ЛЕКЦИЯ

«ПРИНЦИПЫ ШИФРОВАНИЯ И ТРЕБОВАНИЯ К КРИПТОГРАФИЧЕСКИМ СИСТЕМАМ»

ВОПРОСЫ ЛЕКЦИИ

1. Что такое шифрование?
2. Методы шифрования.
3. Криптография и некоторые известные шифры.
4. Требования к криптографическим системам.

ЛИТЕРАТУРА:

1. Адаменко, М.В. Основы классической криптологии: секреты шифров и кодов / М.В. Адаменко. - 2-е изд., испр. и доп. - Москва : ДМК Пресс, 2016. - 296 с.

2. Криптографическая защита информации : учеб. пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.]; под ред. проф. С.О. Крамарова. — Москва : РИОР : ИНФРА-М, 2019. — 321 с.

3. Жданов, О. Н. Методика выбора ключевой информации для алгоритма блочного шифрования: Монография / Жданов О.Н. - Москва :НИЦ ИНФРА-М, 2016. - 88 с.

1. Что такое шифрование?

Шифрование – обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, доступа к ней авторизованным пользователям. Шифрование — это средство обеспечения конфиденциальности данных, хранящихся в памяти компьютера или передаваемых по проводной или беспроводной сети.

Главным образом, шифрование служит задаче соблюдения конфиденциальности передаваемой информации. Важной особенностью

любого алгоритма шифрования является использование ключа, который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма.

Пользователи являются авторизованными, если они обладают определённым аутентичным ключом. Вся сложность и, собственно, задача шифрования состоит в том, как именно реализован этот процесс.

В целом, шифрование состоит из двух составляющих – зашифровывание и расшифровывание. Пара процедур — шифрование и дешифрирование — называется криптосистемой.

В криптографии принято руководствоваться принципом нидерландского ученого Огюста Керкгоффса (1835-1903гг.), не путать с известными правилами Густава Роберта Киргофа (Кирхгофа) (1824-1887гг.), заключающееся в том, что в засекреченном виде держится только определённый набор параметров алгоритма, называемый ключом, а сам алгоритм шифрования должен быть открытым. Правила же Киргофа - соотношения, которые выполняются между токами и напряжениями на участках любой электрической цепи.

С помощью шифрования обеспечиваются три состояния безопасности информации:

- Конфиденциальность.

Шифрование используется для скрытия информации от неавторизованных пользователей при передаче или при хранении.

- Целостность.

Шифрование используется для предотвращения изменения информации при передаче или хранении.

- Идентифицируемость.

Шифрование используется для аутентификации источника информации и предотвращения отказа отправителя информации от того факта, что данные были отправлены именно им.

Шифрование изначально использовалось только для передачи конфиденциальной информации. Однако впоследствии шифровать информацию начали с целью её хранения в ненадёжных источниках. Шифрование информации с целью её хранения применяется и сейчас, это позволяет избежать необходимости в физически защищённом хранилище.

Шифром называется пара алгоритмов, реализующих каждое из указанных преобразований. Эти алгоритмы применяются к данным с использованием ключа. Ключи для шифрования и для расшифровывания могут различаться, а могут быть одинаковыми. Секретность второго из них (расшифровывающего) делает данные недоступными для несанкционированного ознакомления, а секретность первого (шифрующего) делает невозможным внесение ложных данных.

Сохранение ключей в секретности и правильное их разделение между адресатами является очень важной задачей с точки зрения сохранения конфиденциальности передаваемой информации. Эта задача исследуется в теории управления ключами (в некоторых источниках она упоминается как разделение секрета).

В настоящий момент существует огромное количество методов шифрования. Главным образом эти методы делятся, в зависимости от структуры используемых ключей, на симметричные методы и асимметричные методы. Кроме того, методы шифрования могут обладать различной криптостойкостью и по разному обрабатывать входные данные – блочные шифры и поточные шифры. Всеми этими методами, их созданием и анализом занимается наука криптография.

Как было сказано, шифрование состоит из двух взаимно обратных процессов: зашифрование и расшифрование. Оба этих процесса на абстрактном уровне представимы математическими функциями, к которым предъявляются определённые требования. Математически данные, используемые в шифровании, представимы в виде множеств, над которыми построены данные функции. Иными словами, пусть существуют два

множества, представляющие данные: M и C. И каждая из двух функций (шифрующая и расшифровывающая) является отображением одного из этих множеств в другое. Зашифровывающая функция: E: M–>C. Расшифровывающая функция: D: C–>M.

Элементы этих множеств m и c являются аргументами соответствующих функций. Также в эти функции уже включено понятие ключа. То есть, тот необходимый ключ для зашифровывания или расшифровывания является частью функции. Это позволяет рассматривать процессы шифрования абстрактно, вне зависимости от структуры используемых ключей. Хотя, в общем случае, для каждой из этих функций аргументами являются данные и вводимый ключ. E_{K_1}(m)=c. D_{K_2}(c)=m.

Если для зашифровывания и расшифровывания используется один и тот же ключ K=K_1=K_2, то такой алгоритм относят к симметричным. Если же из ключа шифрования алгоритмически сложно получить ключ расшифровывания, то алгоритм относят к асимметричным, то есть к алгоритмам с открытым ключом.

Для применения в целях шифрования эти функции, в первую очередь, должны быть взаимно обратными (D=E^{-1}). $D_{K_2}(E_{K_1}(\text{m}))$=m. $E_{K_1}(D_{K_2}(\text{c}))$=c.

Важной характеристикой шифрующей функции E является её криптостойкость. Косвенной оценкой криптостойкости является оценка взаимной информации между открытым текстом и шифротекстом, которая должна стремиться к нулю.

2. Методы шифрования.

В первых методах шифрования использовались одинаковые ключи, однако чуть позже были открыты алгоритмы с применением разных ключей. Наиболее популярным стандартным симметричным алгоритмом шифрования данных является DES (Data Encryption Standard). Алгоритм разработан фирмой IBM и в 1976 году был рекомендован Национальным бюро

стандартов к использованию в открытых секторах экономики. Немного забегая вперед скажем, что в 2001 году Национальное бюро стандартов США приняло новый стандарт симметричного шифрования, который получил название AES (Advanced Encryption Standard).

Стандарт AES был разработан в результате проведения конкурса на разработку симметричного алгоритма шифрования, обладающего лучшим, чем у DES, сочетанием показателей безопасности и скорости работы. Победителем был признан алгоритм Rijndael, который и был положен в основу AES. В результате AES обеспечивает лучшую защиту, так как использует 128-битные ключи (а также может работать со 192- и 256-битными ключами) и имеет более высокую скорость работы, кодируя за один цикл 128-битный блок в отличие от 64-битного блока DES. В настоящее время AES является наиболее распространенным симметричным алгоритмом шифрования.

В 1978 году трое ученых (Ривест, Шамир и Адлеман) разработали ассиметричную систему шифрования с открытыми ключами RSA (Rivest, Shamir, Adleman), полностью отвечающую всем принципам. Криптографический протокол Диффи—Хеллмана позволяет двум и более сторонам получить общий секретный ключ, используя незащищенный от прослушивания канал связи.

Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений, включая PGP, S/MIME, TLS/SSL, IPSEC/IKE и т.д.

Методы шифрования решают определённые задачи и обладают как достоинствами, так и недостатками. Конкретный выбор применяемого метода зависит от целей, с которыми информация подвергается шифрованию.

Как уже говорилось выше, существуют два базовых метода:

Симметричное шифрование использует один и тот же ключ и для зашифровывания, и для расшифровывания. Отсюда название – симметричные. Алгоритм и ключ выбирается заранее и известен обеим сторонам.

Первыми исследователями, которые изобрели и раскрыли понятие шифрования с открытым кодом, были Уитфилд Диффи и Мартин Хеллман из Стэнфордского университета и Ральф Меркле из Калифорнийского университета в Беркли. В 1976 году их работа «Новые направления в современной криптографии» открыла новую область в криптографии, теперь известную как криптография с открытым ключом.

Асимметричное шифрование использует два разных ключа: один для зашифровывания (который также называется открытым), другой для расшифровывания (называется закрытым).

Сохранение ключа в секретности является важной задачей для установления и поддержки защищённого канала связи. В связи с этим, возникает проблема начальной передачи ключа (синхронизации ключей). Кроме того, существуют методы криптоатак, позволяющие так или иначе дешифровать информацию не имея ключа или же с помощью его перехвата на этапе согласования. В целом эти моменты являются проблемой криптостойкости конкретного алгоритма шифрования и являются аргументом при выборе требуемого алгоритма.

Рисунок 1 – Симметричное шифрование

Симметричные, а конкретнее, алфавитные алгоритмы шифрования были одними из первых алгоритмов. Асимметричное шифрование, в котором ключи у собеседников разные, было изобретено позднее.

Благодаря своей скорости, симметричное шифрование широко используется для защиты информации во многих современных компьютерных системах. Например, Advanced Encryption Standard (AES) используется правительством США для шифрования секретной информации.

Многие способы шифрования представляют собой примеры симметричных криптосистем или криптосистем с секретным ключом. Такую систему можно представить в виде, показанном на рисунке 2.

Важная часть такой системы – защищенный канал, по которому секретный ключ Z, порожденный в источнике ключа, передается предполагаемому получателю. Источник сообщений порождает открытый текст X, шифратор преобразует его в криптограмму $Y = f(X, Z)$.

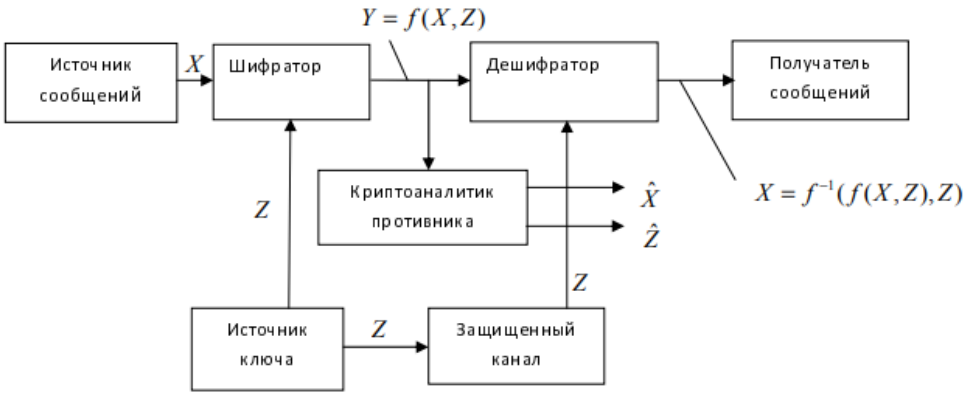

Рисунок 2 – Симметричные криптосистемы

Дешифратор выполняет обратное преобразование $X = f^{-1}(Z, f(X, Z))$. Иногда такие системы называют одноключевыми. Симметричные криптосистемы могут использовать моно- и многоалфавитные подстановки и перестановки, но чаще для повышения криптостойкости используют комбинацию этих методов.

Функциональное различие между симметричным и асимметричным шифрованием связано с длиной ключей, которые измеряются в битах и

напрямую связаны с уровнем безопасности каждого алгоритма. В симметричных системах ключи подбираются случайным образом, а их общепринятая длина варьируется между 128 и 256 бит в зависимости от требуемого уровня безопасности.

В асимметричном шифровании между открытым и приватным ключами должна существовать математическая связь, то есть их связывает определенная математическая формула. По этой причине злоумышленники могут использовать этот шаблон для взлома шифра, в свою очередь асимметричные ключи должны быть намного длиннее, чтобы обеспечить эквивалентный уровень безопасности. Разница в длине ключа настолько существенная, что 128-битный симметричный ключ и 2048-битный асимметричный ключ обеспечивают примерно одинаковый уровень безопасности.

Недостатками симметричного шифрования является проблема передачи ключа собеседнику и невозможность установить подлинность или авторство текста. Поэтому, например, в основе технологии цифровой подписи, чаще всего, лежат асимметричные схемы.

В асимметричном шифровании используются два ключа – открытый и закрытый, связанные, как уже говорилось, определённым математическим образом друг с другом. Открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для шифрования сообщения и для проверки ЭЦП. Для расшифровки сообщения и для генерации ЭЦП используется секретный ключ.

Данный способ решает проблему симметричных схем, связанную с начальной передачей ключа другой стороне. Если в симметричных схемах злоумышленник перехватит ключ, то он сможет как «слушать», так и вносить правки в передаваемую информацию. В асимметричных системах другой стороне передается открытый ключ, который позволяет шифровать, но не расшифровывать информацию. Таким образом, решается проблема симметричных систем, связанная с синхронизацией ключей.

Асимметричное шифрование может применяться к системам, в которых многим пользователям может понадобиться зашифровать и расшифровать сообщения или пакет данных, особенно, когда скорость и вычислительная мощность не является приоритетом. Простым примером такой системы является зашифрованная электронная почта, в которой открытый ключ может использоваться для шифрования сообщений, а приватный ключ для их расшифровки.

Рисунок 3 – Асимметричное шифрование

Во многих приложениях, симметричное и асимметричное шифрование используются вместе. Хорошим примером таких гибридных систем являются криптографические протоколы Security Sockets Layer (SSL) и Transport Layer Security (TLS), которые были разработаны для обеспечения безопасной связи в интернете. Протоколы SSL на данный момент считаются небезопасными и ими не рекомендуют пользоваться. В свою очередь, протоколы TLS считаются безопасными и широко используются всеми современными веб-браузерами.

Методы шифрования используются многими крипто-кошельками в качестве способа обеспечения повышенного уровня безопасности конечных пользователей. Алгоритмы шифрования применяются, когда пользователь устанавливает пароль для файла своего кошелька, который используется для доступа к программному обеспечению.

Однако из-за того, что Биткойн и другие криптовалюты используют пару из открытого и приватного ключа, присутствует распространенное заблуждение, что блокчейн системы используют алгоритмы асимметричного шифрования. Однако, как отмечалось ранее, асимметричное шифрование и цифровые подписи являются двумя основными вариантами использования асимметричной криптографии (криптография с открытым ключом).

Следовательно, не все системы с цифровой подписью используют шифрование, даже если они предоставляют публичный и приватный ключи. Фактически, сообщение может быть подписано цифровой подписью без использования шифра. RSA является одним из примеров алгоритма, который можно использовать для подписи зашифрованных сообщений, но у алгоритма цифровой подписи, который используется в Биткойн (называемый ECDSA) шифрование отсутствует.

Современные симметричные криптосистемы можно разделить на два больших класса. Первый класс – это блочные шифры. Представляют собой семейство обратимых преобразований блоков исходного текста. Второй класс – это поточные. Гаммирование представляет собой преобразование исходного текста, при котором символы исходного текста складываются по модулю мощности алфавита с символами псевдослучайной последовательности, вырабатываемой по некоторому правилу.

Поточные шифры оперируют с битами (реже с байтами), стараясь обеспечить шифрование в режиме реального времени или близком к нему. Высокая скорость работы поточных шифров определяет область их использования - закрытие данных, требующих оперативной доставки потребителю. Например, когда вы разговариваете по закрытому каналу связи, то весь поток аудиоинформации переводится в цифровой вид, зашифровывается и передается по каналу связи в зашифрованном виде. На приемной стороне поток расшифровывается и восстанавливается.

По принципу работы поточные шифры делят на комбинированные, синхронные и самосинхронизирующиеся. Комбинированные методы

шифрования (а точнее, поточные режимы использования блочных шифров) используют принцип формирования потока ключей (гаммы шифра) с помощью генераторов псевдослучайных последовательностей, в качестве функции обратной связи или функции выхода которых используется функция зашифрования блочного шифра. Как правило, для комбинированных методов шифрования используются блочные шифры, являющиеся государственными стандартами шифрования данных: ГОСТ 28147-89 (российский стандарт) и AES (стандарт США).

Потоковые шифры представляют собой разновидность гаммирования и преобразуют открытый текст в шифрованный по 1 биту. Генератор ключа выдает последовательность ключевых битов $z_1, z_2, \dots, z_i, \dots$ Эта ключевая последовательность складывается по модулю 2 с последовательностью битов исходного текста $x_1, x_2, \dots, x_i, \dots$для получения шифрованного текста $y_i = x_i \oplus z_i$.

Следующим являются блочные шифры. Общие принципы построения блокового шифра были определены Клодом Элвудом Шенноном (1916-2001гг.). Они состоят в том, что алгоритм блокового шифра должен использовать: подстановки (нелинейные преобразования коротких частей (подблоков шифра); перестановки символов в блоках; итерирование операций, т.е. многократное повторение их с разными ключами.

Подстановки обычно применяются к подблокам, длина которых существенно меньше длины блока. Это связано со сложностью реализации таблиц, типично задающих нелинейные подстановки. Перестановки служат для уменьшения зависимости между символами различных подблоков, которая может присутствовать в сообщении. Одним из наиболее распространенных способов генерации блочных шифров является использование так называемых сетей Фейстеля.

Сетью Фейстеля называется метод обратимых преобразований текста, при котором значение, вычисленное по одной части (половине) текста,

накладывается на другие части (половину). Независимые потоки информации, порожденные из исходного блока, называются ветвями сети. При переходе от одной ячейки к другой меняется ключ, причём выбор ключа зависит от конкретного алгоритма. Операции шифрования и расшифрования на каждом этапе очень просты, и при определённой доработке совпадают, требуя только обратного порядка используемых ключей. Большинство современных блочных шифров используют сеть Фейстеля в качестве основы.

В классической схеме их две. Функция F называется образующей. Действие, состоящее из однократного вычисления образующей функции и последующего наложения ее результата на другую ветвь с обменом их местами, называется циклом или раундом (англ. round) сети Фейстеля. Число раундов зависит от требуемой стойкости шифра. Один раунд сети Фейстеля показан на рисунке 4.

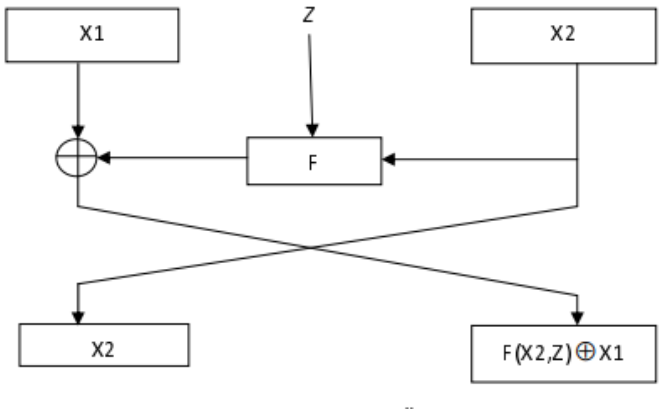

Рисунок 4 – Сеть Фейстела

Функция F практически всегда выбирается нелинейной и необратимой. Несмотря на необратимость функции F, преобразование обратимо. Инверсия последнего обмена ветвей и использование функции XOR , которая обратима со своим повтором, позволяют восстановить исходный текст. В нашем примере из X2 и F(X2,Z)⊕X1 сначала, зная Z и X2, получаем F(X2,Z). Затем F(X2,Z)⊕X1 ⊕ F(X2,Z)=X1. Тем самым получили X1 и X2.

Достоинство: процедуры шифрования и дешифрования совпадают, с тем исключением, что ключевая информация при дешифровании используется в обратном порядке. Обе половины блока постоянно меняются

местами и поэтому они шифруются с одинаковой стойкостью. Недостаток: только половина блока изменяется на каждой итерации.

Следует так же сказать несколько слов о хэшировании, без которого в настоящее время не обходится практически ни одно приложение криптографии. Хэш-функции – это функции, предназначенные для «сжатия» произвольного сообщения или набора данных, записанных, как правило, в двоичном алфавите, в некоторую битовую комбинацию фиксированной длины, называемую сверткой. Хэш-функции имеют разнообразные применения при проведении статистических экспериментов, при тестировании логических устройств, при построении алгоритмов быстрого поиска и проверки целостности записей в базах данных. Основным требованием к хэш-функциям является равномерность распределения их значений при случайном выборе значений аргумента. Криптографической хеш-функцией называется всякая хеш-функция, являющаяся криптостойкой, то есть удовлетворяющая ряду требований специфичных для криптографических приложений. В криптографии хэш-функции применяются для решения следующих задач: построения систем контроля целостности данных при их передаче или хранении, аутентификация источника данных.

Хэш-функцией называется всякая функция $h:X \to Y$, легко вычислимая и такая, что для любого сообщения M значение $h(M) = H$ *(свертка)* имеет фиксированную битовую длину. X — множество всех сообщений, Y — множество двоичных векторов фиксированной длины.

Как правило хэш-функции строят на основе так называемых одношаговых сжимающих функций $y = f(x_1, x_2)$ двух переменных, где x_1, x_2 и y — двоичные векторы длины m, n и n соответственно, причем n — длина свертки, а m — длина блока сообщения. Для получения значения $h(M)$ сообщение сначала разбивается на блоки длины m (при этом, если длина сообщения не кратна m, то последний блок неким специальным образом дополняется до полного), а затем к полученным

блокам M_1, M_2,.., M_N применяют последовательную процедуру вычисления свертки. Выделяют два важных вида криптографических хэш-функций — ключевые и бесключевые. Ключевые хэш-функции называют кодами аутентификации сообщений. Они дают возможность без дополнительных средств гарантировать как правильность источника данных, так и целостность данных в системах с доверяющими друг другу пользователями. Бесключевые хэш-функции называются кодами обнаружения ошибок. Они дают возможность с помощью дополнительных средств (шифрования, например) гарантировать целостность данных. Эти хэш-функции могут применяться в системах как с доверяющими, так и не доверяющими друг другу пользователями.

3. Криптография и некоторые известные шифры

Наукой, изучающей математические методы защиты информации путем ее преобразования, является криптология. Криптология разделяется на два направления – криптографию и криптоанализ.

Криптография изучает методы преобразования информации, обеспечивающие ее конфиденциальность и аутентичность. Под конфиденциальностью понимают невозможность получения информации из преобразованного массива без знания дополнительной информации. Аутентичность информации состоит в подлинности авторства и целостности.

Криптоанализ объединяет математические методы нарушения конфиденциальности и аутентичности информации без знания ключей.

Криптографическая система или шифр представляет собой семейство обратимых преобразований открытого текста в шифрованный. Членам этого семейства можно взаимно однозначно сопоставить число, называемое ключом. Пространство ключей – это набор возможных значений ключа. Следует отличать понятия "ключ" и "пароль". Пароль также является секретной последовательностью букв алфавита, однако используется не для шифрования (как ключ), а для аутентификации субъектов.

Давайте еще раз напомним широко известные алгоритмы шифрования:

IDEA (англ. International Data Encryption Algorithm, международный алгоритм шифрования данных) – симметричный блочный алгоритм шифрования данных, запатентованный швейцарской фирмой Ascom. Используются операции: сложение по модулю, умножение по модулю, побитовое исключающее ИЛИ (XOR).

DES (англ. Data Encryption Standard) – алгоритм для симметричного шифрования, разработанный фирмой IBM и утверждённый правительством США в 1977 году как официальный стандарт (FIPS 46-3).

Triple DES (3DES) – симметричный блочный шифр, созданный Уитфилдом Диффи, Мартином Хеллманом и Уолтом Тачманном в 1978 году на основе алгоритма DES с целью устранения главного недостатка последнего – малой длины ключа (56 бит), который может быть взломан методом полного перебора ключа.

MDC (Modification Detection Code) – код проверки целостности, строящийся на основе блочных шифров.

Blowfish – криптографический алгоритм, реализующий блочное симметричное шифрование с переменной длиной ключа.

CAST-128 (или CAST5) в криптографии – блочный алгоритм симметричного шифрования на основе сети Фейстеля.

Serpent – симметричный блочный алгоритм шифрования, представляющий собой SP-сеть.

Advanced Encryption Standard (AES), также известный как Rijndael – симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США по результатам конкурса AES.

Twofish – симметричный алгоритм блочного шифрования с размером блока 128 бит и длиной ключа до 256 бит.

WAKE – криптоалгоритм, предложенный в 1993 году англичанином Д. Уилером из компьютерной лаборатории Кембриджского университета.

WAKE означает Word Auto Key Encryption или в переводе – шифрование слов саморазвивающимся ключом. Криптоалгоритм формирует псевдослучайную последовательность 32-разрядными словами в режиме обратной связи по шифротексту: предыдущее слово зашифрованного текста используется для порождения следующего слова гаммы. Главное достоинство этого алгоритма – высокое быстродействие, в то же время его криптографическая стойкость не так высока. WAKE реализован в антивирусном пакете программ Dr. Solomons Anti-Virus.

Sapphire II – байт-оринтированный алгоритм, который может использоваться для генерации псевдослучайных чисел. шифрования и хеширования информации. Этот алгоритм использует обратную связь, как по открытому тексту, так и по шифротексту.

ГОСТ 28147-89 (симметричный блочный алгоритм шифрования с 256-битным ключом, оперирует блоками данных по 64 бита).

А теперь приведем несколько примеров простых шифров с которых, по большому счету, все и начиналось. Как правило, в них производится замена каждой буквы сообщения на некоторый определенный символ (обычно также на букву). Например, пусть используется подстановка:

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

Х Е П В К Ю Ы Ж Р Н З Д Э Ф Щ Я Ь Ш О Т А Ц Б Г С Ч М И У Й К

Вместо фразы ОДИН_ПРИМЕР получим ЩКРФ_ЯЬРЭЮЬ.

Расшифровка (криптоанализ) подобных криптограмм не составляет большой проблемы. Все основывается на том, что различные буквы естественного языка – русского, английского или какого-либо другого встречаются в осмысленных текстах неодинаково часто. Следовательно, тоже самое верно и для сопоставляемых им знаков. В еще большей мере это относится к буквосочетаниям из двух или нескольких букв.

Многоалфавитная замена повышает стойкость шифра. В этом случае используются не один, а несколько алфавитов. Смена алфавитов производится последовательно и циклически. Первый символ заменяется на

соответствующий символ из первого алфавита, второй – из второго алфавита и так пока не будут исчерпаны все алфавиты. После чего использование алфавитов повторяется.

В шифре Виженера используется ключ, задаваемый набором из d букв. Над сообщением надписывается повторяющаяся последовательность ключей и две последовательности складываются по модулю числа символов в алфавите N (каждая буква алфавита нумеруется от 0 до N −1). Например, при использовании латинского алфавита ABCDEFGHIJKLMNOPQRSTUVWXYZ Наш новый алфавит будет состоять из цифр от 0 до 25.

Сообщение: THISISATESTMESSAGE

с помощью ключа KEY преобразуется

Исходный текст: THI SIS ATE STM ESS AGE

19,7,8,18,8,18,0,19,4,18,19,12,4,18,18,0,6,4

Ключ: KEYKEYKEYKEYKEYKEY

10,4,24,10,4,24,10,4,24,10,4,24,10,4,24,10,4,24

Зашифрованный текст: 3,11,6,2,12,16,10,23,2,2,23,10,14,22,16,10,10,2

DLG CMQ KXC CXK OWQ KKC

Шифр Виженера с периодом 1 называется шифром Цезаря. Он представляет собой простую подстановку, в которой каждая буква сообщения сдвигается вперед на фиксированное число мест по алфавиту. Это число и является ключом. Например, то же сообщение THISISATESTMESSAGE зашифрованное с помощью шифра Цезаря с ключом 5 имеет вид:

Исходный текст	THI	SIS	ATE	STM	ESS	AGE
	19,7,8	18,8,18	0,19,4	18,19,12	4,18,18	0,6,4
Зашифрованный текст	24,12,13	23,13,23	5,24,9	23,24,17	9,23,23	5,11,9
	YMN	XNX	FYJ	XYR	JXX	FLJ

Повторное применение двух и более шифров Виженера будет называться составным шифром Виженера. Так же существуют перестановочные шифры.

К этому классу относится шифр маршрутная транспозиция и его вариант постолбцовая транспозиция. В каждом из методов сообщение записывается в данный прямоугольник размером n × m, а столбцы нумеруются или обычным порядком следования, или в порядке следования букв ключа (буквенного ключевого слова).

Ниже приведена таблица 1, ниже - таблица 2: в первом случае столбцы занумерованы в порядке следования букв слова «жираф», во втором – просто в порядке следования.

Ж	И	Р	А	Ф
2	3	4	1	5
М	О	Й	Д	Я
Д	Я	С	А	М
Ы	Х	Ч	Е	С
Т	Н	Ы	Х	П
Р	А	В	И	Л
К	О	Г	Д	А
Н	Е	В	Ш	У
Т	К	У	З	А
Н	Е	М	О	Г

Таблица 1 – порядок следования букв слова «жираф»

В первом случае, выписывая буквы из столбцов таблицы (сначала из столбца с номером 1, затем 2 и т.д.), получаем шифрограмму ДАЕХИДШЗОМДЫТРКНТНОЯХНАОЕКЕЙСЧЫВГВУМЯМСПЛАУАГ.

1	2	3	4	5
М	О	Й	Д	Я
Д	Я	С	А	М
Ы	Х	Ч	Е	С
Т	Н	Ы	Х	П
Р	А	В	И	Л
К	О	Г	Д	А
Н	Е	В	Ш	У
Т	К	У	З	А
Н	Е	М	О	Г

Таблица 2 – в порядке следования

Во втором случае считывание текста из таблицы может производиться по столбцам, диагоналям или, в общем случае, некоторому выбранному маршруту обхода таблицы. Ниже приведена шифрограмма, полученная при считывании текста по столбцам

МДЫТРКНТНОЯХНАОЕКЕЙСЧЫВГВУМДАЕХИДШЗОЯМСПЛАУАГ.

Важная особенность перестановочного шифра, с точки зрения возможности расшифрования, состоит в том, что при ограниченном размере ключа и шифровании длинных текстов, ключ используется многократно. Это обстоятельство облегчает взломщику процесс дешифрования.

Наиболее стойким из ручных методов шифрования перестановкой является шифрование с помощью решетки Кардано. Это квадратная таблица размера 2n×2n, в которой n^2 клеток вырезаны как окна. Эти n^2 клеток случайным образом более или менее равномерно распределены по площади квадрата и выбраны так, что при последовательном повороте квадрата на 90, 180, 270 и 360 градусов вырезанные клетки последовательно покрывают все $4n^2$ клеток квадрата. При шифровании решетка Кардано накладывается на чистый лист бумаги и в окошки последовательно по строкам записываются первые n^2 символов открытого текста. Далее решетка поворачивается на 90 градусов и следующие n^2 символов открытого текста вписываются в окна.

Затем те же действия повторяются при повороте на 180 и 270 градусов. Если длина шифруемого текста больше $4n^2$, то решетка Кардано используется для шифрования многократно.

4. Требования к криптографическим системам

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т.д. Программная реализация более практична, допускает известную гибкость в использовании. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования.

1. Знание алгоритма шифрования не должно снижать криптостойкости шифра.
2. Зашифрованное сообщение должно поддаваться чтению только при наличии ключа.
3. Шифр должен быть стойким даже в случае, если нарушителю известно достаточно большое количество исходных данных и соответствующих им зашифрованных данных.
4. Число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей, должно иметь строгую нижнюю оценку и должно либо выходить за пределы возможностей современных компьютеров (с учетом возможности организации сетевых вычислений), либо требовать создания дорогих вычислительных систем.
5. Незначительное изменение ключа или исходного текста должно приводить к существенному изменению вида зашифрованного текста. Этому требованию не соответствуют практически все шифры до научной криптографии.
6. Структурные элементы алгоритма шифрования должны быть неизменными.

7. Длина шифрованного текста должна быть равной длине исходного текста.

8. Дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте.

9. Не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования.

10. Любой ключ из множества возможных должен обеспечивать надежную защиту информации.

Главным действующим лицом в криптоанализе выступает нарушитель – лицо или группа лиц, целью которых является прочтение или подделка защищенных криптографическими методами сообщений.

В отношении нарушителя принимается ряд допущений, которые, как правило, лежат в основе математических или иных моделей.

1. Нарушитель знает алгоритм шифрования (или ЭЦП) и особенности его реализации в конкретном случае, но не знает ключа.

2. Нарушителю доступны все зашифрованные тексты. Нарушитель может иметь доступ к некоторым исходным текстам, для которых известен соответствующий им зашифрованный текст.

3. Нарушитель имеет в своем распоряжении вычислительные, людские, временные и иные ресурсы, объем которых оправдывает потенциальную ценность информации, которая будет добыта в результате криптоанализа.

При анализе криптостойкости шифра необходимо учитывать и человеческий фактор, например, подкуп конкретного человека, в руках которого сосредоточена необходимая информация, может стоить на несколько порядков дешевле, чем создание суперкомпьютера для взлома шифра.

Принято различать несколько уровней криптоатаки в зависимости от объема информации, доступной криптоаналитику. По нарастанию сложности можно выделить три уровня криптоатаки.

1. Атака на шифрованный текст (уровень КА1) – нарушителю доступны все или некоторые зашифрованные сообщения.

2. Атака на пару «исходный текст – шифрованный текст» (уровень КА2) – нарушителю доступны все или некоторые зашифрованные сообщения и соответствующие им исходные сообщения.

3. Атака на выбранную пару «исходный текст – шифрованный текст» (уровень КА3) – нарушитель имеет возможность выбирать исходный текст, получать для него шифрованный текст и на основе анализа зависимостей между ними вычислять ключ.

Предполагается, что нарушителю фактически доступно шифрующее устройство. Он может выбрать исходный текст, получить для него зашифрованный текст и на основании анализа зависимости между ними вычислять ключ.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к расшифрованию без знания ключа. Показатель криптостойкости – главный параметр любой криптосистемы. В качестве показателя криптостойкости можно выбрать:

- количество всех возможных ключей или вероятность подбора ключа за заданное время с заданными ресурсами;
- количество операций или время (с заданными ресурсами), необходимое для взлома шифра с заданной вероятностью;
- стоимость вычисления ключевой информации или исходного текста.

Все эти показатели должны учитывать также уровень возможной криптоатаки. Однако следует понимать, что эффективность защиты информации криптографическими методами зависит не только от криптостойкости шифра, но и от множества других факторов, включая вопросы реализации криптосистем в виде устройств или программ.