## Практическая работа №1 - Алгоритм шифрования

**Цель работы:**

Анализ существующих простейших алгоритмов шифрования.

**Задание:**

- разработать собственный алгоритм шифрования;

- разработать форму содержащую: 3 текстовых поля, кнопку «Шифровать», кнопку «Расшифровать»;

- реализовать разработанный алгоритм на любом языке программирования.

**Методика выполнения Практической работы**

Студентами рассматриваются существующие простые алгоритмы шифрования. В результате просмотра и анализа источников литературы формируются принципы работы алгоритмов шифрования.

**Основные теоретические положения**

Все существующие криптографические методы сводятся к следующим классам преобразований:

*- Многоалфавитная подстановка - н*аиболее простой вид преобразований, заключающийся в замене символов исходного текста на другие (того же алфавита) по более или менее сложному правилу. Для обеспечения высокой криптостойкости требуется использование больших ключей.

*- Перестановки -* несложный метод криптографического преобразования. Используется как правило в сочетании с другими методами.

*- Гаммирование - э*то метод заключается в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа.

*- Блочные шифры –* представляетсобой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к блоку (части) шифруемого текста.

В качестве примера одного из классов преобразований моно привести алгоритм Цезаря. Он относится к первой группе.

Подмножество *Cm={Ck: 0≤k<m}* симметрической группы *SYM(Zm)*, содержащее *m* подстановок *Ck: j→(j+k) (mod m), 0≤k < m*, называется подстановкой Цезаря.

Умножение коммутативно, *CkCj=CjCk=Cj+k, C0* – идентичная подстановка, а обратной к *Cк* является *Ck-1=Cm-k,* где *0<k<m*. Семейство подстановок Цезаря названо по имени римского императора Гая Юлия Цезаря, который поручал Марку Туллию Цицерону составлять послания с использованием 50-буквенного алфавита и подстановки C3.

Подстановка определяется по таблице замещения, содержащей пары соответствующих букв “исходный текст – шифрованный текст”. Для C3 подстановки приведены в Табл. 1. Стрелка (🡪) означает, что буква исходного текста (слева) шифруется при помощи C3 в букву шифрованного текста (справа).

Системой Цезаря называется моноалфавитная подстановка, преобразующая *n*-грамму исходного текста *(x0, x1 ,..,xn-1)* в *n*‑грамму шифрованного текста *(y0 ,y1 ,...,yn-1)* в соответствии с правилом *yi=Ck(xi)*, *0≤i<n*.

Например, «Алгоритм шифрования» посредством подстановки C3 преобразуется в «лоывайьлываждлвыаыв».

Таблица 1

|  |  |  |  |
| --- | --- | --- | --- |
| А🡪г | Й🡪м | Т🡪х | Ы🡪ю |
| Б🡪д | К🡪н | У🡪ц | Ь🡪я |
| В🡪е | Л🡪о | Ф🡪ч | Э🡪\_ |
| Г🡪ж | М🡪п | Х🡪ш | Ю🡪а |
| Д🡪з | Н🡪р | Ц🡪щ | Я🡪б |
| Е🡪и | О🡪с | Ч🡪ъ | \_🡪в |
| Ж🡪й | П🡪т | Ш🡪ы |  |
| З🡪к | Р🡪у | Щ🡪ь |  |
| И🡪л | С🡪ф | Ъ🡪э |  |

Применение подстановки Цезаря.

При своей несложности система легко уязвима. Если злоумышленник имеет

1) шифрованный и соответствующий исходный текст или

2) шифрованный текст выбранного злоумышленником исходного текста, то определение ключа и дешифрование исходного текста тривиальны.

Более эффективны обобщения подстановки Цезаря - *шифр Хилла* и *шифр Плэйфера*. Они основаны на подстановке не отдельных символов, а 2-грамм (шифр Плэйфера) или *n*-грамм (шифр Хилла). При более высокой криптостойкости они значительно сложнее для реализации и требуют достаточно большого количества ключевой информации.[1]

**Требования к предъявляемой работе:**

- Программа шифрования должны быть наделена понятным и удобным пользовательским интерфейсом.

- Алгоритм шифрования в обязательном порядке должен использовать математические и- или побитовые функции.

- Разработанный алгоритм должен приводить к полной утрате всех статистических закономерностей исходного сообщения.