Кафедра информационно-коммуникационных технологий

СОВРЕМЕННЫЕ СИММЕТРИЧНЫЕ И АССИМЕТРИЧНЫЕ КРИПТОСИСТЕМЫ

Методические указания к лабораторной работе по курсу

Методы и средства защиты информации

Москва 2009

ВВЕДЕНИЕ

Обмен документами в электронном виде возможен лишь в том случае, если обеспечивается их конфиденциальность, надежная защита от подделки или несанкционированного изменения, гарантирована доставка адресату, имеется возможность разрешения споров, связанных с фальсификацией сообщений и отказом от авторства.

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.

В современном программном обеспечении (ПО) криптоалгоритмы широко применяются не только для задач шифрования данных, но и для аутентификации и проверки целостности. На сегодняшний день существуют хорошо известные и апробированные криптоалгоритмы (как с симметричными, так и несимметричными ключами), криптостойкость которых либо доказана математически, либо основана на необходимости решения математически сложной задачи (факторизации, дискретного логарифмирования и т.п.).

*Цель работы*

Описание и программная реализация одного из предложенных алгоритмов.

*Теоретические сведения*

Методы и средства защиты информации

На первом этапе развития концепции обеспечения безопасности информации, преимущество отдавалось программным средствам защиты. Когда практика показала, что для обеспечения безопасности информации этого недостаточно, интенсивное развитие получили всевозможные устройства и системы. RoctsttsHHo, по мере формирования системного подхода к проблеме обеспечения информационной безопасности, возникла необходимость комплексного применения методов защиты и созданных на их основе средств и механизмов защиты.

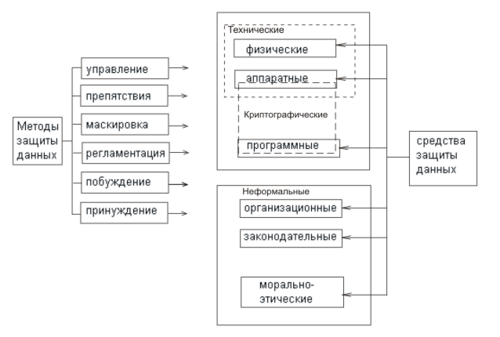


Рис. 1. Классификация методов и средств защиты информации

Кратко рассмотрим основные методы защиты информации. Управление представляет собой направленное воздействие на ресурсы системы в рамках установленного технологического цикла обработки и передачи данных, где в качестве ресурсов рассматриваются технические средства, ОС, программы, БД, элементы данных и т.п.

Препятствия физически преграждают нарушителю путь к защищаемым данным.

Маскировка представляет собой метод защиты данных путем их криптографического закрытия.

Регламентация как метод защиты заключается в разработке и реализации в процессе функционирования ИВС комплексов мероприятий, создающих такие условия технологического цикла обработки данных, при которых минимизируется риск НСД к данным. Регламентация охватывает как структурное построение ИВС, так и технологию обработки данных, организацию работы пользователей и персонала сети.

Побуждение состоит в создании такой обстановки и условий, при которых правила обращения с защищенными данными регулируются моральными и нравственными нормами.

Принуждение включает угрозу материальной, административной и уголовной ответственности за нарушение правил обращения с защищенными данными. На основе перечисленных методов создаются средства защиты данных. Все средства защиты данных можно разделить на формальные и неформальные.

*Формальные средства защиты*

Формальными называются такие средства защиты, которые выполняют свои функции по заранее установленным процедурам без вмешательства человека. К формальным средствам защиты относятся технические и программные средства.

К техническим средствам (вам защиты относятся все устройства, которые предназначены для защиты защиты. Физическими называются средства защиты, которые создают физические препятствия на пути к защищаемым данным и не входят в состав аппаратуры ИВС, а аппаратными - средства защиты данных, непосредственно входящие в состав аппаратуры ИВС.

Программными называются средства защиты данных, функционирующие в составе программного обеспечения ИВС.

Отдельную группу формальных средств составляют криптографические средства, которые реализуются в виде программных, аппаратных и программно-аппаратных средств защиты.

*Неформальные средства защиты*

Неформальными называются такие средства защиты, которые реализуются в результате деятельности людей, либо регламентируют эту деятельность. Неформальные средства включают организационные, законодательные и морально-этические меры и средства.

Под организационными средствами защиты понимаются организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации ИВС для обеспечения безопасности данных.

К морально-этическим нормам защиты относятся всевозможные нормы, которые традиционно сложились или складываются по мере развития информатизации общества. Такие нормы не являются обязательными, однако их несоблюдение ведет, как правило, к потере авторитета, престижа человека, группы лиц или целой организации. Считается, что Этические нормы оказывают положительное воздействие на персонал и пользователей. Морально-этические нормы могут быть неписаными (например, общепринятые нормы честности, патриотизма и т.п.) и оформленными в качестве свода правил и предписаний (кодексов).

1. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования расшифрования. В соответствии со стандартом ГОСТ 28147-89 под шифром понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом криптографического преобразования.

Ключ - это конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

Основной характеристикой шифра является криптостойкость, которая определяет его стойкость к раскрытию методами криптоанализа. Обычно эта характеристика определяется интервалом времени, необходимым для раскрытия шифра.

К шифрам, используемым для криптографической защиты информации, предъявляется ряд требований:

* достаточная криптостойкость (надежность закрытия данных);
* простота процедур шифрования и расшифрования;
* незначительная избыточность информации за счет шифрования;
* нечувствительность к небольшим ошибкам шифрования и др.

В той или иной мере этим требованиям отвечают:

* шифры перестановок:
* шифры замены;
* шифры гаммирования;
* шифры, основанные на аналитических преобразованиях шифруемых данных.

Шифрование перестановкой заключается в том, что символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста. При достаточной длине блока, и пределах которого осуществляется перестановка, и сложном неповторяющемся порядке перестановки можно достигнуть приемлемой для простых практических приложений стойкости шифра.

Шифрование заменой (подстановкой) заключается в том, что символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены.

Шифрование гаммированием заключается в том, что символы шифруемою текста складываются с символами некоторой случайной последовательности, именуемой гаммой шифра. Стойкость шифрования определяется в основном длиной (периодом) неповторяющейся части гаммы шифра. Поскольку с помощью ЭВМ можно генерировать практически бесконечную гамму шифра, то данный способ является одним из основных для шифрования информации в автоматизированных системах.

Шифрование аналитическим преобразованием заключается в том, что шифруемый текст преобразуется по некоторому аналитическому правилу (формуле).

Например, можно использовать правило умножения вектора на матрицу, причем умножаемая матрица является ключом шифрования (поэтому ее размер и содержание должны храниться в секрете), а символами умножаемого вектора последовательно служат символы шифруемого текста. Другим примером может служить использование так называемых однонаправленных функций для построения криптосистем с открытым ключом.

Процессы шифрования и расшифрования осуществляются в рамках некоторой криптосистемы.

1.1 Традиционные симметричные криптосистемы. Принципы криптографической защиты информации

Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для противника. Такие преобразования позволяют решить две главные проблемы защиты данных: проблемы конфиденциальности (путем лишения противника возможности извлечь информацию из канала связи) и проблему целостности (путем лишения противника возможности изменить сообщение так, чтобы изменился его смысл, или ввести ложную информацию в канал связи). Проблемы конфиденциальности и целостности информации тесно связаны между собой, поэтому методы решения одной из них часто применимы для решения другой.

Обобщенная схема криптографической системы, обеспечивающей шифрование передаваемой информации, показана на рис.1. Отправитель генерирует открытый текст исходного сообщения , которое должно быть передано законному получателю по незащищенному каналу. За каналом следит перехватчик с целью перехватить и раскрыть передаваемое сообщение. Для того чтобы перехватчик не смог узнать содержание сообщения , отправитель шифрует его с помощью обратимого преобразования и получает шифртекст (или криптограмму) , который отправляет получателю.



Законный получатель, приняв шифртекст С, расшифровывает его с помощью обратного преобразования и получает исходное сообщение ввиде открытого текста :



Рис. 2. Обобщённая схема криптосистемы

Преобразование выбирается из семейства криптографических преобразований, называемых криптоалгоритмами. Параметр, c помощью которого выбирается отдельное используемое преобразование, называется криптографическим ключом . Криптосистема имеет разные варианты реализации: набор инструкции, аппаратные средства, комплекс программ компьютера, которые позволяют зашифровать открытый текст и расшифровать шифртекст различными способами, один из которых выбирается с помощью конкретного ключа .



Говоря более формально, криптографическая система - это однопараметрическое семействообратимых преобразований из пространства сообщений открытого текста в пространство С шифрованных текстов. Параметр (ключ) выбирается из конечного множества К, называемого пространством ключей.



Преобразование шифрования может быть симметричным или асимметричным относительно преобразования расшифрования. Это важное свойство функции преобразования определяет два класса криптосистем:

* симметричные (одноключевые) криптосистемы;
* асимметричные (двухключевые) криптосистемы (с открытым ключом).

Схема симметричной криптосистемы с одним секретным ключом показана на рис.2. В ней используются одинаковые секретные ключи в блоке шифрования и блоке расшифрования.

Обобщенная схема асимметричной криптосистемы с двумя разными ключами и показана на рис. 3.



Рис. 3. Обобщённая схема ассиметричной криптосистемы с открытым ключом.

В этой криптосистеме один из ключей является открытым, а другой - секретным.

В симметричной криптосистеме секретный ключ надо передавать отправителю и получателю по защищенному каналу распространения ключей, например такому, как курьерская служба. На рис. 2 этот канал показан "экранированной" линией. Существуют и другие способы распределения секретных ключей. В асимметричной криптосистеме передают по незащищенному каналу только открытый ключ, а секретный ключ сохраняют на месте его генерации.

Существуют два основных современных класса шифров: поточные и блочные шифры.

1.2 Поточные шифры

Шифр Вернама - практически и теоретически неуязвим (строится на ключевом потоке случайных бит).

Шифры на псевдослучайном ключевом потоке бит - уязвимы для криптоанализа. Их достоинства - ошибки не влияют на дешифрование последующих за ошибкой данных. Необнаруженные добавления или удаления битов и потока зашифрованного текста приводят к потере возможности дешифрования; более того, они неприемлемы, так как отсутствие размножения ошибок затрудняет развитие методов для обнаружения воздействия по изменению длины сообщений и внесению ошибок другого рода.

Шифр с авто ключом: его ключевой поток зависит от открытого текста, шифрованного текста или самого себя, а также некоторого начального (первичного) кода: этот шифр обеспечивает межбитовую зависимость и обнаружение ошибок. В шифрах с шифрованным текстом в качестве ключа (штак) - шифрованный текст используется как входная информация для выработки ключевого потока, имеющего межбитовую зависимость. В случае ошибки при передаче правильная работа дешифратора возобновляется после получения некоторого фиксированного числа неискаженных битов шифрованного текста.

1.3 Блочные шифры

Блочное шифрование под управлением единственного ключа - это определение одной из 2n перестановок в наборе n-битных блоков. На практике блочное шифрование не реализует все возможные перестановки ввиду необходимости обеспечения требуемого размера ключа и логической сложности шифрования. Шифр является предметом анализа, осуществляемого сравнением частоты распределения отдельных блоков с известной частотой распределения знаков в больших образцах открытого текста. Если увеличивать размер блока и строить шифр таким образом, чтобы скрывались частотные характеристики компонентов блоков посредством смешивания преобразований, то такое частотное распределение и его анализ становятся невыполнимыми из-за возрастании размера используемого алфавита и полученная криптографическая схема считается очень хорошей.

На основе блочных шрифтов строятся: алгоритм шифрования данных DES, являющийся стандартом США подробно изложенный ниже, а также алгоритм Риаеста.

1.4 Алгоритм шифрования данных DES

Применяется блочный шифр, оперирующий с 64-битными блоками с использованием 56-битного ключа - режим книги электронных кодов (КЭК). В режиме КЭК (см. рис.4.) необходимая для правильного дешифрования сообщений криптографическая синхронность достигается тогда, когда отправитель и получатель используют один и тот же ключ и правильно определяют границы блока.

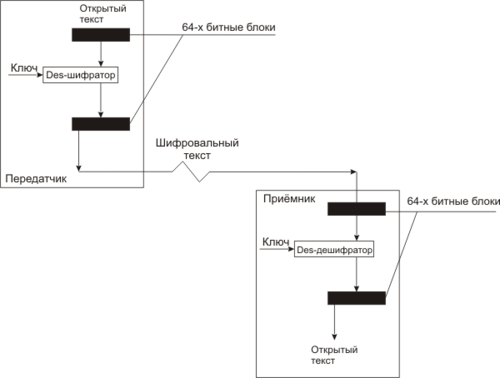


Рис. 4. Криптосистема DES в режиме электронной кодировочной книги.

DES может использоваться различными способами как часть генератора ключевого потока для шифров ШТАК (в режиме поточного шифра). В режиме работы в качестве шифра с обратной связью (ШОС), шифр DES превращается в самосинхронизирующийся поточный шифр, который обрабатывает строки открытого текста (см. рис.5).

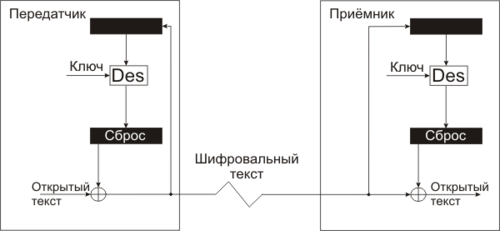


Рис. 5. Криптосистема DES в режиме с обратной связью.

DES является стойким к обычному криптоанализу, хотя он и является теоретически слабым и может быть чувствительным к средствам анализа, основанным на применении больших специализированных вычислительных устройств с большой степенью распараллеливания процессов анализа и обработки информации (шифра).

Режим КЭК и ШОС использования DES позволяют достичь только первой цели - предотвращения раскрытия содержания сообщения (криптозащита) применением их к данным, которые нужно защитить. Однако эти режимы также лежат в основе построения контрмер для достижения остальных целей, перечисленных ранее и связанных с защитой от навязывания ложной информацией (имитозащитой), полученной нарушителем различными перечисленными способами.

1.5 Алгоритм Ривеста

Применяется блочный шифр с общим ключом. Размер блока от 256 до 650 бит в зависимости от желаемого уровня защиты. При шифровании сообщение М рассматривается как целое число и шифруется возведением степень "1" (по модулю "n"). При дешифровании полученный текст c дешифруется возведением его в степень d (по модулю "n").

Шифрующий ключ-пара (1, n). Дешифрующий ключ-пара (d, n). Значение d, 1, n вычисляются из пары больших простых чисел (p, q). Правила вычисления d, 1, пи методы выбора р и q даны Ривсстом. Алгоритм основан на очевидной трудности разложения на множители, больших сложных чисел. В отличие от DES. по-видимому не существует пути преобразования этого алгоритма в поточный шифр одновременно с сохранением характеристик алгоритма с открытым ключом.

Сравнение режимов поточного и блочного шифрования показывает, что проблемы, связанные с использованием основного блочного режима работы (КЭК) в обычных шифрах или в системах с общим ключом состоят в следующем:

1. В общем случае длина сообщения не соответствует размеру блока шифра, поэтому используется разбиение сообщения (пакета) на части, соответствующая по размеру блоку шифра с дополнением сообщения пустыми символами до целого числа блоков. В результате имеет место потеря пропускной способности до 1/2 размера блока па каждое сообщение;
2. Два блока открытого текста, состоящие из одинакового набора битов приводят к одинаковым блокам шифрованного текста;
3. В этом режиме размножение ошибки происходит строго внутри блока и это требует применения методов обнаружения изменения сообщений.

Из-за указанных трудностей режим КЭК не всегда пригоден для текста сообщения общего вида. Усиленным вариантом этого режима, пригодным как для обычных шифров, так и для систем с общим ключом, является режим сцепления блоков в шифре (СБШ) (см. рис. 6.).

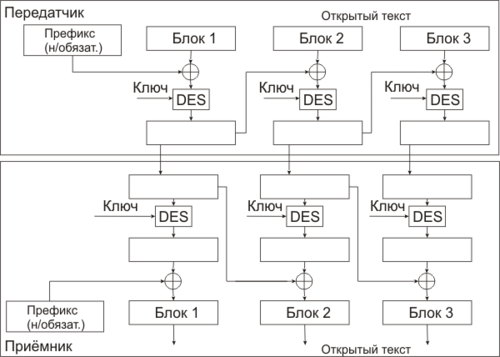


Рис. 6. Криптосистемы DES в режиме сцепления блоков в шифре.

Поточные шифры ШТАК, такие как режим ШОС использования DBS, дают ключевой поток, соответствующий длине текста, подлежащего шифрованию без пустых символов в последнем неполном блоке сообщения. Недостаток этого подхода - значительно снижается пропускная способность алгоритма блочного шифрования в режиме ШОС (для DES с 8-и битными байтами в режиме ШОС снижение в 8 и более раз). Эта задача решается, если применять два размера блока при шифровании каждого сообщения: - размер блока основного шифра и - длину сообщения по модулю этого размера блока. Это приводит к пропускной способности, сравнимой с той, которую обеспечивает режим КЭК, однако исключает дополнение пустыми символами открытого текста. Другая особенность шифров ШТАК - необходимость начального заполнения для синхронизации сдвиговых регистров на обоих концах соединения.

Существует два способа начального заполнения:

* для каждого сообщения отдельно и независимо.
* заполнение - как функция сообщения, переданного ранее.

Последний способ не пригоден для общего случая, когда имеет место неупорядоченное поступление сообщений или при наличии ошибок. Так как режимы КЭК и ШОС - самосинхронизирующиеся, размножение ошибок ограничивается и этот факт следует принимать во внимание при разработке методов обнаружения изменения сообщений за счет размножения ошибок.

1.6 Ассиметричные криптосистемы

Концепция криптосистемы с открытым ключом

Эффективными системами криптографической защиты данных являются асимметричные криптосистемы, называемые также криптосистемами с открытым ключом. В таких системах для зашифровки данных используется один ключ, а для расшифровки - другой ключ (отсюда и название - асимметричные). Первый ключ является открытым и может быть опубликован для использования всеми пользователями системы, которые зашифровывают данные. Расшифровка данных с помощью открытого ключа невозможно

Для расшифровки данных получатель зашифрованной информации использует второй ключ, который является секретным. Разумеется, ключ расшифровки не может быть определен из ключа зашифровки.

Обобщенная схема асимметричной криптосистемы с открытым ключом показана на рис. 7. В этой криптосистеме применяют два различных ключа: - открытый ключ отправителя А; - секретный ключ получателя В. Генератор ключей целесообразно располагать на стороне получателя В (чтобы не пересылать секретный ключ по незащищенному каналу). Значения ключей и зависят от начального состояния генератора ключей.



Раскрытие секретного ключа по известному открытому ключу должно быть вычислительно неразрешимой задачей.



Характерные особенности асимметричных криптосистем:

1. Открытый ключ и криптограмма могут быть отправлены по незащищенным каналам, т.е. противнику известны и .



1. Алгоритмы шифрования и расшифровки. Открытый ключ и являются открытыми.

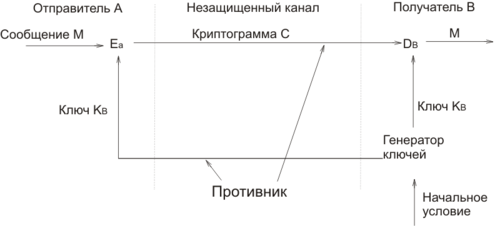


Рис. 7. Обобщенная схема асимметричной криптосистемы с открытым ключом.



Защита информации в асимметричной криптосистеме основана на секретности ключа . У. Диффи и М. Хеллман сформулировали требования, выполнение которых обеспечивает безопасность асимметричной криптосистемы:



* вычисление пары ключей (,) получателем В на основе начального условия должно быть простым;



* отправитель А, зная открытый ключ , и сообщение , может легко вычислить криптограмму



* получатель В, используя секретный ключ и криптограмму , может легко восстановить исходное сообщение



* противник, зная открытый ключ , при попытке вычислить секретный ключ наталкивается на непреодолимую вычислительную проблему;



* противник, зная пару (,), при попытке вычислить исходное сообщение наталкивается на непреодолимую вычислительную проблему.



1.8 Однонаправленные функции

Концепция асимметричных криптографических систем с открытым ключом основана на применении однонаправленных функций. Пусть и некоторые произвольные множества.Функции является однонаправленной, если для всех можно легко вычислить функцию , где .



И в то же время для большинства достаточно сложно получить значение , такое, что (при этом полагают, что существует по крайней мере одно такое значение ). Основным критерием отнесения функции к классу однонаправленных функций является отсутствие эффективных алгоритмов обратного преобразования .



Функция относится к классу однонаправленных функций с "потайным ходом" в том случае, если она является однонаправленной и, кроме того, возможно эффективное вычисление обратной функции, если известен "потайной ход" (секретное число, строка или другая информация, ассоциирующаяся с данной функцией).



1.9 Электронно-цифровая подпись

Проблема аутентификации данных и электронная цифровая подпись

При обмене электронными документами по сети связи существенно снижаются затраты на обработку и хранение документов, убыстряется их поиск.

Целью аутентификации электронных документов является их защита от возможных видов злоумышленных действий, к которым относятся:

* активный перехват - нарушитель, подключившийся к сети, перехватывает документы (файлы) и изменяет их;
* маскарад - абонент С посылает документ абоненту В от имени абонента А;
* ренегатство - абонент А заявляет, что не посылал сообщения абоненту В, хотя на самом деле послал;
* подмена - абонент В изменяет или формирует новый документ и заявляет, что получил его от абонента А;
* повтор - абонент С повторяет ранее переданный документ, который абонент А посылал абоненту В.

Электронная цифровая подпись используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. Функционально она аналогична обычной рукописной подписи и обладает ее основными достоинствами:

* удостоверяет, что подписанный текст исходит от лица, поставившего подпись;
* не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом;
* гарантирует целостность подписанного текста.

Цифровая подпись представляет собой относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом.

Система ЭЦП. включает две процедуры:

1. Процедуру постановки подписи;
2. Процедуру проверки подписи.

В процедуре постановки подписи используется секретный ключ отправителя сообщения, в процедуре проверки подписи - открытый ключ отправителя.

При формировании ЭЦП отправитель прежде всего вычисляет хеш-функцию h(М) подписываемого текста М. Вычисленное значение хеш-функции h(М) представляет собой один короткий блок информации m, характеризующий весь текст М в целом. Затем число m шифруется секретным ключом отправителя. Получаемая при этом пара чисел представляет собой ЭЦП для данного текста М.

При проверке ЭЦП получатель сообщения снова вычисляет хеш-функцию m = h(М) принятого по каналу текста М, после чего при помощи открытого ключа отправителя проверяет, соответствует ли полученная подпись вычисленному значению m хеш-функции.

Принципиальным моментом в системе ЭЦП является невозможность подделки ЭЦП пользователя без знания его секретного ключа подписи.

В качестве подписываемого документа может быть использован любой файл. Подписанный файл создается из неподписанного путем добавления в него одной или более электронных подписей.

Каждая подпись содержит следующую информацию:

1. Дату подписи;
2. Срок окончания действия ключа данной подписи;
3. Информацию о лице, подписавшем файл (Ф.И.О., должность, краткое наименование фирмы);
4. Идентификатор подписавшего (имя открытого ключа);
5. Собственно цифровую подпись.

1.10 Однонаправленные хеш-функции

Хеш-функция предназначена для сжатия подписываемого документа до нескольких десятков или сотен бит. Хеш-функция h(-) принимает в качестве аргумента сообщение (документ) М произвольной длины и возвращает хеш-значение фиксированной длины. Обычно хешированная информация является сжатым двоичным представлением основного сообщения произвольной длины. Следует отметить, что значение хеш-функции сложным образом зависит от документа и не позволяет восстановить сам документ .



Хеш-функция должна удовлетворять целому ряду условий:

* хеш-функция должна быть чувствительна к всевозможным изменениям в тексте М, таким как вставки, выбросы, перестановки и т.п.;
* хеш-функция должна обладать свойством необратимости, то есть задача подбора документа , который обладал бы требуемым значением хеш-функции, должна быть вычислительно неразрешима;



* вероятность того, что значения хеш-функции двух различных документов (вне зависимости от их длин) совпадут, должна быть ничтожно мала.

Большинство хеш-функции строится на основе однонаправленной функции f(-), которая образует выходное значение длиной n при задании двух входных значений длиной n. Этими входами являются блок исходного текста m и хеш-значение предыдущего блока текста (рис.8):

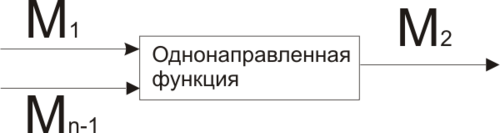


Рис. 8. Построение однонаправленной хеш-функции.

Хеш-значение, вычисляемое при вводе последнего блока текста, становится хеш-значением всего сообщения М.

В результате однонаправленная хеш-функция всегда формирует выход фиксированной длины n (независимо от длины входного текста).

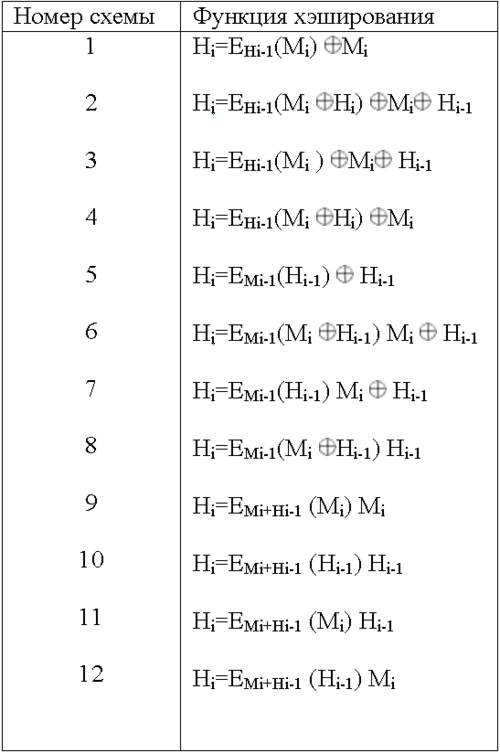
1.11 Однонаправленные хеш-функции

на основе симметричных блочных алгоритмов

Однонаправленную хеш-функцию можно построить, используя симметричный блочный алгоритм. Наиболее очевидный подход состоит в том, чтобы шифровать сообщение М посредством блочного алгоритма в режиме СВС или СFВ с помощью фиксированного ключа и некоторого вектора инициализации, Последний блок шифр текста можно рассматривать в качестве хеш-значения сообщения М. При таком подходе не всегда возможно построить безопасную однонаправленную хеш-функцию, но всегда можно получить код аутентификации сообщения MAC (Message Authentication Code).

Более безопасный вариант хеш-функции можно получить, используя блок сообщения в качестве ключа, предыдущее хеш-значение - в качестве входа, а текущее хеш-значение - в качестве выхода. Реальные хеш-функции проектируются еще более сложными. Длина блока обычно определяется длиной ключа, а длина хеш-значения совпадает с длиной блока. Поскольку большинство блочных алгоритмов являются 64-битовыми, некоторые схемы хеширования проектируют так, чтобы хеш-значение имело длину, равную двойной длине блока.

Табл. 1. Схема безопасного хеширования, у которых длина хеш-значения равна длине блока



Первые четыре схемы хеширования, являющиеся безопасными при всех атаках, приведены на рис. 9.

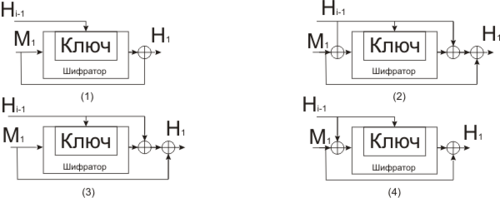


Рис. 9. Четыре схемы безопасного хеширования.

2. ОБЪЕКТЫ И СРЕДСТВА ИССЛЕДОВАНИЯ

Объектами исследования являются алгоритмы шифрования, алгоритмы электронной цифровой подписи и соответствующие стандарты.

2.1 Результаты работы

Отчет должен содержать:

1) постановку задачи;

2) описание работы алгоритма, системы;

3) структурную схему работы алгоритма, системы;

4) листинг;

5) тестовые примеры (входные и выходные данные).

2.2 Варианты заданий для выполнения лабораторной работы

|  |  |
| --- | --- |
|  | Реализация алгоритма Ривеста. |
|  | Реализация алгоритма DES – общий. |
|  | Реализация алгоритма DES – режим сцепления блоков в СВС шифре. |
|  | Реализация алгоритма DES – режим работы ECB (электронный блокнот). |
|  | Реализация алгоритма DES – режим работы CFB – обратная связь по шифротексту. |
|  | Реализация алгоритма DES – OFB – обратная связь по выходу. |
|  | Алгоритм формирования ключей в процессе функционирования DES. |
|  | Алгоритм федерального стандарта х9.9. |
|  | Алгоритм криптографического преобразования – общий. |
|  | Алгоритм криптографического преобразования в режиме простой замены. |
|  | Алгоритм криптографического преобразования в режиме гаммирования. |
|  | Алгоритм криптографического преобразования в режиме гаммирования с обратной связью |
|  | Алгоритм криптографического преобразования в режиме имитовставки. |
|  | Алгоритм RSA – общий. |
|  | Алгоритм, основанный на схеме шифрования Эль Гамаля. |
|  | Алгоритм, основанный на комбинированном методе шифрования |
|  | Алгоритм, основанный на комбинированном методе шифрования (симметричные системы с секретном ключом + ассиметричные системы с открытым ключом) – общий. |
|  | Алгоритм открытого распределения ключей Диффи-Хеллмана |
|  | Алгоритм на основе протокола Kerberos (Цербер) с применением алгоритма DES и других. |
|  | Алгоритм цифровой подписи RSA. |
|  | Алгоритм цифровой подписи DSA. |
|  | Отечественный стандарт цифровой подписи ГОСТ Р34.10-94 (близок к алгоритму DSA). |
|  | Алгоритм цифровой подписи с дополнительными функциями по схеме «слепой подписи». |
|  | Алгоритм цифровой подписи с дополнительными функциями по схеме «неоспоримой подписи». |
|  | Реализация модели защиты ОС – Харрисона-Руззо-Ульмана (модель доступа к данным). |
|  | Реализация матричной модели доступа. |

2.3 Контрольные вопросы

* + - 1. Концепция криптосистем с открытым ключом. Однонаправленные функции.
      2. Особенности симметричных криптосистем.
      3. Модель доступа к данным при защите ОС.
      4. Электронная цифровая подпись
      5. Алгоритмы электронной цифровой подписи
      6. Проблемы аутентификации данных и электронная цифровая подпись.
      7. Управление криптографическими ключами.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Защита информации в персональных ЭВМ/ А.В. Спесивцев, В.А. Вернер, А.Ю. Крутяков и др..- М.: Радио и связь, 1993 г.
2. Теоретические основы компьютерной безопасности. Уч. Пособие для вузов по спец. "Компьютерная безопасность", "Компьютерное обеспечение информационной безопасности автоматизированных систем"/ П.Н. Девытин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербатов. – М.: Радио и связь.2000 – 190 с.
3. Основы информационной безопасности. Учебное пособие для вузов/Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов – М.: Горячая линия – Телеком, 2006-544 с.
4. Введение в защиту информации в автоматизированных системах: Учебное пособие для вузов. – 2-е издание. – М.: Горячая линия – Телеком, 2004-147 с.