ЧАСТЬ 3. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

10. ОСНОВНЫЕ ПРИНЦИПЫ КРИПТОГРАФИЧЕСКОЙ ЗАШИТЫ ИНФОРМАЦИИ

10.1 Понятие криптографии

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: ***проблему 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).

Обобщенная схема криптографической системы, обеспечивающей шифрование передаваемой информации, показана на рисунке 10.1.

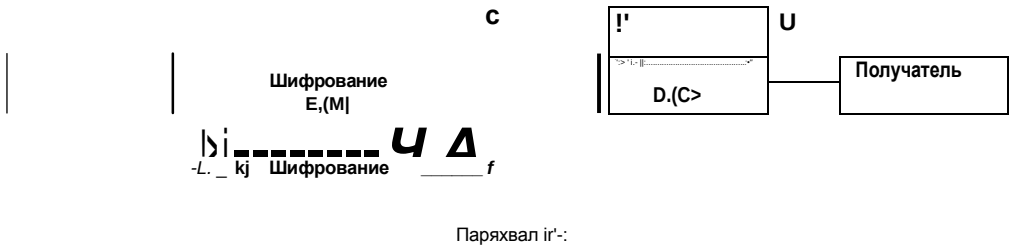

Рис. 10.1 - Обобщенная схема криптосистемы

Отправитель генерирует ***открытый текст*** исходного сообщения *M,* 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 *M,* отправитель шифрует его с помощью обратимого преобразования $E_к$ и получает ***шифртекст*** (или ***криптограмму***) $C = E_K (M)$, который отправляет получателю.

Законный получатель, приняв шифртекст С, расшифровывает его с помощью обратного преобразования $D = E_K^{-1}$ и получает исходное сообщение в виде открытого текста *M:*

$$D_k(C^{\wedge} = E_k^{1} (E_k (M)) = M$$

Преобразование $E_к$ выбирается из семейства криптографических преобразований, называемых ***криптоалгоритмами****. Параметр, с помощью которого выбирается отдельное используемое преобразование, называется* ***криптографическим ключом К.***

Криптосистема имеет разные варианты реализации: набор инструкций, аппаратные средства, комплекс программ компьютера, которые позволяют

зашифровать открытый текст и расшифровать шифртекст различными способами.

Формально, ***криптографическая система*** *- это однопараметрическое семейство* $(E_k)_{k\&k}$ *обратимых преобразований вида:*

$$E_k : M \rightarrow C$$

из пространства М сообщений открытого текста в пространство С шифрованных текстов. Параметр ***К*** *(ключ) выбирается из конечного множества К , называемого* ***прост ранством ключей.***

Шифр *(в соответствии со стандартом ГОСТ 28147-89) - совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом криптографического преобразования.*

Общая классификация алгоритмов шифрования представлена на рис. 10.2.

Рис. 10.2 - Общая классификация алгоритмов шифрования

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

Криптостойкость *- основная характеристика шифра является, 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:

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

В той или иной мере этим требованиям отвечает:

- ***Шифрование перестановкой*** *заключается в том, что символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста.* При достаточной длине блока, в 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 шифруемого текста складываются с символами некоторой случайной последовательности, именуемой* ***гаммой-шифром.*** 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.

10.2 Понятия о симметричных и асимметричных криптосистемах

В общем случае шифрование может быть симметричным или асимметричным относительно преобразования расшифрования, что определяет два класса криптосистем:

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

Схема симметричной криптосистемы с одним секретным ключом была показана на рис. 10.1. В ней используются одинаковые секретные ключи в блоке шифрования и блоке расшифрования.

Обобщенная схема асимметричной криптосистемы с двумя разными ключами K_1 и K_2 показана на рис. 10.3. В этой криптосистеме один из ключей является открытым, а другой - секретным.

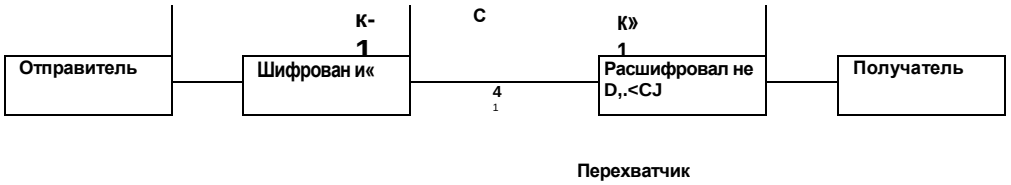

Рис. 10.3 - Обобщенная схема асимметричной криптосистемы с открытым ключом

В симметричной криптосистеме секретный ключ надо передавать отправителю и получателю по защищенному каналу распространения ключей, например такому, как курьерская служба. На рис. 10.1 этот канал показан «экранированной» линией. *В асимметричной криптосистеме передают по незащищенному каналу только открытый ключ, а секретный ключ сохраняют на месте его генерации.*

10.3 Понятие криптоанализа

Криптоанализ - *это наука о раскрытии исходного текста зашифрованного сообщения без доступа к ключу.* Успешный анализ может раскрыть исходный текст или ключ. Он позволяет также обнаружить слабые места в криптосистеме, что, в конечном счете, ведет к тем же результатам.

Фундаментальное правило криптоанализа (впервые сформулированное голландцем А. Керкхоффом еще в XIX веке) ***заключается в том, что стойкость шифра (криптосистемы) должна определяться только секретностью ключа***. Иными словами, правило Керкхоффа состоит в том, что весь алгоритм шифрования, кроме значения секретного ключа, известен криптоаналитику противника. Это обусловлено тем, что криптосистема, реализующая семейство криптографических преобразований, обычно рассматривается как открытая система. Такой подход отражает очень важный принцип технологии защиты информации: защищенность системы не должна зависеть от секретности чего-либо такого, что невозможно быстро изменить в случае утечки секретной информации.

Другое почти общепринятое допущение в криптоанализе состоит в том, что криптоаналитик имеет в своем распоряжении шифртексты сообщений.

Криптоаналитическая атака - *любая попытка со стороны перехватчика расшифровать шифртекст С для получения открытого текста М или зашифровать свой собственный текст М' для получения правдоподобного шифртекста С', не имея подлинного ключа.*

На рис. 10.4 показан поток информации в криптосистеме в случае активных действий перехватчика. Активный перехватчик не только

считывает все шифртексты, передаваемые по каналу, но может также пытаться изменять их по своему усмотрению.

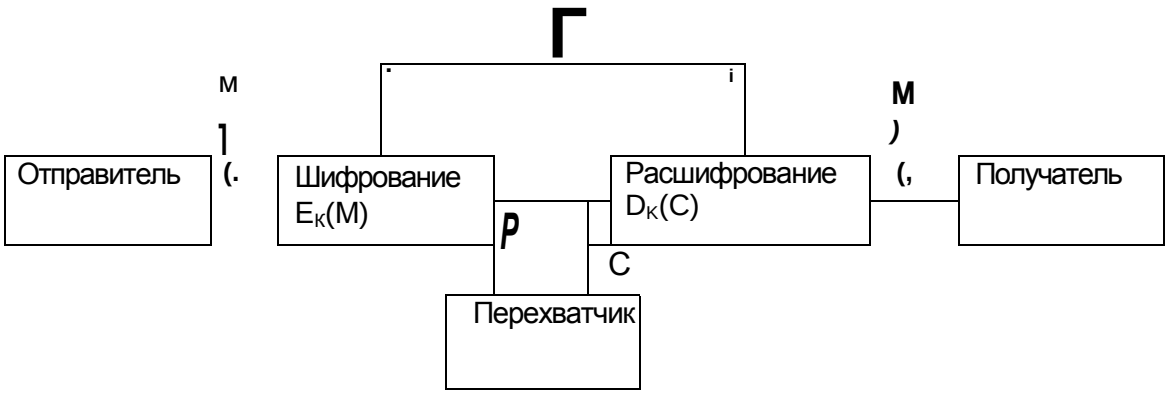

Рис. 10.4 - Поток информации в криптосистеме при активном перехвате сообщений

Если предпринятые криптоаналитические атаки не достигают поставленной цели и криптоаналитик не может, не имея подлинного ключа, вывести M из C или C' из M', то полагают, что такая криптосистема является ***криптостойкой.***

Существует четыре основных типа криптоаналитических атак (все они формулируются в предположении, что криптоаналитику известны применяемый алгоритм шифрования и шифртексты сообщений):

- ***Криптоаналитическая атака при наличии только известного шифртекста.*** Криптоаналитик имеет только шифртексты C_1, C_2, ..., C_i нескольких сообщений, причем все они зашифрованы с использованием одного и того же алгоритма шифрования E_K. Работа криптоаналитика заключается в том, чтобы раскрыть исходные тексты M_1, M_2, ..., M_i по возможности большинства сообщений или, еще лучше, вычислить ключ K, использованный для шифрования этих сообщений, с тем, чтобы расшифровать и другие сообщения, зашифрованные этим ключом.
- ***Криптоаналитическая атака при наличии известного открытого текста.*** Криптоаналитик имеет доступ не только к шифртекстам C_1, C_2, ..., C_i нескольких сообщений, но также к открытым текстам M_1, M_2, ..., M_i этих сообщений. Его работа заключается в нахождении ключа K, используемого при шифровании этих сообщений, или алгоритма расшифрования D_K любых новых сообщений, зашифрованных тем же самым ключом.
- ***Криптоаналитическая атака при возможности выбора открытого текста.*** Криптоаналитик не только имеет доступ к шифртекстам C_1, C_2, ..., C_i и связанным с ними открытым текстам нескольких сообщений, но и может по желанию выбирать открытые тексты, которые затем получает в зашифрованном виде. Такой

криптоанализ получается более мощным по сравнению с криптоанализом с известным открытым текстом, потому что криптоаналитик может выбрать для шифрования такие блоки открытого текста, которые дадут больше информации о ключе. Работа криптоаналитика состоит в поиске ключа K, использованного для шифрования сообщений, или алгоритма расшифрования D_K новых сообщений, зашифрованных тем же ключом. - ***Криптоаналитическая атака с адаптивным выбором открытого текста.*** Это особый вариант атаки с выбором открытого текста. Криптоаналитик может не только выбирать открытый текст, который затем шифруется, но и изменять свой выбор в зависимости от результатов предыдущего шифрования. При криптоанализе с простым выбором открытого текста криптоаналитик обычно может выбирать несколько крупных блоков открытого текста для их шифрования; при криптоанализе с адаптивным выбором открытого текста он имеет возможность выбрать сначала более мелкий пробный блок открытого текста, затем выбрать следующий блок в зависимости от результатов первого выбора, и т.д. Эта атака предоставляет криптоаналитику еще больше возможностей, чем предыдущие типы атак.

Кроме перечисленных основных типов криптоаналитических атак, можно отметить, по крайней мере, еще два типа:

1. ***Криптоаналитическая атака с использованием выбранного шифртекста.*** Криптоаналитик может выбирать для расшифрования различные шифртексты $C_1, C_2, ..., C_i$ и имеет доступ к расшифрованным открытым текстам $M_1, M_2, ..., M_i$. Например, криптоаналитик получил доступ к защищенному от несанкционированного вскрытия блоку, который выполняет автоматическое расшифрование. Работа криптоаналитика заключается в нахождении ключа. Этот тип криптоанализа представляет особый интерес для раскрытия алгоритмов с открытым ключом.
2. ***Криптоаналитическая атака методом полного перебора всех возможных ключей.*** Эта атака предполагает использование криптоаналитиком известного шифртекста и осуществляется посредством полного перебора всех возможных ключей с проверкой, является ли осмысленным получающийся открытый текст. Такой подход требует привлечения предельных вычислительных ресурсов и иногда называется силовой атакой.

10.4 Аппаратно-программные криптографические средства защиты информации

Аппаратно-программные средства, обеспечивающие повышенный уровень защиты, можно разбить на пять основных групп (рис. 10.4).

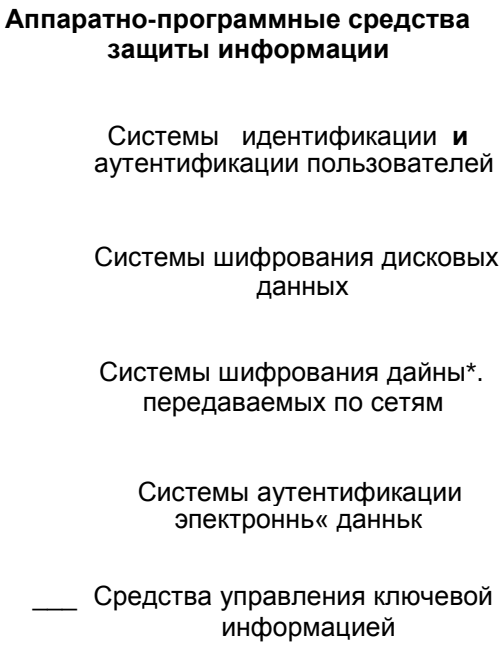

Рис. 10.5 - Аппаратно-программные средства защиты компьютерной информации

10.4.1 Системы идентификации и аутентификации пользователей

Системы идентификации и аутентификации пользователей *применяются для ограничения доступа случайных и незаконных пользователей к ресурсам компьютерной системы. Общий алгоритм работы этих систем заключается в том, чтобы получить от пользователя информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить (или не предоставить) этому пользователю возможность работы с системой.*

При построении подобных систем возникает проблема выбора информации, на основе которой осуществляются процедуры идентификации и аутентификации пользователя. Можно выделить следующие типы:

- секретная информация, которой обладает пользователь (пароль, персональный идентификатор, секретный ключ и т.п.); эту информацию пользователь должен запомнить или же могут быть применены специальные средства хранения этой информации;
- физиологические параметры человека (отпечатки пальцев, рисунок радужной оболочки глаза и т.п.) или особенности поведения человека (особенности работы на клавиатуре и т. п.).

Системы идентификации, основанные на первом типе информации, принято считать *традиционными.* Системы идентификации, использующие второй тип информации, называются *биометрическими.*

10.4.2 Системы шифрования дисковых данных

Вторую группу средств, обеспечивающих повышенный уровень защиты, составляют *системы шифрования дисковых данных.* ***Основная задача, решаемая такими системами, состоит в защите от несанкционированного использования данных, расположенных на магнитных носителях.***

Обеспечение конфиденциальности данных, располагаемых на магнитных носителях, осуществляется путем их шифрования с использованием симметричных алгоритмов шифрования. Основным классификационным признаком для комплексов шифрования служит уровень их встраивания в компьютерную систему.

Работа прикладных программ с дисковыми накопителями состоит из двух этапов

1. ***Логический этап*** соответствует уровню взаимодействия прикладной программы с операционной системой (например, вызов сервисных функций чтения/записи данных). На этом уровне основным объектом является файл.
2. ***Физический этап*** соответствует уровню взаимодействия операционной системы и аппаратуры. В качестве объектов этого уровня выступают структуры физической организации данных - сектора диска.

В результате системы шифрования данных могут осуществлять криптографические преобразования данных на уровне файлов (защищаются отдельные файлы) и на уровне дисков (защищаются диски целиком).

Другим классификационным признаком систем шифрования дисковых данных является способ их функционирования. По способу функционирования системы шифрования дисковых данных делят на два класса:

1. **системы «прозрачного» шифрования**, в которых криптографические преобразования осуществляются в режиме реального времени, незаметно для пользователя. Например, пользователь записывает подготовленный в текстовом редакторе документ на защищаемый диск, а система защиты в процессе записи выполняет его шифрование.
2. **системы, специально вызываемые для осуществления шифрования**. Как правило, это утилиты, которые необходимо специально вызывать для выполнения шифрования. К ним относятся, например, архиваторы со встроенными средствами парольной защиты.

10.4.3 Системы шифрования данных

К третьей группе средств, обеспечивающих повышенный уровень защиты, относятся *системы шифрования данных, передаваемых по компьютерным сетям.*

Различают два основных способа шифрования:

1. *канальное шифрование*
2. *оконечное (абонентское) шифрование.*

В случае ***канального шифрования*** *защищается вся передаваемая по каналу связи информация, включая служебную.* Соответствующие процедуры шифрования реализуются с помощью протокола канального уровня семиуровневой эталонной модели взаимодействия открытых систем OSI (Open System Interconnection).

Способ *канального шифрования* обладает следующим достоинством - встраивание процедур шифрования на канальный уровень позволяет использовать аппаратные средства, что способствует повышению производительности системы.

Однако, у данного подхода имеются существенные недостатки:

- шифрованию на данном уровне подлежит вся информация, включая служебные данные транспортных протоколов; это осложняет механизм маршрутизации сетевых пакетов и требует расшифрования данных в устройствах промежуточной коммутации (шлюзах, ретрансляторах и т.п.);
- шифрование служебной информации, неизбежное на данном уровне, может привести к появлению статистических закономерностей в шифрованных данных; это влияет на надежность защиты и накладывает ограничения на использование криптографических алгоритмов.

Оконечное (абонентское) шифрование *позволяет обеспечить конфиденциальность данных, передаваемых между двумя прикладными объектами (абонентами).* Оконечное шифрование реализуется с помощью протокола прикладного или представительного уровня эталонной модели OSI. В этом случае защищенным оказывается только содержание сообщения, вся служебная информация остается открытой. Данный способ позволяет избежать проблем, связанных с шифрованием служебной информации, но при этом возникают другие проблемы. В частности, злоумышленник, имеющий доступ к каналам связи компьютерной сети, получает возможность анализировать информацию о структуре обмена сообщениями, например об отправителе и получателе, о времени и условиях передачи данных, а также об объеме передаваемых данных.

10.4.4 Системы аутентификации электронных данных

При обмене электронными данными по сетям связи возникает проблема ***аутентификации*** - *т.е. установление подлинности автора документа и проверка отсутствия изменений в полученном документе.*

Для аутентификации электронных данных применяют:

- код аутентификации сообщения (имитовставку);
- электронную цифровую подпись.

При формировании кода аутентификации сообщения и электронной цифровой подписи используются разные типы систем шифрования.

Код аутентификации сообщения формируют с помощью симметричных систем шифрования данных. В частности, симметричный алгоритм шифрования данных DES при работе в режиме сцепления блоков шифра CBC позволяет сформировать с помощью секретного ключа и начального вектора IV код аутентификации сообщения MAC (Message Authentication Code). Проверка целостности принятого сообщения осуществляется путем проверки кода MAC получателем сообщения.

Аналогичные возможности предоставляет отечественный стандарт симметричного шифрования данных ГОСТ 28147-89. В этом алгоритме предусмотрен режим выработки имитовставки, обеспечивающий *имитозащиту,* т.е. защиту системы шифрованной связи от навязывания ложных данных.

Имитовставка вырабатывается из открытых данных посредством специального преобразования шифрования с использованием секретного ключа и передается по каналу связи в конце зашифрованных данных. Имитовставка проверяется получателем сообщения, владеющим секретным ключом, путем повторения процедуры, выполненной ранее отправителем, над полученными открытыми данными.

Электронная цифровая подпись **(ЭЦП)** представляет собой относительно небольшое количество дополнительной аутентифи-цирующей цифровой информации, передаваемой вместе с подписываемым текстом. Для реализации ЭЦП используются принципы асимметричного шифрования. Система ЭЦП включает процедуру формирования цифровой подписи отправителем с использованием секретного ключа отправителя и процедуру проверки подписи получателем с использованием открытого ключа отправителя.

10.4.5 Средства управления ключевой информацией

Пятую группу средств, обеспечивающих повышенный уровень защиты, *образуют средства управления ключевой информацией.*

Под ключевой информацией понимается *совокупность всех используемых в компьютерной системе или сети криптографических*

ключей. Безопасность любого криптографического алгоритма определяется используемыми криптографическими ключами. В случае ненадежного управления ключами злоумышленник может завладеть ключевой информацией и получить полный доступ ко всей информации в компьютерной системе или сети.

Основным классификационным признаком средств управления ключевой информацией является вид функции управления ключами. Различают следующие основные виды функций управления ключами:

1. генерация ключей;
2. хранение ключей;
3. распределение ключей.

Способы *генерации ключей* различаются для симметричных и асимметричных криптосистем.

Для генерации ключей симметричных криптосистем используются аппаратные и программные средства генерации случайных чисел.

Генерация ключей для асимметричных криптосистем представляет существенно более сложную задачу в связи с необходимостью получения ключей с определенными математическими свойствами.

Функция *хранения ключей* предполагает организацию безопасного хранения, учета и удаления ключей. Для обеспечения безопасного хранения и передачи ключей применяют их шифрование с помощью других ключей. Такой подход приводит к *концепции иерархии ключей.* В иерархию ключей обычно входят главный ключ (мастер-ключ), ключ шифрования ключей и ключ шифрования данных. Следует отметить, что генерация и хранение мастер-ключей являются критическими вопросами криптографической защиты.

Распределение ключей является самым ответственным процессом в управлении ключами. Этот процесс должен гарантировать скрытность распределяемых ключей, а также оперативность и точность их распределения.

Различают два основных способа распределения ключей между пользователями компьютерной сети:

1. применение одного или нескольких центров распределения ключей;
2. прямой обмен сеансовыми ключами между пользователями.