УДК 003.26.09

КРИПТОГРАФИЯ В СОВРЕМЕННОМ МИРЕ

Иванов А.А., студент гр. ПИм-171, 1 курс
Научный руководитель: Пимонов А.Г., д.т.н., профессор
Кузбасский государственный технический университет имени Т.Ф. Горбачева
г. Кемерово

В современном обществе информационные технологии шагнули далеко вперед и просочились во все сферы жизнедеятельности человека. Новые технологии позволяет передавать информацию из одной точки земного шара в другую за считанные секунды. Помимо личных переписок, электронный обмен сообщениями используется для передачи информации между государственными органами, органами местного самоуправления, военными частями и так далее. И все эти сообщения можно перехватить и использовать в своих корыстных целях. И для того, чтобы информация не была известна злоумышленникам используется различные способы шифрования, которые предоставляет современная криптография.

Криптография - наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), а также невозможности отказа от авторства [1].

Криптография изучает методы шифрования информации с использованием открытых и закрытых ключей. Также, традиционная криптография составляет симметричные криптосистемы, а современная криптография включает в себя множество разделов: асимметричные криптосистемы, электронная цифровая подпись, управление ключами, хэш-функции и т.д.

Для защиты информации, которая передается в сети Интернет, используются различные способы шифрования. Существует два основных вида шифрования:

- Симметричный. Один ключ используется для шифрования и расшифрования данных;
- Ассиметричный. Один ключ используется для шифрования, а другой ключ используется для расшифрования данных.

Одним из простых способов шифрования является простая перестановка. Простая перестановка без ключа - один из самых простых

методов шифрования. Сообщение записывается в таблицу по столбцам. После того, как открытый текст записан колонками, для образования шифртекста он считывается по строкам. Для использования этого шифра отправителю и получателю нужно договориться об общем ключе в виде размера таблицы. Объединение букв в группы не входит в ключ шифра и используется лишь для удобства записи несмыслового текста [2]. Ключ, по которому шифруется и расшифровывается сообщение, передается обоим пользователям до процесса передачи информации. Данный способ исключает перехват ключей, так как они хранятся у сторон обмена сообщениями. Минусы данного алгоритма в том, что нужно заранее обмениваться ключами, а также, если злоумышленник сможет украсть данный ключ у пользователя, то сможет расшифровать информацию, которая передавалась по данному каналу.

Сейчас также используется ГОСТ 28147-8. ГОСТ 28147-8. Стандарт Российской Федерации на шифрование и имитозащиту данных. Первоначально имел гриф (ОВ или СС - точно не известно), затем гриф последовательно снижался, и к моменту официального проведения алгоритма через Госстандарт СССР в 1989 году был снят. Алгоритм остался ДСП (как известно, ДСП не считается грифом). В 1989 году стал официальным стандартом СССР, а позже, после распада СССР, федеральным стандартом Российской Федерации [3].

На данный момент, шифрование используется везде, где ведется работа с персональными данными. Зашифрованный обмен информацией между государственными и муниципальными образованиями, а также простыми гражданами используется для того, чтобы скрыть личную информацию одной стороны от злоумышленников.

Например, для передачи информации по электронным больничным листам в Фонд социального страхования используется специальное программное обеспечение по шифрованию, которое разрабатывалось самим фондом. Российский рынок позволяет пользоваться различными специализированными программными продуктами, например, ViPNet компании ИнфоТеКС [4].

Программные продукты, которые специализируются на шифровании обычно состоят из нескольких модулей:

- Генератор ключей. Модуль, который занимается созданием ключей шифрования;
- Хранилище ключей. Модуль, который хранит все ключи;
- Шифратор. Модуль, который шифрует информацию;
- Дешифратор. Модуль, который расшифровывает информацию.

Используя такую структуру построения ПО можно создать стандартную программу, которая может использовать различные способы шифрования и расшифровки сообщения.

Криптография не ограничивается использованием программ для шифрования. Данная наука занимается созданием новых способов защиты информации, которые используется в современных информационных системах для защиты информации как личности, так и всего государства.

Список литературы:

- Криптография // Википедия URL: https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F
- Симметричные криптосистемы // Википедия URL: https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BC%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%BD%D1%8B%D0%B5_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B
- Обзор алгоритмов Шифрования // rohos URL: http://www.rohos.ru/help/crypto_algorithms.htm
- ViPNet // ИнфоТеКС URL: https://infotecs.ru/product/