14. Общие принципы построения современных асимметричных криптосистем. Асимметричные криптоалгоритмы RSA и Рабина

Асимметричные криптосистемы шифрования

Асимметричные криптографические системы были разработаны в 1970-х гг. Принципиальное отличие асимметричной криптосистемы от криптосистемы симметричного шифрования состоит в том, что для шифрования информации и ее последующего расшифровывания **используются различные ключи:**

- открытый ключ К используется для шифрования информации, вычисляется из секретного ключа к;
- секретный ключ к используется для расшифровывания информации, зашифрованной с помощью парного ему открытого ключа К.

Эти ключи различаются таким образом, что с помощью вычислений нельзя вывести секретный ключ к из открытого ключа К. Поэтому открытый ключ К может свободно передаваться по каналам связи.

Асимметричные системы называют также двух ключевыми криптографическими системами, или криптосистемами с открытым ключом.

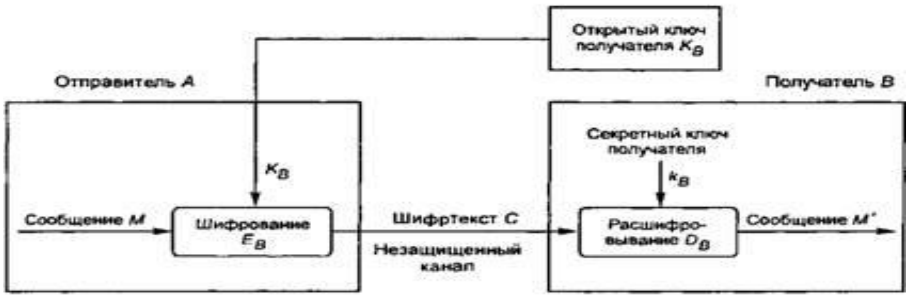

Рис. 5.3. Обобщенная схема асимметричной криптосистемы шифрования

Обобщенная схема асимметричной криптосистемы шифрования с открытым ключом показана на рис. 5.3. Для криптографического закрытия и последующего расшифровывания передаваемой информации используются открытый и секретный ключи получателя В сообщения.

В качестве ключа зашифровывания должен использоваться открытый ключ получателя, а в качестве ключа расшифровывания - его секретный ключ.

Секретный и открытый ключи генерируются попарно. Секретный ключ должен оставаться у его владельца и быть надежно защищен от НСД (аналогично ключу шифрования в симметричных алгоритмах). Копия открытого ключа должна находиться у каждого абонента криптографической сети, с которым обменивается информацией владелец секретного ключа.

Процесс передачи зашифрованной информации в асимметричной криптосистеме осуществляется следующим образом.

Подготовительный этап:

- абонент В генерирует пару ключей: секретный ключ $к_в$ и открытый ключ $К_в$;
- открытый ключ $К_в$ посылается абоненту А и остальным абонентам (или делается доступным, например на разделяемом ресурсе).

Использование — обмен информацией между абонентами А и В:

- абонент А зашифровывает сообщение с помощью открытого ключа $К_в$ абонента В и отправляет шифртекст абоненту В;
- абонент В расшифровывает сообщение с помощью своего секретного ключа $к_в$. Никто другой (в том числе абонент А) не может расшифровать данное сообщение, так как не имеет секретного ключа абонента В. Защита информации в асимметричной криптосистеме основана на секретности ключа $к_в$ получателя сообщения.

Характерные особенности асимметричных криптосистем:

- открытый ключ $К_в$ и криптограмма С могут быть отправлены по незащищенным каналам, т. е. противнику известны $К_в$ и С;

- алгоритмы шифрования и расшифровывания: $E_в : M \rightarrow C$; $D_B : C \rightarrow M$ являются открытыми.

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

1. Вычисление пары ключей ($К_в$, $к_в$) получателем В должно быть простым.
2. Отправитель А, зная открытый ключ $К_в$ и сообщение М, может легко вычислить криптограмму $C=E_{Кв}(M)$.
3. Получатель В, используя секретный ключ $к_в$ и криптограмму С, может легко восстановить исходное сообщение $M=O_{кя}(C)$.
4. Противник, зная открытый ключ $К_в$, при попытке вычислить секретный ключ $к_в$ наталкивается на непреодолимую вычислительную проблему.
5. Противник, зная пару ($К_в$, С), при попытке вычислить исходное сообщение М наталкивается на непреодолимую вычислительную проблему.

Концепция асимметричных криптографических систем с открытым ключом основана на применении однонаправленных функций.

Однонаправленной функцией называется функция F(X), обладающая двумя свойствами:

- существует алгоритм вычисления значений функции Y= F(X);
- не существует эффективного алгоритма обращения (инвертирования) функции F (т. е. не существует решения уравнения F(X) = Y относительно X).

В качестве примера однонаправленной функции можно указать целочисленное умножение. **Прямая задача** — вычисление произведения двух очень больших целых чисел P и Q, т. е. нахождение значения $N = P \times Q$ — относительно несложная задача для компьютера.

Обратная задача — факторизация, или разложение на множители большого целого числа, т. е. нахождение делителей P и Q большого целого числа $N = P \times Q$, — является практически неразрешимой при достаточно больших значениях N.

Другой характерный пример однонаправленной функции — это модульная экспонента с фиксированными основанием и модулем.

Как и в случае симметричных криптографических систем, с помощью асимметричных криптосистем обеспечивается не только конфиденциальность, но также подлинность и целостность передаваемой информации. Подлинность и целостность любого сообщения обеспечивается формированием цифровой подписи этого сообщения и отправкой в зашифрованном виде сообщения вместе с цифровой подписью. Проверка соответствия подписи полученному сообщению после его предварительного расшифровывания представляет собой проверку целостности и подлинности принятого сообщения. Процедуры формирования и проверки электронной цифровой подписи рассмотрены в разделе «Электронная цифровая подпись и функция хеширования».

Преимущества асимметричных криптографических систем перед симметричными криптосистемами:

- в асимметричных криптосистемах решена сложная проблема распределения ключей между пользователями, так как каждый пользователь может сгенерировать свою пару ключей сам, а открытые ключи пользователей могут свободно публиковаться и распространяться по сетевым коммуникациям;
- исчезает квадратичная зависимость числа ключей от числа пользователей; в асимметричной криптосистеме число используемых ключей связано с числом абонентов линейной зависимостью (в системе из N пользователей используются 2Nключей), а не квадратичной, как в симметричных системах;
- асимметричные криптосистемы позволяют реализовать протоколы взаимодействия сторон, которые не доверяют друг другу, поскольку при использовании асимметричных криптосистем закрытый ключ должен быть известен только его владельцу.

Недостатки асимметричных криптосистем:

- на настоящий момент нет математического доказательства необратимости используемых в асимметричных алгоритмах функций;
- асимметричное шифрование существенно медленнее симметричного, поскольку при шифровании и расшифровке используются весьма ресурсоемкие операции. По этой же причине реализовать аппаратный шифратор с асимметричным алгоритмом существенно сложнее, чем реализовать аппаратно - симметричный алгоритм;
- необходимость защиты открытых ключей от подмены.