Основы шифрования

Центральное место среди программно-технических средств безопасности занимает шифрование или криптография.

Криптографические методы защиты информации:

1. шифрование;

2. стеганография;

3. кодирование;

4. сжатие.

Процесс шифрования заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов. Исходными данными для алгоритма шифрования служат информация, подлежащая шифрованию, и ключ шифрования.

В настоящее время используются два основных метода шифрования – симметричное и асимметричное:

1. В симметричном шифровании один и тот же ключ используется и для шифровки, и для расшифровки сообщений. Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю.

2. В асимметричных методах применяются два ключа. Один из них, несекретный, используется для шифровки и может без всяких опасений передаваться по открытым каналам, другой – секретный – применяется для расшифровки и известен только получателю. Асимметричные методы шифрования позволяют реализовать электронную подпись или электронное заверение сообщения.

В отличие от других методов криптографического преобразования информации, методы стеганографии позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации.

Содержанием процесса кодирования информации является замена смысловых конструкций исходной информации (слов, предложений) кодами. При кодировании и обратном преобразовании используются специальные таблицы или словари.

Сжатие информации может быть отнесено к методам криптографического преобразования информации с определенными оговорками. Целью сжатия является сокращение объема информации. В то же время сжатая информация не может быть прочитана или использована без обратного преобразования. Даже если держать в секрете алгоритмы, то они могут быть сравнительно легко раскрыты статистическими методами обработки. Поэтому сжатые файлы конфиденциальной информации подвергаются последующему шифрованию.

В целом шифрование возникло со времени появления письменности, когда возникла и получила свое дальнейшее развитие потребность в обеспечении стойкости отдельных сообщений, передаваемых почтовыми отправлениями. Первые шифротексты носили некоторый коммерческий характер. В дальнейшем стали шифроваться тексты медицинского характера, купли-продажи скота и недвижимости.

Активное проведение военных действий явилось мощным стимулирующим воздействием на разработку методов шифрования при передаче секретных сообщений. Так, в 56 году до н.э. во времена войны с галлами римский диктатор К. Цезарь при подчинении Риму заальпийской Галлии использовал в системе передачи секретных сообщений шифр замены. Идея шифра замены используется и в современных методах шифрования, так как является частным случаем отображения множества символов исходного текста на множестве символов зашифрованного текста. Шифрование, применявшееся К. Цезарем, осуществлялось следующим образом. Под символами греческого алфавита приписывался тот же алфавит, но сдвинутый по циклу на "n" позиций (в частности, К. Цезарь в письменности, которая дошла до наших времен, осуществлял сдвиг на три позиции). При шифровании исходного текста буквы открытого текста из верхней строки записи заменялись на буквы нижнего алфавита. В этом случае, 42

ключом шифрования и дешифрования является число сдвигов нижней строки алфавита по отношению к верхней.

Шифрование и криптографию можно увидеть и в обычной жизни каждого человека.

Существуют персональные данные, которые представляют собой набор цифр, позволяющие определить конкретного человека. Такими персональными данными являются: номер и серия паспорта, страховой номер индивидуального лицевого счета (СНИЛС), индивидуальный номер налогоплательщика (ИНН), номер банковского счета, номер банковской карты. Такие «кодовые данные» представляют собой некий набор зашифрованной информации о человеке. Шифрование этих данных может производиться государством. Например, когда ребенку исполняется 14 лет, ему выдают паспорт в ФМС. Такой паспорт содержит серию и номер, а также иную информацию.

Для подписания электронных документов также используются инструменты криптографического преобразования - Электронная цифровая подпись (ЭЦП).

ЭЦП может признаваться равнозначной собственноручной подписи лица и использоваться для подтверждения любой информации, передаваемой в электронном виде. Все экземпляры электронного сообщения, подписанного ЭЦП, имеют силу оригинала.

ЭЦП может использоваться физическими и юридическими лицами, органами государственной власти и органами местного самоуправления.

ЭЦП представляет собой последовательность символов, полученную в результате преобразования исходной информации с использованием закрытого ключа ЭЦП (последовательность символов, предназначенная для выработки ЭЦП и известная только владельцу).

Для получения ЭЦП гражданину или организации необходимо получить сертификат открытого ключа ЭЦП (сертификат ключа подписи) – это документ, выданный и заверенный специальным удостоверяющим центром, подтверждающий принадлежность ключа ЭЦП лицу.

Несовершеннолетние граждане имеют право на использование ЭЦП и получение сертификата ключа подписи.