**3. Основы построения криптосистем**

Для защиты информации в каналах связи используются два вида шифрования: линейное (канальное) и абонентское.

Линейное шифрование производится на выходе узла связи, расшифрование - на входе узла связи. При этом используются поточные шифры и между узлами поддерживается сплошной поток битов шифрованного текста. Шифруется и заголовок, и информационная часть пакетов. Все это затрудняет анализ потоков сообщений, так как адреса источника и получателя зашифрованы, непрерывность трафика обеспечивается передачей пустых (незначащих) сообщений. При линейном шифровании трафик уязвим только в узлах связи, так как там информация обрабатывается в открытом виде, поэтому узлы связи должны быть хорошо защищены.

При абонентском шифровании каждое сообщение шифруется в его источнике и расшифровывается только получателем, при этом используется ключ, известный только этой паре абонентов. Сообщение, зашифрованное абонентом, может еще подвергаться и линейному шифрованию. Таким образом, абонентское шифрование обеспечивает конфиденциальность передаваемого сообщения, линейное - конфиденциальность, защиту трафика от анализа.

**Криптография** – это наука о методах, алгоритмах, программных и аппаратных средствах преобразования информации в целях сокрытия ее содержания, предотвращения видоизменения или несанкционированного использования.

Обобщенная схема криптографической системы, обеспечивающей шифрование передаваемой информации, имеет вид (рисунок 5.2).

|  |
| --- |
| Рисунок 5.2. – Обобщенная схема симметричной криптографической системы |

Отправитель генерирует открытый текст исходного сообщения , которое должно передаваться по открытому каналу. Отправитель шифрует текст с помощью обратимого преобразования  и ключа :  и получает шифротекст , который отправляет получателю. Получатель, приняв шифротекст , расшифровывает его с помощью обратного преобразования  и получает исходное сообщение в виде открытого текста :.

Преобразование  выбирается из семейства криптографических преобразований, называемых **криптоалгоритмами**. Параметр, с помощью которого выбирается конкретное преобразование, называется **криптографическим ключом** . Система, в которой осуществляется шифрование и расшифрование сообщений, называется **криптосистемой***.*

Формально криптосистема – это однопараметрическое семейство  обратимых преобразований  из пространства  сообщений открытого текста в пространство  шифрованных текстов. Параметр  (ключ) выбирается из конечного множества , называемого пространством ключей. Криптосистема может иметь разные варианты реализации: набор инструкций; аппаратные или программные средства; аппаратно-программные средства.

Вообще говоря, преобразование шифрования может быть симметричным или асимметричным относительно преобразования расшифрования. Поэтому различают два класса криптосистем: симметричные криптосистемы и асимметричные криптосистемы. Иногда их называют: одноключевые (с секретным ключом) и двухключевые (с открытым ключом). Схема симметричной криптосистемы с одним секретным ключом  была показана на рисунок 5.2. Обобщенная схема асимметричной криптосистемы с двумя разными ключами  и  показана на рисунок 5.3.

В этой криптосистеме один из ключей является открытым , а другой  – секретным. Для этой криптосистемы , а .

|  |
| --- |
| Рисунок 5.3. – Обобщенная схема асимметричной криптографической системы |

В симметричной криптосистеме секретный ключ надо передавать отправителю и получателю по защищенному каналу распространения ключей, например, спецсвязью. В асимметричной криптосистеме передают по незащищенному каналу только открытый ключ, а секретный ключ сохраняют в месте его генерации.

Злоумышленник при атаке на криптосистему может не только считывать шифротексты, передаваемые по каналу связи, но и пытаться их изменить по своему усмотрению.

Любая попытка со стороны злоумышленника расшифровать шифротекст  для получения открытого текста  или зашифровать свой собственный текст  для получения правдоподобного шифротекста , не имея подлинного ключа, называется криптоатакой.

Свойство криптосистемы, противостоять криптоатаке называется криптостойкостью. Оно измеряется в затратах злоумышленника, которые он несет, вскрывая криптосистему. Например, криптостойкость может выражаться в количестве машинного времени, затраченного на вскрытие криптосистемы.

Фундаментальное правило криптоанализа заключается в том, что стойкость шифра (криптосистемы) должна определяться только секретностью ключа. 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.

Эффективными системами криптографической защиты данных являются асимметричные криптосистемы, называемые также криптосистемами с открытым ключом. В таких системах для шифрования данных используется один ключ, а для расшифрования другой (отсюда и название - асимметричные). Первый ключ является открытым и может быть опубликован для использования всеми пользователями системы, которые зашифровывают данные. Расшифрование данных с помощью открытого ключа невозможно. Для расшифровывания данных получатель шифрованной информации использует второй ключ, который является секретным. Разумеется, ключ расшифровывания не может быть определен из ключа шифрования.

Обобщенная схема асимметричной криптосистемы с открытым ключом показана на рисунок 5.4.

|  |
| --- |
| Рисунок 5.4. – Обобщенная схема асимметричной криптосистемы с открытым ключом |

В этой криптосистеме применяют два различных ключа: - открытый ключ отправителя А; - секретный ключ получателя В. Генератор ключа целесообразно располагать на стороне получателя В (чтобы не пересылать секретный ключ  по незащищенному каналу). Значения ключей ,  – зависят от начального состояния генератора ключей.

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

Характерные особенности асимметричных криптосистем:

1. Открытый ключ  и криптограмма С могут быть отправлены по незащищенному каналу, т.е. могут быть известны противнику.
2. Алгоритмы шифрования  и расшифрования  являются открытыми.
3. Защита информации в асимметричной криптосистеме основана на секретности ключа .

У.Диффи и М.Хелман сформулировали требования, выполнение которых обеспечивает безопасность асимметричной криптосистемы:

1. Вычисление пары ключей  получателем В на основе начального условия должно быть простым.
2. Отправитель А, зная открытый ключ  и сообщение М, может легко вычислить криптограмму .
3. Получатель В, используя секретный ключ  и криптограмму С, может легко восстановить исходное сообщение .
4. Противник, зная открытый ключ , при попытке вычислить секретный ключ  наталкивается на непреодолимую вычислительную проблему.
5. Противник, зная пару , при попытке вычислить исходное сообщение М, наталкивается на непреодолимую вычислительную проблему.

**Последовательность действий абонентов криптосистемы RSA**

**Действия получателя криптограммы В:**

1. В генерирует два произвольных больших простых числа  и . Эти числа должны быть примерно одинаковыми, размерностью 100‑150 десятичных разрядов. Они должны быть секретными.
2. В вычисляет значение модуля  и функции Эйлера  и выбирает значение открытого ключа  с соблюдением условий: , , т.е.  и  должны быть взаимно простыми.
3. В вычисляет значение секретного ключа , используя расширенный алгоритм Евклида: .
4. В посылает А пару чисел  по открытому каналу.

**Действия отправителя криптограммы А:**

1. Разбивает исходный текст  на блоки , , т.е. . Величина .
2. Шифрует каждое число  по формуле  и отправляет криптограмму .

Получатель В, получив криптограмму, расшифровывает каждый блок секретным ключом , , и восстанавливает весь текст .

**Реализуемость и безопасность RSA**

Покажем, что при расшифровании восстанавливается исходный текст. Согласно обобщению Эйлером малой теоремы Ферма: если , то , или . Открытый  и закрытый  ключи в алгоритме связаны соотношением , или  для некоторого целого . Таким образом, процесс шифрования, а затем расшифрования некоторого сообщения  выглядит следующим образом:

.

В процессе применения RSA злоумышленник может иметь: , ,  – и организовать дешифрование двумя способами:

1. По , ,  получить . Для этого он решает задачу вычисления  из уравнения . Эта задача вычислительно трудна.
2. По  вычислить , , затем найти  и вычислить  и дешифровать сообщение .

Однако задача разложения большого числа на простые множители вычислительно сложна.

Пользователи А и В должны быстро осуществлять все вычисления: вычислять , шифровать и расшифровывать.

Вычисление  с использованием алгоритма Евклида ‑ довольно быстрый процесс и не представляет трудности. Шифрование и расшифрование ‑ возведение большого числа в большую степень ‑ требует определенных затрат времени, но, с учетом наличия быстрых алгоритмов и быстродействия современных компьютеров, это приемлемая процедура.

При обмене сообщениями через сети телекоммуникаций возникает задача подтверждения их подлинности (подтверждения авторства и целостности). Такая же проблема существует и при переходе от юридически значимых бумажных документов к электронным. Сообщения, для которых эта проблема актуальна, будем в дальнейшем называть электронными документами.

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.

В обычной (бумажной) информатике эти проблемы решаются за счет того, что информация в документе и рукописная подпись автора жестко связаны с физическим носителем (бумагой). В электронных документах на машинных носителях такой связи нет.

Естественно, что для электронных документов традиционные способы установления подлинности по рукописной подписи и оттиску печати на бумажном документе совершенно непригодны, поэтому для подтверждения подлинности документа используется специфическая криптографическая процедура, называемая электронной цифровой подписью (ЭЦП).

**ЭЦП функционально 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.

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

Технология 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 хэш-функцию  подписываемого документа . Вычисленное значение хэш-функции  представляет собой один короткий блок информации , характеризующий весь документ  в целом. Затем число  «шифруется» секретным ключом отправителя. По­лучаемая при этом пара чисел представляет собой ЭЦП для дан­ного документа . В принципе можно обойтись без предварительного хэширования документа, а «шифровать» весь документ, однако в этом случае придется иметь дело с гораздо большим по размерам файлом. Употребление слова «шифровать» здесь весьма условное и справедливо при использовании алгоритма RSA, для других алгоритмов точнее говорить «преобразовывать».

При проверке ЭЦП получатель сообщения снова вычис­ляет хэш-функцию  принятого по каналу документа , по­сле чего при помощи открытого ключа отправителя проверяет, со­ответствует ли полученная подпись вычисленному значению  хэш-функции.

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

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:

* дату подписи;
* срок окончания действия ключа данной подписи;
* информацию о лице, подписавшем файл (Ф.И.0., должность, краткое наименование фирмы);
* идентификатор подписавшего (имя открытого ключа);
* собственно цифровую подпись.