

В стойкости шифратора продолжала убеждать гроссадмирала служба связи. Ее специалисты вновь заявили, что длительное чтение немецких шифрсообщений невозможно, а возможные кратковременные успехи союзников по-прежнему объяснялись утечкой информации в результате предательства или захвата ключевой информации противником.

Вскоре немецкие разведчики дополнили информацию из своего швейцарского источника. Новым источником стал некий американец, входивший в военно-морскую делегацию и часто совершавший поездки в Лондон. Он был в курсе англо-американского сотрудничества в области военно-морской разведки. Источник утверждал, что с самого начала войны у англичан функционирует центр по дешифрованию и анализу разведывательной информации. Деятельность центра весьма успешна: на момент получения информации, по сообщению агента, англичане читают все приказы немецкого командования своим подводным лодкам, что облегчает англичанам охоту за ними. Однако специалисты службы связи продолжали убеждать Деница в стойкости «Энигмы».

В конце 1942 года к анализу стойкости главного немецкого шифратора был привлечен один из главных криптографов вермахта Карл Штейн. В ходе своих исследований он пришел к следующему выводу: теоретически взломать «Энигму» можно, но практически это должно занять слишком много времени, так что шифратор можно считать достаточно надежным.

В начале 1944 года английское Адмиралтейство вновь подкинуло Деницу «информацию для размышления». В Блетчли-Парке из дешифрованных сообщений установили местонахождение

немецкого танкера «Шарлотта Шлиманн», который направлялся в Индийский океан для снабжения действовавших там немецких подводных лодок. 12 февраля 1944 года англичане потопили это судно. Спустя месяц в Индийском океане по наводке из Блетчли-Парка был потоплен другой немецкий танкер «Браке». История с «Питоном» и «Атлантидой» повторилась один к одному. Англичане рискнули тайной «Ультра» ради того, чтобы лишить немецких подводников горючего и боеприпасов, а проведенное службой связи расследование пришло к обычному выводу: версия о взломе «Энигмы» маловероятна, скорее всего снова имеет место предательство. Дениц опять согласился со своими криптографами. Тем не менее, была произведена экстренная смена ключевых установок, Дениц приказал командирам подводных лодок использовать новые ключи из первых букв фамилий определенных офицеров своих лодок. Но союзные криптоаналитики вскрыли эти ключи.

Благодаря стараниями специалистов из службы связи Дениц считал, что «Энигма» надежна, а неудачи немецких подводников объясняются другими причинами. Вот что он писал в 1944 году: «За исключением двух-трех сомнительных случаев, выводы англичан основывались на легко доступной для них информации о наших подводных лодках, на данных радиопеленгации работы их радиостанций и на данных прокладки движения лодок в сочетании с вполне осуществимым процессом логической дедукции. Наиболее важный результат нашего исследования – неоспоримое доказательство того, что с помощью оснащенной радиолокацией авиации противник способен с достаточной точностью вскрывать диспозицию наших подводных сил и соответственно изменять направление движения своих конвоев... Мы, естественно, должны были предполагать, что в наших базах на территории оккупированной Франции действовала разветвленная шпионская сеть противника. ...Хорошо организованная разведка противника, во всяком случае, имела возможность собирать данные о распределении подводных лодок по различным базам, о времени их выхода в море и возвращении в базы, а возможно, также и о предназначенных для лодок районах действий в море» [Дениц]. В действительности английская агентурная сеть на базах немецких подводных лодок (особенно норвежских) стала эффективной лишь на последних стадиях войны.

В июле 1944 года сотрудники немецкой военно-морской разведки вновь высказали опасения по поводу надежности немецких шифров, но сами же их развеяли: «Современное положение характеризуется серьезной тревогой экипажей подводных лодок, вызванной неудовлетворительным ходом боевых действий. Однако каких-либо прямых доказательств ненадежности наших шифров нет... Случаи предательства, которые произошли до настоящего времени и которые обсуждали в ВМС, с нашими главными шифрсистемами связаны не были». Немецкие криптографы были уверены в том, что «надежность шифров, используемых в нашей скрытой связи, очень высокая» [Бизли, 1981].

В целом штаб Деница переоценивал возможности воздушной разведки, фотографирования и обнаружения немецких субмарин при помощи авиационных и корабельных радаров. Это привело к тому, что немцы не хотели поверить, что англичане или американцы могут когда-либо добиться успехов в дешифровании их радиообмена. Они никогда не теряли уверенности в надежности своих шифровальных систем, использовавшихся кригсмарине, и строго следили за своевременностью смены ключей.

Итак, до самого конца войны службе связи удавалось развеять сомнения Деница в надежности «Энигмы». Не сомневались в стойкости «Энигмы» и другие немецкие военачальники.

Подводя итог вышесказанному, следует отметить, что, несмотря на чрезвычайные меры по обеспечению секретности (безусловно, давшие свои результаты), операция «Ультра» много раз находилась на грани провала. Но по разным причинам тайну все же удалось сохранить. Этому благоприятствовала твердая уверенность специалистов службы связи в надежности «Энигмы», несмотря на то, что факты много раз говорили об обратном. А в некоторых случаях англичанам просто фантастически везло.

Англичане добились больших успехов в дешифровании «Энигмы». В то же время они недостаточно совершенствовали свои методы шифрования. Это давало немцам возможность вскрывать многие английские шифры. Как уже было сказано выше, этим занималась служба наблюдения – подразделение кригсмарине, созданное в начале 1920-х годов.

Первого крупного успеха криптоаналитики кригсмарине достигли в середине 1930-х годов. В октябре 1935 года Италия напала на Абиссинию (ныне Эфиопия). В период между октябрём 1935 и

июнем 1936 года несколько кораблей британских королевских ВМС, базировавшихся в южноафриканском порту Аден, осуществляли патрулирование в Красном и Средиземных морях. Они следили за приготовлениями итальянцев к вторжению в Абиссинию, а в ходе начавшихся боевых действий – за воинскими перевозками. Поскольку эти корабли находились, по существу, на военном положении, радиобмен велся с использованием шифров и кодов, предназначенных для военно-морских сил в военное время. Район патрулирования был небольшим, они были хорошо видны с берега, поэтому узнать их названия было очень просто (тем более, что они указывались в репортажах лондонской прессы). Дешифровать позывные и сигналы оказалось совсем нетрудно, так как в сообщениях англичан было много стандартных формулировок, а основные слова и фразы регулярно повторялись.

После окончания операции коды и шифры англичане изменили незначительно. Это облегчило дальнейшую работу немецких криптоаналитиков. К 1938 году немцы уже раскрыли значительную часть кода, который английские ВМС использовали еще с 1934 года для административной (а не оперативной) связи. Шифр оперативной связи раскрыт, правда, не был. Однако большая часть радиообмена касающегося действий военных кораблей и конвоев, читалась немецкой службой наблюдения. Получаемые данные анализировались и накапливались немецкой военно-морской разведкой и передавались органам, занимавшимся оперативным планированием боевых действий подводных лодок, надводных рейдеров и авиации дальнего действия.

С самого начала войны дешифровальщики немецких ВМС приступили к работе по вскрытию шифров английского Адмиралтейства. Вскоре были достигнуты значительные успехи. В течение первых недель войны немецкие криптоаналитики получили возможность чтения зашифрованных радиোগрам англичан, касающихся движения кораблей и судов в Северном море и в проливе Скагеррак. Немцы узнали строго охраняемую англичанами тайну относительно использования бухты Лох-Ю в качестве базы Флота метрополии (наиболее сильное соединение английских ВМС, базировавшееся непосредственно на Британских островах). Специалисты службы наблюдения поставляли информацию капитанам крупных немецких надводных кораблей вышедших в Атлантику в ноябре 1939 года. Результатом работы дешифровальщиков, в частности, стало

потопление линкором «Шарнхорст» английского военного корабля «Равалпинди». Командование английских ВМС предпринимало меры противодействия немецким рейдерам, но они становились известными руководству кригсмарине из дешифрованных английских радиোগрамм.

Успешная работа криптоаналитиков кригсмарине продолжалась и в 1940 году. Весной во время кампаний в Норвегии, а позднее и во Франции, немецкая дешифровальная служба обеспечила возможность заблаговременного получения информации о действиях английских сил в Норвегии и у побережья этой страны. Немцам в этот период удавалось читать от тридцати до пятидесяти процентов радиообмена королевских ВМС. Кроме того, немецкое командование располагало точнейшей информацией о диспозиции кораблей Флота метрополии. Только за три месяца 1940 года, используя информацию службы наблюдения кригсмарине, удалось потопить шесть английских подводных лодок.

Во время вторжения немцев в Норвегию специалисты службы наблюдения получили информацию о намерениях англичан напасть на транспорты с немецким десантом. В ответ кригсмарине нанесли отвлекающий удар. Английский флот был брошен на его отражение, и немецкие транспорты благополучно дошли до берегов Норвегии.

Во время подготовки вторжения на Британские острова (операция «Морской лев», лето 1940 года) служба наблюдения предоставляла командованию немецких ВМС важную разведывательную информацию. Возможно, в Адмиралтействе появились подозрения об успехах немецких криптоаналитиков, и 20 августа англичане сменили шифры. Это означало некоторый перерыв и известные трудности для немецкой дешифровальной службы, однако и новые английские морские шифры вскоре были вскрыты службой наблюдения.

В январе 1941 года по предложению 10-го отдела разведывательного управления британских ВМС (подразделение, отвечавшее за безопасность связи на английском флоте) в методы и порядок скрытой связи были внесены некоторые изменения. Это доставило немцам лишь временные трудности.

Информация из дешифрованных английских сообщений часто позволяла немецким кораблям и подводным лодкам уклоняться от столкновений с превосходящими силами английского флота. Поступали и другие ценные сведения. Так, в 1941 году немецкие криптоаналитики предоставляли капитанам своих подводных лодок

указания командующего английским флотом капитанам конвоев, следовавших в Англию, как им миновать опасные зоны на подходе к родным берегам. Разумеется, такая информация была крайне полезна немецким подводникам. К сожалению, для англичан, дальнейшие изменения в организации шифрованной связи, произведенные в сентябре 1941 года и имевшие своей целью еще больше затруднить работу немецкой дешифровальной службы, наоборот, облегчили ее. К началу 1942 года специалисты службы наблюдения снова поставляли руководству кригсмарине ценную информацию.

На основании немецких архивов, захваченных после войны, англичанам стало известно, что в тот период руководство немецких ВМС получало от дешифровальной службы информацию, основанную на чтении более 2000 радиোগрамм в месяц. Немцы получали весьма подробные сведения о времени прибытия атлантических конвоев в прибрежные воды Великобритании, данные о распределении прибывавших судов по портам назначения, районах подхода конвоев или одиночно следовавших судов, их количестве, о метеорологических условиях. Они получали информацию об успехах эскортных сил, об атаках немецких подводных лодок и причиненных им повреждениях. О некоторых успехах службы наблюдения в 1941-1942 годах уже было рассказано выше.

В октябре 1941 года в проводке конвоев через Атлантику начали играть активную роль США. В результате объем радиообмена значительно возрос, и немцы вскоре это заметили. Радиообмен конвоев отличался от других передач характерным позывным сигналам, а также тем, он происходил почти исключительно между силами охранения конвоев. Используемый в этом радиообмене шифр немецкая дешифровальная служба назвала «конвойным шифром».

К февралю 1942 года немцы достигли значительных результатов в раскрытии «конвойного шифра» и читали большую часть зашифрованных с его помощью радиোগрамм, которые относились не только к североатлантическим конвоям, но и к операциям в средиземноморье и в других районах. Вскоре службе наблюдения удалось раскрыть еще один шифр союзников, используемый на Атлантике. К октябрю 1942 года немецкие дешифровальщики читали радиообмен с конвоями союзников настолько быстро, что Дениц иногда получал информацию о предстоящем движении судов за десять-двадцать часов до фактического осуществления того или иного маневра. Эта

информация дополнялась той, которую немцы без труда извлекали из чтения повседневного радиообмена между командованием английских ВМС на западных подходах к Британским островам и Галифаксом (город в Канаде, где был расположен штаб конвойных операций). По этим сообщениям немцы, в частности, знакомились с указаниями командирам конвоев об обходе опасных зон у берегов Англии.

Примерно в это же время службе наблюдения удалось вскрыть код торговых судов. Это был старый код. Новые, более совершенные коды, вовремя не ввели из-за желания сэкономить. Это желание подкреплялось господствовавшим в английском правительстве в 1920-30-е годы убеждения, что «войны больше не будет». В результате огромный торговый флот Британии вступил в борьбу с немецкими подводными силами, не располагая средствами надежной скрытой связи.

Специалисты службы наблюдения вскрывали не только военно-морские шифры англичан. До июня 1942 года англичане не располагали каким-либо специальным шифром для связи между различными видами вооруженных сил. В масштабных операциях, таких как операция в Норвегии, или рейды на Дьепп и Сен-Назер, вместо специальной действовала не очень стойкая шифрсистема, применявшаяся для связи вооруженных сил с отделениями министерства иностранных дел в доминионах и в колониях. Этот шифр использовался консульствами для донесений о движении судов в нейтральных портах, что служило дополнительным источником информации для немцев. Дешифровальщики кригсмарине быстро раскрыли эту систему и легко узнавали о маршрутах судов и о мерах английских ВМС, предпринимавшихся для борьбы с вооруженными немецкими рейдерами. К счастью для англичан, в ноябре 1941 года для береговых военно-морских властей была введена новая более стойкая шифрсистема.

Использование старых кодов привело к потере сотен кораблей с грузами и гибели около 30 000 английских моряков. С начала войны до лета 1943 года лишь в одной Северной Атлантике суммарное водоизмещение потопленных судов составило 11,5 миллиона тонн, не говоря уже о потерях, понесенных англичанами в ходе Норвежской кампании 1940 года и в других районах. Так, в результате дешифрования английского военно-морского кода №3 немцы получили информацию о маршрутах конвоев, что позволило «волчьим стаям» немецких подводных лодок устраивать эффективные засады.

Как немцы использовали информацию, получаемую из радиоперехвата и дешифрования, и насколько ценной она была для командиров подводных лодок, хорошо видно на примере проводки конвоев HX.229 и SC.122. В период с 16 по 19 марта 1943 года кораблям этих конвоев пришлось вести долгую борьбу с большой группой немецких субмарин. Атаке немцев предшествовало вскрытие службой наблюдения шестнадцати радиogramм, в которых содержалась подробная информация о движении обоих конвоев. Особенно важными среди них были радиogramмы, отправленные в 22.10 4 марта и в 19.32 13 марта. В первой сообщались подробности маршрута для конвоя HX.229 и для отставших от него одиночных судов, а во второй обоим конвоям давался приказ уклониться от маршрута на основании данных о диспозиции немецких подводных лодок, полученных оперативно-информационным центром Адмиралтейства. Хорошо информированный штаб немецких подводных сил сосредоточил для атаки этих конвоев сорок подводных лодок, и это закончилось для союзников потерей двадцати одного судна суммарным водоизмещением 140 000 тонн, в то время как немцы потеряли всего одну субмарину. Официальный английский военно-морской историк назвал эту операцию «серьезным бедствием для дела союзников» [Бизли, 1981].

Немцы вскрыли основные английские морские шифры к осени 1942 года, а новые шифры доставили судовым радистам британского ВМФ лишь в июне 1943 года. 10 июня был наконец-то заменен код №3, новый код оказался гораздо более стойким. Между тем, в торговом флоте англичан старые шифры использовались еще около 6 месяцев.

В марте 1943 года, во многом благодаря успехам службы наблюдения, немецким подводникам удалось почти полностью прервать морское сообщение между США и Великобританией. Английский морской штаб сделал заключение: «Немцы никогда не были столь близки к полному нарушению коммуникаций между Новым и Старым светом, как это им удалось в первые десять дней марта 1943 года» [Кан, 2004, с. 194]. Только героические усилия тысяч моряков и летчиков союзников позволили восстановить это сообщение. Причем немалую помощь в этом, как видно из вышесказанного, им оказали английские криптоаналитики из Блетчли-Парк.

Но и успехи немцев были весьма значительными. По заявлению пленного немецкого криптоаналитика, они не читали всю английскую переписку лишь потому, что не хватало переводчиков с серьезной языковой практикой. Немцы продолжали перехватывать до 2000 сообщений британских морских конвоев ежемесячно, следили за передвижением судов. Полученные данные позволяли оперативно наводить группы немецких подводных лодок, находящихся в Атлантике.

Один из английских военно-морских шифров немцы дешифровали весьма оригинальным образом. По сути дела, это был шифр гаммирования, основным ключом которого являлась специальная шифровальная книга. Основную роль при его вскрытии сыграло сосредоточение внимания немецких криптоаналитиков на анализе адресов сообщений. Адреса были зашифрованы тем же шифром, но они всегда находились в начале криптограмм. По большому количеству перехваченных сообщений немцы восстановили фрагменты книги, а затем и всю книгу целиком.

Гроссадмирал Дениц придавал огромное значение работе службы наблюдения, тем более, что немецкая авиация не могла в полной мере обеспечить воздушную разведку на большом удалении от баз. Дениц писал в своих мемуарах: «Я уже несколько раз упоминал о замечательной работе немецкой дешифровальной службы, которой неоднократно удавалось раскрывать шифры противника. В результате командование подводных сил читало не только английские радиogramмы и указания конвоям о маршруте движения, но и сводку адмиралтейства о диспозиции немецких подводных лодок (в январе и феврале 1943 года), которая ежедневно передавалась по радио командирам конвоев и в которой указывались известные английской разведке и предполагаемые места нахождения немецких лодок в различных районах» [Дениц].

Содержащиеся в этих сводках данные, – подчеркивал Дениц, – являлись для него весьма ценным материалом, который позволял представить, что именно было известно англичанам о диспозиции немецких подводных лодок и с какой степенью точности они определяли места и районы их действий. Эта информация позволяла оценить возможности противника по обнаружению немецких подводных лодок и понять, насколько эти возможности эффективны.

После того, как англичане в 1943 году сменили свои шифры, у службы наблюдения начались серьезные трудности. Чтение

шифрпереписки союзников почти прекратилось. Однако на последних стадиях войны криптоаналитики кriegсмарине снова смогли прочесть некоторые тактические коды и шифры противника. Благоприятным фактором здесь явилось то, что боевые действия надводных кораблей и авиации союзников в битве за Атлантику к тому времени значительно активизировались. В эфир стали отправлять большее количество сообщений, и это облегчало немцам процесс дешифрования. Немцам в этот период удавалось читать до 1500 радиogramм в месяц. Однако летом 1944 года союзники ввели новый, значительно более надежный шифр для связи с судами конвоев. Все попытки немцев раскрыть и его успехом не увенчались.

Хотя основные усилия служб радиоперехвата и дешифрования кriegсмарине были сосредоточены против западных союзников, не обошли они своим вниманием и восточный фронт. В 1941 – 1944 годах немецкие подводные лодки активно действовали в советском Заполярье. Их целью были конвои и отдельные суда, осуществлявшие перевозки по Северному морскому пути. Немецкие подводники активно действовали в Баренцевом, Белом и Карском морях, нередко их лодки заходили и далее на Восток. Присутствие немецких подлодок в эти годы отмечалось в Обской губе, устье Енисея, в районе порта Диксон, в море Лаптевых и у побережья полуострова Таймыр. Для наведения «арктических волков» адмирала Деница на цели активно использовались данные радиоперехвата. До нападения на СССР, для наблюдения за районом Баренцева моря немцы использовали радиопеленгаторную станцию в норвежском городе Киркенес. Более восточные районы были вообще не доступны. Разумеется, такая ситуация немцев не устраивала.

В 1942 году на советской территории (остров Земля Александра архипелага Земля Франца-Иосифа) тайно была развернута 24 база метеорологической и пеленгаторной службы кriegсмарине. Здесь находились пункт отдыха и пополнения запасов немецких подводников и аэродром. Посты радиоперехвата были развернуты и на других тайных базах немецких подводников в советской Арктике. Советская служба радиоразведки неоднократно фиксировала сеансы связи немецких подлодок и радиостанций, находящихся на территории СССР (радиостанции на немецких базах использовались не только для радиоперехвата, но и для управления действиями немецких субмарин). Обнаруживали следы работы немцев в советском Заполярье уже после окончания войны. Например, во время

осмотра брошенного немецкого наблюдательного пункта на острове Вардропер (Юго-восточная часть Карского моря) были найдены радиодетали и кусок антенны.

Немцами подводниками для связи использовались различные средства. Применялась связь с помощью радио, света, звука. В конце лета 1943 года в районе мыса Желания (архипелаг Новая Земля) акустикам тральщика, входившего в советский конвой, с помощью гидрофона «удалось выявить признаки сразу четырех ПЛ противника, которые находясь в проливе, обменивались между собой четырехзначными текстами по звукоподводной связи» [Ковалев, 2006]. Очевидно, здесь речь идет о каких-либо шумовых эффектах, например ударах о металлические предметы, которые гидроакустик другой лодки мог слышать на довольно значительных расстояниях. Во второй половине войны немецкие подводные лодки могли принимать радиосообщения, даже находясь под водой на глубине до 20 метров. Световая сигнализация применялась, как правило, для переговоров между всплывавшими подлодками и судами обеспечения.

К сожалению, советские моряки в первый период войны не всегда должным образом защищали информацию. Если на военном флоте всегда понимали необходимость обеспечения скрытности и безопасности связи, то сотрудники Главного управления Северного морского пути таких мер не предпринимали. Именно суда этой организации осуществляли основную часть перевозок в Заполярье. Капитаны торговых судов и ледоколов, летчики полярной авиации, зимовщики полярных станций практически не пользовались шифрсвязью. Переговоры о местонахождении судов, маршрутах конвоев и т.д. велись открытым текстом. Несмотря на неоднократные предупреждения военных специалистов о недопустимости подобного состояния дел, полярники не использовали документы скрытой связи (так на флоте называли шифры). Мало того, на некоторых судах они просто отсутствовали. Только понесенные потери от действий немецких подводных лодок заставили сотрудников Главсевморпути осознать необходимость использования шифрованной радиосвязи. К лету 1943 года передачи открытым текстом важной информации прекратились. На этом театре военных действий немцы иногда получали доступ к криптографической информации в ходе боевых операций. Так в сентябре 1944 года немецкий десант, высадившийся с подводной лодки, захватил на сутки советскую полярную станцию на

мысе Стерлигова, среди прочих трофеев немцам достались радиошифры.

Советская радиоразведка также активно работала в Заполярье. Радиоперехват вели специальные береговые радиостанции, морские суда, в том числе и гражданские, полярные станции. Полученная информация тщательно анализировалась разведкой Северного флота. В результате этих мероприятий удалось установить районы действия немецких подводных лодок. Маршруты конвоев стали прокладывать в обход опасных участков. При невозможности обогнуть опасный участок туда направлялись дополнительные противолодочные силы и усиливалась охрана транспортных судов. Эти меры позволили существенно снизить потери наших судов от действий немецких подводников, а в некоторых случаях и уничтожить врага. В августе 1943 года в предполагаемом районе действия немецких субмарин патрулировала советская подводная лодка С-101. 28 августа советские подводники обнаружили идущую в надводном положении немецкую лодку U-639 и потопили ее залпом трех торпед. На месте гибели U-639 среди плавающих обломков советские моряки обнаружили почти неповрежденную сигнальную книгу [Ковалев, 2006].

В заключение повествования о службе наблюдения отметим, что на протяжении большей части войны дешифровальная служба кригсмарине состояла не более чем из пятидесяти криптоаналитиков. При большем штате они, несомненно, достигли бы еще более значительных результатов. Значительная часть материалов радиоперехвата оставалась необработанной. После того, как Дениц в 1944 году был назначен главнокомандующим ВМС, специалисты службы наблюдения стали пользоваться его особой протекцией. Но ранее им было намного труднее получать необходимые для работы средства и аппаратуру. По словам пленных немецких дешифровальщиков, захваченные документы и шифровальные машины противника оказали им лишь незначительную помощь. Информация, которую они получили при знакомстве с трофеями, оказалась только небольшим дополнением к тому, что они уже знали.

В последние дни существования Третьего рейха Дениц приказал специалистам службы наблюдения выехать из Берлина в Фленсбург (город на севере Германии недалеко от датской границы) и вступить в сотрудничество с англичанами и американцами путем предоставления им любой информации и оказания помощи, о которой их попросят союзники.

Англичане и американцы, безусловно, очень хотели узнать о достижениях немецких криптографов в течение шести лет войны. Им было интересно знать об успехах, которых достигли немцы в отношении радиообмена военно-морских сил союзников. Получить доступ к документам и войти в контакт с немецкими криптографами было одной из основных целей специальных полевых групп английского разведывательного управления ВМС во время продвижения союзных войск весной 1945 года к балтийским портам, в которых находились немецкие военно-морские штабы. Помимо других соображений существенную роль при этом сыграло и то обстоятельство, что был нежелателен захват немецких экспертов советскими войсками, поскольку немецким дешифровальщикам было слишком много известно об английской системе скрытой радиосвязи.

Летом 1945 года англичане активно допрашивали пленных немецких специалистов. В Лондон были перевезены немецкие военно-морские архивы. Англичане хотели знать, какие изменения и усовершенствования, осуществленные ими в шифрах и кодах, сработали; как и когда немецкие дешифровальщики раскрыли высоконадежные коды и шифры; какие поражения в операциях флота можно было бы отнести целиком на счет отлично работавшей немецкой радиоразведки и дешифровальной службы; какие силы и средства имели в своем распоряжении эти службы. Факт за фактом, документ за документом убедительно доказывали, что успехи немецкой дешифровальной службы в раскрытии английских кодов и шифров оказались намного большими, чем предполагали англичане. Через несколько месяцев был подготовлен доклад, обобщающий полученные англичанами сведения о деятельности службы наблюдения кригсмарине. С этим докладом было ознакомлено высшее руководство Адмиралтейства.

Следует отметить, что в отличие от немцев, до конца войны так и не поверивших в возможность дешифрования «Энигмы», англичане допускали возможность компрометации своих шифров. Однако консерватизм чиновников Адмиралтейства и организационные трудности нередко мешали своевременно принимать соответствующие меры. И все же английские специалисты, отвечавшие в королевских ВМС за безопасность связи, делали все возможное, чтобы затруднить работу немецких дешифровальщиков. Так, например, немцы очень редко могли заблаговременно извлекать информацию о передвижении английских военных кораблей. В

частности, они не прочитали ни одной радиограммы во время операции Флота метрополии по потоплению «Шарнхорста» у норвежских берегов в декабре 1943 года, хотя перехватили около 30 радиограмм.

В операции «Торч» (высадка союзников в Марокко и Тунисе) в ноябре 1942 года был использован специально созданный для нее шифр, и немцы не смогли его раскрыть. Специальные шифры применяли и во время других крупных операций. Например, при высадке на Сицилии в 1943 году и в Анцио (Италия) в январе 1944 года. В последней операции службе наблюдения удалось перехватить 158 радиограмм, но ни одной из них прочитать немцы не смогли.

ОЧЕНЬ СИРОТЛИВО БЕЗ ЗАКЛЮЧЕНИЯ хорошо, подумаем. Спасибо.