Лабораторная работа № 1

«Изучение криптографических систем, основанных на методе подстановки»

1.1. Цель работы:

Изучение способов шифрования информации в криптографических системах, основанных на методе подстановки.

1.2. Теоретическая часть

Криптографические системы, основанные на методе подстановки, разделяются на четыре основных класса:

1) monoalphabetic;
2) homophonic;
3) polyalphabetic;
4) polygram.

В системах класса monoalphabetic символ исходного текста заменяется другим символом таким образом, что между ними существует однозначное соответствие. То есть каждый символ исходного текста однозначно заменяется его подстановкой. Криптографическим ключом такой системы является таблица соответствия исходного алфавита алфавиту подстановки. Например, для английского алфавита существует $26!=4*10^{26}$ различных криптографических систем первого класса. Наиболее простые системы данного класса предполагают аналитическое описание подстановок. Так, простейший шифратор, основанный на принципе подстановки, сдвигает каждую букву английского алфавита на k позиций, где k является ключом шифра. В так называемом алгоритме Цезаря i-ая буква алфавита заменяется (i+k)-й буквой по модулю 26. Юлий Цезарь использовал подобную систему для k=3. Аналитически криптосистема Цезаря описывается выражением

$$E_k(i) = (i+k) \bmod 26. \qquad (1.1)$$

Например, в соответствии с приведенным выражением буква A исходного английского алфавита, имеющая номер i =0, заменяется буквой D, имеющей номер (i+k) mod 26=(0+3) mod 26=3, а буква Z (i=25) заменяется буквой C, имеющей номер (i+k) mod 26=(25+3) mod 26=2. Следующий пример иллюстрирует алгоритм шифрования Цезаря:

Исходный текст: CRYPTOGRAPHYANDDATASECURITY.
Шифротекст : FUBSWRJUDSKBDQSGDWDVHFXULWB.

Алгоритм дешифрования имеет вид

$$D_k(i) = (i+26-k) \bmod 26. \qquad (1.2)$$

Существуют более сложные методы подстановки. Шифраторы, основанные на умножении номера каждого символа исходного текста на значение ключа k, описываются следующим отношением:

$$E_k(i) = (i*k) \bmod n, \qquad (1.3)$$

где i – номер символа исходного текста, n – количество символов в исходном алфавите (n=26для английского алфавита и n=256 для ASCII-кодов), k – ключ, n и k должны быть взаимно простыми.

Шифраторы, основанные на сдвиге и умножении, описываются выражением

$$E_k(i) = (i*k_1+k_0) \bmod n. \quad (1.4)$$

Любой шифратор класса monoalphabetic может быть представлен в виде полиномиального преобразования порядка t:

$$E_k(i) = (k_0+k_1*i+k_2*i^2+\ldots+k_{t-1}*i^{t-1}+k_t*i^t) \bmod n. \quad (1.5)$$

Алгоритм Цезаря является полиномиальным преобразованием нулевого порядка.

В криптографических системах класса homophonic имеется несколько вариантов замены исходного символа. Например, буква A может быть заменена цифрами 24, 35, 37, а буква B – цифрами 41, 17, 76. Тогда слово ABBA может быть зашифровано как (37,17,76,24), или (35,41,76,37) и т.д.

Подобные системы характеризуются значительно большей криптографической стойкостью, чем системы класса homophonic.

Криптографические системы класса polyalphabetic основаны на использовании нескольких различных ключей. Большинство шифраторов подобного типа являются периодическими с периодом P. Исходный текст вида

$$X=x_1x_2x_3x_4\ldots x_px_{p+1}\ldots x_{2p}\ldots$$

шифруется с помощью ключей $k_1,k_2,\ldots k_p$:

$$E_k(X)=E_{k1}(x_1)\ E_{k2}(x_2)\ldots E_{kp}(x_p)\ E_{k1}(x_{p+1})\ldots E_{kp}(x_{2p}) \quad (1.6)$$

Для p=1 будем иметь шифр класса monoalphabetic.

Один из таких алгоритмов был предложен в XVI веке французом Вигеном (Vigenere).

В данном случае ключ K представляется последовательностью

$$K=k_1\ k_2\ldots k_p,$$

где k_i $(1 \le i \le p)$ представляет собой число сдвигов в исходном алфавите.

Символы исходного текста шифруются по формуле

$$E_k(i) = (i+k_j) \bmod n, \quad (1.7)$$

где i – номер символа исходного текста, K_j – ключ, $j \in \{1, \ ,n\}$.

Пусть ключом является слово BAD. Тогда слово CRYPTOGRAPHY будет зашифровано следующим образом:

i = CRY PTO GRA PHY,
K= BAD BAD BAD BAD,
$E_k(i)$ = DRB QTR HRD QHB.

Криптосистемы третьего класса, основанные на полиалфавитной подстановке, широко использовались и используются на практике. На их основе разработано целое семейство роторных шифраторов, которые широко применялись во время второй мировой войны и в после-

военное время. Среди них можно выделить машину Хагелина М-209 (США), немецкую шифровальную машину «Энигма», японский «Пурпурный код».

Криптографические системы класса polygram характеризуются подстановкой не одного, а нескольких символов в исходном тексте. В общем случае n символов исходного текста заменяются n символами шифротекста.

Порядок выполнения работы

1 Реализовать алгоритм и программу шифрования исходного текста (на базе произвольно выбранного алфавита) в системе класса monoalphabetic.

Алгоритм шифрования реализовать с использованием

– формулы (1.3) для бригад с нечетными номерами;

– формулы (1.4) для бригад с четными номерами.

2. Реализовать алгоритм и программу дешифрования сформированного согласно пункту 1 шифротекста.

Алгоритм дешифрования должен быть разработан самостоятельно. Алгоритм может быть реализован, как на основе формулы, так и с использованием логико-смыслового анализа исходных данных задачи.

3. Оформить лабораторную работу на листах формата А4 в соответствии с правилами оформления студенческих лабораторных работ. Отчет по лабораторной работе должен содержать:

– титульный лист (оформленный по правилам) с указанием названия работы и следующие разделы:

– цель работы;

– краткие теоретические сведения;

– задание на выполнение работы;

– алгоритм решения поставленной задачи (блок-схема и словесное описание по блокам);

– текст программы;

– описание входных / выходных данных программы;

– контрольный пример;

– выводы;

– список использованной литературы.

Необходимо разработать четкий и удобный интерфейс пользователя для задания исходных данных и вывода результатов работы программы.