Криптографические методы

Криптографические методы защиты информации — это специальные методы шифрования, кодирования или иного преобразования информации, в результате которого ее содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования.

Криптографический метод защиты, безусловно, самый надежный метод защиты, так как охраняется непосредственно сама информация, а не доступ к ней (например, зашифрованный файл нельзя прочесть даже в случае кражи носителя). Данный метод защиты реализуется в виде программ или пакетов программ.

Современная криптография включает в себя четыре крупных раздела:

Симметричные криптосистемы. В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ.

Шифрование — преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом, дешифрование — обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

Криптосистемы с открытым ключом (ассимитричные). В системах с открытым ключом используются два ключа — открытый и закрытый, которые математически связаны друг с другом.

Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.(Ключ — информация, необходимая для беспрепятственного шифрования и дешифрования текстов.).

Электронная подпись. Системой электронной подписи. называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

Управление ключами. Это процесс системы обработки информации, содержанием которых является составление и распределение ключей между пользователями.

Основные направления использования криптографических методов — передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

Требования к криптосистемам

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т.д. Программная реализация более практична, допускает известную гибкость в использовании.

Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

- ✔ зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
- ✔ число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;
- ✔ число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);
- ✔ знание алгоритма шифрования не должно влиять на надежность защиты;

- ✔ незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;
- ✔ структурные элементы алгоритма шифрования должны быть неизменными;
- ✔ дополнительные биты, вводимые в сообщение в процессе шифрования, должен быть полностью и надежно скрыты в шифрованном тексте;
- ✔ длина шифрованного текста должна быть равной длине исходного текста;

- ✔ не должно быть простых и легко устанавливаемых зависимостью между ключами, последовательно используемыми в процессе шифрования;
- ✔ любой ключ из множества возможных должен обеспечивать надежную защиту информации;
- ✔ алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.