Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технический университет
имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления»

КАФЕДРА «Программное обеспечение ЭВМ и информационные технологии»

РАСЧЕТНО-ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

К НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ

НА ТЕМУ:

«Криптографические методы защиты информации»

Студент __ИУ7-55Б__ _____ ____**Е. А. Фролов**____
(Группа) (Подпись, дата) (И.О.Фамилия)

Руководитель _____ ____**И. В. Рудаков**____
(Подпись, дата) (И.О.Фамилия)

Консультант _____ _____
(Подпись, дата) (И.О.Фамилия)

2021 г.

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технический университет имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

УТВЕРЖДАЮ

Заведующий кафедрой ИУ-7
_____ И. В. Рудаков
« _____ » _____ 20 ____ г.

ЗАДАНИЕ
на выполнение научно-исследовательской работы

по теме ____Криптографические методы защиты информации_____

_____

_____

Студент группы _____ИУ7-55Б_____

_____Фролов Евгений Алексеевич_____
(Фамилия, имя, отчество)

Направленность НИР (учебная, исследовательская, практическая, производственная, др.)

_____учебная_____

Источник тематики (кафедра, предприятие, НИР) ___НИР_____

График выполнения НИР: 25% к 4 нед., 50% к 7 нед., 75% к 11 нед., 100% к 14 нед.

Техническое задание *Провести анализ наиболее распространенных методов защиты информации. Определить достоинства и недостатки каждого и их применимость в различных областях*

Оформление научно-исследовательской работы:

Расчетно-пояснительная записка на 15-25 листах формата А4.
Перечень графического (иллюстративного) материала (чертежи, плакаты, слайды и т.п.)
Презентация на 8-10 слайдах.

Дата выдачи задания « ___ » _____ 20__ г.

Руководитель НИР _____ _____
(Подпись, дата) (И.О.Фамилия)

Студент _____ _____
(Подпись, дата) (И.О.Фамилия)

Примечание: Задание оформляется в двух экземплярах: один выдается студенту, второй хранится на кафедре.

Содержание

Введение

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом волновала человеческий ум с давних времен. История криптографии - ровесница истории человеческого языка.

С широким распространением письменности криптография стала формироваться как самостоятельная наука. Первые криптосистемы встречаются уже в начале нашей эры. Так, Цезарь в своей переписке использовал уже более менее систематический шифр, получивший его имя.

Бурное развитие криптографические системы получили в годы первой и второй мировых войн. Начиная с послевоенного времени и по нынешний день появление вычислительных средств ускорило разработку и совершенствование криптографических методов.

Почему проблема использования криптографических методов в ИС стала в настоящий момент особо актуальна?

С одной стороны, расширилось использование компьютерных сетей, в частности глобальной сети Интернет, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера, не допускающего возможность доступа к ней посторонних лиц.

С другой стороны, появление новых мощных компьютеров, технологий сетевых и нейронных вычислений сделало возможным дискредитацию криптографических систем, еще недавно считавшихся практически нераскрываемыми.

Криптографические методы защиты информации в автоматизированных системах могут применяться как для защиты информации, обрабатываемой в ЭВМ или хранящейся в различного типа ЗУ, так и для закрытия информации, передаваемой между различными элементами системы по линиям связи.

1 Анализ предметной области

В настоящее время разработано большое колличество различных методов шифрования, созданы теоретические и практические основы их применения. Подавляющие число этих методов может быть успешно использовано и для закрытия информации.

Проблемой защиты информации путем ее преобразования занимается криптология (kryptos - тайный, logos - наука).

Современная криптография включает в себя четыре крупных раздела.

1. Симметричные криптосистемы.
2. Криптосистемы с открытым ключом.
3. Системы электронной подписи.
4. Управление ключами.

Основные направления использования криптографических методов - передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений ,хранение информации (документов,баз данных) на носителях в зашифрованном виде.

Итак, криптография дает возможность преобразовать информацию таким образом, что ее прочтение (восстановление) возможно только при знании ключа.

В качестве информации, подлежащей шифрованию и дешифрованию, будут рассматриваться тексты, построенные на некотором алфавите.

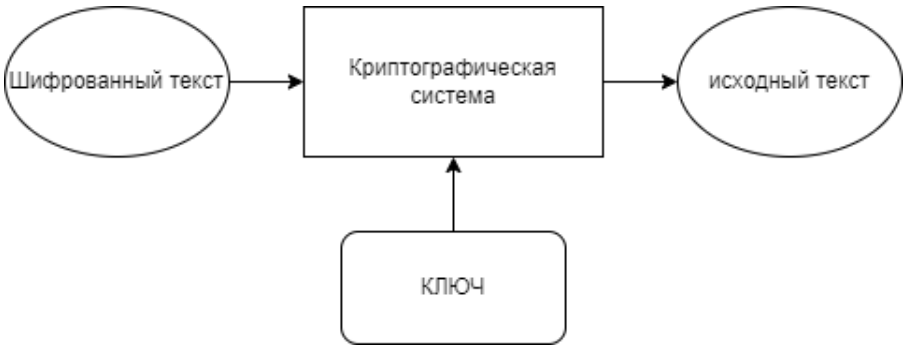

Рисунок 1 – Процедура шифрования файлов.

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.

- Зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
- число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;
- число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей, должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров;
- знание алгоритма шифрования не должно влиять на надежность защиты;

- незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;
- структурные элементы алгоритма шифрования должны быть неизменными;
- дополнительные биты, вводимые в сообщение в процессе шифрования, должен быть полностью и надежно скрыты в шифрованном тексте;
- длина шифрованного текста должна быть равной длине исходного текста;
- не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования;
- любой ключ из множества возможных должен обеспечивать надежную защиту информации;
- алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

2 Классификация существующих решений

Основные современные методы шифрования

Среди разнообразнейших способов шифровании можно выделить следующие основные методы.

- Алгоритмы замены или подстановки - символы исходного текста заменяются на символы другого алфавита в соответствии с заранее определенной схемой, которая и будет ключом данного шифра. Отдельно этот метод в современных криптосистемах практически не используется из-за чрезвычайно низкой криптостойкости;

- алгоритмы гаммирования — символы исходного текста складываются с символами некой случайной последовательности. Когда пользователь вводит свой пароль при входе в компьютер, операционная система по алгоритму шифрования RC4 генерирует гамму, применяемая для шифрования сетевых паролей. В зависимости от ОС, гамма может быть всегда одной либо каждый раз новой;

- алгоритмы, основанные на сложных математических преобразованиях исходного текста по некоторой формуле. Многие из них используют нерешенные математические задачи. Например, широко используемый в Интернете алгоритм шифрования RSA основан на свойствах простых чисел;

- комбинированные методы. Последовательное шифрование исходного текста с помощью двух и более методов.

2.1 Системы подстановок

Определение Подстановкой на алфавите Z_m называется автоморфизм (преобразование - отображение само на себя) Z_m, при котором буквы исходного текста t замещены буквами шифрованного текста $\pi(t)$:

$$Z_m \to Z_m : \qquad \pi : t \to \pi(t).$$

Набор всех подстановок называется симметрической группой Z_m и будет в дальнейшем обозначаться как SYM(Z_m).

Утверждение SYM(Z_m) с операцией произведения является группой, т.е. операцией, обладающей следующими свойствами.

- Замкнутость: произведение подстановок $\pi_1\pi_2$ является подстановкой.

$$\pi : t \to \pi_1(\pi_2(t)).$$

- Ассоциативность: результат произведения $\pi_1\pi_2\pi_3$ не зависит от порядка расстановки скобок.

$$(\pi_1\pi_2)\pi_2 = \pi_1(\pi_2\pi_3);$$

- Существование нейтрального элемента: постановка i, определяемая как $i(t) = t, 0 \leq t \leq m$, является нейтральным элементом SYM(Z_m) по операции умножения.

$$i\pi = \pi i \text{ для } \forall\pi \in SYM(Z_m).$$

- Существование обратного: для любой подстановки (π_1 существует единственная обратная подстановка π^-1, удовлетворяющая условию

$$\pi_1\pi^-1 = \pi^-1\pi = i.$$

Число возможных подстановок в симметрической группе Z_m называется порядком SYM(Z_m) и равно m!

2.1.1 Шифр Цезаря

Подстановка Цезаря является самым простым вариантом подстановки. Она относится к группе моноалфавитных подстановок.

При моноалфавитной замене каждой букве алфавита открытого текста ставится в соответствие одна буква шифртекста из этого же алфавита.

Определение Подмножество $C_m = \{c_k : 0 \leq k \leq m\}$ симметрической группы $\mathrm{SYM}(Z_m)$, содержащее m подстановок

$$c_k : j \to (j + k) \mod m, \qquad 0 \leq k \leq m, \tag{1}$$

называется подстановкой Цезаря.

Подстановка определяется по таблице замещения, содержащей пары соответсвующих букв "исходный текст - шифрованный текст".

А →г	Й →м	Т →х	Ы →ю
Б →д	К →н	У →ц	Ь →я
В →е	Л →о	Ф →ч	Э →_
Г →ж	М →п	Х →ш	Ю →а
Д →з	Н →р	Ц →щ	Я →б
Е →и	О →с	Ч →ъ	_ →в
Ж →й	П →т	Ш →ы	
З →к	Р →у	Щ →ь	
И →л	С →ф	Ъ →э	

Таблица 1 – Подстановка для c_3

Определение. Системой Цезаря называется моноалфавитная подстановка, преобразующая n-грамму исходного текста $(x_0, x_1, .., x_{n-1})$ в n-грамму шифрованного текста $(y_0, y_1, ..., y_{n-1})$ в соответствии с правилом

$$y_i = c_k(x_i), \qquad 0 \leq i \leq n. \tag{2}$$

2.1.2 Многоалфавитные подстановки. Системы одноразового использования

Многоалфавитная подстановка определяется ключом $\pi = (\pi_1, \pi_2, ...)$, содержащим не менее двух различных подстановок.

Система одноразового использования

Система одноразового использования преобразует исходный текст

$$X = (x_0, x_1, ..., x_{n-1})$$

в шифрованный текст

$$Y = (y_0, y_1, ..., y_{n-1})$$

при помощи подстановки Цезаря

$$y_i = C_{k_i}(x_i) = (k_i + x_i) \mod m \qquad i = 0...n-1$$

Рассмотрим небольшой пример шифрования с бесконечным ключом. В качестве ключа примем текст "БЕСКОНЕЧНЫЙ_КЛЮЧ". Зашифруем с его помощью текста “ШИФР_НЕРАСКРЫВАЕМ”. Шифрование оформим в таблицу 2.

Шифруемый текст	24	8	20	16	19	5	12	27	9	32	18	5	10	17	18
БЕСКОНЕЧНЫЙ	1	5	17	10	14	13	5	23	13	27	9	32	10	11	30
ЩРДЪАТТССЦЪЫДФЬП	25	13	4	26	0	18	17	17	22	23	27	4	20	28	15

Таблица 2 – Пример шифрования с бесконечным ключом

Исходный текст невозможно восстановить без ключа. Наложение белого шума в виде бесконечного ключа на исходный текст меняет статисти-

ческие характеристики языка источника. Системы одноразового использования теоретически не расшифруемы, так как не содержат достаточной информации для восстановления текста.

2.2 Асимметричное шифрование

Асимметричное шифрование — это метод шифрования данных, предполагающий использование двух ключей — открытого и закрытого. Открытый (публичный) ключ применяется для шифрования информации и может передаваться по незащищенным каналам. Закрытый (приватный) ключ применяется для расшифровки данных, зашифрованных открытым ключом. Открытый и закрытый ключи — это очень большие числа, связанные друг с другом определенной функцией, но так, что, зная одно, крайне сложно вычислить второе.

Асимметричное шифрование используется для защиты информации при ее передаче, также на его принципах построена работа электронных подписей.

2.2.1 Принцип действия асимметричного шифрования

Схема передачи данных между двумя субъектами (А и Б) с использованием открытого ключа выглядит следующим образом.

- Субъект А генерирует пару ключей, открытый и закрытый (публичный и приватный);
- субъект А передает открытый ключ субъекту Б. Передача может осуществляться по незащищенным каналам;
- субъект Б шифрует пакет данных при помощи полученного открытого ключа и передает его А передача может осуществляться по незащищенным каналам;

- субъект А расшифровывает полученную от Б информацию при помощи секретного, закрытого ключа;

В такой схеме перехват любых данных, передаваемых по незащищенным каналам, не имеет смысла, поскольку восстановить исходную информацию возможно только при помощи закрытого ключа, известного лишь получателю и не требующего передачи.

2.2.2 Криптосистемы на основе эллиптических уравнений

Криптосистемы на основе эллиптической кривой. Последние достижения теории вычислительной сложности показали, что общая проблема логарифмирования в конечных полях, не может считаться достаточно прочным фундаментом. Наиболее эффективные на сегодняшний день алгоритмы дискретного логарифмирования имеют уже не экспоненциальную, а субэкспоненциальную временную сложность.

Эллиптические кривые - математический объект, который может определен над любым полем (конечным, действительным, рациональным или комплексным). В криптографии обычно используются конечные поля. Эллиптическая кривая есть множество точек (x, y), удовлетворяющее следующему уравнению.

$$y_2 = x_3 + ax + b,$$

а также бесконечно удаленная точка. Для точек, на кривой, довольно легко вводится операция сложения, которая играет ту же роль, что и операция умножения в криптосистемах RSA и Эль-Гамаля.

Надлежащий выбор типа эллиптической кривой позволяет многократно усложнить задачу взлома схемы ЭЦП и уменьшить рабочий размер блоков данных.

В реальных криптосистемах на базе эллиптических уравнений используется уравнение

$$y_2 = x_3 + ax + b \mod p, \qquad \text{где p - простое.}$$

Криптосистемы на основе эллиптической кривой получают все большее распространение скорее как альтернатива, а не замена системам на основе RSA. Они имеют некоторые преимущества, особенно при использовании в устройствах с маломощными процессорами и/или маленькой памятью. Типичные области применения.

- m-commerce - мобильная торговля (WAP, сотовые телефоны, карманные компьютеры);
- смарт-карты (например, EMV);
- e-commerce - электронная торговля и банковские операции (например, SET);
- интернет-приложения (например, в протоколе SSL).

Существуют, однако, и некоторые проблемы, которые ограничивают широкое распространение систем на основе эллиптических кривых.

- Реальная безопасность таких систем все еще недостаточно осознана;
- трудность генерации подходящих кривых;
- несовместимость;
- лицензирование и патентование;
- относительно медленная проверка цифровой подписи.

2.2.3 Криптосистемы с открытым ключом

В асимметричной криптографии для зашифрования и расшифрования используются различные функции. Асимметричные алгоритмы основаны на ряде математических проблем, на которых и базируется их стойкость. Пока не найден полиномиальный алгоритм решения этих проблем,

данные алгоритмы будут стойки. В этом заключается ещё одно отличие симметричного и асимметричного шифрования: стойкость первого является непосредственной и научно доказуемой, стойкость второго – предположительной.

Наиболее известные криптосистемы с открытым ключом.

- Рюкзачная криптосистема (Knapsack Cryptosystem);
- криптосистема RSA;
- криптосистема Эль-Гамаля EGCS (El Gamal Cryptosystem);
- криптосистема, основанная на свойствах эллиптических кривых ECCS (Elliptic Curve Cryptosystems).

Применение алгоритмов шифрования с открытым ключом позволяет.

- Избавиться от необходимости секретных каналов связи для предварительного обмена ключами;
- свести проблему взлома шифра к решению трудной математической задачи, т.е. в конечном счете, принципиально по-другому подойти к обоснованию стойкости криптосистемы;
- решать средствами криптографии задачи, отличные от шифрования, например, задачу обеспечения юридической значимости электронных документов.

Последний пункт означает, что подтверждение авторства сообщений может осуществляться при помощи криптографических средств, что абсолютно необходимо для дистанционного управления ресурсами. Лицо, управляющее чьими-либо ресурсами по распоряжениям владельца, должно обладать возможностью доказать, что выполненное им распоряжение было получено именно от владельца. Данная задача стала особенно актуальной

с появлением электронной коммерции, в качестве ресурса здесь выступают деньги на банковском счету владельца.

Любая схема ЭЦП обязана определить три следующих алгоритма.

- Алгоритм генерации ключевой пары для подписи и ее проверки;
- алгоритм подписи;
- алгоритм проверки подписи.

RSA [1]. RSA криптографическая система с открытым ключом, обеспечивающая оба механизма защиты: шифрование и цифровую подпись. Криптосистема RSA была разработана в 1977 году и названа в честь авторов: Рональда Ривеста, Ади Шамира и Леонарда Адельмана. В PGP алгоритм RSA также используется для шифрования и генерации ЭЦП.

Принцип её действия в следующем. Берутся два больших случайных простых числа и приблизительно равной разрядности и вычисляется их произведение $n = p \cdot q$. Затем выбирается число e, взаимно простое с произведением $(p-1)\cdot(q-1)$ и вычисляется число $d = e^{-1}(\mod (p-1)\cdot(q-1))$, взаимно простое с n.

Числа e и n становятся открытым ключом, число d закрытым. Чтобы создать шифротекст c, отправитель возводит сообщение m в степень e по модулю , где e и n – показатели открытого ключа получателя: $c = m^e(\mod n)$.

Чтобы расшифровать полученный шифротекст c, получатель вычисляет c в степени d по модулю n: $m = c^d(\mod n)$.

Большим преимуществом RSA является его масштабируемость, ключи могут быть разной длины шифрования: 768-битный, 1024-битный, 2048-битный, 4096-битный и т. д.

2.3 Симметричное шифрование

Симметричное шифрование — это способ шифрования данных, при котором один и тот же ключ используется и для кодирования, и для восстановления информации.

2.3.1 Принцип работы симметричных алгоритмов

В целом симметричным считается любой шифр, использующий один и тот же секретный ключ для шифрования и расшифровки.

Например, если алгоритм предполагает замену букв числами, то и у отправителя сообщения, и у его получателя должна быть одна и та же таблица соответствия букв и чисел: первый с ее помощью шифрует сообщения, а второй — расшифровывает.

Однако такие простейшие шифры легко взломать — например, зная частотность разных букв в языке, можно соотносить самые часто встречающиеся буквы с самыми многочисленными числами или символами в коде, пока не удастся получить осмысленные слова. С использованием компьютерных технологий такая задача стала занимать настолько мало времени, что использование подобных алгоритмов утратило всякий смысл.

Поэтому современные симметричные алгоритмы считаются надежными, если отвечают следующим требованиям.

- Выходные данные не должны содержать статистических паттернов исходных данных (как в примере выше: наиболее частотные символы осмысленного текста не должны соответствовать наиболее частотным символам шифра);
- шифр должен быть нелинейным (то есть в шифрованных данных не должно быть закономерностей, которые можно отследить, имея на руках несколько открытых текстов и шифров к ним);

Виды алгоритмов симметричного шифрования

В зависимости от принципа работы алгоритмы симметричного шифрования делятся на два типа.

- блочные;
- потоковые.

Блочные алгоритмы шифруют данные блоками фиксированной длины (64, 128 или другое количество бит в зависимости от алгоритма). Если все сообщение или его финальная часть меньше размера блока, система дополняет его предусмотренными алгоритмом символами, которые так и называются дополнением

Потоковое шифрование данных предполагает обработку каждого бита информации с использованием гаммирования, то есть изменения этого бита с помощью соответствующего ему бита псевдослучайной секретной последовательности чисел, которая формируется на основе ключа и имеет ту же длину, что и шифруемое сообщение. Как правило, биты исходных данных сравниваются с битами секретной последовательности с помощью логической операции XOR (исключающее ИЛИ, на выходе дающее 0, если значения битов совпадают, и 1, если они различаются).

2.3.2 Блочный алгоритм AES

Расширенный стандарт шифрования (Advanced Encryption Standard, AES) — алгоритм шифрования данных, созданный Национальным институтом стандартов и технологий США (NIST) в 2002 году в качестве замены стандарту DES (Data Encryption Standard), который считался уязвимым для брутфорс-атак (атаки методом перебора). Основан на алгоритме Rijndael (название возникло от совмещения имен его разработчиков: Джо-

на Дэймена и Винсерна Риджмена), который был выбран в ходе конкурса, организованного NIST.

AES — симметричный алгоритм: один и тот же ключ используется и для шифрования, и для дешифровки.

2.4 Алгоритмы гаммирования

Гаммирование – метод последовательного симметричного шифрования, суть которого состоит в том, что символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, которая называется гаммой. Такой метод чаще всего представляют как наложение гаммы на исходный текст, поэтому он получил название "гаммирование".

По стойкости данные шифры относятся к классу совершенных. Для зашифрования и дешифрования используются элементарные арифметические операции – открытое/зашифрованное сообщение и гамма, представленные в числовом виде, складываются друг с другом по модулю (mod).

Полученный зашифрованный текст является достаточно трудным для раскрытия в том случае, если гамма шифра не содержит повторяющихся битовых последовательностей и изменяется случайным образом для каждого шифруемого слова. Если период гаммы превышает длину всего зашифрованного текста и неизвестна никакая часть исходного текста, то шифр можно раскрыть только прямым перебором (подбором ключа). В этом случае криптостойкость определяется размером ключа.

Метод гаммирования становится бессильным, если известен фрагмент исходного текста и соответствующая ему шифрограмма. В этом случае простым вычитанием по модулю 2 получается отрезок псевдослучайной последовательности и по нему восстанавливается вся эта последовательность.

2.4.1 Системы шифрования Вижинера

Определение. Ключ пользователя - конечная последовательность ключа.

$$k = (k_0, k_1, ..., k_{r-1})$$

Продлим ее до бесконечной последовательности, повторяя цепочку. Таким образом, получим рабочий ключ

$$k = (k_0, k_1, ..., k_j, ..., k_n), \quad k_j = k_{j \mod r}, \qquad 0 \leq j \leq n.$$

Определение. Подстановка Винжинера VIG_k определяется как.

$$VIG_k : (x_0, x_1, ..., x_{n-1}) \to (y_0, y_1, ..., y_{n-1}) = (x_0 + k_0, x_1 + k_1, ..., x_{n-1} + k_{n-1})$$

Последовательность шифрования.

1. Исходный текст X делится на s фрагментов

$$X_i = (x_i, x_{i+1}, ..., x_{i+r-1}), \qquad 0 \leq i \leq s;$$

2. i-й фрагмент исходного текста x_i шифруется при помощи подстановки Цезаря c_k.

$$(x_i, x_{i+1}, ..., x_{i+r-1}) \to (y_i, y_{i+1}, ..., y_{i+r-1}) =$$
$$(c_{k_i}(x_i), c_{k_i}(x_{i-1}), ..., c_{k_{i-1}}(x_{i+r-1}))$$

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

Рисунок 2 – Таблица Вижнера.

На рисунке [2] предствлена таблица Вижнера, где голубая строка - Алфавит открытого текста, фиолетовая - Алфавит ключа.

Очень распространена плохая с точки зрения секретности практика, использовать слово или фразу в качестве ключа для того, чтобы $k = (k_0, k_1, ..., k_{-1})$ было легко запомнить. В ИС для обеспечения безопасности информации это недопустимо. Для получения ключей должны использоваться программные или аппаратные средства случайной генерации ключей.

Многоалфавитные подстановки в принципе доступны криптоаналитическому исследованию. Криптостойкость многоалфавитных систем резко убывает с уменьшением длины ключа.

Тем не менее такая система как шифр Вижинера допускает несложную аппаратную или программную реализацию и при достаточно большой длине ключа может быть использован в современных ИС.

2.5 Комбинированный метод шифрования

Комбинированный (гибридный) метод шифрования позволяет сочетать преимущества высокой секретности, предоставляемые асимметричными криптосистемами с открытым ключом, с преимуществами высокой скорости работы, присущими симметричным криптосистемам с секретным ключом. При таком подходе криптосистема с открытым ключом применяется для шифрования, передачи и последующего расшифрования только секретного ключа симметричной криптосистемы. А симметричная криптосистема применяется для шифрования и передачи исходного открытого текста. В результате криптосистема с открытым ключом не заменяет симметричную криптосистему с секретным ключом, а лишь дополняет ее, позволяя повысить в целом защищенность передаваемой информации.

Если пользователь A хочет передать зашифрованное комбинированным методом сообщение M пользователю B, то порядок его действий будет таков.

1. Создать (например, сгенерировать случайным образом) симметричный ключ, называемый в этом методе сеансовым ключом KS.

2. Зашифровать сообщение M на сеансовом ключе KS.

3. Зашифровать сеансовый ключ KS на открытом ключе KB пользователя B и своем секретном ключе kA.

4. Передать по открытому каналу связи в адрес пользователя B зашифрованное сообщение вместе с зашифрованным сеансовым ключом.

Действия пользователя B при получении зашифрованного сообщения и зашифрованного сеансового ключа должны быть обратными.

1. Расшифровать на своем секретном ключе kB и открытом ключе ka пользователя KA сеансовый ключ KS.

2. С помощью полученного сеансового ключа KS расшифровать и прочитать сообщение M.

При использовании комбинированного метода шифрования можно быть уверенным в том, что только пользователь B сможет правильно расшифровать ключ KS и прочитать сообщение M.

Таким образом, при комбинированном методе шифрования применяются криптографические ключи как симметричных, так и асимметричных криптосистем. Очевидно, выбор длин ключей для каждого типа криптосистемы следует осуществлять таким образом, чтобы злоумышленнику было одинаково трудно атаковать любой механизм защиты комбинированной криптосистемы.

Комбинированный метод допускает возможность выполнения процедуры аутентификации, т.е. проверки подлинности передаваемого сообщения. Для этого пользователь A на основе функции хэширования сообщения

и своего секретного ключа kA с помощью известного алгоритма электронной цифровой подписи (ЭЦП) генерирует свою подпись и записывает ее, например, в конец передаваемого файла.

Пользователь B, прочитав принятое сообщение, может убедиться в подлинности цифровой подписи абонента A. Используя тот же алгоритм ЭЦП и результат хэширования принятого сообщения, пользователь B проверяет полученную подпись. Комбинированный метод шифрования является наиболее рациональным, объединяя в себе высокое быстродействие симметричного шифрования и высокую криптостойкость, гарантируемую системами с открытым ключом.

Заключение

В данной работе был сделан обзор наиболее распространенных методов защиты информации. Выбор для конкретных систем должен быть основан на глубоком анализе сильных и слабых сторон тех или иных методов защиты. До сих пор не разработаны подходящие методы оценки эффективности защитных систем.

Вывод по симметричном и асимметричном шифровании.

Теоретически приватный ключ от асимметричного шифра можно вычислить, зная публичный ключ и механизм, лежащий в основе алгоритма шифрования. Надежными считаются шифры, для которых это нецелесообразно с практической точки зрения.

При этом фактическая надежность шифрования зависит в основном от длины ключа и сложности решения задачи, лежащей в основе алгоритма шифрования, для существующих технологий. Поскольку производительность вычислительных машин постоянно растет, длину ключей необходимо время от времени увеличивать.

Симметричные алгоритмы требуют меньше ресурсов и демонстрируют большую скорость шифрования, чем асимметричные алгоритмы. Большинство симметричных шифров предположительно устойчиво к атакам с помощью квантовых компьютеров, которые в теории представляют угрозу для асимметричных алгоритмов.

Слабое место симметричного шифрования — обмен ключом. Поскольку для работы алгоритма ключ должен быть и у отправителя, и у получателя сообщения, его необходимо передать; однако при передаче по незащищенным каналам его могут перехватить и использовать посторонние. На практике во многих системах эта проблема решается шифрованием ключа с помощью асимметричного алгоритма.

Список литературы

[1] Криптографические методы защиты информационных систем (ВШЭ) - Авдошин С.М., Савельева А.А. - 2018

[2] Нормативная база и стандарты в области информационной безопасности - Родичев Ю. - 2017

[3] "Информационная безопасность и защита информации"3-е изд. - Баранова Е., Бабаш А. - 2016

[4] Южно Российский институт управления - филиал РАНХиГС, г. Ростов на Дону - 2017

[5] Криптографические методы защиты информации - Панасенко С. - 2006

[6] Использование средств криптографической защиты информации в огранизациях (СГТУ, Самара, Россия) - Баранов А.С. - Июнь 2020

[7] Качество информации. М.: Радио и связь - Дружинин Т. В., Сергеева И. В. - 1990.

[8] Криптографические методы защиты информации для предприятий наукоёмких отраслей - Сукиасян А.А. Мисинёва И.А. - 2019

[9] Криптографические методы защиты информации - Назарова А.П. - 2017

[10] Безопасность информации на предприятиях сервиса - Егоров В.И. , Баклакова В.В. - 2016

[11] Проблемы защиты информации с учетом человеческого фактора - Буркитбаев А.М. , Абеуов Р.Р. - 2017

[12] Минимизация рисков в кредитно-финансовой сфере - Глотов В.И. , Михайлов М.И. - 2018