Система криптографической защиты

Составила: Виноградова К.Н.

Общие сведения

- **Процедура шифрования** – превращает информацию из обычного «понятного» вида в «нечитабельный» зашифрованный вид перед передачей. Она дополняется процедурой дешифрования информации при приеме.
- Криптосистема **– процедуры – шифрование и дешифрования.**
- **Правило Керкхоффа**: «Стойкость шифра должна определяться только секретностью ключа».
- **Алгоритм шифрования считается раскрытым, если найдена процедура, позволяющая подобрать ключ за реальное время.**

Общие сведения

- Сложность алгоритма раскрытия является одной из важных характеристик криптосистемы и называется **криптостойкостью**.

Понятия

- **Криптология** – применение криптографических методов, разделяется на криптографию и криптоанализ.
- **Криптография** – поиск и исследование математических методов преобразования информации.
- **Криптоанализ** – исследование возможности расшифровывания информации без знания ключей.

Что такое криптография

- **Криптография** – наука о методах обеспечения конфиденциальности и аутентичности информации.
- Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для злоумышленника. Такие преобразования позволяют решить два главных вопроса, касающихся безопасности информации:
- Защиту конфиденциальности;
- Защиту целостности.

Криптография подразделяется на несколько методов криптозащиты информации:

- **Методы криптографического преобразования информации:**
  - Шифрование
  - Кодирование
  - Стенография
  - сжатие

Шифрование

- 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.

- Для шифрования информации используются **алгоритм преобразования и ключ**. Как правило, алгоритм для определенного метода шифрования является неизменным. Исходными данными для алгоритма шифрования служит информация, подлежащая зашифрованию, и ключ шифрования. Ключ содержит управляющую информацию, которая определяет выбор преобразования на определенных шагах алгоритма и величины операндов, используемых при реализации алгоритма шифрования. Операнд – это константа, переменная, функция, выражение и другой объект языка программирования, над которым производятся операции.

Стенография

- В основе всех методов стеганографии лежит маскирование закрытой информации среди открытых файлов, т.е. скрываются секретные данные, при этом создаются реалистичные данные, которые невозможно отличить от настоящих. Обработка мультимедийных файлов в информационных системах открыла практически неограниченные возможности перед стеганографией.

Кодирование

- Содержанием процесса кодирование информации является замена исходного смысла сообщения (слов, предложений) кодами. В качестве кодов могут использоваться сочетания букв, цифр, знаков. При кодировании и обратном преобразовании используются специальные таблицы или словари. В информационных сетях кодирование исходного сообщения (или сигнала) программно-аппаратными средствами применяется для повышения достоверности передаваемой информации.

- Часто кодирование и шифрование ошибочно принимают за одно и тоже, забыв о том, что для восстановления закодированного сообщения, достаточно знать правило замены, в то время как для расшифровки сообщения помимо знания правил шифрования, требуется ключ к шифру.

Сжатие

- 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. Учитывая доступность средств сжатия и обратного преобразования, эти методы нельзя рассматривать как надежные средства криптографического преобразования информации.
- Даже если держать в секрете алгоритмы, то они могут быть сравнительно легко раскрыты статистическими методами обработки. Поэтому сжатые файлы конфиденциальной информации подвергаются последующему шифрованию. Для сокращения времени передачи данных целесообразно совмещать процесс сжатия и шифрования информации.

Шифр Цезаря

- Шифр Цезаря Один из древнейших шифров. При шифровании каждая буква заменяется другой, отстоящей от неё в алфавите не на одну, а на большее число позиций. Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки.

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В

Например

- Зашифруем слово «ИНФОРМАТИКА»

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В

- Получим: ЛРЧСУПГХЛНГ