Математика и математическое моделирование. 2019.
№ 06. С. 35 – 58.

DOI: **10.24108/mathm.0619.0000210**

Математика и Математическое моделирование

Сетевое научное издание

http://mathmelpub.ru ISSN 2412-5911

УДК 003.26

Атаки на шифр случайного гаммирования

Бабаш А.В.[1,2,*]

[1]Национальный исследовательский университет «Высшая школа экономики», Москва, Россия
[2]Российский экономический университет имени Г.В. Плеханова, Москва, Россия
*babash@yandex.ru

Представлены атаки на шифр случайного гаммирования с расчетом их трудоемкости и надежности.

Ключевые слова: шифр случайного гаммирования; трудоемкость криптографического метода; надежность криптографического метода

Представлена в редакцию: 08.11.2019, исправлена 22.11.2019

Введение

В 1942 году американский инженер, криптоаналитик и математик Клод Э́лвуд Ше́ннон ввел понятие совершенности шифра, понимая под этим такой шифр, который невозможно дешифровать, то есть определить открытый текст по известному шифрованному тексту не зная ключа шифра. В современных терминах это означает, что для такого шифра не существует атаки с конечной трудоемкостью и ненулевой надежностью. Он же привел пример такого шифра – шифр случайного гаммирования и его частный случай шифр Вернама. Целью работы явилось доказательство наличия атак на этот шифр. Доказательство основано на том, что в случайной ключевой последовательности данного шифра должно встретиться с ненулевой вероятностью хотя бы две одинаковые мультиграммы алфавита ключа. Примером таких ключей являются ключи шифра Виженера, которые содержатся в множестве ключей шифра случайного гаммирования. Основной результат исследования состоит в разработке двух атак на шифр случайного гаммирования с расчетом их трудоемкостей и надежностей.

1. Обоснование недешифруемости ШСГ

Определение 1. Шифр считается совершенно секретным «если для каждого распределения вероятностей на множестве M для каждого сообщения $m \in M$ и каждого зашифрованного текста $y \in Y$ (для которого вероятность $p(y) > 0$) выполняется равенство:

$$p(m / y) = p(m). \qquad (1)$$

(Требование $p(y) > 0$ является техническим, оно необходимо для предотвращения принадлежности события с нулевой вероятностью)» [3, стр.32].

Описание шифра случайного гаммирования дано во многих монографиях [1-5, 14] всемирно известных криптографов. Описание и анализ этого шифра российскими специалистами представлен в учебниках С. В. Запечникова, О.В. Казарина, А.А. Тарасова А.П. [6], Алферова, А.Ю. Зубова, А.С. Кузьмина, А.В. Черемушкина [7], Фомичева В.М [13], И.Н. Васильевой, О.Н. Жданова, В.В. Золотарева [37] и др.

Обозначим через I={0,1,…n-1} номера упорядоченного алфавита используемого языка. Пусть $X = K = Y = I^L$, и подмножество $M \subseteq X$, есть множество содержательных текстов длины L. Для шифрования открытого содержательного текста буквы текста кодируются своими номерами в упорядоченном алфавите. При расшифровании номера шифрованного текста декодируются в буквы. Для $x = i_1 i_2 ... i_L \in M$ и $k = \gamma_1 \gamma_2 ... \gamma_L \in K$ уравнение шифрования $f(x,k) = y$ имеет вид

$$i_j + \gamma_j = y_j \bmod n, j \in \{1,...,L\}, \quad y = y_1 y_2 ... y_L \in Y. \qquad (2)$$

Уравнение расшифрования имеет вид $y_j - \gamma_j + n = i_j \bmod n$, $j \in \{1,...,L\}$, $n = |I|$. Предполагается, что на множестве открытых текстов задано не равновероятное распределение, а ключи выбираются случайно, равновероятно и независимо от открытого текста. В учебниках по криптографии доказано, что ШСГ является совершенно секретным шифром.

1.1 Цитаты о недешифруемости ШСГ

Авторы источников [1-11] утверждают, что такие шифры недешифруемы. Приведем частично их утверждения.

- «В этой главе мы рассмотрим другие экстремальные схемы и изучим схемы шифрования, которые доказуемо безопасны даже против злоумышленника, обладающего неограниченными вычислительными возможностями. Такие схемы называются совершенно секретными» [пер. гугл, 3, p. 35].

- «Горячая линия между США и бывшим Советским Союзом была (по-прежнему активна?). По слухам, зашифрована одноразовым блокнотом. Многие советские шпионские сообщения агентам были зашифрованы одноразовыми блокнотами. Эти сообщения все еще безопасны сегодня и останутся такими навсегда. Неважно, как долго суперкомпьютеры работают над этой проблемой. Даже после того, как инопланетяне из Андромеды высадятся на своих массивных космических кораблях с невообразимой вычислительной мощности, они не смогут читать советские шпионские сообщения, зашифрованные одно-

разовыми планшетами (если только они не смогут вернуться назад во времени и получить одноразовые подушечки» [пер. гугл, 4, p. 26].

- «Кодирование одноразового использования это единственный имеющийся у нас алгоритм, безопасность которого может быть доказана» [5, стр. 104].

- «Теоретически существует совершенно секретный шифр (иными словами, абсолютно стойкий шифр), но единственным таким шифром является одна из форм так называемого одноразового шифрблокнота, в которой открытый текст комбинируется с полностью случайным ключом и имеющимся у нас алгоритмом такой же длины» [6, стр. 22].

«При рассмотрении вопроса о теоретической стойкости шифров отвлекаются от реальных временных и сложностных затрат по вскрытию шифра (что определяет подход к практической стойкости). Во главу угла ставится принципиальная возможность получения некоторой информации об открытом тексте или использованном ключе. Впервые такой подход исследовал К. Шеннон. Он рассматривал уже знакомую нам модель шифра и единственную криптоатаку на основе шифртекста. Проследим за его рассуждениями. Как мы указывали, конечной целью работы криптоаналитика является текст сообщения или ключ шифрования. Однако весьма полезной может быть даже некоторая вероятностная информация об открытом тексте. Например, уже предположение о том, что открытый текст написан по-английски, представляет криптоаналитику определенную априорную информацию об этом сообщении даже до того, как он увидит шифртекст» [7, стр. 172].

In some systems, the amount of information available to the cryptanalyst is actually insufficient to determine the enciphering and deciphering transformations, no matter how much computing power the cryptanalyst has available. A system of this kind if called unconditionally secure. [8, стр. 399].

«Для совершенного шифра открытый текст «локализуется» во всем множестве открытых текстов. Тем самым, для него сама задача расшифрования становится бессмысленной. Никакой метод криптоанализа, включая полный перебор ключей, не позволяет не только определить ключ или открытый текст, но даже получить некоторую информацию о них. Алгоритм безусловно стоек, если восстановление открытого текста невозможно при любом объеме шифртекста, полученного криптоаналитиком. Безопасность безусловно стойких криптоалгоритмов основана на доказанных теоремах о невозможности раскрытия ключа» [9, стр. 5].

«В работах К. Шеннона в середине 20-го века было показано, что существуют совершенные шифры, которые не поддаются дешифровке никаким способом. Это утверждение математически доказано и справедливо при любой модели языка. В частности, таким является гаммирование с помощью равновероятной гаммы» [10, стр. 3].

«Иными словами, совершенным по тексту называется шифр, который имеет свойство: никакая перехваченная противником криптограмма не добавляет противнику никакой информации об исходном тексте, т.е. вероятность определения исходного текста при знании соответствующей ему криптограммы равна вероятности использования этого текста в языке. Если противник попытается вскрыть такой шифр методом полного перебора, то он

получит набор из всех возможных осмысленных текстов соответствующей криптограмме длины» [11, стр. 8].

«Shannon makes it very clear that there are two basic types of secrecy systems: those designed to protect against an attacker with unlimited computational resources and those designed to protect against an attacker with a given finite computational capability. Shannon called the kind of secrecy achieved by the former “theoretical secrecy” and that furnished by the latter “practical secrecy”— these terms have been replaced by “unconditiona security” (or sometimes “information-theoretic security”) and “computational security” in modern usage, but their meaning is unchanged. Shannon’s treatment of theoretical secrecy is conceptually rich. He gave the first precise definition of the “unbreakability” of a cipher, restricting himself to a ciphertext-only attack, as meaning that the cryptogram and the message it represents are statistically independent. He showed that the cipher proposed by G. S. Vernam in 1926, now often called the “one-time pad”, achieves “perfect secrecy”—which was Shannon’s term for such unbreakability» [12, p.14].

«История развития шифров поставила перед специалистами ряд неизбежных вопросов: существуют ли нераскрываемые шифры? Если существуют, то как они устроены? Каковы условия, обеспечивающие нераскрываемость шифра? Исследование этих и других подобных вопросов привело специалистов к понятию совершенной или теоретической стойкости шифрсистем» [13, стр. 259].

Итак, авторы приведенных источников утверждают, что такие шифры недешифруемы противником с неограниченной вычислительной мощностью. Согласно этому тезису шифры, не являющиеся таковыми, т.е. несовершенные шифры, необходимо отнести к дешифруемым шифрам. Как правило, при обсуждении совершенных шифров в качестве примера совершенного шифра приводится шифр случайного гаммирования [14-21].

1.2. Обоснование недешифруемости ШСГ с помощью его математической модели

Недешифруемость ШСГ можно пояснить, рассмотрев уравнения шифрования ШСГ

$$i_j + \gamma_j = y_j \bmod n,\ j \in \{1,2,...,L],\ y = y_1 y_2 ... y_L \in Y.$$

При фиксированном $y = y_1 y_2 ... y_L \in Y$ для каждого символа i_j существует единственный символ ключа γ_j, при котором справедливы указанные равенства. Ключ $k = \gamma_1 \gamma_2 ... \gamma_L \in K$ выбирался равновероятно. Следовательно, каждый открытый текст мог со своей априорной вероятностью быть решением данной системы уравнений. Поэтому определить открытый текст не представляется возможным.

2. Обоснование дешифруемости ШСГ

Ниже приводятся ранее полученные результаты криптоанализа совершенных шифров, в частности, шифра случайного гаммирования.

2.1.Краткий обзор работ о дешифруемости ШСГ.

В работах [22 - 24] было заявлено, что мнение о недешифруемости совершенных шифров ошибочно. Обоснование было основано на уточнениях понятия совершенности шифра введенных в работе [25]. Именно, данное выше определение ([3, стр. 32]) имеет ввиду атаки на открытый текст $m \in M$ по перехваченному шифрованному тексту $y \in Y$. Аналог же определения совершенности шифра по атакам на ключ $k \in K$ по перехваченному шифрованному тексту $y \in Y$ выглядит так:

$$p(k / y) = p(k) \qquad (3)$$

для любых $k \in K$ и $y \in Y$ [25]. Логично считать, что из выполнения (3) следует недешифруемость шифра по ключу, а не выполнение (3) следует понимать как дешифруемость шифра по ключу.

При случайном независимом от открытого текста и равновероятном выборе ключа шифра правая часть приведенного выше равенства является константой, а левая часть равна вероятности открытого текста зашифрованного ключом k в шифрованный текст y. Условие (2) не выполняется для ШСГ. Следовательно, шифр ШСГ дешифруем. Этот результат был получен в [22 - 24]. Однако конкретных атак на этот шифр приведено не было.

Описание предполагаемых атак на ШСГ было дано в [26]. Прежде чем переходить к описанию конкретных атак на шифр случайного гаммирования введем необходимые понятия и напомним основные идеи дешифрования шифра Виженера.

2.2. Основные понятия

Используем введенные ранее обозначения для ШСГ.

Определение 2. Ключ $k = \gamma_1\gamma_2...\gamma_{L"}$ длины L" содержит d-ключ Виженера $\gamma_1\gamma_2...\gamma_L$ длины L=qd, если его d-граммы $\gamma_{vd+1}\gamma_{vd+2}...\gamma_{(v+1)d}, v \in \{0,1,d+1,...,(q-1)\}$ одинаковы и $q \geq 2$.

Определение 3. Ключ $k = \gamma_1\gamma_2...\gamma_L$ длины L=qd называется d-ключом Виженера (имеет локальный периодом d [25]), если его d-граммы $\gamma_{vd+1}\gamma_{vd+2}...\gamma_{(v+1)d}, v \in \{0,1,d+1,...(q-1)\}$ одинаковы.

Ниже необходимо учитывать, что d-ключ Виженера при L=qd+r, r<d является одновременно и wd-ключом Виженера при $2w \leq q$.

Определение 4. d'-ключ Виженера назовем минимальным, если он не является d-ключом Виженера при любом d<d'.

Каждый d-ключ Виженера является одновременно и минимальным d'-слабым ключом при некотором d' делящим d.

Обозначим через M(d) множество всех отрезков длины d открытых текстов из M.

Определение 5. Минимальное d, при котором отрезок $i_1 i_2 ... i_d$ открытого текста распознается (читается) в множестве $|I|^d$ назовем расстоянием распознаваемости открытого текста и обозначим его через d*.

2.3. Дешифрование шифра Виженера [27 - 35].

Шифр, который известен под именем Виженера, впервые описал Джованни Баттиста Беллазо (итал. Giovanni Battista Bellaso) в своей книге La cifra del Sig. Giovan Battista Belaso. Часто этот шифр называют «лозунговым шифром», или «шифром с коротко периодической гаммой». Краткое описание такого шифра состоит в следующем.

В множестве I^L ключей ШСГ выделим подмножество минимальных d-ключей Виженера $d \in \{2,3,...,[\frac{L}{2}]\}$. Шифр Виженера получается из ШСГ, если для шифрования открытых текстов выбирать только минимальные d-ключи шифра Виженера называемые «лозунгами» длины d, $d \in \{2,3,...,[\frac{L}{2}]\}$. Процесс шифрования и расшифрования остается таким же, как и в ШСГ.

Методы дешифрования шифра Виженера широко известны специалистам по криптографии. Эти методы с примерами дешифрования можно найти в [36 - 42]. Все методы состоят из двух этапов. Первый этап состоит в определении по известному шифрованному тексту длины лозунга, то есть значения d в использованном ключе шифра Виженера. Эта задача решается двумя методами.

1. Метод Фридриха Казиского, представленный в 1863 году, анализирует повторения в шифртексте для шифра Виженера. Этот же метод независимо от Казиского был разработан советским криптографом Михаилом Соколовым. Данный метод широко известен в криптографической литературе. Метод основан на том, что если ключ периодический, то две одинаковые m-граммы открытого текста, отстоящие друг от друга на расстояние, кратное периоду ключа, будут одинаково зашифрованы в некоторые одинаковые m-граммы, находящиеся на том же расстоянии друг от друга. Появление же одинаковых m-грамм в шифрованном тексте по другим причинам маловероятно (при некоторых разумных ограничениях на величину m и на длину шифрованного текста L). Следовательно, большинство расстояний (т.е., возможно не все) между одинаковыми m-граммами шифртекста делятся на минимальный период d. Поэтому на практике в качестве предполагаемой длины лозунга в шифре Виженера рассматривают наибольший общий делитель длин большинства расстояний между повторениями m-грамм. Эксперименты для английского языка показали хорошую надежность этого метода, если в шифртексте имеются повторения m-грамм при m > 1 [25, стр. 167].

2. Метод Фридмана (англ. William Frederick Friedman) был опубликован в 1920 [27]. Затем появилось много работ уточняющих результаты Фридмана, расширяющие границы их применимости [28 - 35]. Фридман ввел в рассмотрение так называемый «индекс совпадения», на основе которого предложил алгоритм нахождения длины лозунга по известно-

му шифрованному тексту, полученному с шифра Виженера. Основой метода явился тот факт, что если взять элементы шифрованного текста шифра Виженера, выбранные с шагом выборки равным длине лозунга, и рассчитать вероятность совпадения выбранных элементов на случайно и равновероятно выбранных местах то эта вероятность будет приблизительно равна $\sum_{i\in I} p_i^2$, где p_i – вероятность появления буквы i в открытых текстах [25].

В [25] было дано обоснование методов дешифрования шифра Виженера разработанных Казиским и Фридманом. В применении этих методов к ШСГ первый этап дешифрования состоит в определении использования d-ключа Виженера по известному шифрованному тексту. Пусть $y = y_1 y_2 ... y_L$ шифрованный текст ШСГ полученный при шифровании открытого текста $x = i_1 i_2 ... i_L \in M$ при случайно и равновероятно выбранном ключе $k = \gamma_1 \gamma_2 ... \gamma_L \in K$. Без ограничения общности считаем, что L=qd, q>1.

Критерий Фридмана. Ниже будем считать, что на I задано вероятностное распределение $(p_i,\ i \in I)$. Ключ k ШСГ является d-ключом Виженера тогда и только тогда, когда при каждом j из {1,2,…d} для последовательности $y_j y_{j+d} y_{j+2d} \ldots$ выполняется приближенное равенство

$$\sum_{i\in I} \frac{v_i(v_i-1)}{q(q-1)} \approx \sum_{i\in I} p_i^2, \qquad (4)$$

где v_i - частота символа $i \in I$ в подпоследовательности $y_j y_{j+d} y_{j+2d} \ldots y_{j+(q-1)d}$ шифрованного текста $y_1 y_2 ... y_L$ ШСГ. Более точная правая часть (4) указана в [25, стр. 84-89].

Применяя этот критерий к шифрованному тексту ШСГ определяем, был ли использован d-ключ Виженера.

Второй этап метода дешифрования шифра Виженера состоит в нахождении двух открытых текстов зашифрованных одним ключом. Дело в том, что на первом этапе для ШСГ было определено значение d (d-ключа Виженера $k = \gamma_1 \gamma_2 ... \gamma_L$). Следовательно, ключ можно представить в виде $k = \gamma_1 \gamma_2 ... \gamma_{qd}$ с повторяющимися q раз отрезками ключа длины d. Поэтому неизвестный открытый текст $x = i_1 i_2 ... i_{qd}$ задает неизвестные открытые тексты $x(1) = i_1 i_2 ... i_{(q-1)d}$ и $x(2) = i_{d+1} i_{d+2} ... i_{qd}$ зашифрованные одним ключом $k = \gamma_1 \gamma_2 ... \gamma_{qd} ... \gamma_{qd}$. Методы определения этих двух текстов широко известны [13, 17, 25,]. Они работают с малой трудоемкостью. Один из них называется «методом протяжки вероятного слова». В более общей ситуации, а именно в задаче дешифрования шифра поточной замены при известном периоде ключевой последовательности этот метод подробно изложен в [25, стр. 180]. Обычно этот метод широко используют в учебных целях.

Второй метод называется «метод одновременного зигзагообразного чтения двух открытых текстов в колонках» [25, стр.180-185, 34 стр. 98-102]. Для дальнейшего удобства назовем этот метод *методом чтения в колонках*. В случае принятия решения на первом этапе дешифрования ШСГ о том, что был использован d-ключ Виженера применяем метод

чтения в колонках для дешифровании двух открытых текстов $x(1)=i_1 i_2 ... i_{(q-1)d}$ и $x(2)=i_{d+1} i_{d+2} ... i_{qd}$ зашифрованных на одном ключе.

Дадим его краткое описание. Из законов функционирования шифра Виженера вытекают следующие следствия

$$i_j - i_{d+j} = y_j - y_{d+j} \bmod n,\ j \in \{1,2,...,(q-1)d\}. \quad (5)$$

Правые части $\Delta_j = y_j - y_{d+j} \bmod n,\ j \in \{1,2,...,(q-1)d\}$ уравнений известны. Поэтому число возможных пар (i_j, i_{d+j}) в каждой левой части каждого j-того уравнения равно |I|. Каждому открытому тексту $x(1)=\mathrm{i}_1 i_2 ... \mathrm{i}_{(q-1)d}$ соответствует единственный открытый текст $x(2)=\mathrm{i}_{1+d} i_{2+d} ... \mathrm{i}_{qd}$. На этом свойстве основан метод чтения открытых текстов в колонках. В более общей ситуации он детально изложен в [25, стр. 181].

Практика использования метода чтения в колонках двух открытых текстов показала, если открытые тексты длины d распознаются (читаются) в множестве $|I|^d$, то ложные решения отсутствуют. Дополнительным обоснованием этого можно считать наличие общей части $i_{d+1} i_{d+2} ... i_{(q-1)d}$ в двух открытых текстах (в этом случае минимальное значение d=d* можно уменьшить). Эффективность метода чтения в колонках подтверждает и следующий важный исторический факт [3, стр. 34]: «Интересным примером этого является проект VENONA, в рамках которого США и Великобритания смогли расшифровать зашифрованные тексты, посланные Советским Союзом, которые ошибочно были зашифрованы повторяющимися ключами с помощью одноразового блокнота». Таким образом, подтверждено практическое дешифрование двух открытых текстов зашифрованных одним ключом ШСГ. Таким образом, надежность предложенного метода дешифрования равна вероятности $\frac{|I|^d}{|I|^L}$ использования d-ключа Виженера для зашифрования шифром случайного гаммирования открытого текста, а трудоемкость состоит из одной операции проверки наличия d-ключа Виженера и, в случае успеха, применения метода чтения в колонках.

Для разработки новых методов дешифрования ШСГ приведем новые критерии использования d-ключа Виженера в ШСГ.

2.4. Первый этап атак на ШСГ

С целью формулировки первого критерия d-ключа Виженера построим критерий Неймана Пирсона различающего две простые гипотезы с ошибками первого рода α и второго рода β относительно выборки $y_j y_{j+d} y_{j+2d} \dots y_{j+(q-1)d}$, где $j \in \{1,2,...d\}$, для двух вероятностных дискретных распределений: $H_{(i+c) \bmod n}$ - распределение

$$(\mathrm{p}'_i = p_{(i+c) \bmod n},\ i \in I, c \in I);$$

H_1 - равновероятное распределения на I.

1. Критерий d-ключа Виженера. Ключ k является d-ключом Виженера тогда и только тогда, когда при каждом j из {1,2,…d} для выборки $y_j y_{j+d} y_{j+2d} \dots y_{j+(q-1)d}$ нашлось c из I, при котором принята гипотеза $H_{(i+c) \bmod n}$.

Рекомендуем использовать критерий при больших значениях q.

Перейдем к формулировке второго критерия наличия d-ключа Виженера в ШСГ. При каждом j из {1,2,…d} последовательность $y_j y_{j+d} y_{j+2d} \dots y_{j+(q-1)d}$ будем трактовать как выборку из одного из двух вероятностных распределений двухграмм $y_{j+td}y_{j+(t+1)d}$ из множества I^2: $H_{(i+c) \bmod n,(i' \oplus c) \bmod n}$ - вероятностное распределение $(p_{(i+c) \bmod n} \cdot p_{(i'+c) \bmod n}, i \in I, i' \in I, c \in I)$, а H_1 - равновероятное распределения на I^2. Для различения гипотез используем наиболее мощный критерий с ошибками α, β первого и второго рода.

2. Критерий d-ключа Виженера. Ключ k является d-ключом Виженера тогда и только тогда, когда при каждом j из {1,2,…d} для выборки $y_j y_{j+d} y_{j+2d} \dots y_{j+(q-1)d}$ нашлось c(j) из I, при котором принята гипотеза $H_{(i+c(j)) \bmod n,\ (i'+c(j)) \bmod n}$.

Рекомендуем использовать критерий при больших значениях q.

С целью формулировки третьего критерия d-ключа Виженера предположим, что использованный ключ $k = \gamma_1 \gamma_2 \dots \gamma_{qd}$ в ШСГ является d-ключом Виженера. Тогда из законов функционирования ШСГ вытекают равенства (5). Правые части $\Delta_j = y_j - y_{d+j} \bmod n,\ j \in \{1,2,\dots,(q-1)d\}$ уравнений известны.

Их значения $\Delta \in I$ будем рассматривать как случайную величину из вероятностного распределения

$$p(\Delta = c) = \sum_{(i,i'):(i-i')=\Delta \bmod n} p(i)p(i').$$

Последовательность значений разностей $\Delta_j = i - i' \bmod n,\ j \in \{1,2,\dots,(q-1)d\}$ будем считать выборкой из вероятностного распределения $P(C) = p(\Delta = c, c \in I)$ или из равновероятного распределения Δ на I. Используем критерий Неймана Пирсона различающего две простые гипотезы с ошибками первого и второго рода α и β относительно выборки $\Delta_1, \Delta_2, \dots, \Delta_{(q-1)d}$ для двух вероятностных дискретных распределений: H_0 - распределение $P(C) = p(\Delta = c,\ c \in I)$; H_1 - равновероятного распределения на I.

3. Критерий d-ключа Виженера. Ключ k является d-ключом Виженера тогда и только тогда, когда для выборки $\Delta_1, \Delta_2, \dots, \Delta_{(q-1)d}$ принята гипотеза H_0.

Рекомендуем использовать критерий при больших значениях d или L.

В критериях 1, 2, 3 в качестве надежности P(L,d) критерия выступает величина $(1-\alpha)^d$.

2.5. Атаки на шифр случайного гаммирования

Целью данного раздела является изложение методов дешифрования ШСГ с конечной верхней оценкой их трудоемкости и ненулевой надежности. Предполагаем, что полученные ниже сложностные параметры методов могут быть в дальнейшем улучшены.

Атака 1. Пусть L=qd принимает большое значение.

1. Проверяем, зашифрован ли данный шифрованный текст $y_1 y_2 ... y_L$ d-ключом Виженера. Для этого применяем один из критериев 1 - 3. В случае неуспеха мы затратили одну операцию. Атака завершена.

2. В случае успеха применяем метод чтения в колонках для получения двух открытых текстов $x(1) = i_1 i_2 ... i_{(q-1)d}$ и $x(2) = i_{1+d} i_{2+d} ... i_{qd}$.

Надежность метода равна

$$\frac{1}{|I|^{L-d}}(1-\alpha).$$

Подсчитаем трудоемкость метода. Если был использован d-ключ Виженера и принята гипотеза H(0), то с вероятностью $\frac{1-\alpha}{|I|^{L-d}}$ мы осуществляем 2 операции: реализация критерия и реализация метода чтения в колонках. Если был использован d-слабый ключ и принята гипотеза H(1), то мы также осуществляем 2 операции с вероятностью $\frac{\beta}{|I|^{L-d}}$. Но в этом случае мы не получаем открытые тексты. Если не был использован d-слабый ключ и принята гипотеза H(1), то мы проводим 2 операции с вероятностью $(1-\frac{1}{|I|^{L-d}})\beta$. Ситуация, когда был использован d-слабый ключ, а критерий принял гипотезу H(0) невозможна. Следовательно, общая трудоемкость атаки равна

$$(2\frac{1-\alpha}{|I|^{L-d}} + \frac{\beta}{|I|^{L-d}} + (1-\frac{1}{|I|^{L-d}})\beta).$$

Атака 2. Пусть $d \geq d^*$. Цель атаки прочитать два отрезка открытого текста длины d по известному шифрованному тексту $y = y_1, y_2, ..., y_L$. Обозначим через p(d,L) вероятность того, что в равновероятно выбранном ключе длины L содержатся два одинаковых отрезка длины d.

Первая задача состоит в нахождении их, если они есть в используемом ключе $k = \gamma_1 \gamma_2 ... \gamma_L$. Рассмотрим упорядоченные d-граммы шифрованного текста $y = y_1, y_2, ..., y_L$.

1. Для первой d-граммы образуем пары $(y_1, y_2, ..., y_d; y_{j+1}, y_{j+2}, ..., y_{j+d})$, $j \in \{1, 2, ..., L-d\}$. Для второй образуем пары $(y_2, ..., y_{d+1}; y_{j+1}, y_{j+2}, ..., y_{j+d+1})$, $j \in \{2, ..., L-d\}$ и так далее. Всех пар

$$\frac{(L-d+1)(L-d)}{2} = W.$$

2. Проводим опробование всех пар. Для каждой пары делаем предположение о том, что неизвестные им соответствующие d-граммы открытого текста шифровались одинаковыми отрезками ключа. Для проверки этого предположения применяем метод чтения в колонках. Если этим методом получены два читаемых отрезка длины d, то метод завершил работу успешно. Если при опробовании всех пар не найдены два открытых текста длины d, то метод завершил работу неуспешно.

Перейдем к расчету параметров сложности данной атаки.

Ложное срабатывание метода чтения в колонках возможно в случае, когда при расшифровании шифрованных текстов $y = y_1 y_2 ... y_d$, $y' = y'_1 y'_2 ... y'_d$ случайными и равновероятно выбранными ключами $k = \gamma_1 \gamma_2 ... \gamma_d$, $k' = \gamma'_1 \gamma'_2 ... \gamma'_d$. расшифрованные тексты $x = i_1 i_2 ... i_d$, $x' = i'_1 i'_2 ... i'_d$ будут открытыми текстами из M(d). Подсчитаем вероятность такого события.

Предполагаем, что при расшифровании любого шифрованного текста случайным и равновероятным ключом каждое слово из I^d может быть получено с равной вероятностью $\frac{1}{|I|^d}$. Данное предположение является обычным для криптографии. Так в работах [1, 2, 15, 25, 35] это предположение использовано в расчетах расстояния единственности шифра. В связи с чем, вероятность получения открытого содержательного текста при расшифровании случайным равновероятным ключом равна $\frac{|M(d)|}{|I|^d}$, а вероятность получения пары открытых текстов при расшифровании пары шифрованных текстов есть $\frac{|M(d)|^2}{|I|^{2d}}$. Среднее число пар открытых текстов полученных из W расшифрованных пар шифрованных текстов по указанному выше правилу равно $W \cdot \frac{|M(\mathrm{d})|^2}{|I|^{2d}}$ (число ложных пар). Несложно проверить, что при $|M(\mathrm{d})| \le \frac{|I|^d}{(L-d)}$ указанное среднее значение не превосходит величины $\frac{1}{2} + \frac{1}{L-d}$. То есть, ложных пар не должно быть.

Вероятность неполучения ложных открытых текстов длины d при проведении метода чтения в колонках W раз равна

$$(1-(\frac{|M(d)|}{|I|^d})^2)^W,$$

а надежность метода есть

$$\mathrm{p}(d,L) \cdot (1-(\frac{|M(d)|}{|I|^d})^2)^W.$$

Трудоемкость метода равна числу опробуемых пар d-грамм шифрованного текста

$$W = \frac{(L-d+1)(L-d)}{2}.$$

Приведем расчет параметров сложности атаки 2 для русского языка с мощностью алфавита |I|=32. Тогда (см. атака 1 модель 3). Надежность метода равна

$$\mathrm{p}(d,L)\cdot(1-(\frac{|M(d)|}{|I|^d})^2)^W = \mathrm{p}(d,L)\cdot(1-\frac{1}{2^{10d}}) \approx \mathrm{p}(d,L).$$

Рассчитаем вероятность p(d,L). Всех d-грамм на длине L содержится L-d+1. Очевидно, что p(d,L)=1 при $L-d+1>|I|^d$. Будем считать, что d-граммы выбраны случайно и равновероятно из I^d. Тогда при $L-d+1\le|I|^d$ вероятность того, что все они различны, есть

$$(1-p(d,L)) = (1-\frac{1}{|I|^d})\cdot(1-\frac{2}{|I|^d})\cdot\ldots\cdot(1-\frac{L-d+1}{|I|^d}).$$

Из [43] следует

$$(1-p(d,L)) \le e^{-(L-d)(L-d+1)/2|I|^d}$$

и, следовательно,

$$p(d,L) \ge 1-e^{-(L-d)(L-d+1)/2|I|^d}.$$

3. Что же понимать под дешифруемостью и недешифруемостью ШСГ

Пример 1. Рассмотрим модель шифра случайного гаммирования $X=K=Y=I$ в алфавите русского языка, для шифрования содержательных текстов M={0,1} – команд на пуск ракет. Пусть команда 0 поступает на шифр с вероятностью p(0), а команда 1 с вероятностью $p(1)\ne p(0)$. Легко проверить, что этот шифр является совершенным по нападению на открытый текст. Подсчитаем p(k/y) и p(k). Очевидно, p(k)=1/|I| при любом k. Далее, при k=c p(k/c)=p(0), а при k=c-1 p(k/c)=p(1). Таким образом, p(k/c) не равно p(k) при k=c и k=c-1. Данный шифр несовершенен по ключу. Можно ли найти открытый текст *m* из множества {0,1} для данного шифра гаммирования по заданному шифрованному тексту c? Наша гипотеза состоит в ответе «нет». Но в предыдущем разделе было доказано, что ШСГ дешифруем. В чем же дело?

Читатель уже догадался, что, говоря о дешифровании ШСГ, необходимо фиксировать длину сообщений. Но это не все, следует фиксировать и мощность |M| множества открытых текстов, и условие: известно ли оно, и многозначность возможного дешифрования, и некоторую дополнительную информацию. Необходимо также конкретизировать формулировку задачи, какую информацию мы хотим определять, формализовав понятие информации. Конечно, это видимо не все.

Ниже приводится попытка формализации понятия дешифрования открытого текста ШСГ. Центральным словом в таких уточнениях будет слово «модель».

Нам потребуется вероятностная модель шифра К. Шеннона. С этой целью используем следующие обозначения [25]:

X - конечное множество, состоящее из двух или более элементов, названное множеством открытых текстов;

K - конечное множество, состоящее из двух или более элементов, названное множеством ключей;

Y - конечное множество, состоящее из двух или более элементов, названное множеством шифрованных текстов;

$(f_k)_{k\in K}$ - семейство инъективных отображений $X \to Y$;

$f_k(\mathrm{x}) = y$ – уравнение шифрования $x \in X, y \in Y$;

$(f_k^{-1})_{k\in K}$ - обратные отображения к $(f_k)_{k\in K}$, если $(f_k(\mathrm{x}) = y$, то $f_k^{-1}(\mathrm{y}) = x$;

$f_k^{-1}(\mathrm{y}) = x$ - уравнение расшифрования;

$f : \mathrm{X}\times K \to Y$ - сюръективное отображение, $f(\mathrm{x}, k) = f_k(x)$;

M – подмножество множества X, названное множеством содержательных текстов, имеющих некоторую «структуру», позволяющую отличить элемент x из M от элемента из X\M с некоторой надежностью. Например, $\mathrm{X}=\mathrm{I}^{\mathrm{L}}$ состоит из конечных слов $x = i_1 i_2 ... i_L$ в алфавите I длины L некоторого естественного языка, а M состоит из читаемых последовательностей вида $m = i_1 i_2 ... i_L$, то есть имеющих некоторое содержание.

$P(M = (p(m), m \in M)$ - дискретное вероятностное распределение на множестве M;

$P(K) = (p(k), k \in K)$ - дискретное вероятностное распределение на множестве K.

Определение 6.Пятерку введенных объектов

$$(\mathrm{X}, \mathrm{M}, \mathrm{K}, \mathrm{Y}, (f_k)_{k\in K}, (f_k^{-1})_{k\in K}, P(M), P(K))$$

назовем вероятностной моделью шифра (схемы шифрования) Клода Шеннона. Кратко – моделью шифра.

Определение 7. [25]. Модель шифра с множеством открытых текстов M и множеством ключей K является совершенной по нападению на открытый текст, при перехвате шифрованного текста, если для заданных распределений вероятностей на множествах M и K для каждого сообщения $\mathrm{m} \in \mathrm{M}$ и каждого зашифрованного текста $y \in Y, \mathrm{p(y)} \neq 0$, выполняется равенство $p(m / y) = p(m)$.

Необходимость такого уточнения диктуется тем, что каждый шифр может иметь несколько своих моделей. Например, легко доказывается, что в модели шифра простой замены, с помощью которой шифруются открытые тексты единичной длины, т.е. буквы, эта модель шифра является совершенной по нападению на открытый текст при перехвате шифрованного текста [25]. Модель же этого шифра, где шифрованию подлежат биграммы заданного алфавита, не является совершенной по нападению на открытый текст при перехвате шифрованного текста [25].

Атаки на шифры делятся на два класса: бесключевые атаки, когда атаки дают возможность определить открытый текст, не определяя секретный ключ, и атаки с предварительным определением ключа. В случае атаки с предварительным определением ключа,

как правило, сначала ищется секретный ключ или подмножество множества всех ключей шифра, содержащее с некоторой вероятностью секретный ключ или его эквивалент. Затем, в ряде случаев, открытый текст определяется путем расшифрования шифрованного текста на ключах данного подмножества.

Аналогично определению 6 уточняется и понятие совершенности шифра по ключу.

Определение 8. [24] Модель шифра с множеством открытых текстов M и множеством ключей K является совершенной по нападению на ключ, при перехвате шифрованного текста, если для заданных распределений вероятностей на множествах M и K для каждого сообщения $k \in K$ и каждого зашифрованного текста $y \in Y$, $\mathrm{p(y)} \neq 0$, выполняется равенство $p(k / \mathrm{y}) = \mathrm{p(k)}$.

Пример 2. Пусть для модели шифра $f_k(\mathrm{m}) = \mathrm{m}$ при любых $m \in M$, $k \in K$. Тогда данная модель шифра является совершенной по нападению на ключ, при перехвате шифрованного текста.

Определение 9. Эффективной атакой на открытый текст m модели шифра по перехвату шифрованного текста называется атака (способ, метод) определения открытого текста m шифра, (т.е. определение решений уравнения $f(m,k) = y$ относительно m из M) требующая конечных ненулевых временных (сложностных) затрат и дающая результат с ненулевой вероятностью. В противном случае, атака называется неэффективной.

Замечание 1. Атака на открытый текст путем его отгадывания не является эффективной атакой.

Определение 10. Модель шифра является недешифруемой, если для нее не существует эффективных атак определения открытого текста по перехвату шифрованного текста. В противном случае, модель шифра называется дешифруемой.

Примерами недешифруемой модели шифра являются модели шифра простой замены и ШСГ при шифровании естественных открытых текстов длины 1. Общеизвестно, что при достаточно длинном открытом тексте модель шифра простой замены дешифруема. Приведенные выше атаки на модель шифра случайного гаммирования при достаточно длинном открытом тексте являются доказательством его дешифруемости.

Таким образом, совершенность модели шифра по нападению на открытый текст при перехвате шифрованного текста не гарантирует ее недешифруемость. Отметим, что в классе дешифруемых шифров содержатся шифры практической стойкости [25].

Практика дешифрования шифров (например, шифра простой замены) приводит в некоторых моделях к неоднозначному определению открытого текста. В связи с этим в [13] такие шифры названы идеальными, а в более ранней работе [25] такие шифры были отнесены к группе теоретически стойких шифров.

Наше предложение состоит в том, чтобы назвать их шифрами многозначного дешифрования.

Аналогично определению 4, вводится понятие: эффективной атаки на «содержание открытого текста» (при заданной формализации данного понятия) по заданному перехвату информации. Примером такой атаки изложенная ранее атака 2 на ШСГ.

4. Обсуждение результатов

1. Изложенные атаки на шифр случайного гаммирования имеют два явно выраженных этапа: определение повторений в неизвестном использованном ключе, если оно имеются и дешифрование двух открытых текстов зашифрованных одним ключом. Наиболее сложным этапом является первый этап – применение и расчет статистических методов определения параметра d в неизвестном d-ключе Виженера. Практические примеры применения таких методов для шифра Виженера и других разнообразных шифров содержатся прекрасной работе [44].
2. Границы применения атак 1, 2 определены фиксированным значением d. Их можно расширить, введя предварительный этап опробования каждого возможного значения параметра d. Подсчет трудоемкости и надежности таких расширенных атак не вызывает затруднений.
3. Атаки делятся на бесключевые и на атаки с предварительным определением ключа. Теорию К. Шеннона о недешифруемости совершенных шифров следует понимать как недешифруемомть этих шифров при знании шифрованного текста для бесключевых атак на открытый текст.
4. Ряд публикаций использует теорию совершенных шифров К. Шеннона, например [45-49], а ряд работ расширяют границы применимости этой теории, например [50 - 5 1]. Результаты этих работ следует теперь понимать с учетом третьего замечания.
5. Шифр случайного гаммирования в настоящее время редко применяется на практике. Зачастую используются шифры гаммирования. Они состоят из генераторов псевдослучайных чисел (гаммы) и узла наложения гаммы [например, 52 - 54]. Указанные в работе атаки применимы и к таким шифрам.

Выводы

Представлены две атаки на шифр случайного гаммирования с расчетом параметров их сложности. Мнение о недешифруемости шифра случайного гаммирования ошибочно.

Список литературы

1. Shannon C.E. Communication theory of secrecy systems // Bell Systems Technical J. 1949. Vol. 28. No. 4. Pp. 656-715; Claude E. Shannon: Collected papers / ed. by N.J.A. Sloane, A.D. Wyner. N.Y.: Wiley-IEEE Press, 1993. Ch. 2. Pp. 84-143. DOI: 10.1109/9780470544242.ch2
2. Шеннон К.Э. Работы по теории информации и кибернетике: пер. с англ. М.: Изд-во иностр. лит, 1963. 829 с.

3. Katz J., Lindell Y. Introduction to modern cryptography. Boca Raton: Chapman & Hall: CRC Press, 2008. 534 p.
4. Schneier B. Applied cryptography: Protocols, algorithms and source code in C. 2nd ed. N.Y.: Wiley, 1996. 758 p.
5. Шнайер Б. Секреты и ложь: Безопасность данных в цифровом мире: пер с англ. М. и др.: Питер, 2003. 367 с. [Schneier B. Secrets and lies: Digital security in a networked world. N.Y.: Wiley, 2000. 412 p.].
6. Запечников С. В., Казарин О.В., Тарасов А.А. Криптографические методы защиты информации: учеб. М.: Юрайт, 2017. 309 с.
7. Основы криптографии: учеб. пособие / А.П. Алферов, А.Ю. Зубков, А.С. Кузьмин и др. 2-е изд. М.: Гелиос АРВ, 2002. 480 с.
8. Diffie W., Hellman M.E. Privacy and authentication: An introduction to cryptography // Proc. of the IEEE. 1979. Vol. 67. No. 3. Pp. 397-427. DOI: 10.1109/PROC.1979.11256
9. Авдошин С.М., Савельева А.А. Криптоанализ: современное состояние и перспективы развития // Информационные технологии. 2007. Прил. к журн. № 3. С. 1-32.
10. Зубов А.Ю. Совершенные шифры. М.: Гелиос АРВ, 2003. 160 с.
11. Жданов О.Н, Золотарев В.В. Методы и средства криптографической защиты информации: учеб. пособие. Красноярск: Изд-во Сибир. гос. аэрокосмич. ун-та (СибГАУ), 2007. 217 с.
12. Golomb S.W., Berlekamp E., Cover T.M., Gallager R.G., Massey J.L., Viterbi A.J. Claude Elwood Shannon (1916 – 2001) // Notices of the Amer. Math. Soc. 2002. Vol. 49. No. 1. Pp. 8-16.
13. Фомичев В.М. Дискретная математика и криптология: Курс лекций. М.: Диалог-МИФИ, 2003. 400 с.
14. Ferguson N., Schneier B. Practical cryptography. N.Y.: Wiley, 2003. 410 p.
15. Encyclopedia of cryptography and security / Ed. by C.A. Henk van Tilborg, Sushil Jajodia. 2nd ed. N.Y.: Springer, 2011. Vol. 1-2. 1475 p.
16. Mohamed Barakat, Eder Ch., Hanke T. An introduction to cryptography. 2nd ed. Technische Univ. Kaiserlautern, 2018. 138 p.
17. Buchmann J. Introduction to cryptography. N.Y.: Springer, 2012. 281 p.
18. Stinson D.R. Cryptography: Theory and practice. 3rd ed. Boca Raton : Chapman & Hall/CRC, 2006. 593 p.
19. Trappe W., Washington L.C. Introduction to cryptography: with coding theory. 2nd ed. Upper Saddle River: Pearson Prentice-Hall, 2006. 577 p.
20. Carroll J.M, Martin S. The automated cryptanalysis of substitution ciphers // Cryptologia. 1986. Vol. 10. No. 4. Pp. 193-209. DOI: 10.1080/0161-118691861001
21. Aumasson J.-P. Serious cryptography: a practical introduction to modern encryption. San Francisco: No Starch Press, [2017]. 282 p.

22. Бабаш А.В., Баранова Е.К. Совершенные шифры и как к ним относиться // Методы и технические средства обеспечения безопасности информации: 27-я науч.-техн. конф. (С.-Петербург, Россия, 24-27 сентября 2018 года): Материалы. СПб.: Изд-во С.-Петербург. политехн. ун-та, 2018. С. 77-81.
23. Babash A.V., Sizov V.A., Baranova E.K., Mikrukov A.A. Theoretically unbreakable ciphers as they should be understood // Современные информационные технологии и ИТ-образование. 2018. Т. 14. № 3. С. 573-577. DOI: 10.25559/SITITO.14.201803
24. Бабаш А.В., Баранова Е.К. Новый совершенный шифр тук-тук // Методы и технические средства обеспечения безопасности информации: 27-я науч.-техн. конф. (С.-Петербург, Россия, 24-27 сентября 2018 года): Материалы. СПб.: Изд-во С.-Петербург. Политехн. ун-та, 2018. С. 70-72.
25. Бабаш А.В., Шанкин Г.П. Криптография: учеб. пособие. М.: СОЛОН-ПРЕСС, 2007. 512 с.
26. Бабаш А.В., Баранова Е.К. Избранные вопросы криптоанализа шифра случайного гаммирования // Методы и технические средства обеспечения безопасности информации: 28-я науч.-техн. конф. (С.-Петербург, Россия, 24-27 июня 2019 г.): Материалы. СПб.: Изд-во С.-Петербург. Политехн. ун-та, 2019. С. 76-77.
27. Friedman W. F. The index of coincidence and its applications in cryptography. Geneva, Ill.: Riverbank Laboratories, 1922. 87 p.
28. Carroll J.M., Robbins L.E. Computer cryptanalysis of product ciphers // Cryptologia. 1989. Vol. 13. No. 4. Pp. 303-326. DOI: 10.1080/0161-118991863989
29. Denning D.E.R. Cryptography and data security. Reading, Mass.: Addison-Wesley, 1982. 400 p.
30. Gaines H.F. Cryptanalysis: A study of ciphers and their solution. [2nd ed.]. N.Y.: Dover Publ., 1956. 244 p.
31. Kahn D. The codebreakers: The story of secret writing. N.Y.: McMillan Publ. Co., 1967. 1164 p.
32. King J.C., Bahler D.R. An implementation of probabilistic relaxation in the cryptanalysis of simple substitution ciphers // Cryptologia. 1992. Vol. 16. No. 3. Pp. 215-225. DOI: 10.1080/0161-119291866892
33. Matthews R. An empirical method for finding the keylength of periodic ciphers // Cryptologia. 1988. Vol. 12. No. 4. Pp. 220-224. DOI: 10.1080/0161-118891862963
34. King J.C. An algorithm for the complete automated cryptanalysis of periodic polyalphabetic substitution ciphers // Cryptologia. 1994. Vol. 18. No. 4. Pp. 332-355. DOI: 10.1080/0161-119491882928
35. Kasiski F.W. Die Geheimschriften und die Dechiffrir-Kunst. B.: Mittler & Sohn, 1863. 95 p.
36. Васильева И.Н. Криптографические методы защиты информации: учеб. М.: Юрайт, 2016. 349 с.

37. Салий В.Н. Криптографические методы и средства защиты информации: учеб. пособие. Саратов, 2017. 43 с.
38. Цыганов А.В. Криптография и криптоанализ. СПб.: Изд-во С.-Петербург. гос. ун-та, 2009. 60 с.
39. Реализация и криптоанализ шифра гаммирования / Чертоги разума: личный блог Кузьминых Кирилла. Режим доступа: http://mindhalls.ru/gamma-code/ (дата обращения 12.08.2019).
40. Banks M.J. A search-based tool for the automated cryptanalysis of classical ciphers. The Univ. of York; Dep. of Computer Science, 2008. 76 p.
41. Бабаш А.В. Криптографические методы защиты информации: учебно-метод. пособие. 2-е изд. Т. 1. М.: РИОР: ИНФРА-М, 2013. 412 с.
42. Кормен Т., Лейзерсон Ч., Ривест Р. Алгоритмы: построение и анализ. М.: МЦНМО, 2002. 955 с. [Cormen T., Leiserson Ch., Rivest R. Introduction to algorithms. Camb.: MIT Press; N.Y.: McGraw-Hill, 1990. 1028 p.].
43. Kullback S. Statistical methods in cryptanalysis / War Dep.; Office of the Chief Signal Officer; Signal Intelligence Service. Revised ed. Wash.: U.S. Government Printing Office, 1959. 206 p.
44. Omolara A.E., Oludare I.A., Aman Bin Jantan, Humaira Arshad. An enhanced practical difficulty of one-time pad algorithm resolving the key management and distribution problem // Intern. MultiConf. of Engineers and Computer Scientists: IMECS 2018 (Hong Kong, March 14-16, 2018): Proc. Vol. 1. 2018. Pp. 409-415.
45. Lee C.-Y., Wang Z.-H., Harn L., Chang C.-C. Secure key transfer protocol based on secret sharing for group communications // IEICE Trans. on Information and Systems. 2011. Vol. E94-D. No. 11. Pp. 2069–2076. DOI: 10.1587/transinf.E94.D.2069
46. Yingbin Liang, Poor H.V., Shiomo Shamai (Shitz). Information-theoretic security // Foundations and Trends in Communications and Information Theory. 2009. Vol. 5. No. 4-5. Pp. 355-580. DOI: 10.1561/0100000036
47. Maurer U., Wolf S. The intrinsic conditional mutual information and perfect secrecy // IEEE intern. symp. on information theory: ISIT 1997 (Ulm, Germany, June 29–July 4, 1997): Proc. N.Y.: IEEE, 1997. P. 88. DOI: 10.1109/ISIT.1997.613003
48. Stallings W. Cryptography and network security: principles and practice. 5th ed. Boston: Prentice Hall, 2011. 719 p.
49. Godlewsky P., Mitchell C. Key-minimal cryptosystems for unconditional secrecy // J. of Cryptology. 1990. Vol. 3. No. 1. Pp. 1-25. DOI: 10.1007/BF00203966
50. Kessler G.C. An overview of cryptography. 2019. 65 p. Режим доступа: http://works.bepress.com/gary_kessler/67 (дата обращения 6.02.20).
51. Poonam Jindal, Brahmjit Singh. RC4 encryption - a literature survey // Procedia Computer Science. 2015. Vol. 46. Pp. 697-705. DOI: 10.1016/j.procs.2015.02.129

52. Johansson T., Jönsson F. On the complexity of some cryptographic problems based on the general decoding problem // IEEE Trans. on Information Theory. 2002. Vol. 48. No. 10. Pp. 2669–2678. DOI: 10.1109/TIT.2002.802608

Mathematics and Mathematical Modeling, 2019.
no. 06. pp. 35 – 58.

DOI: **10.24108/mathm.0619.0000210**

Mathematics & Mathematical Modelling

Electronic journal

http://mathmelpub.ru ISSN 2412-5911

Attacks on the Random Gamming Code

A.V. Babash[1,2,*]

[1]National Research University Higher School of Economics, Moscow, Russia
[2]Plekhanov Russian University of Economics, Moscow, Russia
[*]babash@yandex.ru

Keywords: random gamming code; complexity of the cryptographic method; reliability of the cryptographic method

Received: 08.11.2019, Revised: 22.11.2019

In 1917, Hilbert Vernam patented a top-secret encryption scheme, which at first was called a one-time notepad and later a Vernam cipher. At the time that Vernam proposed this scheme, there was no evidence that it was completely secret, since, in fact, at that time yet there was no idea what the perfect secret of the cipher was. However, about 25 years later, Claude Shannon introduced the definition of perfect secrecy (perfect cipher) and demonstrated that the random gamming cipher reaches this level of security. Cryptographers believe that there are no effective attacks for attacks of random gamming. In particular, there are no effective attacks for the Vernam cipher.

Objective: to justify the fallacy of this proposition to build effective attacks.

Methods: analysis of the relationship between the cipher key and the received encrypted text.

Results: an attack on the plaintext of a random gamming cipher based on a given encrypted text was developed. In addition, there was a suggestion for another attack on the plaintext contents based on the encrypted text. For all attacks, parameters of their complexity are calculated. These results are new. Previously, an attack on the random gamma code was unavailable. The results disprove the opinion that there are no attacks on this cipher.

Practical relevance: firstly, it has become possible to carry out attacks on the random gamming code. Secondly, when using this cipher, it is necessary to strictly limit the length of the message.

Discussion: the idea that there is an effective attack on a random gamming cipher arose in 2002, due to the possibility of introducing a similar concept, in which in a definition of the perfect cipher the plaintext is changed for a key. The first idea in creating attacks is that when the key is long its elements are repeated. The second idea is that attacks on two plaintexts are encrypted with one key. And the main idea was that it is necessary to improve the mathematical

model of the Shannon code. Therein, when interpreting the concept of the perfect cipher, we should talk about the cipher model perfection.

The publication place: in the Yandex search engine a query "Perfect ciphers" resulted in 22 million links, on a query "schemes perfectly secret" there were 43 million links. Yandex on the query "random gamming code" gave 13 million results.

References

1. Shannon C.E. Communication theory of secrecy systems. *Bell Systems Technical J.*, 1949, vol. 28, no. 4, pp. 656-715; *Claude E. Shannon: Collected papers* / ed. by N.J.A. Sloane, A.D. Wyner. N.Y.: Wiley-IEEE Press, 1993. Ch. 2. Pp. 84-143. DOI: 10.1109/9780470544242.ch2
2. Shannon C.E. *Raboty po teorii informatsii i kibernetiki* [Works on information theory and cybernetics]. Moscow: Foreign Literature Publ., 1963. 829 p. (in Russian).
3. Katz J., Lindell Y. Introduction to modern cryptography. Boca Raton: Chapman & Hall: CRC Press, 2008. 534 p.
4. Schneier B. Applied cryptography: Protocols, algorithms and source code in C. 2nd ed. N.Y.: Wiley, 1996. 758 p.
5. Schneier B. *Secrets and lies: Digital security in a networked world*. N.Y.: Wiley, 2000. 412 p. (Russ. ed.: Schneier B. *Sekrety i lozh': Bezopasnost' dannykh v tsifrovom mire*. Moscow a.o.: Piter Publ., 2003. 367 p.).
6. Zapechnikov S.V., Kazarin O.V., Tarasov A.A. *Kriptograficheskie metody zashchity informatsii* [Cryptographic methods of information security]: a textbook. Moscow: Urajt Publ., 2017. 309 p. (in Russian).
7. *Osnovy kriptografii* [Foundations of cryptography]: a textbook / A.P. Alferov, A.Yu. Zubkov, A.S. Kuz'min a.o. 2nd ed. Moscow: Gelios ARV Publ., 2002. 480 p. (in Russian).
8. Diffie W., Hellman M.E. Privacy and authentication: An introduction to cryptography. *Proc. of the IEEE*, 1979, vol. 67, no. 3, pp. 397-427. DOI: 10.1109/PROC.1979.11256
9. Avdoshin S.M., Savel'eva A.A. Cryptanalysis: Current state and future trends. *Informatsionnye tekhnologii* [Information Technologies], 2007, suppl. 3, pp. 1-32 (in Russian).
10. Zubov A.Yu. *Sovershennye shifry* [Perfect ciphers]. Moscow: Gelios ARV Publ., 2003. 160 p. (in Russian).
11. Zhdanov O.N., Zolotarev V.V. *Metody i sredstva kriptograficheskoj zashchity informatsii* [Methods and means of cryptographic protection of information]: a textbook. Krasnoiarsk, 2007. 217 p. (in Russian).
12. Golomb S.W., Berlekamp E., Cover T.M., Gallager R.G., Massey J.L., Viterbi A.J. Claude Elwood Shannon (1916 – 2001). *Notices of the Amer. Math. Soc.*, 2002, vol. 49, no. 1, pp. 8-16.

13. Fomichev V.M. *Diskretnaia matematika i kriptologiia* [Discrete mathematics and cryptology]: a textbook. Moscow: Dialog-MIFI Publ., 2003. 400 p. (in Russian).
14. Ferguson N., Schneier B. Practical cryptography. N.Y.: Wiley, 2003. 410 p.
15. Encyclopedia of cryptography and security / Ed. by C.A. Henk van Tilborg, Sushil Jajodia. 2nd ed. N.Y.: Springer, 2011. Vol. 1-2. 1475 p.
16. Mohamed Barakat, Eder Ch., Hanke T. An introduction to cryptography. 2nd ed. Technische Univ. Kaiserlautern, 2018. 138 p.
17. Buchmann J. Introduction to cryptography. N.Y.: Springer, 2012. 281 p.
18. Stinson D.R. Cryptography: Theory and practice. 3rd ed. Boca Raton: Chapman & Hall/CRC, 2006. 593 p.
19. Trappe W., Washington L.C. Introduction to cryptography: with coding theory. 2nd ed. Upper Saddle River: Pearson Prentice-Hall, 2006. 577 p.
20. Carroll J.M, Martin S. The automated cryptanalysis of substitution ciphers. *Cryptologia*, 1986, vol. 10, no. 4, pp. 193-209. DOI: 10.1080/0161-118691861001
21. Aumasson J.-P. Serious cryptography: a practical introduction to modern encryption. San Francisco: No Starch Press, [2017]. 282 p.
22. Babash A.V., Baranova E.K. Sovershennye shifry i kak k nim otnositsia [Perfect ciphers and how to treat them]. *Metody i tekhnicheskie sredstva obespecheniia bezopasnosti informatsii: 27-ia nauchno-tekhnicheskaia konferentsiia* [Methods and technical means for ensuring information security: 27th scientific and technical conf. (S.-Petersburg, Russia, September 24-27, 2018)]: Proc. S.-Petersburg, 2018. Pp. 77-81 (in Russian).
23. Babash A.V., Sizov V.A., Baranova E.K., Mikrukov A.A. Theoretically unbreakable ciphers as they should be understood. *Sovremennye informatsionnye tekhnologii i IT-obrazovanie* [Modern Information Technologies and IT-education], 2018, vol. 14, no. 3, pp. 573-577. DOI: 10.25559/SITITO.14.201803
24. Babash A.V., Baranova E.K. Novyj sovershennyj shifr tuk-tuk [New perfect tuk-tuk cipher]. *Metody i tekhnicheskie sredstva obespecheniia bezopasnosti informatsii: 27-ia nauchno-tekhnicheskaia konferentsiia* [Methods and technical means for ensuring information security: 27th scientific and technical conf. (S.-Petersburg, Russia, September 24-27, 2018)]: Proc. S.-Petersburg, 2018. Pp. 70-72 (in Russian).
25. Babash A.V., Shankin G.P. *Kriptografiia* [Cryptography]: a textbook. Moscow: SOLON-Press. 2007. 512 p. (in Russian).
26. Babash A.V., Baranova E.K. Izbrannye voprosy kriptoanaliza shifra sluchajnogo gammirovaniia [Selected issues of cryptanalysis of the random gamming cipher]. *Metody i tekhnicheskie sredstva obespecheniia bezopasnosti informatsii: 28-ia nauchno-tekhnicheskaia konferentsiia* [Methods and technical means for ensuring information security: 28th scientific and technical conf. (S.-Petersburg, Russia, June 24-27, 2019)]: Proc. S.-Petersburg, 2019. Pp. 76-77 (in Russian).

27. Friedman W.F. The index of coincidence and its applications in cryptography. Geneva, Ill.: Riverbank Laboratories, 1922. 87 p.
28. Carroll J.M., Robbins L.E. Computer cryptanalysis of product ciphers. *Cryptologia*, 1989, vol. 13, no. 4, pp. 303-326. DOI: 10.1080/0161-118991863989
29. Denning D.E.R. Cryptography and data security. Reading, Mass.: Addison-Wesley, 1982. 400 p.
30. Gaines H.F. Cryptanalysis: A study of ciphers and their solution. [2nd ed.]. N.Y.: Dover Publ., 1956. 244 p.
31. Kahn D. The codebreakers: The story of secret writing. N.Y.: McMillan Publ. Co., 1967. 1164 p.
32. King J.C., Bahler D.R. An implementation of probabilistic relaxation in the cryptanalysis of simple substitution ciphers. *Cryptologia*, 1992, vol. 16, no. 3, pp. 215-225. DOI: 10.1080/0161-119291866892
33. Matthews R. An empirical method for finding the keylength of periodic ciphers. *Cryptologia*, 1988, vol. 12, no. 4, pp. 220-224. DOI: 10.1080/0161-118891862963
34. King J.C. An algorithm for the complete automated cryptanalysis of periodic polyalphabetic substitution ciphers. *Cryptologia*, 1994, vol. 18, no. 4, pp. 332-355. DOI: 10.1080/0161-119491882928
35. Kasiski F.W. Die Geheimschriften und die Dechiffrir-Kunst. B.: Mittler & Sohn, 1863. 95 p.
36. Vasil'eva I.N. *Kriptograficheskie metody zashchity informatsii* [Cryptographic methods of information security]: a textbook. Moscow: Urajt Publ., 2016. 349 p. (in Russian).
37. Salij V.N. *Kriptograficheskie metody i sredstva zashchity informatsii* [Cryptographic methods and information security tools]: a textbook. Saratov, 2017. 43 p. (in Russian).
38. Tsyganov A.V. *Kriptografiia i kriptoanaliz* [Cryptography and cryptanalysis]. S.-Petersburg, 2009. 60 p. (in Russian).
39. *Realizatsiia i kriptoanaliz shifra gammirovaniia* [Implementation and cryptanalysis of the gamming cipher]. Available at: http://mindhalls.ru/gamma-code/, accessed 12.08.2019 (in Russian).
40. Banks M.J. A search-based tool for the automated cryptanalysis of classical ciphers. The Univ. of York; Dep. of Computer Science, 2008. 76 p.
41. Babash A.V. *Kriptograficheskie metody zashchity informatsii* [Cryptographic methods of information security]: a textbook. 2nd ed. Vol. 1. Moscow: RIOIR: INFRA-M Publ., 2013. 412 p. (in Russian).
42. Cormen T., Leiserson Ch., Rivest R. *Introduction to algorithms*. Camb.: MIT Press; N.Y.: McGraw-Hill, 1990. 1028 p. (Russ. ed.: Cormen T., Leiserson Ch., Rivest R. *Algoritmy. Postroenie i analiz*. Moscow: MTSNMO Publ., 2002. 955 p.).

43. Kullback S. Statistical methods in cryptanalysis / War Dep.; Office of the Chief Signal Officer; Signal Intelligence Service. Revised ed. Wash.: U.S. Government Printing Office, 1959. 206 p.
44. Omolara A.E., Oludare I.A., Aman Bin Jantan, Humaira Arshad. An enhanced practical difficulty of one-time pad algorithm resolving the key management and distribution problem. *Intern. MultiConf. of Engineers and Computer Scientists: IMECS 2018* (Hong Kong, March 14-16, 2018): Proc. Vol. 1. 2018. Pp. 409-415.
45. Lee C.-Y., Wang Z.-H., Harn L., Chang C.-C. Secure key transfer protocol based on secret sharing for group communications. *IEICE Trans. on Information and Systems*, 2011, vol. E94-D, no. 11, pp. 2069–2076. DOI: 10.1587/transinf.E94.D.2069
46. Yingbin Liang, Poor H.V., Shiomo Shamai (Shitz). Information-theoretic security. *Foundations and Trends in Communications and Information Theory*, 2009, vol. 5, no. 4-5, pp. 355-580. DOI: 10.1561/0100000036
47. Maurer U., Wolf S. The intrinsic conditional mutual information and perfect secrecy. *IEEE intern. symp. on information theory: ISIT 1997* (Ulm, Germany, June 29–July 4, 1997): Proc. N.Y.: IEEE, 1997. P. 88. DOI: 10.1109/ISIT.1997.613003
48. Stallings W. Cryptography and network security: principles and practice. 5th ed. Boston: Prentice Hall, 2011. 719 p.
49. Godlewsky P., Mitchell C. Key-minimal cryptosystems for unconditional secrecy. *J. of Cryptology*, 1990, vol. 3, no. 1, pp. 1-25. DOI: 10.1007/BF00203966
50. Kessler G.C. An overview of cryptography. 2019. 65 p. Available at: http://works.bepress.com/gary_kessler/67, accessed 6.02.20.
51. Poonam Jindal, Brahmjit Singh. RC4 encryption - a literature survey. *Procedia Computer Science*, 2015, vol. 46, pp. 697-705. DOI: 10.1016/j.procs.2015.02.129
52. Johansson T., Jönsson F. On the complexity of some cryptographic problems based on the general decoding problem. *IEEE Trans. on Information Theory*, 2002, vol. 48, no. 10, pp. 2669–2678. DOI: 10.1109/TIT.2002.802608