ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ
Криптография является методологической основой современных систем обеспечения безопасности информации в компьютерных системах и сетях.
Криптография (от др.-греч. ксхрфьт -- скрытый и гсЬцщ -- пишу) -- наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.
Изначально криптография изучала методы шифрования информации -- обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа.
Помимо этого раздела современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.
Криптография не занимается: защитой от обмана, подкупа или шантажа законных абонентов, кражи ключей и других угроз информации, возникающих в защищенных системах передачи данных.
Основным достоинством криптографических методов является то, что они обеспечивают высокую гарантированную стойкость защиты, которую можно рассчитать и выразить в числовой форме (средним числом операций или временем, необходимым для раскрытия зашифрованной информации или вычисления ключей).
К числу основных недостатков криптографических методов следует отнести:
· значительные затраты ресурсов (времени, производительности процессоров) на

выполнение криптографических преобразований информации;
· трудности совместного использования зашифрованной (подписанной) информации, связанные с управлением ключами (генерация, распределение и т.д.);
· высокие требования к сохранности секретных ключей и защиты открытых ключей от подмены.
цифровой сертификат ключ криптография шифрование

1. ИСТОРИЯ
История криптографии насчитывает около 4 тысяч лет. В качестве основного критерия периодизации криптографии возможно использовать технологические характеристики используемых методов шифрования.
Рис. Использовавшийся в Древней Греции шифр «скитала», чья современная реконструкция показана на фото, вероятно был первым устройством для шифрования.
Первый период (приблизительно с 3-го тысячелетия до н. э.) характеризуется господством моноалфавитных шифров (основной принцип -- замена алфавита исходного текста другим алфавитом через замену букв другими буквами или символами). Второй период (хронологические рамки -- с IX века на Ближнем Востоке (Ал-Кинди) и с XV века в Европе (Леон Баттиста Альберти) -- до начала XX века) ознаменовался введением в обиход полиалфавитных шифров. Третий период (с начала и до середины XX века) характеризуется внедрением электромеханических устройств в работу шифровальщиков. При этом продолжалось использование полиалфавитных шифров.
Четвертый период -- с середины до 70-х годов XX века -- период перехода к математической криптографии. В работе Шеннона появляются строгие математические определения количества информации, передачи данных, энтропии, функций шифрования. Обязательным этапом создания шифра считается изучение его уязвимости к различным известным атакам -- линейному и дифференциальному криптоанализам. Однако, до 1975 года криптография оставалась «классической», или же, более корректно, криптографией с секретным ключом.
Рис. Роторная шифровальная машина Энигма, разные модификации которой использовались германскими войсками с конца 1920-х годов до конца Второй мировой войны
Современный период развития криптографии (с конца 1970-х годов по настоящее время) отличается зарождением и развитием нового направления -- криптография с открытым ключом. Её появление знаменуется не только новыми техническими возможностями, но и сравнительно широким распространением криптографии для использования частными лицами (в предыдущие эпохи использование криптографии было исключительной прерогативой государства). Правовое регулирование использования криптографии частными лицами в разных странах сильно различается -- от разрешения до полного запрета.
Современная криптография образует отдельное научное направление на стыке математики и информатики -- работы в этой области публикуются в научных

журналах, организуются регулярные конференции. Практическое применение криптографии стало неотъемлемой частью жизни современного общества -- её используют в таких отраслях как электронная коммерция, электронный документооборот (включая цифровые подписи), телекоммуникации и других.

2. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

2.1 КЛАССИФИКАЦИЯ МЕТОДОВ КРИПТОГРАФИЧЕСКОГО ЗАЩИТЫ ИНФОРМАЦИИ

Известны различные подходы к классификации методов криптографического преобразования информации. По виду воздействия на исходную информацию методы криптографического преобразования информации могут быть разделены на четыре группы (рис. 2.1.1).

Рис. 2.1.1. Классификация методов криптографического преобразования информации

Процесс шифрования заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов. Для шифрования информации используются алгоритм преобразования и ключ. Как правило, алгоритм для определенного метода шифрования является неизменным. Исходными данными для алгоритма шифрования служат информация, подлежащая зашифрованию, и ключ шифрования. Ключ содержит управляющую информацию, которая определяет выбор преобразования на определенных шагах алгоритма и величины операндов, используемые при реализации алгоритма шифрования. В отличие от других методов криптографического преобразования информации, методы стеганографии позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации. В компьютерных системах практическое использование стеганографии только начинается, но проведенные исследования показывают ее перспективность. В основе всех методов стеганографии лежит маскирование закрытой информации среди открытых файлов. Обработка мультимедийных файлов в КС открыла практически неограниченные возможности перед стеганографией.

Существует несколько методов скрытой передачи информации. Одним из них является простой метод скрытия файлов при работе в операционной системе MS-DOS. За текстовым открытым файлом записывается скрытый двоичный файл, объем которого много меньше текстового файла. В конце текстового файла помещается метка EOF (комбинация клавиш Control и Z). При обращении к этому текстовому файлу стандартными средствами ОС считывание прекращается по достижению метки EOF, и скрытый файл остается недоступен. Для двоичных файлов никаких меток в конце файла не предусмотрено. Конец такого файла определяется при обработке атрибутов, в которых хранится длина файла в байтах. Доступ к скрытому файлу может быть получен, если файл открыть как двоичный. Скрытый файл может быть зашифрован. Если кто-то случайно обнаружит скрытый файл, то зашифрованная информация будет воспринята как сбой в работе системы.

Графическая и звуковая информация представляются в числовом виде. Так в графических объектах наименьший элемент изображения может кодироваться

одним байтом. В младшие разряды определенных байтов изображения в соответствии с алгоритмом криптографического преобразования помещаются биты скрытого файла. Если правильно подобрать алгоритм преобразования и изображение, на фоне которого помещается скрытый файл, то человеческому глазу практически невозможно отличить полученное изображение от исходного. Очень сложно выявить скрытую информацию и с помощью специальных программ. Наилучшим образом для внедрения скрытой информации подходят изображения местности: фотоснимки со спутников, самолетов и т. п. С помощью средств стеганографии могут маскироваться текст, изображение, речь, цифровая подпись, зашифрованное сообщение. Комплексное использование стеганографии и шифрования многократно повышает сложность решения задачи обнаружения и раскрытия конфиденциальной информации.

Содержанием процесса кодирования информации является замена смысловых конструкций исходной информации (слов, предложений) кодами. В качестве кодов могут использоваться сочетания букв, цифр, букв и цифр. При кодировании и обратном преобразовании используются специальные таблицы или словари. Кодирование информации целесообразно применять в системах с ограниченным набором смысловых конструкций. Такой вид криптографического преобразования применим, например, в командных линиях АСУ. Недостатками кодирования конфиденциальной информации является необходимость хранения и распространения кодировочных таблиц, которые необходимо часто менять, чтобы избежать раскрытия кодов статистическими методами обработки перехваченных сообщений.

Сжатие информации может быть отнесено к методам криптографического преобразования информации с определенными оговорками.

Целью сжатия является сокращение объема информации. В то же время сжатая информация не может быть прочитана или использована без обратного преобразования. Учитывая доступность средств сжатия и обратного преобразования, эти методы нельзя рассматривать как надежные средства криптографического преобразования информации. Даже если держать в секрете алгоритмы, то они могут быть сравнительно легко раскрыты статистическими методами обработки. Поэтому сжатые файлы конфиденциальной информации подвергаются последующему шифрованию. Для сокращения времени целесообразно совмещать процесс сжатия и шифрования информации.

2.2 ШИФРОВАНИЕ. ОСНОВНЫЕ ПОНЯТИЯ

Основным видом криптографического преобразования информации в КС является шифрование. Под шифрованием понимается процесс преобразования открытой информации в зашифрованную информацию (шифртекст) или процесс обратного преобразования зашифрованной информации в открытую. Процесс преобразования открытой информации в закрытую получил название зашифрование, а процесс преобразования закрытой информации в открытую - расшифрование.

За многовековую историю использования шифрования информации человечеством изобретено множество методов шифрования или шифров. Методом шифрования

(шифром) называется совокупность обратимых преобразований открытой информации в закрытую информацию в соответствии с алгоритмом шифрования. Большинство методов шифрования не выдержали проверку временем, а некоторые используются и до сих пор. Появление ЭВМ и КС инициировало процесс разработки новых шифров, учитывающих возможности использования ЭВМ как для зашифрования/расшифрования информации, так и для атак на шифр. Атака на шифр (криптоанализ) - это процесс расшифрования закрытой информации без знания ключа и, возможно, при отсутствии сведений об алгоритме шифрования.
Современные методы шифрования должны отвечать следующим требованиям:
· стойкость шифра противостоять криптоанализ (криптостойкость) должна быть такой, чтобы вскрытие его могло быть осуществлено только путем решения задачи полного перебора ключей;
· криптостойкость обеспечивается не секретностью алгоритма шифрования, а секретностью ключа;
· шифртекст не должен существенно превосходить по объему исходную информацию;
· ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации;
· время шифрования не должно быть большим;
· стоимость шифрования должна быть согласована со стоимостью закрываемой информации.
Криптостойкость шифра является его основным показателем эффективности. Она измеряется временем или стоимостью средств, необходимых криптоаналитику для получения исходной информации по шифртексту, при условии, что ему неизвестен ключ.
Сохранить в секрете широко используемый алгоритм шифрования практически невозможно. Поэтому алгоритм не должен иметь скрытых слабых мест, которыми могли бы воспользоваться криптоаналитики. Если это условие выполняется, то криптостойкость шифра определяется длиной ключа, так как единственный путь вскрытия зашифрованной информации - перебор комбинаций ключа и выполнение алгоритма расшифрования. Таким образом, время и средства, затрачиваемые на криптоанализ, зависят от длины ключа и сложности алгоритма шифрования.
В качестве примера удачного метода шифрования можно привести шифр DES (Data Encryption Standard), применяемый в США с 1978 года в качестве государственного стандарта. Алгоритм шифрования не является секретным и был опубликован в открытой печати. За все время использования этого шифра не было обнародовано ни одного случая обнаружения слабых мест в алгоритме шифрования.
В конце 70-х годов использование ключа длиной в 56 бит гарантировало, что для раскрытия шифра потребуется несколько лет непрерывной работы самых мощных по тем временам компьютеров. Прогресс в области вычислительной техники позволил значительно сократить время определения ключа путем полного перебора. Согласно заявлению специалистов Агентства национальной безопасности США 56-битный ключ для DES может быть найден менее чем за 453 дня с использованием

суперЭВМ Cray T3D, которая имеет 1024 узла и стоит 30 млн. долл. Используя чип FPGA (Field Programmably Gate Array - программируемая вентильная матрица) стоимостью 400 долл., можно восстановить 40-битный ключ DES за 5 часов. Потратив 10000 долл. за 25 чипов FPGA, 40-битный ключ можно найти в среднем за 12 мин. Для вскрытия 56-битного ключа DES при опоре на серийную технологию и затратах в 300000 долл. требуется в среднем 19 дней, а если разработать специальный чип, то - 3 часа. При затратах в 300 млн. долл. 56-битные ключи могут быть найдены за 12 сек. Расчеты показывают, что в настоящее время для надежного закрытия информации длина ключа должна быть не менее 90 бит.
Все методы шифрования могут быть классифицированы по различным признакам. Один из вариантов классификации приведен на рис. 2.2.1.
Рис.2.2.1 Варианты классификации методов шифровании

2.3 КРИПТОГРАФИЯ С СИММЕТРИЧНЫМИ КЛЮЧАМИ

В криптографии с симметричными ключами (классическая криптография) абоненты используют один и тот же (общий) ключ (секретный элемент) как для шифрования, так и для расшифрования данных.
Следует выделить следующие преимущества криптографии с симметричными ключами:
· относительно высокая производительность алгоритмов;
· высокая криптографическая стойкость алгоритмов на единицу длины ключа.
К недостаткам криптографии с симметричными ключами следует отнести:
· необходимость использования сложного механизма распределения ключей;
· технологические трудности обеспечения неотказуемости.

2.3.1 МЕТОДЫ ЗАМЕНЫ

Сущность методов замены (подстановки) заключается в замене символов исходной информации, записанных в одном алфавите, символами из другого алфавита по определенному правилу. Самым простым является метод прямой замены. Символам s0i исходного алфавита A0, с помощью которых записывается исходная информация, однозначно ставятся в соответствие символы s1i шифрующего алфавита A1. В простейшем случае оба алфавита могут состоять из одного и того же набора символов. Например, оба алфавита могут содержать буквы русского алфавита. Задание соответствия между символами обоих алфавитов осуществляется с помощью преобразования числовых эквивалентов символов исходного текста T0, длиной - K символов, по определенному алгоритму. Алгоритм моноалфавитной замены может быть представлен в виде последовательности шагов.
Шаг 1. Формирование числового кортежа L0h путем замены каждого символа , представленного в исходном алфавите A0 размера [1xK], на число h0i(s0i), соответствующее порядковому номеру символа s0i в алфавите A0.
Шаг 2. Формирование числового кортежа L1h путем замены каждого числа кортежа L0h на соответствующее число h1i кортежа L1h, вычисляемое по формуле:
hli=k1*h0i(s0i)+k2)(mod R),
где k1 - десятичный коэффициент; k2 - коэффициент сдвига. Выбранные

коэффициенты k1, k2 должны обеспечивать однозначное соответствие чисел h0i и h1i, а при получении h1i=0 выполнить замену h1i=R.
Шаг 3. Получение шифртекста T1 путем замены каждого числа hli(sli) кортежа L1h соответствующим символом алфавита шифрования A1размера [1xR].
Шаг 4. Полученный шифртекст разбивается на блоки фиксированной длины b. Если последний блок оказывается неполным, то в конец блока помещаются специальные символы-заполнители (например, символ *).
Пример. Исходными данными для шифрования являются:
T0=<М Е Т О Д _ Ш И Ф Р О В А Н И Я>;
A0=<А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _>;
A1=<О Р Щ Ь Я Т Э _ Ж М Ч Х А В Д Ы Ф К С Е З П И Ц Г Н Л Ъ Ш Б У Ю>;
R=32; k1=3; k2=15; b=4.
Пошаговое выполнение алгоритма приводит к получению следующих результатов.
Шаг 1. L0h=<12, 6, 18, 14, 5, 32, 24, 9, 20, 16, 14, 3, 1, 13, 9, 31>.
Шаг 2. L1h=<19, 1, 5, 25, 30, 15, 23, 10, 11, 31, 25, 24, 18, 22, 10, 12>.
Шаг 3. T1=<С О Я Г Б Д И М Ч У Г Ц К П М Х>.
Шаг 4. T2=<С О Я Г Б Д И М Ч У Г Ц К П М Х>.
При расшифровании сначала устраняется разбиение на блоки. Получается непрерывный шифртекст T1 длиной K символов. Расшифрование осуществляется путем решения целочисленного уравнения:
k1h01+k2=nR+h1i,
При известных целых величинах k1, k2, h1i и R величина h0i вычисляется методом перебора n.
Последовательное применение этой процедуры ко всем символам шифртекста приводит к его расшифрованию.
По условиям приведенного примера может быть построена таблица замены, в которой взаимозаменяемые символы располагаются в одном столбце (табл. 2.3.1.1).
Использование таблицы замены значительно упрощает процесс шифрования. При шифровании символ исходного текста сравнивается с символами строки s0i таблицы. Если произошло совпадение в i-м столбце, то символ исходного текста заменяется символом из строки s1i, находящегося в том же столбце i таблицы. Расшифрование осуществляется аналогичным образом, но вход в таблицу производится по строке s1i.
Основным недостатком метода прямой замены является наличие одних и тех же статистических характеристик исходного и закрытого текста. Зная, на каком языке написан исходный текст и частотную характеристику употребления символов алфавита этого языка, криптоаналитик путем статистической обработки перехваченных сообщений может установить соответствие между символами обоих алфавитов.
Существенно более стойкими являются методы полиалфавитной замены. Такие методы основаны на использовании нескольких алфавитов для замены символов исходного текста. Формально полиалфавитную замену можно представить следующим образом. При N - алфавитной замене символ s01 из исходного алфавита A0 заменяется символом s11 из алфавита A1, s02 заменяется символом s22 из

алфавита A2 и так далее. После замены s0Nсимволом sNN из AN символ s0(N+1) замещается символом s1(N+1) из алфавита A1 и так далее.
Наибольшее распространение получил алгоритм полиалфавитной замены с использованием таблицы (матрицы) Вижинера ТВ, которая представляет собой квадратную матрицу [RxR], где R - количество символов в используемом алфавите. В первой строке располагаются символы в алфавитном порядке. Начиная со второй строки, символы записываются со сдвигом влево на одну позицию. Выталкиваемые символы заполняют освобождающиеся позиции справа (циклический сдвиг). Если используется русский алфавит, то матрица Вижинера имеет размерность [32 x 32] (рис. 2.3.1.2).
Рис.2.3.1.2. Матрица Вижинера
Шифрование осуществляется с помощью ключа, состоящего из M неповторяющихся символов. Из полной матрицы Вижинера выделяется матрица шифрования Тш, размерностью [(M+1), R]. Она включает первую строку и строки, первые элементы которых совпадают с символами ключа. Если в качестве ключа выбрано слово <ЗОНД>, то матрица шифрования содержит пять строк (рис. 2.3.1.3).
Рис. 2.3.1.3. Матрица шифрования для ключа <ЗОНД>
Алгоритм зашифрования с помощью таблицы Вижинера представляет собой следующую последовательность шагов.
Шаг 1. Выбор ключа К длиной М символов.
Шаг 2. Построение матрицы шифрования Тш=(bij) размерностью [(M+1), R] для выбранного ключа К.
Шаг 3. Под каждым символом s0r исходного текста длиной I символов размещается символ ключа km (рис. 2.3.1.3). Ключ повторяется необходимое число раз.
Шаг 4. Символы исходного текста последовательно замещаются символами, выбираемыми из Тш по следующему правилу:
1. определяется символ km ключа К, соответствующий замещаемому символу sor;
2. находится строка i в Тш, для которой выполняется условие km=bi1;
3. определяется столбец j, для которого выполняется условие: sor=b1j;
4. символ sor замещается символом bij.
Шаг 5. Полученная зашифрованная последовательность разбивается на блоки определенной длины, например, по четыре символа. Последний блок дополняется, при необходимости, служебными символами до полного объема.
Расшифрование осуществляется в следующей последовательности:
Шаг 1. Под шифртекстом записывается последовательность символов ключа по аналогии с шагом 3 алгоритма зашифрования.
Шаг 2. Последовательно выбираются символы s1r из шифртекста и соответствующие символы ключа Km. В матрице Тш определяется строка i, для которой выполняется условие Km = bi1. В строке 1 определяется элемент bij = s1r. В расшифрованный текст на позицию r помещается символ b1j.
Шаг 3. Расшифрованный текст записывается без разделения на блоки. Убираются служебные символы.
2.3.2 МЕТОДЫ ПЕРЕСТАНОВКИ

Суть методов перестановки заключается в разделении исходного текста на блоки фиксированной длины и последующей перестановке символов внутри каждого блока по определенному алгоритму.
Перестановки получаются за счет разницы путей записи исходной информации и путей считывания зашифрованной информации в пределах геометрической фигуры. Примером простейшей перестановки является запись блока исходной информации в матрицу по строкам, а считывание - по столбцам. Последовательность заполнения строк матрицы и считывания зашифрованной информации по столбцам может задаваться ключом. Криптостойкость метода зависит от длины блока (размерности матрицы). Так для блока длиной 64 символа (размерность матрицы 8 х 8) возможны 1,6 х 109 комбинаций ключа. Для блока длиной 256 символов (матрица размерностью 16 х 16) число возможных ключей достигает 1,4 х 1026. Решение задачи перебора ключей в последнем случае даже для современных ЭВМ представляет существенную сложность. Перестановки используются также в методе, основанном на применении маршрутов Гамильтона. Этот метод реализуется путем выполнения следующих шагов.
Шаг 1. Исходная информация разбивается на блоки. Если длина шифруемой информации не кратна длине блока, то на свободные места последнего блока помещаются специальные служебные символы-заполнители (например *).
Шаг 2. Символами блока заполняется таблица, в которой для каждого порядкового номера символа в блоке отводится вполне определенное место (рис. 2.3.2.1).
Шаг 3. Считывание символов из таблицы осуществляется по одному из маршрутов. Увеличение числа маршрутов повышает Криптостойкость шифра. Маршруты выбираются либо последовательно, либо их очередность задается ключом К.
Шаг 4. Зашифрованная последовательность символов разбивается на блоки фиксированной длины L. Величина L может отличаться от длины блоков, на которые разбивается исходная информация на шаге 1.
Расшифрование производится в обратном порядке. В соответствии с ключом выбирается маршрут и заполняется таблица согласно этому маршруту.
Рис. 2.3.2.1. Вариант 8-элементной таблицы и маршрутов Гамильтона
Из таблицы символы считываются в порядке следования номеров элементов. Ниже приводится пример шифрования информации с использованием маршрутов Гамильтона.
Пусть требуется зашифровать исходный текст Т0 = <МЕТОДЫ_ПЕРЕСТАНОВКИ>. Ключ и длина зашифрованных блоков соответственно равны: К = <2, 1, 1>, L = 4. Для шифрования используются таблица и два маршрута, представленные на рис. 19. Для заданных условий маршруты с заполненными матрицами имеют вид, показанный на рис. 2.3.2.2.
Рис. 2.3.2.2. Пример шифрования с помощью маршрутов Гамильтона
Шаг 1. Исходный текст разбивается на три блока:
Б1 = <МЕТОДЫ_П>;
Б2 = <ЕРЕСТАНО>;
Б3 = <ВКИ*****>.

Шаг 2. Заполняются три матрицы с маршрутами 2, 1, 1 (рис. 2.3.2.2).
Шаг 3. Получение шифртекста путем расстановки символов в соответствии с маршрутами.
Т1 = <ОП_ТМЕЫДЕСРЕТАОНИ*КВ****>.
Шаг 4. Разбиение на блоки шифртекста
Т1 = <ОП_Т МЕЫД ЕСРЕ ТАОН И*КВ ****>.
В практике большое значение имеет использование специальных аппаратных схем, реализующих метод перестановок (рис. 2.3.2.3).
Рис. 2.3.2.3. Схема перестановок
Параллельный двоичный код блока исходной информации (например, два байта) подаются на схему. За счет внутренней коммутации в схеме осуществляется перестановка бит в пределах блока. Для расшифрования блока информации входы и выходы схемы меняются местами.
Методы перестановок просто реализуются, но имеют два существенных недостатка. Во-первых, они допускают раскрытие шифртекста при помощи статистической обработки. Во-вторых, если исходный текст разбивается на блоки длиной К символов, то криптоаналитику для раскрытия шифра достаточно направить в систему шифрования К-1 блок тестовой информации, в которых все символы за исключением одного одинаковы.

2.3.3 АНАЛИТИЧЕСКИЕ МЕТОДЫ ШИФРОВАНИЯ

Для шифрования информации могут использоваться аналитические преобразования. Наибольшее распространение получили методы шифрования, основанные на использовании матричной алгебры. Зашифрование k-го блока исходной информации, представленного в виде вектора Bk = ||bj||, осуществляется путем перемножения матрицы-ключа A = ||aij|| и вектора Bk. В результате перемножения получается блок шифртекста в виде вектора Ck = ||ci|| , где элементы вектора Ck определяются по формуле:
Расшифрование информации осуществляется путем последовательного перемножения векторов Ck и матрицы A-1, обратной матрице A.
Пример шифрования информации с использованием алгебры матриц.
Пусть необходимо зашифровать и расшифровать слово
Т0 = < ЗАБАВА> с помощью матрицы-ключа А:
Для зашифрования исходного слова необходимо выполнить следующие шаги. Шаг 1. Определяется числовой эквивалент исходного слова как последовательность соответствующих порядковых номеров букв слов Тэ:
Тэ = <8, 1, 2, 1, 3, 1>
Шаг 2. Умножение матрицы А на векторы В1 = {8, 1, 2} и В2 = {1, 3, 1}:
;
.
Шаг 3. Зашифрованное слово записывается в виде последовательности чисел Т1 = <28, 35, 67, 21, 26, 38>.
Расшифрование слова осуществляется следующим образом.

Шаг 1. Вычисляется определитель |A| = -115.
Шаг 2. Определяется присоединенная матрица A*, каждый элемент которой является алгебраическим дополнением элемента матрицы A
.
Шаг 3. Получается транспонированная матрица AT
.
Шаг 4. Вычисляется обратная матрица A-1 по формуле:
A-1 = AT/|A|.
В результате вычислений обратная матрица имеет вид:
.
Шаг 5. Определяются векторы B1 и B2:
B1 = A-1*C1; B2 = A-1*C2.
,
.
Шаг 6. Числовой эквивалент расшифрованного слова
Тэ = <8, 1, 2, 1, 3, 1> заменяется символами, в результате чего получается исходное слово Т0 = <ЗАБАВА>.

2.3.4 АДДИТИВНЫЕ МЕТОДЫ ШИФРОВАНИЯ

Сущность аддитивных методов шифрования заключается в последовательном суммировании цифровых кодов, соответствующих символам исходной информации, с последовательностью кодов, которая соответствует некоторому кортежу символов. Этот кортеж называется гаммой. Поэтому аддитивные методы шифрования называют также гаммированием.

Для данных методов шифрования ключом является гамма. Криптостойкость аддитивных методов зависит от длины ключа и равномерности его статистических характеристик. Если ключ короче, чем шифруемая последовательность символов, то шифртекст может быть расшифрован криптоаналитиком статистическими методами исследования. Чем больше разница длин ключа и исходной информации, тем выше вероятность успешной атаки на шифртекст. Если ключ представляет собой непериодическую последовательность случайных чисел, длина которой превышает длину шифруемой информации, то без знания ключа расшифровать шифртекст практически невозможно. Как и для методов замены в качестве ключа могут использоваться неповторяющиеся последовательности цифр, например, в числах p, e и других.

На практике самыми эффективными и распространенными являются аддитивные методы, в основу которых положено использование генераторов (датчиков) псевдослучайных чисел. Генератор использует исходную информацию относительно малой длины для получения практически бесконечной последовательности псевдослучайных чисел.

Для получения последовательности псевдослучайных чисел (ПСЧ) могут использоваться конгруэнтные генераторы. Генераторы этого класса вырабатывают псевдослучайные последовательности чисел, для которых могут быть строго математически определены такие основные характеристики генераторов как

периодичность и случайность выходных последовательностей.
Среди конгруэнтных генераторов ПСЧ выделяется своей простотой и эффективностью линейный генератор, вырабатывающий псевдослучайную последовательность чисел T(i) в соответствии с соотношением
T(i+1) = (a * T(i) + c) mod m,
где a и c - константы, T(0) - исходная величина, выбранная в качестве порождающего числа.
Период повторения такого датчика ПСЧ зависит от величин a и c. Значение m обычно принимается равным 2s, где s - длина слова ЭВМ в битах. Период повторения последовательности генерируемых чисел будет максимальным тогда и только тогда, когда c - нечетное число и a (mod 4) = 1: Такой генератор может быть сравнительно легко создан как аппаратными средствами, так и программно.

2.4 КРИПТОГРАФИЯ С ОТКРЫТЫМИ КЛЮЧАМИ

Наряду с традиционным шифрованием на основе секретного ключа в последние годы все большее признание получают системы шифрования с открытым ключом. В таких системах используются два ключа. Информация шифруется с помощью открытого ключа, а расшифровывается с использованием секретного ключа.
В основе применения систем с открытым ключом лежит использование необратимых или односторонних функций. Эти функции обладают следующим свойством. По известному x легко определяется функция y = f(x). Но по известному значению y практически невозможно получить x. В криптографии используется односторонние функции, имеющие так называемый потайной ход. Эти функции с параметром z обладают следующими свойствами. Для определенного z могут быть найдены алгоритмы Ez и Dz. С помощью Ez легко получить функцию fz(x) для всех x из области определения. Так же просто с помощью алгоритма Dz получается и обратная функция x = f-1(y) для всех y из области допустимых значений. В то же время практически для всех z и почти для всех y из области допустимых значений нахождение f-1(y) при помощи вычислений невозможно даже при известном Ez. В качестве открытого ключа используется y, а в качестве закрытого - x.
При шифровании с использованием открытого ключа нет необходимости в передаче секретного ключа между взаимодействующими субъектами, что существенно упрощает криптозащиту передаваемой информации.
Криптосистемы с открытыми ключами различаются видом односторонних функций. Среди них самыми известными являются системы RSA, Эль-Гамаля и Мак-Элиса. В настоящее время наиболее эффективным и распространенным алгоритмом шифрования с открытым ключом является алгоритм RSA, получивший свое название от первых букв фамилий его создателей: Rivest, Shamir и Adleman.
Алгоритм основан на использовании операции возведения в степень модульной арифметики. Его можно представить в виде следующей последовательности шагов.
Шаг 1. Выбираются два больших простых числа p и q. Простыми называются числа, которые делятся только на самих себя и на 1 . Величина этих чисел должна быть больше 200.

Шаг 2. Получается открытая компонента ключа n:
n = p * q.
Шаг 3. Вычисляется функция Эйлера по формуле:
f(p, q) = (p-1) * (q-1).
Функция Эйлера показывает количество целых положительных чисел от 1 до n, которые взаимно просты с n. Взаимно простыми являются такие числа, которые не имеют ни одного общего делителя, кроме 1.
Шаг 4. Выбирается большое простое число d, которое является взаимно простым со значением f(p, q).
Шаг 5. Определяется число e, удовлетворяющее условию:
e * d = 1(modf(p, q)).
Данное условие означает, что остаток от деления (вычет) произведения e*d на функцию f(p, q) равен 1. Число e принимается в качестве второй компоненты открытого ключа. В качестве секретного ключа используются числа p и q. Шаг 6. Исходная информация, независимо от ее физической природы, представляется в числовом двоичном виде. Последовательность бит разделяется на блоки длиной L бит, где L - наименьшее целое число, удовлетворяющее условию: L?log2(n+1). Каждый блок рассматривается как целое положительное число X(i), принадлежащее интервалу [0, n-1]. Таким образом, исходная информация представляется последовательностью чисел X(i),i= . Значение I определяется длиной шифруемой последовательности.
Шаг 7. Зашифрованная информация получается в виде последовательности чисел Y(i), вычисляемых по формуле:
Y(i) = (X(i))e(mod n).
Шаг 8. Для расшифрования информации используется следующая зависимость:
X(i) = (Y(i))d(mod n).
Пример применения метода RSA для криптографического закрытия информации. Примечание: для простоты вычислений использованы минимально возможные числа.
Пусть требуется зашифровать сообщение на русском языке "ГАЗ".
Для зашифрования и расшифрования сообщения необходимо выполнить следующие шаги.
Шаг 1. Выбирается p = 3 и q = 11.
Шаг 2. Вычисляется n = 3 * 11 = 33.
Шаг 3. Определяется функция Эйлера
f(p, q) = (3-1)*(11-1) = 20.
Шаг 4. В качестве взаимно простого числа выбирается число
Шаг 5. Выбирается такое число e, которое удовлетворяло бы ношению: (e*3) (mod 20) = 1. Пусть e = 7.
Шаг 6. Исходное сообщение представляется как последовательность целых чисел. Пусть букве А соответствует число 1, букве Г - число 4, букве З - число 9. Для представления чисел в двоичном коде требуется 6 двоичных разрядов, так как в русском алфавите используются 33 буквы (случайное совпадение с числом n).

Исходная информация в двоичном коде имеет вид:
000100 000001 001001.
Длина блока L определяется как минимальное число из целых чисел, удовлетворяющих условию: L?log2(33+1), так как n=33. Отсюда L = 6. Тогда исходный текст представляется в виде кортежа X(i) = <4, 1, 9>.
Шаг 7. Кортеж X(i) зашифровывается с помощью открытого ключа {7, 33}:
Y(1) = (47) (mod 33) = 16384 (mod 33) = 16;
Y(2) = (17) (mod 33) = 1 (mod 33) = 1;
Y(3) = (97) (mod 33) = 4782969 (mod 33) = 15.
Получено зашифрованное сообщение Y(i) = <16, 1, 15>.
Шаг 8. Расшифровка сообщения Y(i) = <16, 1, 15> осуществляется с помощью секретного ключа {3, 33}:
X(1) = (163) (mod 33) = 4096 (mod 33) = 4;
X(2) = (13) (mod 33) = 1 (mod 33) = 1;
X(3) = (153) (mod 33) = 3375 (mod 33) = 9.
Исходная числовая последовательность в расшифрованном виде X(1) = <4, 1, 9> заменяется исходным текстом "ГАЗ".
Система Эль-Гамаля основана на сложности вычисления дискретных логарифмов в конечных полях. Основным недостатком систем RSA и Эль-Гамаля является необходимость выполнения трудоемких операций в модульной арифметике, что требует привлечения значительных вычислительных ресурсов. Криптосистема Мак-Элиса использует коды, исправляющие ошибки. Она реализуется в несколько раз быстрее, чем криптосистема RSA, но имеет и существенный недостаток. В криптосистеме Мак-Элиса используется ключ большой длины и получаемый шифртекст в два раза превышает длину исходного текста.
Для всех методов шифрования с открытым ключом математически строго не доказано отсутствие других методов криптоанализа кроме решения NP-полной задачи (задачи полного перебора). Если появятся методы эффективного решения таких задач, то криптосистемы такого типа будут дискредитированы. Например, ранее считалось, что задача укладки рюкзака является NP-полной. В настоящее время известен метод решения такой задачи, позволяющий избежать полного перебора.
2.4.1 ДВА ВАЖНЫХ СВОЙСТВА КРИПТОГРАФИИ С ОТКРЫТЫМИ КЛЮЧАМИ
Рисунок 2.4.1.1 Два свойства криптографии с открытыми ключами
Схема шифрования данных с использованием открытого ключа приведена на Рисунке 2.4.1.1 и состоит из двух этапов. На первом из них производится обмен по несекретному каналу открытыми ключами. При этом необходимо обеспечить подлинность передачи ключевой информации. На втором этапе, собственно, реализуется шифрование сообщений, при котором отправитель зашифровывает сообщение открытым ключом получателя.Зашифрованный файл может быть прочитан только владельцем секретного ключа, т.е. получателем. Схема расшифрования, реализуемая получателем сообщения, использует для этого секретный ключ получателя.

2.4.2 ШИФРОВАНИЕ

Рисунок 2.4.2.1 Схема шифрования в криптографии с открытыми ключами.
Реализация схемы ЭЦП связанна с вычислением хэш-функции (дайджеста) данных, которая представляет собой уникальное число, полученное из исходных данных путем его сжатия (свертки) с помощью сложного, но известного алгоритма. Хэш-функция является однонаправленной функцией, т.е. по хэш-значению не возможно восстановить исходные данные. Хэш-функция чувствительна к всевозможным искажениям данных. Кроме того, очень трудно отыскать два набора данных, обладающих одним и тем же значением хэш-функции.

2.4.3 ФОРМИРОВАНИЕ ЭЦП С ХЭШИРОВАНИЕМ

Схема формирования подписи ЭД его отправителем включает вычисление хэш-функции ЭД и шифрование этого значения посредством секретного ключа отправителя. Результатом шифрования является значение ЭЦП ЭД (реквизит ЭД), которое пересылается вместе с самим ЭД получателю. При этом получателю сообщения должен быть предварительно передан открытый ключ отправителя сообщения.
Рисунок 2.4.3.1 Схема ЭЦП в криптографии с открытыми ключами
Схема проверки (верификации) ЭЦП, осуществляемая получателем сообщения, состоит из следующих этапов. На первом из них производится расшифрование блока ЭЦП посредством открытого ключа отправителя. Затем вычисляется хэш-функция ЭД. Результат вычисления сравнивается с результатом расшифрования блока ЭЦП. В случае совпадения, принимается решение о соответствии ЭЦП ЭД. Несовпадение результата расшифрования с результатом вычисления хеш-функции ЭД может объясняться следующими причинами:

· в процессе передачи по каналу связи была потеряна целостность ЭД;
· при формировании ЭЦП был использован не тот (поддельный) секретный ключ;
· при проверке ЭЦП был использован не тот открытый ключ (в процессе передачи по каналу связи или при дальнейшем его хранении открытый ключ был модифицирован или подменен).

Реализация криптографических алгоритмов с открытыми ключами (по сравнению с симметричными алгоритмами) требует больших затрат процессорного времени. Поэтому криптография с открытыми ключами обычно используется для решения задач распределения ключей и ЭЦП, а симметричная криптография для шифрования. Широко известна схема комбинированного шифрования, сочетающая высокую безопасность криптосистем с открытым ключом с преимуществами высокой скорости работы симметричных криптосистем. В этой схеме для шифрования используется случайно вырабатываемый симметричный (сеансовый) ключ, который, в свою очередь, зашифровывается посредством открытой криптосистемы для его секретной передачи по каналу в начале сеанса связи.

2.4.4 КОМБИНИРОВАННЫЙ МЕТОД

Рисунок 2.4.4.1 Схема комбинированного шифрования

2.4.5 ДОВЕРИЕ К ОТКРЫТОМУ КЛЮЧУ И ЦИФРОВЫЕ СЕРТИФИКАТЫ

Центральным вопросом схемы открытого распределения ключей является вопрос доверия к полученному открытому ключу партнера, который в процессе передачи или хранения может быть модифицирован или подменен.

Для широкого класса практических систем (системы электронного документооборота, системы Клиент-Банк, межбанковские системы электронных расчетов), в которых возможна личная встреча партнеров до начала обмена ЭД, эта задача имеет относительно простое решение - взаимная сертификация открытых ключей.

Эта процедура заключается в том, что каждая сторона при личной встрече удостоверяет подписью уполномоченного лица и печатью бумажный документ - распечатку содержимого открытого ключа другой стороны. Этот бумажный сертификат является, во-первых, обязательством стороны использовать для проверки подписи под входящими сообщениями данный ключ, и, во-вторых, обеспечивает юридическую значимость взаимодействия. Действительно, рассмотренные бумажные сертификаты позволяют однозначно идентифицировать мошенника среди двух партнеров, если один из них захочет подменить ключи. Таким образом, для реализации юридически значимого электронного взаимодействия двух сторон необходимо заключить договор, предусматривающий обмен сертификатами.

Сертификат представляет собой документ, связывающий личностные данные владельца и его открытый ключ. В бумажном виде он должен содержать рукописные подписи уполномоченных лиц и печати.

В системах, где отсутствует возможность предварительного личного контакта партнеров, необходимо использовать цифровые сертификаты, выданные и заверенные ЭЦП доверенного посредника - удостоверяющего или сертификационного центра.

ЗАКЛЮЧЕНИЕ

Как показывает практика, криптографические методы защиты действительно обеспечивают безопасность на достаточно высоком уровне. Несомненно, что данное направление будет быстро развиваться с появлением новых коммуникационных аппаратно-программных средств. Большинство современных компаний стараются разработать универсальные криптографические интерфейсы и избавить разработчика программного обеспечения от самостоятельных реализаций сложных алгоритмов.

На основании всего вышесказанного можно смело говорить о том, что тенденции развития рынка средств криптографической защиты информации совпадают с тенденциями, наблюдаемыми в прочих сегментах рынка прикладного программного обеспечения.

Среди основных тенденций следует особо выделить унификацию параметров криптографических алгоритмов, форматов криптографических сообщений и протоколов, используемых в СКЗИ.

На сегодняшний день криптография применяется практически во всех отраслях

человеческой деятельности, что является немаловажной задачей в более детальном ее изучении и дальнейшем развитии.

СПИСОК ЛИТЕРАТУРЫ

[1] Хоффман Л.Дж. Современные методы защиты информации / Пер. с англ. - М: Сов. радио, 1980.

[2] Мельников В.В. Защита информации в компьютерных системах. - М.: Финансы и статистика; Электронинформ, 1997.

[3] https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F

[4] http://sec4all.net/modules/myarticles/article.php?storyid=605

[5] http://sumk.ulstu.ru/docs/mszki/Zavgorodnii/