ФУНКЦИОНАЛЬНАЯ СХЕМА ВЗАИМОДЕЙСТВИЯ УЧАСТНИКОВ СИММЕТРИЧНОГО КРИПТОГРАФИЧЕСКОГО ОБМЕНА. НЕДОСТАТКИ СИММЕТРИЧНЫХ КРИПТОСИСТЕМ

Выполнила:
Аюрова Д.Ч
Проверил:
Тенгайкин Е.А

В *симметричных криптосистемах* (*криптосистемах с секретным ключом*) шифрование и дешифрование информации осуществляется на одном ключе *K*, являющемся секретным. Рассекречивание ключа шифрования ведет к рассекречиванию всего защищенного обмена. Для того, чтобы подчеркнуть факт использования одного и того же ключа в шифраторе источника и дешифраторе получателя сообщений, криптосистемы с секретными ключами называют также *одно ключевыми*.

Симметри́чные криптосисте́мы - способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ. До изобретения схемы асимметричного шифрования единственным существовавшим способом являлось симметричное шифрование. Ключ алгоритма должен сохраняться в секрете обеими сторонами. Алгоритм шифрования выбирается сторонами до начала обмена сообщениями.

Функциональная схема взаимодействия участников симметричного криптографического обмена приведена на рис.

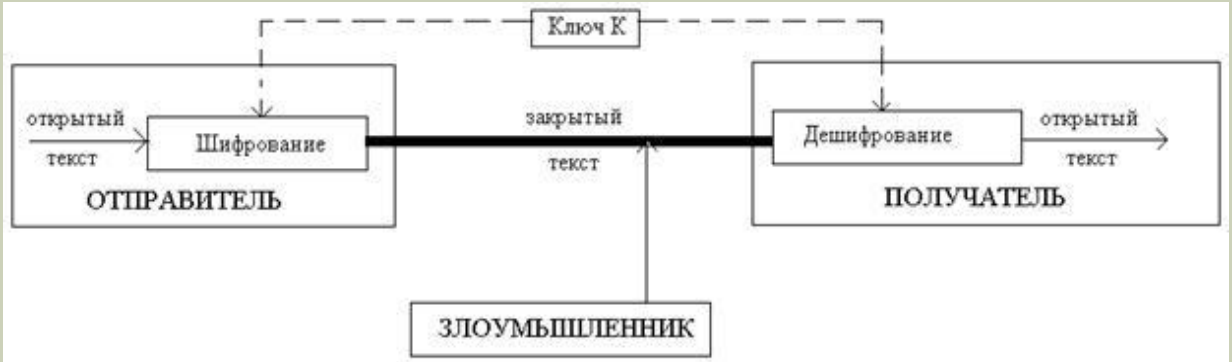

Рис. Функциональная схема симметричной криптосистемы

В симметричной криптосистеме секретный ключ необходимо передать всем участникам криптографической сети по некоторому защищенному каналу.

НЕДОСТАТКИ СИММЕТРИЧНЫХ КРИПТОСИСТЕМ

- К основным недостаткам симметричных криптосистем относят *проблему распространения симметричных ключей* и *проблему их хранения*.
- При использовании симметричных криптосистем для шифрования информации между пользователями криптографической сети необходимо обеспечить безопасную передачу ключей шифрования между всеми доверенными пользователями (участниками криптографического обмена). При этом передача ключа шифрования обязательно должна осуществляться по закрытому каналу, так как перехват злоумышленником данного ключа ведет к компрометации всей криптографической сети, и дальнейшее шифрование информации теряет смысл. Однако наличие закрытого канала связи позволяет передавать и сам открытый текст по данному каналу. Таким образом, необходимость шифрования как бы отпадает. Аргументы вида «ключ шифрования необходимо передавать достаточно редко по сравнению с передачей закрытых сообщений» хотя и приемлемы, но оставляют данную проблему нерешенной.

НЕДОСТАТКИ

- 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

Для компенсации недостатков симметричного шифрования в настоящее время широко применяется комбинированная (гибридная) криптографическая схема, где с помощью асимметричного шифрования передаётся сеансовый ключ, используемый сторонами для обмена данными с помощью симметричного шифрования.

Важным недостатком симметричных шифров является **невозможность** их использования в механизмах формирования электронной цифровой подписи и сертификатов, так как ключ известен каждой стороне.

- Проблема хранения симметричных ключей шифрования заключается в том, что все участники криптографической сети должны обладать ключом шифрования, то есть иметь к нему доступ. При большом количестве участников криптографического обмена данный факт значительно повышает вероятность компрометации ключей шифрования. В связи с этим, использование симметричных алгоритмов предполагает наличие взаимного доверия сторон. Недобросовестность отношения одного из тысячи участников криптографического обмена к вопросу хранения ключей может привести к утечке ключевой информации, из-за чего пострадают все участники, в том числе и добросовестно относящиеся к своим обязанностям по хранению ключей. Вероятность компрометации ключей тем выше, чем большее количество пользователей входит в криптографическую сеть. Это является большим недостатком симметричных криптосистем.