УДК 004.056.55

СИММЕТРИЧНЫЕ И АСИММЕТРИЧНЫЕ ШИФРЫ

Р.Ю. КАРАБАНОВ
(Представлено: канд. физ.-мат. наук, доц. Ю.Ф. ПАСТУХОВ)

Рассматриваются и сравниваются два самых распространенных типа шифров – симметричные и а симметричные. Выделены их достоинства и недостатки. Для криптографического закрытия и последующего расшифровывания передаваемой информации используются открытый и секретный ключи.

Шифр (от фр. chiffre «цифра» от араб. صِفْر, sifr «ноль») – какая-либо система преобразования текста с секретом (ключом) для обеспечения секретности передаваемой информации. Шифр может представлять собой совокупность условных знаков (условная азбука из цифр или букв) либо алгоритм преобразования обычных цифр и букв.

По количеству используемых ключей шифры разделяются на *симметричные* (используют один ключ для шифрования и дешифрования) и *асимметричные* (используют два различных ключа) [1].

Симметричные шифры

Исторически первыми появились симметричные криптографические системы. В симметричной криптосистеме шифрования используется один и тот же ключ для зашифровывания и расшифровывания информации. Это означает, что любой, кто имеет доступ к ключу шифрования, может расшифровать сообщение.

Соответственно, с целью предотвращения несанкционированного раскрытия зашифрованной информации все ключи шифрования в симметричных криптосистемах должны держаться в секрете. Именно поэтому симметричные криптосистемы называют *криптосистемами с секретным ключом* – ключ шифрования должен быть доступен только тем, кому предназначено сообщение. Симметричные криптосистемы называют еще одноключевыми криптографическими системами, или криптосистемами с закрытым ключом.

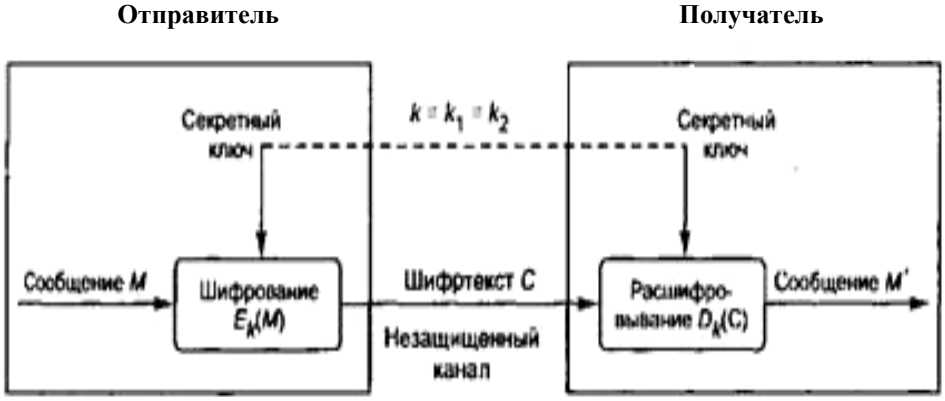

Схема симметричной криптосистемы шифрования

Данные криптосистемы характеризуются наиболее высокой скоростью шифрования, и с их помощью обеспечиваются как конфиденциальность и подлинность, так и целостность передаваемой информации. Конфиденциальность передачи информации с помощью симметричной криптосистемы зависит от надежности шифра и обеспечения конфиденциальности ключа шифрования [2].

С одной стороны, такая схема имеет те недостатки, что необходимо кроме открытого канала для передачи шифрограммы наличие также секретного канала для передачи ключа, а кроме того, при утечке информации о ключе, невозможно доказать, от кого из двух корреспондентов произошла утечка.

С другой стороны, среди шифров именно этой группы есть единственная в мире схема шифровки, обладающая абсолютной теоретической стойкостью. Все прочие можно расшифровать хотя бы в принципе. Такой схемой является обычная шифровка с ключом, длина которого равна длине сообщения. При этом ключ должен использоваться только раз. Любые попытки расшифровать такое сообщение беспо-

лезны, даже если имеется априорная информация о тексте сообщения. Осуществляя подбор ключа, можно получить в результате любое сообщение [3].

Асимметричные шифры

Асимметричные криптографические системы были разработаны в 1970-х годах. 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 двухключевыми криптографическими системами, или криптосистемами с открытым ключом.

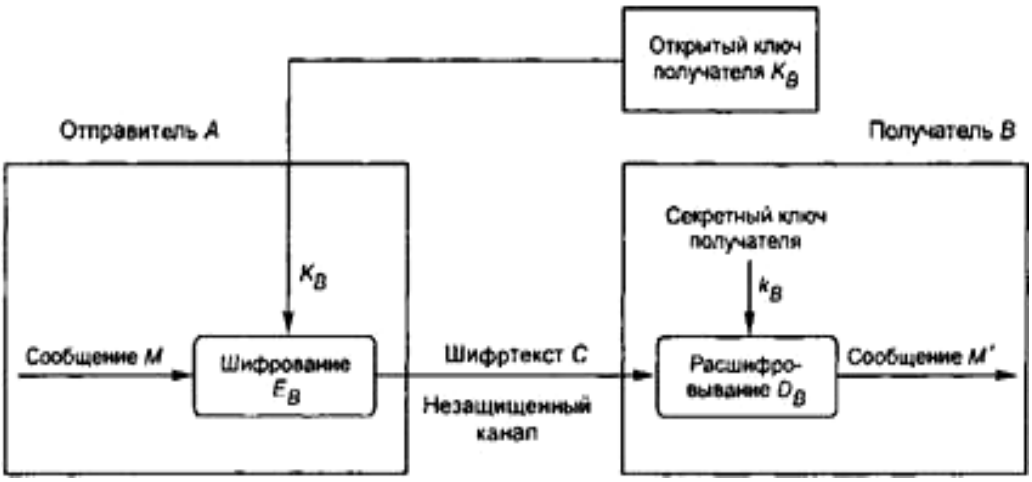

Схема асимметричной криптосистемы шифрования

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 [5].

Сравнение шифров

Достоинства симметричной криптосистемы:

- скорость;
- простота реализации (за счёт более простых операций);
- меньшая требуемая длина ключа для сопоставимой стойкости;
- изученность (за счёт большего возраста);

Недостатки симметричной криптосистемы:

- сложность управления ключами в большой сети;
- сложность обмена ключами. Для применения необходимо решить проблему надёжной передачи ключей каждому абоненту, так как нужен секретный канал для передачи каждого ключа обеим сторонам [6].

Достоинства асимметричной криптосистемы:

- не нужно предварительно передавать секретный ключ по надёжному каналу;
- только одной стороне известен ключ дешифрования, который нужно держать в секрете (в симметричной криптографии такой ключ известен обеим сторонам и должен держаться в секрете обеими);
- в больших сетях число ключей в асимметричной криптосистеме значительно меньше, чем в симметричной.

Недостатки асимметричной криптосистемы:

- в алгоритм сложнее внести изменения;
- более длинные ключи – ниже приведена таблица, сопоставляющая длину ключа симметричного алгоритма с длиной ключа RSA с аналогичной криптостойкостью;
- шифрование-расшифровывание с использованием пары ключей проходит на два-три порядка медленнее, чем шифрование-расшифрование того же текста симметричным алгоритмом;
- требуются существенно бóльшие вычислительные ресурсы, поэтому на практике асимметричные криптосистемы используются в сочетании с другими алгоритмами [5].

ЛИТЕРАТУРА

1. Шифр [Электронный источник]. – 2017. – Режим доступа: https://ru.wikipedia.org/ wiki/% D0% A8% D0%B8%D1%84%D1%80. – Дата доступа: 24.09.2017.
2. Симметричные криптосистемы шифрования [Электронный источник]. – 2017. – Режим доступа: http: //ypn.ru/193/symmetric-encryption-system. – Дата доступа: 24.09.2017.
3. Типы шифров [Электронный источник]. – 2017. – Режим доступа: http://studbooks.net/2243124/informatika/tipy_shifrov. – Дата доступа: 24.09.2017.
4. Асимметричные криптосистемы шифрования [Электронный источник]. – 2017. – Режим доступа: http: //ypn.ru/197/asymmetric-encryption-system/. – Дата доступа: 24.09.2017.
5. Криптосистема с открытым ключом [Электронный источник]. – 2017. – Режим доступа: https: // ru.wikipedia. org/wiki/Криптосистема_с_открытым_ключом. – Дата доступа: 24.09.2017.
6. Симметричные криптосистемы [Электронный источник]. – 2017. – Режим доступа: https: //ru.wikipedia. org/wiki/Симметричные_криптосистемы. – Дата доступа: 24.09.2017.