Лабораторная работа № 8
«Шифрование информации методом простой замены»

Цель работы:

1. Закрепление теоретического материала на тему «Шифрование информации методом простой замены».
2. Получение шифротекста по исходным данным.
3. Получение исходного текста по заданному шифротексту и ключу.

Пояснения к работе:

Сущность методов замены (подстановки) заключается в замене символов исходной ин-формации, записанных в одном алфавите, символами из другого алфавита по определенному правилу.

Самым простым является метод прямой замены. Символам Soi исходного алфавита Ao, с помощью которых записывается исходная информация, однозначно ставятся в соответствие символы S1i шифрующего алфавита Ai. В простейшем случае оба алфавита могут состоять из одного и того же набора символов. Например, оба алфавита могут содержать буквы алфавита кириллица.

Задание соответствия между символами обоих алфавитов осуществляется с помощью преобразования числовых эквивалентов символов исходного текста To, длиной - К символов, по определенному алгоритму.

Алгоритм моноалфавитной замены может быть представлен в виде последовательности шагов.

Шаг 1. Формирование числового кортежа Loh путем замены каждого символа Soi To (i=l,K), представленного в исходном алфавите Ao размера [lxR], на число hoi(soi), соответствующее порядковому номеру символа soi в алфавите Ao.

Шаг 2. Формирование числового кортежа L1h путем замены каждого числа кортежа Loh на соответствующее число h1i кортежа L1h, вычисляемое по формуле:

$$h_{1i} = (k_1 \times h_{0i}(s_{0i}) + k_2) (\mathrm{mod}\ R),$$

где ki - десятичный коэффициент; к2 - коэффициент сдвига. Выбранные коэффициенты K1, K2 должны обеспечивать однозначное соответствие чисел hoi и h1i, а при получении h1i = 0 выполнить замену h1i = R.

Шаг 3. Получение шифротекста T1 путем замены каждого числа h1i(s1i) кортежа L1h со-ответствующим символом s1i Ti (i=l,K) алфавита шифрования A1 размера [1XR].

Шаг 4. Полученный шифротекст разбивается на блоки фиксированной длины b. Если последний блок оказывается неполным, то в конец блока помещаются специальные символы-заполнители (например, символ *).

Пример. Исходными данными для шифрования являются:

T0 = <МЕТОД_ШИФРОВАНИЯ>;

Ao = <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩ ЪЫЬЭЮЯ >;

A1 = <ОРЩЬЯТЭ_ЖМЧХАВДЫФКСЕЗПИЦГНЛЪШБУЮ>;

R=32; k1=3; k2=15, b=4.

Пошаговое выполнение алгоритма приводит к получению сле¬дующих результатов.

Шаг1. L0h = <12,6,18,14,5,32,24,9,20,16,14,3,1,13,9,31>.

Шаг 2. L1h = <19,1,5,25,30,15,23,10,11,31,25,24,18,22,10,12>.

Шаг 3. T1 =<С О Я Г Б Д И М Ч У Г Ц К П М Х >.

Шаг4. T2 = <СОЯГ БДИМ ЧУГЦ КПМХ>.

При расшифровании сначала устраняется разбиение на блоки. Получается непрерывный шифротекст Ti длиной К символов. Расшифрование осуществляется путем решения целочисленного уравнения:

$$k_1 h_{0i} + k_2 = nR + h_{1i},$$

При известных целых величинах ki, k2, h1i и R величина hoi вычисляется методом пере-бора n.

Последовательное применение этой процедуры ко всем символам шифротекста приводит к его расшифрованию.

По условиям приведенного примера может быть построена таблица замены, в которой взаимозаменяемые символы располагаются в одном столбце (табл. 1).

s_{0i}	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш							
h_{0i}	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24							
s_{1i}	К	З	Ц	Л	Б	О	Ь	Э	М	А	Ы	С	П	Г	Ъ	У	Р	Я	_	Ч	В	Ф	Е	И							
h_{1i}	18	21	24	27	30	1	4	7	10	13	16	19	22	25	28	31	2	5	8	11	14	17	20	23							

s_{0i}	Щ	Ъ	Ы	Ь	Э	Ю	Я	_
h_{0i}	25	26	27	28	29	30	31	32
s_{1i}	Н	Ш	Ю	Щ	Т	Ж	Х	Д
h_{1i}	26	29	32	3	6	9	12	15

Таблица 1. Таблица замены

Использование таблицы замены значительно упрощает процесс шифрования. При шифровании символ исходного текста сравнивается с символами строки soi таблицы. Если произошло совпадение в i-м столбце, то символ исходного текста заменяется символом из строки s1j, находящегося в том же столбце i таблицы.

Расшифрование осуществляется аналогичным образом, но вход в таблицу производится по строке s1i.

Ход выполнения лабораторной работы:

1. Изучить приведенные в методическом описании к лабораторной работе материал и пример шифрования методом простой замены.
2. Получить у преподавателя исходный текст и ключ для шифрования.
3. Выполнить по шагам процедуру шифровании, полученный шифротекст представить в виде блоков информации.
4. Представить результаты преподавателю.
5. Получить у преподавателя шифротекст и ключ для расшифрования.
6. Выполнить по шагам процедуру расшифрования, полученный исходный текст представить преподавателю для проверки.
7. Оформить отчет в установленной форме.
8. Представить результаты работы преподавателю и защитить работу ответами на контрольные вопросы.

Контрольные вопросы:

1. Определение метода шифрования (шифра)
2. Понятие атаки на шифр (криптоанализа).
3. Понятие криптостойкости и требования, предъявляемые к криптостойкости.
4. Понятие и особенности метода простой замены.
5. Недостатки метода простой замены.