МЕТОДИЧЕСКАЯ РАЗРАБОТКА
для проведения лекции

Занятие № 16: «Основы шифрования».

Учебные вопросы:
1. Основные понятия в криптографии
2. Обобщенная модель системы шифрования.
3. Формы описания шифров
4. Шифры перестановки и шифры замены
5. Шифры гаммирования и их свойства

Заключительная часть

Введение

Криптография – одна из старейших наук. В переводе с древнегреческого языка означает «тайнопись», поэтому основное предназначение криптографии – сохранить в тайне некоторую информацию на различных этапах ее хранения, обработки и передачи.

Особую роль криптография играет при передаче информации заданному адресату втайне от других. Для этого существуют три основных способа:

1. Создание абсолютно надежного канала связи между абонентами, не доступного для других, на основе нетрадиционных методов передачи (что практически нереально при современном уровне развития науки и техники для неоднократной передачи больших объемов информации между удаленными абонентами).

2. Использование общедоступного канала связи, но сокрытие самого факта передачи информации. Разработкой средств и методов скрытия факта передачи сообщения занимается *стеганография*.

В настоящее время широкое распространение информационных технологий дало мощный толчок развитию цифровой стеганографии, появилось огромное количество методов сокрытия защищаемой информации внутри файлов различных форматов.

3. Использование общедоступного канала связи, но передача информации в виде, преобразованном таким образом, чтобы восстановить ее мог только заданный адресат. Разработкой методов преобразования информации с целью ее защиты от незаконных пользователей занимается *криптография*.

1. Основные понятия в криптографии

В современном представлении *криптография* – область научных, инженерно-технических, прикладных знаний, исследований и практической деятельности, которая связана с разработкой, анализом и обоснованием криптографической стойкости средств защиты информации от угроз со стороны злоумышленника.

Криптография не скрывает передаваемые сообщения, а преобразует их в форму, недоступную для понимания злоумышленником. Поэтому стеганография и криптография – принципиально разные направления в теории и практике защиты информации.

С некоторой долей условности криптография делится на две части – криптосинтез и криптоанализ, – а также включает в себя криптологию, рассматриваемую как область математики, изучающую различные математические модели криптографических систем. Подобная трактовка устанавливает соответствие между терминами «криптография» и «криптология», а также отражает исторически сложившуюся связь между теоретической и практической криптографией и роль в этом взаимодействии математики, физики, математической кибернетики, теории связи и др. (рис. 1).

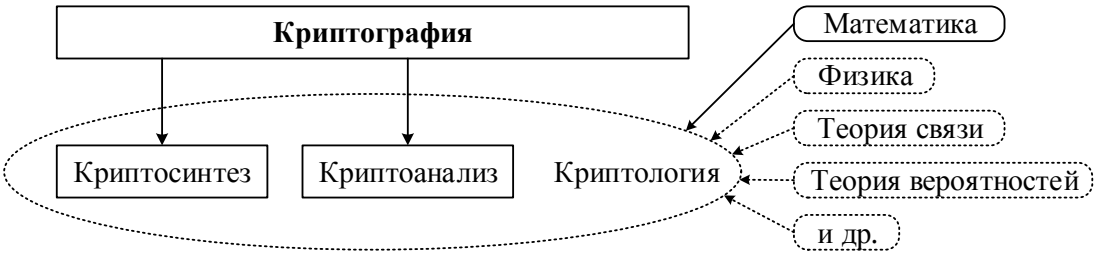


Рис. 1 – Структура криптографии

Криптосинтез непосредственно связан с разработкой криптографических систем (криптографических протоколов).

Криптоанализ заключается в исследовании какой-либо криптосистемы с целью получения обоснованных оценок ее криптостойкости. Причем результаты криптоанализа могут использоваться как для оценки эффективности системы защиты информации от потенциального злоумышленника, так и для подготовки и реализации атаки на криптосистему потенциальным злоумышленником.

Криптосистема – система обеспечения защиты информации криптографическими методами.

В качестве подсистем криптосистема может включать системы шифрования, системы идентификации, системы имитозащиты, системы цифровой подписи и др., а также ключевую систему, обеспечивающую работу остальных систем (рис. 2).

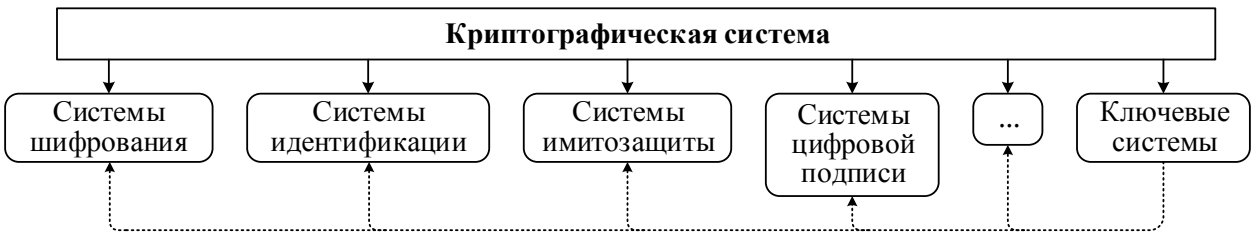


Рис. 2. – Основные подсистемы криптографической системы

В свою очередь, *система шифрования* предназначена для защиты информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней.

Понятие «система шифрования» включает в себя такие понятия, как «шифр», «ключ», «зашифрование», «расшифрование», «дешифрование».

Шифр – семейство обратимых отображений множества открытых сообщений в множество шифрованных сообщений и обратно, задаваемых функцией шифрования, каждое из которых определяется некоторым параметром, называемым *ключом*, и описываемых некоторым алгоритмом шифрования, а также порядком его применения, называемым *режимом шифрования*.

Шифрование – термин, объединяющий понятия зашифрования и расшифрования.

Ключ – важнейший компонент шифра – изменяемый параметр, каждому значению которого однозначно соответствует одно из отображений, реализуемых криптосистемой.

Зашифрование – процесс применения шифра к защищаемой информации, т. е. преобразование открытого сообщения в шифрованное сообщение (шифртекст, криптограмму) с помощью функции зашифрования, зависящей от ключа.

Расшифрование – процесс, обратный зашифрованию и реализуемый при известном значении ключа.

Дешифрование – процесс аналитического раскрытия злоумышленником открытого сообщения без предварительного полного знания всех элементов криптосистемы.

Система идентификации предназначена для аутентификации сторон в процессе информационного взаимодействия.

Система имитозащиты выполняет аутентификацию сообщений и предназначенная для защиты от несанкционированного изменения информации или навязывания ложной информации.

Ключевая система определяет алгоритмы и процедуры генерации, распределения, передачи и проверки ключей, порядок их регистрации, использования, смены, хранения и архивирования, резервного копирования и восстановления, замены или изъятия из обращения скомпрометированных, а также уничтожения старых ключей.

Основным требованием к криптосистемам и вместе с тем одним из фундаментальных понятий криптографии является стойкость.

Криптостойкость – свойство криптосистемы, характеризующее ее способность противостоять атакам злоумышленника, имеющего целью получить секретный ключ или открытое сообщение.

Злоумышленник может пытаться не получить, а уничтожить или модифицировать защищаемую информацию в процессе ее передачи и хранения, что является реализацией другого типа угроз для информации, для защиты от

которых используются специфические методы, обеспечивающие проверку и подтверждение подлинности содержания и источника сообщения.

Имитостойкость – свойство криптосистемы, характеризующее способность противостоять активным атакам злоумышленника, целью которых является навязывание ложного сообщения, подмена передаваемого сообщения или изменение хранимых данных.

Большое значение в криптографии имеет понятие алгоритма. Так, формальное описание функций, реализуемых системой шифрования, определяется соответствующими алгоритмами зашифрования и расшифрования.

Для других типов криптосистем рассматриваются алгоритмы формирования цифровой подписи, алгоритмы имитозащиты и др.

В последние годы одним из основных понятий криптографии стало понятие «криптографический протокол».

Криптопротоколом называется протокол, предназначенный для выполнения функций криптосистемы, в процессе выполнения которого участники используют криптоалгоритмы.

Криптопротоколы могут рассматриваться как отдельно, так и как часть конкретной криптосистемы, иметь как общий, так и прикладной характер.

Необходимость предотвращения и обнаружения нарушений со стороны участников информационного обмена разделяет общее понятие «злоумышленник» на отдельные понятия «нарушитель» и «противник».

Нарушитель – участник криптопротокола, нарушающий предписанные протоколом действия.

Противник – внешний по отношению к криптосистеме или участникам криптопротокола субъект, наблюдающий за передаваемыми сообщениями и/или вмешивающийся в работу участников путем перехвата, искажения, ввода, повтора и перенаправления сообщений, блокирования передачи и т. п. с целью нарушения одной или нескольких функций безопасности.

Нарушитель и противник могут быть как *пассивными*, которые получают некоторую информацию о выполнении криптопротокола или работе криптосистемы, не вмешиваясь в их работу, так и *активными*, которые вмешиваются в ход выполнения криптопротокола или работу криптосистемы.

Таким образом, основными задачами криптографии являются:

– *обеспечение конфиденциальности* – решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней;

– *обеспечение целостности* – гарантирование невозможности несанкционированного изменения информации с помощью простых и надежных критериев обнаружения любых манипуляций с данными (вставки, удаления и замены);

– *обеспечение аутентификации* – разработка методов подтверждения подлинности сторон и самой информации в процессе информационного взаимодействия (информация, передаваемая по каналу связи, должна быть аутентифицирована по источнику, времени создания, содержанию данных, времени пересылки и т. д.);

– *обеспечение невозможности отказа от авторства* – предотвращение возможности отказа субъектов от некоторых из совершенных ими действий.

Криптография использует самые последние достижения фундаментальных наук и существенно зависит от уровня развития техники и технологии, а также от применяемых средств связи и способов передачи информации.

2. Обобщенная модель системы шифрования.

Рассмотрим задачу обеспечения конфиденциальности информации с помощью обобщенной модели системы шифрования, позволяющей понять самые общие подходы, характеризующие ее функционирование, без учета физического представления сигналов и схем связи.

Обобщенная модель системы шифрования включает способ кодирования исходной и выходной информации, шифр и ключевую систему. При этом основными требованиями, определяющими качество системы шифрования являются криптостойкость, имитостойкость, помехоустойчивость шифра и др.

Пусть X, K, Y – конечные множества открытых сообщений, ключей и криптограмм соответственно; $E_k : X \to Y$ – алгоритм зашифрования на ключе $k \in K$; $D_k : Y \to X$ – алгоритм расшифрования на ключе $k \in K$.

Обобщенная модель системы шифрования информации представлена на рисунке 3.

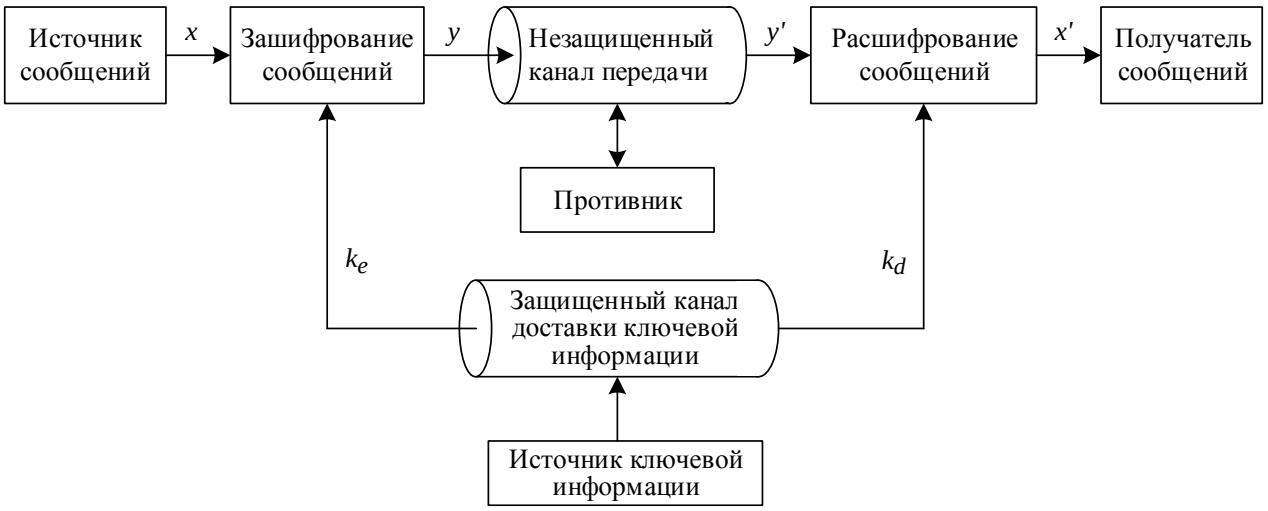


Рис. 3. – Обобщенная модель системы шифрования информации

Источнику сообщений при их передаче по каналу связи получателю необходимо сохранить все сообщения в тайне от противника, который пытается осуществлять пассивные (перехват данных, анализ трафика) и активные (искажение и навязывание передаваемых данных) атаки.

Каналы передачи информации, в которых противник может осуществлять пассивные или активные атаки, называются *незащищенными каналами передачи информации*.

В рассматриваемой модели имеется защищенный от противника источник ключевой информации, который вырабатывает некоторый ключ $k_e \in K$, предназначенный для зашифрования сообщений на передаче отправителем, и ключ $k_d \in K$, предназначенный для расшифрования криптограмм получателем при приеме. С помощью одной пары ключей зашифрования и расшифрования (k_e, k_d) нельзя обеспечить секретность всего множества сообщений, поэтому ключи зашифрования и расшифрования выбираются из некоторого множества ключей *K*, куда они входят парами. Ключи зашифрования и расшифрования зависят друг от друга, иначе получатель не сможет восстановить сообщение из криптограммы.

На практике стремятся добиться, чтобы вероятность выбора любого ключа из множества всех возможных имела одинаковое значение, т. е.

$$P(k_1) = P(k_2) = \ldots = P(k_L) = \frac{1}{L},$$

где L – количество возможных ключей.

Сформированная ключевая информация должна доставляться отправителю и получателю сообщений по защищенному каналу, в котором противник не способен на пассивные и/или активные атаки (например, по каналу спецсвязи Министерства связи России или Фельдъегерской специальной связи Министерства обороны России).

В качестве отправителя и получателя сообщений могут выступать абоненты телефонной, телеграфной, факсимильной, видеотелефонной связи, передачи данных и др.

Согласно обобщенной модели, источник сообщений генерирует сообщение $x \in X$ и перед отправлением получателю зашифровывает его на ключе $k_e \in K$, формируя криптограмму

$$y = E_{k_e}(x).$$

Образованная криптограмма $y \in Y$ передается по незащищенному каналу передачи информации получателю, который способен ее расшифровать, зная ключ расшифрования $k_d \in K$, и восстановить исходное сообщение

$$x = D_{k_d}(y).$$

Кроме того, для однозначного восстановления открытых сообщений из криптограмм требуется, чтобы отображение *D* являлось обратным к отображению *E*. Тогда для каждого сообщения $x \in X$ будет справедливо выражение

$$x = D_{k_d}(E_{k_e}(x)).$$

Следует отметить, что если $|X| < |Y|$, то для некоторых $y \in Y$ определить $D_{k_d}(y)$ невозможно.

В системах шифрования алгоритмы зашифрования и расшифрования обычно являются фиксированными и общеизвестными. Секретными элементами являются исключительно ключи, так как защищенность системы не должна зависеть от секретности чего-либо, что нельзя быстро заменить в случае утечки секретной информации.

Существуют системы шифрования с секретными криптопреобразованиями, стойкость которых в общем случае оценивается выше стойкости аналогичных систем с общеизвестными преобразованиями. Однако для подавляющего большинства используемых криптосистем в течение длительного срока их массовой эксплуатации обеспечить секретность криптопреобразований практически невозможно, поэтому общепринят подход к анализу криптосистем, предусматривающий возможность злоумышленнику достаточно детально ознакомиться с криптосистемой (принцип Керкгоффса).

В 1883 г. нидерландский криптограф Огюст Керкгоффс сформулировал шесть основных требований к криптосистемам, являющиеся с определенными допущениями актуальными до настоящего времени, которые можно интерпретировать следующим образом.

1. Система должна быть стойкой если не теоретически, то хотя бы практически, т. е. в системе шифрования на основе шифрованного текста должно быть невозможно раскрыть ключ или открытый текст (заметим, что если множество ключей конечно, то ключ всегда можно найти перебором, однако сложность перебора должна быть достаточно велика, чтобы обеспечить практическую стойкость).

2. Система не должна быть секретной, так как если она попадет в руки противника, то это не должно причинить неудобства ее легальным пользователям. При этом в системах шифрования знание открытых и соответствующих шифрованных сообщений не должно позволять противнику раскрыть ключ или другие открытые сообщения.

3. Система должна обеспечивать возможность хранения и смены ключевой информации.

4. Система должна допускать передачу дискретной информации (в XIX в. требовалась передача сообщений по телеграфу).

5. Система должна быть легко переносимой, а для ее обслуживания должно быть достаточно одного человека.

6. Система должна быть простой в эксплуатации.

Система шифрования является некоторой совокупностью сложных и дорогостоящих средств криптографической защиты, которые можно изменить только при значительных временных и экономических затратах, тогда как ключи представляют собой легко изменяемые объекты. В то же время именно ключи являются теми секретными элементами, которые в конечном итоге

определяют степень защищенности системы и одновременно могут быть оперативно, с небольшими затратами, заменены.

Характеристики систем шифрования информации

По соотношению ключей зашифрования k_e и расшифрования k_d системы шифрования разделяются на два класса:

– симметричные системы шифрования;

– несимметричные (асимметричные) системы шифрования.

Система шифрования информации называется *симметричной*, если для любой допустимой пары ключей зашифрования и расшифрования (k_e, k_d) вычислительно просто определить один ключ, зная другой, т. е. из k_e можно вычислить k_d, и, зная k_d, легко определить k_e. В таких системах оба ключа должны быть секретными.

Во многих симметричных системах ключ зашифрования совпадает с ключом расшифрования, т. е. выполняется равенство $k_e = k_d$. Поэтому симметричные системы шифрования иногда называют *одноключевыми* системами, или системами *с секретным ключом*. В таких системах для обеспечения идентичности ключей взаимодействующих сторон доставка ключевой информации должна осуществляться по каналам передачи, не имеющих ошибок.

Система шифрования информации называется *несимметричной*, если для любой допустимой пары ключей (k_e, k_d) вычислительно невозможно определить ключ расшифрования k_d, зная ключ зашифрования k_e.

В несимметричной системе ключ зашифрования k_e является открытым (общедоступным). Поэтому такие системы шифрования иногда называют системами *с открытым ключом*, или *двухключевыми*. Однако в таких системах обязательно должна обеспечиваться секретность ключа расшифрования k_d.

Несимметричные системы шифрования для практического использования удобны тем, что при доставке ключевой информации отправителям сообщений нет необходимости обеспечения секретности ключей зашифрования.

С точки зрения устойчивости систем шифрования к воздействию противника и/или нарушителя важной характеристикой является их способность противостоять криптоанализу. По степени доказуемости их безопасности существуют системы шифрования:

– безусловно стойкие (теоретически);

– практически стойкие, которые, в свою очередь, делятся на доказуемо стойкие и предположительно стойкие;

– временной стойкости.

По соотношению во времени процессов преобразования информации от источника, ее шифрования и передачи в канал связи системы шифрования делятся на два класса:

– системы линейного шифрования;

– системы предварительного шифрования.

Если функции шифрования и передачи в канал связи реализуются в реальном масштабе времени, то система реализует *линейное* шифрование. При этом криптограмма формируется и передается в канал (линию) связи по мере поступления элементов сообщения. Если же сначала из сообщения формируется криптограмма, а затем с определенным временем задержки она передается в канал (линию) связи, то такая система реализует *предварительное* шифрование.

Кроме приведенных признаков системы шифрования информации также могут быть классифицированы:

– по размеру обрабатываемого блока – поточные и блочные;

– виду обрабатываемого сигнала – дискретные и аналоговые;

– типу шифруемых сообщений – системы шифрования телеграфных, речевых, факсимильных сообщений, передачи данных;

– виду синхронизации между процессом зашифрования и расшифрования – автономные, с каналом синхронизации, полуавтономные и т. д.

Классификация шифров

Классификация шифров может быть произведена по многим признакам. В качестве наиболее общего показателя классификации шифров принят тип осуществляемых преобразований над отдельными фрагментами текста, называемыми *шифрвеличинами*, которыми могут быть символы, буквы, группы букв, слова, блоки и т. д.

Если шифрвеличины при шифровании меняются местами друг с другом, то соответствующий шифр относится к классу *шифров перестановки*. Если шифрвеличины при шифровании заменяются некоторыми соответствующими образами, называемыми *шифробозначениями*, то соответствующий шифр относится к классу *шифров замены*. Для повышения надежности шифрования шифрованный текст, полученный применением некоторого шифра, может быть еще раз зашифрован с помощью другого шифра. Все возможные композиции различных шифров составляют третий класс *композиционных шифров*. По размеру преобразуемых шифрвеличин шифры делятся на блочные и поточные.

Блочные шифры осуществляют преобразование информации блоками фиксированной длины, составленными из подряд идущих символов сообщения. При этом результат шифрования фактически зависит от всех исходных символов блока.

Поточные шифры предназначены для преобразования сообщения поэлементно (элементом может быть бит, символ и т. п.). В поточных алгоритмах каждый символ открытого сообщения шифруется независимо от других. При этом преобразование каждого символа открытого сообщения может меняться от одного символа к другому, в то время как для блочных алгоритмов в рамках шифрования блока используется одно и то же криптографическое преобразование.

3. Формы описания шифров.

Описание шифров может быть осуществлено в математической, табличной и графической формах.

Математическое описание шифров формализуется алгебраической и вероятностной моделями шифров.

Алгебраическая модель шифра предложена Клодом Элвудом Шенноном и представляет собой совокупность множеств открытых сообщений X, ключей K, шифрованных сообщений Y и отображений E: $X \times K \to Y$ и D: $Y \times K \to X$

$$\Sigma_{\text{а}} = (X, K, Y, E, D),$$

для которых выполняются следующие условия:

1) $D_k(E_k(x)) = x \; \forall \, x \in X, k \in K$ (условие однозначности расшифрования);

2) $\forall \, y \in Y : \exists \, x \in X, k \in K : E_k(x) = y$ (условие полноты).

Алгебраическая модель отражает основные свойства реальных шифров. Однако существенным недостатком алгебраической модели шифра является то, что она не позволяет оценить качество шифра, для анализа которого используется более расширенная вероятностная модель.

Вероятностная модель шифра требует знания распределений вероятностей $P(X)$ и $P(K)$ на множествах X и K соответственно. Данные распределения определяют вероятность $p(x) \in P(X)$ любого открытого сообщения $x \in X$ и вероятность $p(k) \in P(K)$ любого ключа $k \in K$, причем при $p(x) > 0$, $p(k) > 0$ выполняются равенства

$$\sum_{x \in X} p(x) = 1 \;\text{ и }\; \sum_{k \in K} p(k) = 1.$$

Таким образом, вероятностная модель шифра представляет собой совокупность его алгебраической модели и двух вероятностных распределений на множествах открытых сообщений и ключей:

$$\Sigma_{\text{в}} = \Sigma_{\text{а}} \cup \{P(X), P(K)\} = (X, K, Y, E, D, P(X), P(K)).$$

Распределение на множестве шифрованных сообщений $P(Y)$ индуцируется распределениями $P(X)$ и $P(K)$ согласно формуле полной вероятности:

$$p(y) = \sum_{\substack{(x,k) \in X \times K: \\ E_k(x) = y}} p(x) \cdot p(k).$$

Табличное описание шифров представляется в виде составленной таблицы. Вид и целесообразность табличного описания зависит от сложности и количества отображений, осуществляемых шифром. В таблице 1 представлен простейший вариант соответствия между парами (x_i, k_j) и шифрованными сообщениями, согласно которому соответствующее значение шифрованного сообщения y_{ji} находится в ячейке таблицы на пересечении строки k_j и столбца x_i.

Таблица 1

	x_1	x_2	x_3

k_1	y_{11}	y_{12}	y_{13}
k_2	y_{21}	y_{22}	y_{23}
k_3	y_{31}	y_{32}	y_{33}

На практике встречается большое разнообразие табличного описания шифров.

Графическое описание шифров приводится с целью визуализации и обычно представляется с помощью конечного графа, состоящего из двух колонок точек – *двудольного графа*. Каждой точке левой колонки соответствует открытое сообщение, каждой точке правой колонки – одно из шифрованных сообщений. В двудольном графе точка левой колонки соединяется с точкой правой колонки, если существует ключ, при котором соответствующее открытое сообщение преобразуется в соответствующее шифрованное сообщение (рис. 4).

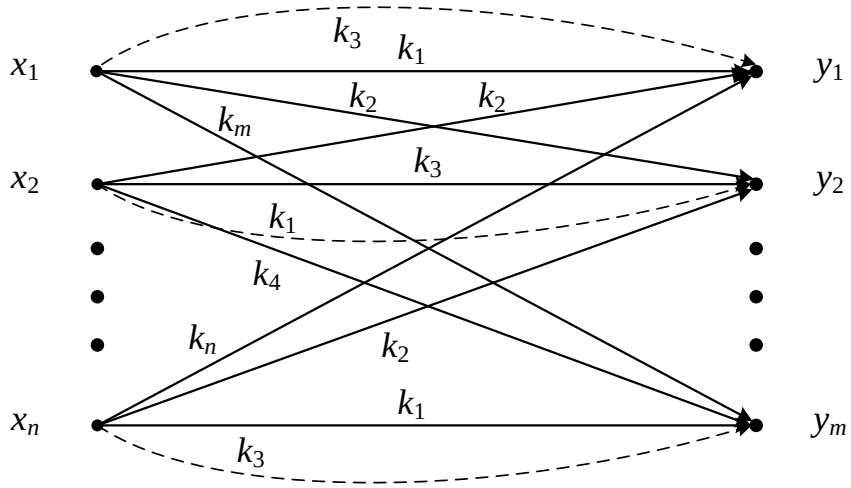


Рис. 4. Пример графического описания шифра

При графическом описании шифра наглядно определяются параллельные ребра, свидетельствующие о возможном существовании эквивалентных ключей, наличие которых снижает стойкость шифра (например, k_1 и k_3 на рис. 4).

Разные ключи $k_i, k_j \in K$ называются *эквивалентными*, если на них одинаково шифруются любые открытые сообщения:

$$E_{k_i}(x) = E_{k_j}(x) \ \forall\, x \in X\ .$$

Следует отметить, что для блочных шифров для отдельных пар (x, y) открытых и соответствующим им шифрованных сообщений вполне допустимо наличие ключей k, k^* таких, что при $k \neq k^*$ $E_k(x) = E_{k^*}(x) = y$.

Выводы по учебному вопросу. Ответы на возникшие вопросы обучающихся.

4. Шифры перестановки и шифры замены.

Шифры перестановки изменяют порядок следования шифрвеличин в тексте, не заменяя их. Преобразование такого вида можно описать следующим образом.

Открытый текст разбивается на n отдельных шифрвеличин, которые нумеруются в естественном порядке: $x_1, x_2, \ldots, x_n$. Конкретное преобразование определяется правилом, изменяющим порядок следования шифрвеличин и указывающим на их новые местоположения. Сформированная таким образом новая последовательность шифрвеличин является шифрованным текстом.

В общем случае ключом преобразования являются перестановки из первых n членов натурального ряда чисел, каждая из которых рассматривается как элемент множества объемом $n!$

При расшифровании производится обратное преобразование шифртекста, заключающееся в расстановке шифрвеличин на первоначальные места для получения исходного сообщения.

Например, если для открытого сообщения «криптография», шифрвеличинами которого являются буквы, принять закон преобразования в виде перестановки (9, 3, 7, 6, 10, 11, 1, 12, 2, 4, 5, 8), означающей, что первая буква исходного текста переместится на девятое место в шифрованном сообщеним, вторая – на третье и т. д., то в итоге получится шифрованное сообщение «гарфипияктор».

Если в шифрах перестановки изменение исходной информации (перестановка символов) производится в пределах некоторого блока данных (всего сообщения, таблицы с текстом), то такие шифры перестановки являются блочными шифрами.

Классическими примерами шифров перестановки являются сцитала (скитала), шифрующие таблицы, решетка Кардано и др.

В V в. до н. э. правители греческого государства Спарты имели хорошо отработанную систему секретной военной связи и шифровали свои послания с помощью сцитала – первого простейшего криптографического устройства, реализующего перестановку шифрвеличин. На стержень в форме цилиндра, который и назывался сцитала, спиралью (виток к витку) наматывали полоску кожи и писали на ней вдоль стержня несколько строк текста сообщения (рис. 5).

Рис. 5. Принцип использования шифра «сцитала»

Снятая со стержня полоска кожи, буквы на которой оказывались расположенными вразнобой, обычно использовалось как пояс.

Для получения исходного сообщения адресату необходимо намотать данную полоску кожи вокруг сциталы того же диаметра. Ключом этого шифра является диаметр стержня.

Шифр «сцитала» многократно совершенствовался в последующие времена. Считается, что автором способа взлома этого шифра является Аристотель, который предложил наматывать перехваченную полоску кожи на

изготовленный длинный конусообразный стержень, начиная с основания, до тех пор, пока не начнут просматриваться читаемые куски сообщения.

Одним из самых примитивных табличных шифров перестановки является перестановка шифрвеличин, для которой ключом служит размер таблицы. Этот шифр в простейшем варианте сходен с шифром «сцитала», когда текст сообщения записывается в таблицу определенного размера в столбик, а считывается по строкам.

Например, если записать сообщение «криптография» в таблицу размером 3×4 по столбцам, а выписать текст из таблицы построчно, то получим зашифрованное сообщение «кпгфртриioая» (табл. 2).

Таблица 2

к	п	г	ф
р	т	р	и
и	о	а	я

Отправитель и получатель сообщения должны заранее договориться об общем ключе в виде размера таблицы. При расшифровании действия выполняют в обратном порядке (построчная запись, чтение по столбцам).

Табличный шифр перестановки может быть усложнен. Например, столбцы могут быть переставлены в некоторой последовательности, определяемой ключом. Также возможна двойная перестановка столбцов и строк.

Решетка Кардано – прямоугольная или квадратная карточка с четным числом строк и столбцов $2l \times 2m$, в которой проделаны отверстия таким образом, что при последовательном отражении или поворачивании и заполнении открытых клеток карточки постепенно будут заполнены все клетки листа.

Карточку сначала зеркально отражают относительно вертикальной оси симметрии, затем – относительно горизонтальной оси, и снова – относительно вертикальной (рис. 6).

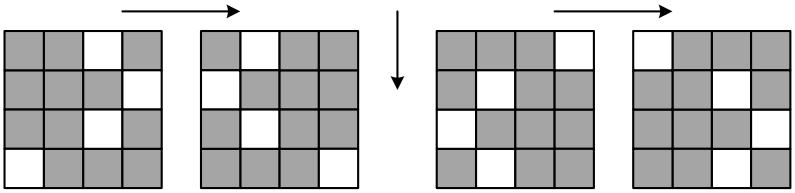


Рис. 6. Пример использования решетки Кардано

Если решетка Кардано квадратная, то возможен и другой вариант ее преобразований – поворот на 90° (рис. 7).

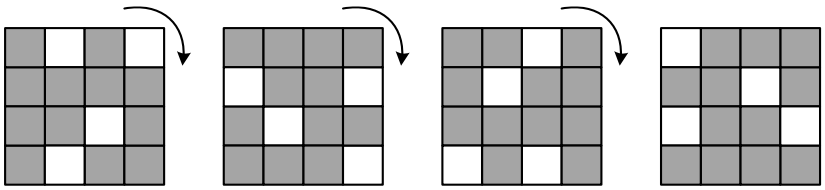


Рис. 7. Пример поворотной решетки Кардано

При записи в свободные клетки поворотной решетки Кардано слева направо и сверху вниз словосочетания «шифрование текста» без пробелов, изображенной на рисунке 7, получим текст в виде таблицы (рис. 8) или в виде одной строки «кшииоесвтафатрен».

к	ш	и	и
о	е	с	в
т	а	ф	а
т	р	е	н

Рис. 8. Пример шифрования с помощью поворотной решетки Кардано

Для расшифрования сообщения получатель должен знать трафарет и наложить его в той же последовательности, что и отправитель при зашифровании. Ключом является выбранный тип перемещения решетки (отражение или поворот) и расположение отверстий.

В шифрах замены каждая очередная шифрвеличина при преобразовании заменяется шифробозначением. При этом существенной характеристикой преобразования является вид отображения множества шифрвеличин на множество шифробозначений.

Шифры замены по виду отображений разделяются на шифры однозначной и многозначной замены (рис. 9).

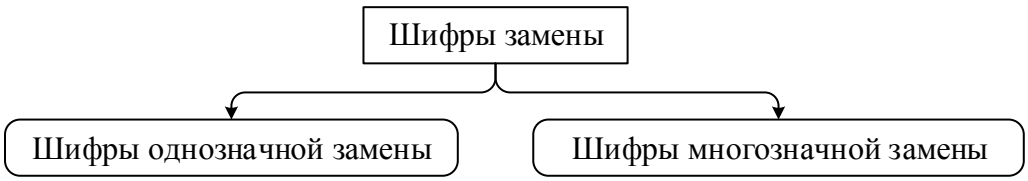


Рис. 9. Классификация шифров замены по виду отображений

В шифрах однозначной замены каждому символу открытого текста (шифрвеличине) ставится в соответствие одно шифробозначение и каждому шифробозначению соответствует только одна шифрвеличина. В шифрах многозначной замены каждая шифрвеличина заменяется различными шифробозначениями.

В зависимости от признака соответствия между алфавитами шифрвеличин и шифробозначений шифры замены разделяются на одноалфавитные и многоалфавитные (рис. 10).

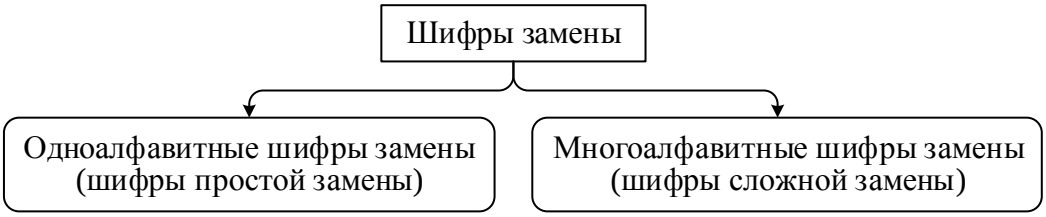


Рис. 10. Классификация шифров замены по признаку соответствия алфавитов шифрвеличин и шифробозначений

В одноалфавитных шифрах замены заданное ключом соответствие между алфавитом шифрвеличин и алфавитом шифробозначений не меняется на всем протяжении шифрования сообщения. В многоалфавитных шифрах замены буква открытого текста может быть представлена различными символами. Кроме того, один и тот же символ шифртекста может обозначать разные буквы.

Шифр простой замены – один из древнейших шифров. Для его реализации выбирается набор символов, которые будут использоваться для составления сообщений (например, русский алфавит). Затем выбирается алфавит шифробозначений, который может состоять из произвольных символов (цифр, букв, графических знаков), в том числе и из букв алфавита шифрвеличин. Между алфавитами шифрвеличин и шифробозначений устанавливается взаимно-однозначное соответствие, определяемое секретным ключом. Шифрование заключается в замене шифрвеличин на соответствующие шифробозначения (рис. 11).

Алфавит шифрвеличин	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
Алфавит шифробозначений	ф	к	с	э	и	у	д	ъ	ч	о	б	ь	р	а	щ	з	г	е	л	ж	в	ю	ё	м	я	т	ы	х	ц	н	й	п	ш

Исходное сообщение: к р и п т о г р а ф и я

Криптограмма: ь е о г ж з э е ф ю о ш

Рис. 11. Пример шифра простой замены

Шифры простой замены, имеющие табличное описание, иногда называют шифрами табличной замены.

Для шифра табличной замены, алфавит шифробозначений которого представляет собой любую возможную перестановку алфавита исходного текста (рис. 11), количество ключей определяется длинной алфавита и, например, для латинского алфавита составляет $26! \approx 4 \cdot 10^{26}$, для русского – $33! \approx 8{,}68 \cdot 10^{36}$. Поэтому определение ключа такого шифра простым перебором на практике является труднореализуемой задачей.

Историческими примерами шифров простой замены являются шифр индийских женщин, квадрат Полибия, шифр Цезаря и др.

Одно из первых описаний шифров простой замены дано в трактате «Камасутра», базирующемуся на манускриптах IV в. до н. э., согласно которым женщина должна овладеть 64 искусствами, в том числе искусством тайнописи для скрытия подробностей своих любовных связей. Один из рекомендуемых способов

реализации такого шифра заключается в случайном расположении попарно букв алфавита и последующей замене букв исходного текста соответствующими шифробозначениями. Пример одной из возможных таблиц подстановок для русского алфавита, описывающей этот шифр, приведен на рис. 12.

а	д	х	и	к	м	о	р	с	ю	у	й	з	ы	ч	ъ
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
в	э	б	г	ж	ц	щ	л	н	е	ф	п	т	ш	ь	я

Исходное сообщение: к р и п т о г р а ф и я

Криптограмма: ж л г й з щ и л в у г ъ

Рис. 12. Пример шифра индийских женщин

Квадрат Полибия изобретен как простая система кодирования в III в. до н. э., изначально предназначенная для греческого алфавита, но затем была распространена на другие языки.

Известно, что греки и римляне использовали для связи друг с другом факелы в качестве семафорной системы, сообщения в которой кодировались по таблице Полибия, заполненной буквами по алфавиту. При этом кодируемые символы заменялись соответствующими номерами строки и столбца.

В исходном виде шифрование с помощью квадрата Полибия является нестойким. Однако если буквы алфавита заносить в таблицу $m \times n$ в произвольном порядке, то может быть получено $(m \times n)!$ вариантов расположения букв, что практически исключает возможность подбора ключа вручную (рис. 13).

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

а

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

б

Рис. 13. Варианты таблиц шифра «Квадрат Полибия» для английского (*а*) и русского (*б*) языков

Например, слово «криптография», зашифрованное вариантом шифра «Квадрат Полибия», представленном на рисунке 13, *б*, примет вид 364326333523514321552615.

Высокая стойкость шифра «квадрат Полибия» при произвольном расположении букв в таблице способствовала его использованию достаточно долгое время.

Первое документально подтвержденное использование шифра простой замены в военных целях появилось в «Галльских войнах» римского императора Юлия Цезаря, который использовал данный шифр при переписке с Цицероном в I в. н. э.

Шифр Цезаря использует правило, согласно которому каждая буква открытого текста заменяется буквой, смещенной от нее в естественно алфавите на k позиций. При достижении конца алфавита выполнялся циклический переход к его началу. Т. е. алфавит шифробозначений циклически сдвинут влево на k позиций относительно алфавита шифрвеличин.

Цезарь использовал шифр простой замены при смещении $k = 3$. Такой шифр можно задать подстановкой, содержащей соответствующие пары букв открытого текста и шифртекста (рис. 14). При использовании шифра Цезаря для русского алфавита смещение k, являющееся ключом шифра, может принимать всего 32 различных значения (значения сдвига 0 или 33 не изменяют исходный алфавит).

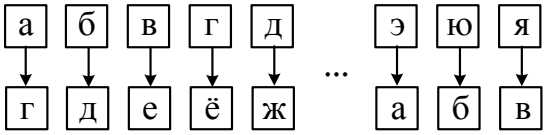


Рис. 14. Шифр Цезаря

Шифры простой замены не нарушают статистических характеристик языка исходного текста, т. е. частоты появления символов, а также различных буквенных сочетаний (n-грамм) сохраняются. Поэтому криптоанализ шифра простой замены основывается на использовании статистических закономерностей естественного языка.

Шифры простой замены легко вскрываются с помощью метода, основанного на анализе частот появления различных букв (чисел, символов) в шифрованном тексте. При этом наиболее часто встречающиеся буквы шифртекста заменяются наиболее вероятными символами алфавита шифрвеличин. Исторически сложившаяся статистическая структура естественных языков определяет существование наиболее часто встречающиеся определенных символов или их комбинаций (например, в русском языке чаще всего встречаются буквы «о», «а», «е», «и», в английском – «*e*», «*t*», «*a*»). Кроме того, для естественных языков характерно наличие вероятных слов, появление которых можно ожидать в перехваченном сообщении (например, для русского текста – «что», «как», «его», «все», «это» и др., для английского – «*the*», «*and*», «*are*» и др.).

Неравновероятность n-грамм тесно связана с избыточностью текста естественного языка, т. е. наличием в нем большого количества повторений отдельных фрагментов текста (корней, окончаний, суффиксов, слов и фраз), поэтому стойкость шифров простой замены пропорционально зависит от статистических характеристик открытого текста.

Шифр сложной замены представляет собой то совокупность шифров простой замены, которые используются для шифрования очередного символа открытого текста согласно некоторому правилу.

Сложную замену также называют многоалфавитной, так как для шифрования определенного количества символов исходного сообщения циклически применяются несколько моноалфавитных шифров.

Примерами шифров сложной замены являются шифр Альберти, шифр Тритемия, шифр Виженера и др.

Шифр Альберти, основанный на использовании шифровального диска, – одна из первых реализаций многоалфавитных шифров, предложенная в 1466 г. Диск Альберти состоял из пары соосных дисков разного диаметра. На большем из них (неподвижном) были записаны 20 букв латинского алфавита и 4 цифры. На меньшем (подвижном) были записаны все 24 буквы алфавита. При шифровании сообщения отправитель ставил индексную букву подвижного диска против любой буквы большого диска, которая являлась первой буквой шифртекста. Очередная буква открытого текста отыскивалась на неподвижном диске и стоящая против нее буква меньшего диска являлась результатом ее зашифрования. Через некоторое время поворотом диска положение индексной буквы менялось (Альберти менял алфавиты после трех–четырех слов). Кроме того, наличие цифр на внешнем диске позволяло осуществлять кодирование с перешифрованием. Для этого был составлен код из кодовых групп, каждой из которых соответствовала некоторая законченная фраза. Фразы заменялись кодовыми группами, а цифры с помощью диска зашифровывались как обычные знаки текста и преобразовывались в буквы.

Шифр Тритемия, описанный в его первой печатной книге о тайнописи в 1518 г., предполагал использование квадратной алфавитной таблицы самым простым способом, согласно которому первая буква текста шифруется первым алфавитом, вторая буква – вторым и т. д. Причем в таблице не было отдельного алфавита открытого текста, а каждый очередной алфавит в строке выглядел как сдвиг на одну позицию влево по сравнению с предыдущим алфавитом.

Шифр Виженера – многоалфавитный шифр замены, основанный на использовании таблицы Виженера, содержащей алфавит открытого текста с последующими алфавитами, каждый из которых циклически сдвинут влево на одну позицию относительно предыдущего. Фактически, каждый ряд таблицы Виженера является шифром Цезаря с возрастающим значением сдвига *k*, указанным в первом столбце таблицы.

Для зашифрования открытого сообщения при замене каждой буквы открытого текста используются различные алфавиты, выбираемые в зависимости от символа ключевого слова. Для расшифрования сообщения необходимо знать, какая строка была использована для шифрования каждой из букв открытого текста, что обеспечивается с помощью ключевого слова.

Например, для зашифрования сообщения «*cryptography*» выберем ключевое слово «*cipher*» и запишем его буквы над буквами шифруемого текста. Если ключевое слово короче открытого текста, его циклически повторяют до достижения конца сообщения. Открытому тексту соответствует первая буквенная строка таблицы Виженера. Каждой букве ключа соответствует та строка таблицы, которая начинается с этой буквы. Буква шифртекста лежит на пересечении столбца, определяемого буквой открытого текста, и строки, определяемой буквой ключа.

Ключ	*c*	*i*	*p*	*h*	*e*	*r*	*c*	*i*	*p*	*h*	*e*	*r*
Сообщение	*c*	*r*	*y*	*p*	*t*	*o*	*g*	*r*	*a*	*p*	*h*	*y*
Криптограмма	*e*	*z*	*n*	*w*	*x*	*f*	*i*	*z*	*p*	*w*	*l*	*p*

Рис. 15. Пример шифрования с помощью таблицы Виженера

Шифр Виженера долгое время считался невзламываемым, однако при ключах, длина которых меньше длины сообщения, он поддается частотному криптоанализу.

5. Шифры гаммирования и их свойства.

Шифры гаммирования относятся к шифрам однозначной замены, но выделяются в собственный класс в связи со своими характерными свойствами и особенностями.

Гаммирование – метод симметричного шифрования, заключающийся в наложении по определенному закону гаммы шифра на открытые или шифрованные данные для их зашифрования или расшифрования соответственно.

Гамма шифра – ключевая последовательность, вырабатываемая по заданному алгоритму, для зашифрования открытых и расшифрования зашифрованных данных.

Шифры гаммирования могут быть описаны с помощью таблицы (шифры табличного гаммирования) или математически (шифры модульного гаммирования).

Пусть $\{x_n\}$ – последовательность символов открытого текста в числовой кодировке ($1 \le x_i \le N$, $i = 1, 2, \ldots, n$), $\{y_n\}$ – последовательность символов шифртекста в числовой кодировке ($1 \le y_i \le N$, $i = 1, 2, \ldots, n$), $\{\Gamma_n\}$ – ключевая числовая последовательность (гамма шифра) ($1 \le \Gamma_i \le N$, $i = 1, 2, \ldots, n$), N – мощность алфавита открытого текста (количество символов в алфавите), n – длина открытого текста.

Тогда для шифров гаммирования зашифрование и расшифрование описываются следующими соответствующими выражениями:

$$y_i = x_i + \Gamma_i \pmod N;$$

$$x_i = y_i - \Gamma_i \pmod N.$$

Результат вычисления по модулю N находится как остаток от деления на целое число N.

Так как в алфавите любого естественного языка буквы следуют друг за другом в определенном порядке, то это дает возможность присвоить каждой букве алфавита порядковый номер. Например, в русском алфавите букве «А» присваивается порядковый номер 1, букве «Б» – порядковый номер 2 и т. д. до буквы «Я», которой присваивается порядковый номер 33. В открытом сообщении каждая буква заменятся ее порядковым номером в рассматриваемом алфавите и зашифровывается выражением (3.1) при заданной гамме.

Предположим, что передается сообщение «атака». Преобразуя буквы сообщения в цифры в соответствии с алфавитом, получим реализацию процесса зашифрования, представленную в таблице 3.

Таблица 3

x_i	1	20	1	12	1
Γ_i	13	25	29	7	14
y_i	14	12	30	19	15

Одним из частных примеров шифров гаммирования является шифр Виженера.

Другим примером шифров гаммирования является шифр, предложенный американским инженером по телекоммуникациям Гильбертом Сэндфордом Вернамом в 1917 г.

В системах шифрования на основе шифра Вернама сообщения и гамма представляются векторами в двоичном алфавите, а шифрование производится сложением по модулю 2 текста с ключом.

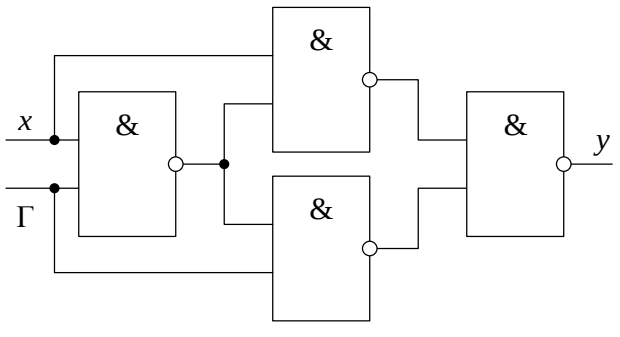
Поскольку результаты сложения и вычитания по модулю 2 двоичных последовательностей совпадают, то выражения (3.1) и (3.2) для шифра Вернама преобразуются к следующему виду:

$$y_i = x_i + \Gamma_i \ (\mathrm{mod}\, 2) = x_i \oplus \Gamma_i;$$

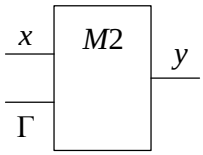
$$x_i = y_i + \Gamma_i \ (\mathrm{mod}\, 2) = y_i \oplus \Gamma_i,$$

где $\oplus$ – знак суммирования по модулю 2, соответствующего булевой функции «Исключающее ИЛИ» (битовая операция *XOR*).

При реализации шифра Вернама для зашифрования и расшифрования сообщений требуется один и тот же узел наложения, в качестве которого используется схема сложения по модулю 2 (рис. 16).



а



б

x	Г	*y*
0	0	0
0	1	1
1	0	1
1	1	0

в

Рис. 16. Логическая структура (*а*), графическое обозначение (*б*), таблица истинности (*в*) сумматора по модулю 2

Ключ в шифре Вернама используется однократно, т. е. каждый бит сообщения шифруется своим битом ключа, что позволяет на основе данного шифра реализовывать безусловно стойкие криптографические системы.

Свойства шифров гаммирования

Основными критериями всех шифров, в значительной мере определяющими их качество, являются криптостойкость, имитостойкость, помехоустойчивость, сложность операций шифрования.

В отличие от имитостойкости шифра, характеризующей его способность противостоять целенаправленным действиям противника и/или нарушителя, *помехоустойчивость шифра* – способность шифра противостоять действию случайных помех, возникающих при передаче шифрованного сообщения по каналу связи.

В соответствии с данными параметрами выделим следующие свойства шифров гаммирования.

1. *Если все элементы гаммы шифра равновероятны и взаимонезависимы, то шифр гаммирования является безусловно стойким.*

Для доказательства данного свойства проверяется выполнение необходимого и достаточного условий существования совершенного шифра, которые представлены в следующем подразделе.

Верно и обратное утверждение, т. е. если шифр гаммирования не является безусловно стойким, то гамма шифра не будет равновероятной (случайной).

2. *Использование одной и той же гаммы для зашифрования различных сообщений, называемое перекрытием шифра, приводит к возможности простого дешифрования данных сообщений.*

Если криптоаналитику известны два шифрованных сообщения, полученные наложением одной и той же гаммы на два разных открытых сообщения:

$$y_1 = x_1 + \Gamma \pmod N;$$

$$y_2 = x_2 + \Gamma \pmod N,$$

то он может найти позначную разность

$$y' = y_1 - y_2 = x_1 - x_2 \pmod N.$$

Т. е. ему необходимо подобрать пару открытых сообщений (x_1, x_2), разность которых совпадает с полученной разностью y'. Для сообщений на естественных языках такое разложение, как правило, является единственным.

Например, для шифра Вернама достаточно поэлементно сложить по модулю 2 шифрованные сообщения y_1 и y_2, полученные с помощью одной и той же гаммы Г:

$$y_1 \oplus y_2 = x_1 \oplus \Gamma \oplus x_2 \oplus \Gamma = x_1 \oplus x_2.$$

Из данного выражения видно, что в результате сложения по модулю 2 гамма исключается, а сам результат сложения представляет собой одно сообщение, зашифрованное по методу гаммирования другим открытым сообщением. Такой способ шифрования носит название шифра с бегущим ключом и легко поддается криптоанализу, основанному на известной статистике естественного языка.

Таким образом, избыточность текста естественного языка при перекрытии шифра всегда приводит к однозначному дешифрованию, поэтому для естественного языка данное явление должно быть категорически исключено.

Частным случаем перекрытия шифра является несовпадение по фазе поступающих при зашифровании символов открытого сообщения x_i и гаммы Γ_i, обусловленное ошибками физической реализации шифра гаммирования. В результате такого наложения шифра каждый символ гаммы Γ_i может участвовать в зашифровании двух соседних символов открытого сообщения, поэтому процесс дешифрования шифрованного сообщения значительно облегчается.

Следует иметь в виду, что анализ линейных сигналов в случае неидеальности схем сложения по модулю 2 также позволяет осуществить дешифрование без знания ключа. Например, для x_i = 0110, Γ_i = 1001 и идеального сумматора по модулю 2 $0 \oplus 1 = 1 \oplus 0 = 1$. Однако из-за неидеальности схемы сложения возможна такая ситуация, что $0 \oplus 1 \neq 1 \oplus 0$. Используя такое различие сумм, противник сможет определить x_i и Γ_i.

3. *При шифровании методом гаммирования не происходит размножения ошибок, возникающих в канале связи из-за помех, если гаммы на передаче и приеме совпадают и правильно синхронизированы.*

На рисунке 17 показан канал связи с помехами, на входе и выходе которого включены узлы наложения и снятия гаммы шифра.

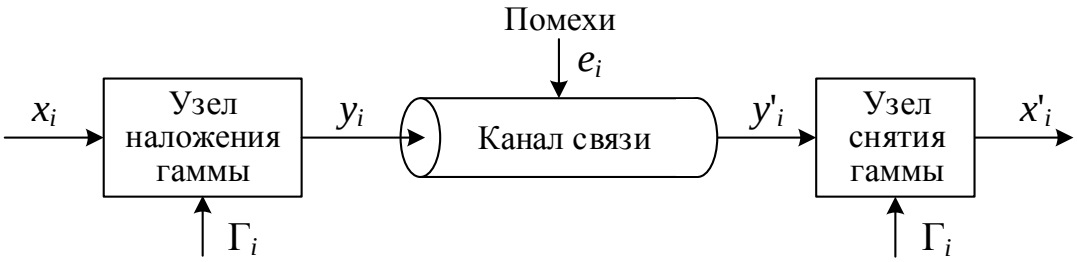


Рис. 17. Модель применения шифра гаммирования в канале с помехами

На узел наложения гаммы подается сообщение x_i и гамма Γ_i. На узел снятия гаммы поступают шифрованное сообщение y'_i, искаженное под действием помех e_i в канале связи, и гамма Γ_i, синхронная с гаммой на передаче, а на выходе формируется сообщение x'_i.

Доказательство третьего свойства вытекает из равенств:

$$x'_i = y'_i - \Gamma_i \pmod N = y_i + e_i - \Gamma_i \pmod N = x_i + \Gamma_i + e_i - \Gamma_i \pmod N = x_i + e_i \pmod N.$$

Таким образом, если пока не рассматривать синхронизацию гамм, то применение шифров гаммирования не предъявляет повышенных требований по помехозащищенности канала связи.

4. *Для шифров гаммирования операции зашифрования и расшифрования просты в реализации.*

Шифры гаммирования использовались немцами в своих дипломатических представительствах в начале 20-х гг. прошлого века, англичанами и американцами – во время Второй мировой войны. Шифр Вернама применялся на правительственной «горячей линии» между Вашингтоном и Москвой, где ключевые материалы представляли собой перфорированные бумажные ленты, производившиеся в двух экземплярах.

Кроме того, отсутствие переноса разрядов в арифметических операциях сложения/умножения при шифровании позволяет снизить потребление энергии узлами наложения и снятии гаммы, а также повысить скорость вычислений путем их распараллеливания.

Таким образом, основными достоинствами шифров гаммирования являются возможность реализации безусловно стойких криптосистем, отсутствие размножения ошибок, а также простота реализации операций шифрования. Однако при шифровании открытых текстов естественного языка может возникнуть существенный недостаток – перекрытия шифра.

Заключительная часть

– напомнить изученные вопросы и цели занятия;

– подвести итоги занятия, определить полноту достижения целей занятия.

Рекомендуемая литература:

– Алферов, А. П. Основы криптографии : учебное пособие / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – Москва : Гелиос АРВ, 2002. – 480 с.

– Васильева, И. Н. Криптографические методы защиты информации. Учебник и практикум для академического бакалавриата / И. Н. Васильева. – Москва : Юрайт, 2016. – 349 с.

– Лось, А. Б. Криптографические методы защиты информации : учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. – Москва : Юрайт, 2016. – 473 с.

Вопросы для контроля:

1. Классификация шифров по различным признакам.
2. Примеры шифров перестановок.
3. Примеры шифров замены.
4. Примеры шифров гаммирования.
5. Свойства шифров гаммирования.