ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ В ИНФОРМАЦИОННОМ ПРОТИВОБОРСТВЕ

Бабаш Александр Владимирович,
доктор ф.м.н., профессор кафедры Информационной безопасности,
НИУ ВШЭ, babash@yandex.ru

ОБОБЩЕННАЯ МОДЕЛЬ ШИФРА

В поисковиках Интернета по запросу «Клод Шеннон» выдается сотни тысяч ссылок, что говорит о значимости криптографических результатов Клода Шеннона. Одна из его значимых идей состоит в разработке математической модели шифра. Суть модели, изложенная на русском языке, можно найти в его знаменитой книге «Работы по теории информации и кибернетике», 1963 (раздел «Теория связи в секретных системах»). Он рассматривал так называемые «секретные системы», в которых смысл сообщения скрывается при помощи шифра или кода, но само шифрованное сообщение не скрывается, и предполагается, что противник обладает любым специальным оборудованием, необходимым для перехвата и записи передаваемых сигналов. При этом рассматривается только дискретная информация, то есть считается, что сообщение, которое должно быть зашифровано, состоит из последовательности дискретных символов, каждый из которых выбран из некоторого конечного множества. Эти символы могут быть буквами или словами некоторого языка, амплитудными уровнями квантованной речи или видеосигнала. Ядром секретной системы является собственно шифр.

Данная работа ставит своей целью современное изложение идеи К. Шеннона и распространение ее на ассиметричные шифры. Использованы материалы монографий [1,2].

Алгебраическая модель шифра. Пусть X, К, У – некоторые конечные множества, которые названы, соответственно, множеством открытых текстов, множеством ключей и множеством шифрованных сообщений (криптограмм). На прямом произведении X×К множеств X и К задана функция f: X×К→У (f(x,χ)=y, x∈X, χ∈К, y∈У). Функции f соответствует семейство отображений f_χ: X→У, χ∈К, каждое отображение задано так: для x∈X

$$f_\chi(x)=f(x,\chi).$$

Таким образом, f_χ – ограничение f на множестве X×{χ}. Здесь {χ} – множество, состоящее из одного элемента. Заметим, что задание семейства отображений $(f_\chi)\chi\in К$, f_χ:X→У однозначно определяет отображение f:X×К→У, $f(x,\chi)=f_\chi(x)$.

Введенная четверка A=(X,K,У,f) определяет трехосновную универсальную алгебру, сигнатура которой состоит из функциональной единственной операции f.

Определение. Введенная тройка множеств X,K,У с функцией f: $X\times K\to У$

$$A=(X,K,У,f)$$

называется алгебраической моделью шифра, коротко – шифром, если выполнены два условия:

1) функция f – сюръективна (осуществляет отображение «на» У);

2) для любого $\chi\in K$ функция f_χ инъективна (образы двух различных элементов различны).

Запись $f(x,\chi)=y$ называется уравнением шифрования. Имеется в виду, что открытое сообщение x зашифровывается шифром A на ключе χ и получается шифрованный текст y. Уравнением расшифрования называют запись $f_\chi^{-1}(y)=x$ $(f^{-1}(y,\chi)=x)$, подразумевая, что шифрованный текст $y=f(x,\chi)$ расшифровывается на ключе χ и получается исходное открытое сообщение x.

Требование инъективности отображений $(f_\chi)\chi\in K$ в определении шифра равносильно требованию возможности однозначного расшифрования криптограммы (однозначного восстановления открытого текста по известным шифрованному тексту и ключу). Требование же сюръективности отображения f не играет существенной роли, и оно обычно вводится для устранения некоторых технических, с точки зрения математики, дополнительных неудобств, то есть для упрощения изложения. Подчеркнем, что множество X названо множеством открытых текстов. Его можно понимать как множество текстов возможных для зашифрования на данном шифре.

Введенная модель шифра отражает лишь функциональные свойства шифрования и расшифрования в классических с точки зрения истории криптографии системах шифрования (в системах с симметричным ключом). В этой модели открытый текст (или шифрованный текст) – это лишь элемент абстрактного множества X (или У), не учитывающий особенностей языка, его статистических свойств, вообще говоря, не являющийся текстом в его привычном понимании. При детализации модели шифра в ряде случаев указывают природу элементов множеств.

Примеры моделей шифров. Обозначим через I некоторый алфавит, а через I* - множество всех слов в алфавите I, то есть множество конечных последовательностей $(i_1,i_2,\ldots,i_L)$, $i_j\in I$, $j\in\{1,\ldots,L\}$, $L\in\{1,2,\ldots.\}$

Шифр простой замены. Пусть $X=M$ – некоторое подмножество из I*, а K – множество всех подстановок на I, т.е. $K=S(I)$ – симметрическая группа подстановок на I. Для каждого $g\in K$ определим f_g , положив для $(i_1,i_2,\ldots,i_L)$ из M $f_g(i_1,i_2,\ldots,i_L)=g(i_1),g(i_2),\ldots,g(i_L)$. Положим дополнительно

$$f(i_1,i_2,\ldots,i_L, g)=f_g(i_1,i_2,\ldots,i_L)$$

и $У=f(M)=\{f(i_1,i_2,\ldots,i_L,g)$: $g\in S(I)$, $(i_1,i_2,\ldots,i_L)\in M\}$. Таким образом, нами определен шифр $A=(M,S(I),У,f)$ простой замены, более точно: алгебраическая модель шифра простой замены с множеством открытых текстов $X=M$.

Шифр перестановки. Положим X – множество открытых (содержательных) текстов в алфавите I длины кратной T. $К=S_T$ – симметрическая группа подстановок степени T, для $g\in S_T$ определим f_g положив для $(i_1,i_2,\ldots,i_T)\in X$

$$f_g(i_1,i_2,\ldots,i_T)=(i_{g(1),}i_{g(2),\ldots,}i_{g(T));}$$

доопределим f_g на остальных элементах из X по правилу: текст $x\in X$ делится на отрезки длины T и каждый отрезок длины T шифруется на ключе g по указанному выше закону шифрования. Последовательность, составленная из букв образов зашифрованных слов, является шифрованным текстом, соответствующим открытому тексту x и ключу g. Таким образом, нами определена функция $f:X\times К\to У$ и шифр перестановки (X,ST,У,f). Для шифрования текста длины не кратной T его дополняют буквами до длины кратной T.

Шифр гаммирования. Пусть буквы алфавита I упорядочены в некотором естественном порядке. «Отождествим» номера этих букв с самими буквами. То есть формально положим $I=\{1,2,\ldots,n\}$, $|I|=n$. Положим X – некоторое подмножество множества I^L, $К\subseteq I^L$. Для ключа $\gamma=\gamma_1,\gamma_2,\ldots,\gamma_L$ из К и открытого текста $x= i_1,i_2,\ldots,i_L$ их X положим $f_\gamma(i_1,i_2,\ldots,i_L)=y_1,y_2,\ldots,y_L$, где $y_j=i_j+\gamma_j \bmod(n)$, $j\in\{1,\ldots,L\}$. Иногда под шифром гаммирования понимают и следующие способы шифрования: $y_j=i_j-\gamma j \bmod(n)$; $y_j=\gamma_j - i_j \bmod(n)$.

Обобщенная модель шифра. В классической модели шифра два абонента используют для связи один ключ, хранящийся от всех других абонентов в секрете. Такой ключ называют секретным, а криптографические системы с секретными ключами называют еще одноключевыми или симметричными шифрами (криптосистемами). При использовании симметричных криптосистем возникает проблема рассылки ключей. Если два человека, которые никогда ранее не встречались, должны передать друг другу секретную информацию, то им необходимо заранее договориться о ключе, причем сделать это нужно так, чтобы ключ был известен только им и больше никому. Для решения этой проблемы в шенноновской модели шифра предусмотрено наличие секретного канала связи, с помощью которого пользователи могут передавать ключи.

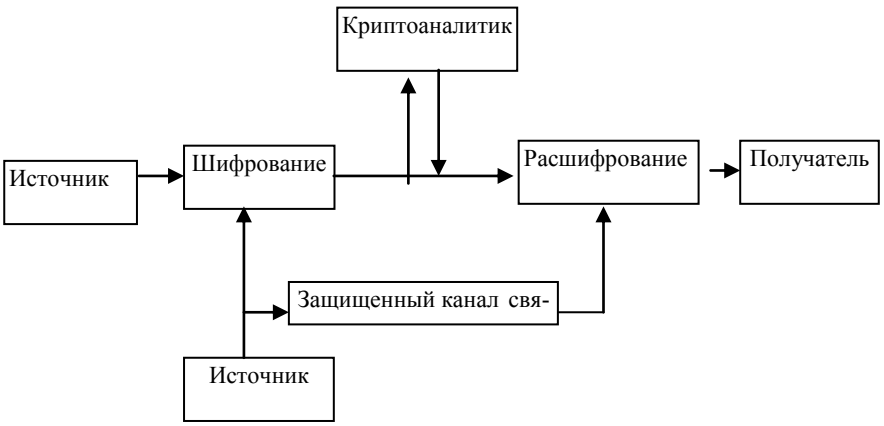

Рис.1. Классическая модель криптографической системы.

Алгебраическая модель шифра по К. Шеннону представляет собой трехосновную алгебру A=(X,K,У,f), где X,K,У – конечные множества, которые названы множеством открытых текстов $x \in X$, множеством ключей $\chi \in K$, множеством шифрованых текстов $y \in У$, соответственно; f – функция шифрования, f: $X \times K \to У$, обладающая свойством: при любом $\chi \in K$ отображение f_χ: $X \to У$, $f_\chi(x)=f(x,\chi)$ – инъективно. Последнее условие К. Шеннона отражает возможность однозначного расшифрования шифрованного текста. Как правило, при таком определении шифра обычно дополнительно считают, что функция F – сюрьективна. В данной модели считается, что при дешифровании противник знает шифр A=(X,K,У,f), однако использованный при зашифровании ключ ему неизвестен. Таким образом, модель Шеннона предназначена для описания шифров с симметричным ключом (шифров с неизвестным ключом шифрования и расшифрования).

Уравнение шифрования записывается в виде:

$$f(x,\chi)=y, \text{ или } f_\chi(x)=y.$$

Уравнение расшифрования записывается в виде:

$$f_\chi^{-1}(y)=x.$$

Достоинством данной модели шифра является ее универсальность. Она описывает практически все известные шифры с симметричным ключом.

Недостатки математической модели заключаются в следующем. 1) Шифры с ассиметричным ключом (шифры с открытым ключом) этой моделью не покрываются.

2) Даже при моделировании шифров с симметричным ключом отображение f_χ^{-1} задано не вполне корректно. Если элемент y не принадлежит множеству $f_\chi(X)=\{y: y=f_\chi(x), x \in X\}$, то значение $f_\chi^{-1}(y)$ не определено.

3) Затруднительно определить понятия «истинный» и «ложный» ключ при дешифровании методом тотального перебора ключей. Дей-

ствительно, если $f(x,\chi)=f(x,\chi`)$, где $\chi$ – ключ шифрования, а $\chi`$ – опробуемый ключ, то, как называть ключ $\chi`$, истинным или ложным?

4) Модель не учитывает наличие канала связи с помехами. Если произошло искажение передаваемого шифрованного текста $y=f(x,\chi)$ и на прием пришло сообщение $y`$, то значение $f_\chi^{-1}(y`)$ может быть не определено по причине того, что $y`$ не принадлежит $f_\chi(X)$, более того это значение может не принадлежать даже У.

5) Содержательная трактовка множества X в некоторых случаях вызывает затруднение. По определению, это множество «текстов» x, для которых определено значение $f(x,\chi)$ при любом $\chi\in К$, и они названы открытыми текстами. Но тексты, которые могут быть зашифрованы, в общем случае, делятся на «содержательные» (это подмножество $Xc\subseteq X$ и «бессодержательные» «хаотические», это множество $X\backslash Xc$). Критерий истинности дешифрования, например, методом опробования ключей $\chi\in К$, обычно строится в проверке условия $f_\chi^{-1}(y)\in Xc$ (критерий на содержательный текст). Если X=Xc (шифруются только содержательные тексты), то критерий вырождается в критерий: значение $f_\chi^{-1}(y)$ определено или нет. Приведенные соображения говорят о целесообразности наряду с множеством X ввести в модель и его подмножество Xc содержательных текстов.

Алгебраическая обобщенная модель шифра. Целью данного раздела является описание новой модели шифра, уточняющей модели К.Шеннона, Диффи и Хелмана и свободной от указанных выше недостатков. Основная концептуальная идея построения такой модели, на наш взгляд, естественна и очевидна. Она состоит во введении шифра шифрования и шифра расшифрования, совокупность которых и составляет алгебраическую модель шифров.

Шифром зашифрования (алгеброй зашифрования) назовем алгебру $А_ш=(X,Xc;Кш,У,Уc,f)$, где $Xc\subseteq X$, $f: X\times Кш\to У$ – сюрьективное отображение, причем для каждого $\chi\in Кш$ отображение $f_\chi:X\to У$, $f_\chi(x)=f(x,\chi)$ инъективно, а $Уc=f(Xc\times Кш)$. Множество Xc трактуется как подмножество всех содержательных текстов из множества «открытых текстов» X. Последнее множество состоит из текстов x, которые могут быть зашифрованы шифром, то есть тех x, для которых определено значение $f_\chi(x)$ для всех $\chi\in Кш$. Введение подмножества $Xc\subseteq X$, как множества содержательных текстов, позволяет корректно вводить критерии на содержательные тексты.

Таким образом, шифр зашифрования есть некоторое уточнение модели шифра Шеннона A=(X,Кш,У,f).

Шифром расшифрования (алгеброй расшифрования) для $А_ш$ назовем алгебру $А_р=(У`,Кр,X`F)$, где $У\subseteq У`$, $X\subseteq X`$, $F: У`\times Кр\to X`$ – сюрьективное отображение, для которого выполняются следующие условия:

1) существует биекция φ: Кш→Кр;

2) для любых x∈X, χ∈Кш из условия f(x,χ)=y вытекает F(y,φ(χ))=x.

При отсутствии искажений в канале связи функция расшифрования F полностью определена на всем множестве У×Кр. Введение множества Y` (а точнее, У`\У) обеспечивает возможность описания реакции приемной стороны на поступление искаженного шифрованного сообщения y`∉У.

Введение множества X`\X обеспечивает возможность описания результата расшифрования приемной стороной искаженного шифрованного сообщения y`∉У.

Отметим, что в определении шифра расшифрования не содержится требований инъективности функции F по переменной k∈Кр.

Алгебраической обобщенной моделью шифра назовем тройку (Аш, Ар, φ).

Отметим следующие положительные свойства этой модели.

1. Возможность моделирования шифров с асимметричным ключом. Здесь учитываются следующие соображения:

ключ χ∈Кш несекретен, а ключ k=φ(χ)∈Кр является секретным;

определение значения k связано с решением сложных проблем;

синтез пар ключей (k, χ) проводится достаточно просто.

Заметим, что здесь проявляется возможность классификации шифров по параметру сложности вычисления значения φ(χ) секретного ключа расшифрования, что определяет основной параметр криптографической стойкости шифров с ассиметричным ключом.

2. Возможность моделирования шифров с симметричным ключом.

Список литературы:

1. Шеннон К. Работы по теории информации и кибернетике. - М. ИЛ, 1963. - 830 стр.

2. Бабаш А.В., Шанкин Г.П. Криптография, Москва. СОЛОН – Р, 2002. -511 стр.

Баяндин Н.И.,
РЭУ им. Плеханова,
bajanick@rambler.ru

НЕКОТОРЫЕ АСПЕКТЫ АСИММЕТРИЧНЫХ МЕТОДОВ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

Информационное противоборство в бизнес-среде имеет много общего с действиями противоборствующих сил в информационной войне. В условиях наличия меньших потенциалов у более слабого объекта (компании) одним из эффективных методов достижения конкурентного