Навыки шифрования

Шифрование (enciphering) - это преобразование открытого текста в зашифрованный текст с целью защитить его конфиденциальность.

```
Encryption
plain text -> cipher text
```

Дешифровка - deciphering.

Огюст Керкгоффс

Сформулировал принципы и требования к криптосистемам.

Принципы

- массовость,
- эмпирическая проверка.

Требования

- сложность расшифровки и модификации исходного сообщения;
- малые изменения исходного текста влечет значительные изменения зашифрованного текста;
- область значений ключа должна исключать перебор;
- стоимость дешифрации значительно превышает стоимость данных.

> Рассеивание - влияние одного символа исходного текста на множество бит зашифрованного текста

Симметричные алгоритмы шифрования

Для шифровки и расшифровки используется один и тот же ключ.

```
M1 -> C(M1) -> C1 -> D(C1) -> M1'
        ^              ^
        |              |
        k --------------
```

- Перестановки (permutation) - P-преобразования
- Замены (substitution) - S-преобразования

Самый древний - перестановки (одноалфавитные)

Например:

- Скитала;
- Перестановки по правилам;
- Шифр Цезаря (сдвиг алфавита);
- Квадрат Полибия (по сути тот же шифр Цезаря, только в таблице);
- PigPen (буквам соответствуют символы)

Многоалфавитные алгоритмы

- Таблица омофонов (количество кодов для одного символа пропорционально частоте встречаемости в тексте)
- Шифр Виженера (по сути комбинация шифра Цезаря, для каждого символа использования)
- Великий шифр Людовика XIV (дополнительно ввел "мусорные" слова в текст, которые помечались как удаляемые)

Алгоритмы шифрования делятся на

- блочные (берут кусок текста и шифруют);
- поточные (очередной следующий блок текста шифруется на основе предыдущего).

Энигма

Электро-механическая машина (состоит из трех роторов и рефлектора) Например, первый ротор шифрует A в C, второй - C в M, третий - M в I, рефлектор замыкает на букву K. Далее энигма идет в обратный ход, и в итоге из A получаем R.

После каждого символа меняется алфавит на первом роторе, после очередного полного оборот первого - оборот второго и т.д. Итого получаем 26^3 алфавитов.

Свойство рефлектора - A -> B, B -> A (прямой и обратный ход симметричные). Поэтому рефлектор не крутится.

Лабораторная работа №2

Энигма для работы с файлами (произвольными)

Лекция 2

Лекция 4