Лабораторная работа №1
Простейшие алгоритмы шифрования

Цель работы: изучить простейшие алгоритмы шифрования.

Выполнение работы.

1 ШИФРОВАНИЕ ПЕРЕСТАНОВОЧНЫМИ ШИФРАМИ

Исходный текст: *Тупальский Марк Евгеньевич.*

1.1 Шифрование простейшими перестановочными шифрами

Шифрования текста простейшими перестановочными шифрами:
1) Удаление пробелов и запись слова только большими буквами.
Результат шифрования:

ТУПАЛЬСКИЙМАРКЕВГЕНЬЕВИЧ.

2) Разбиение текста на блоки по 2 буквы.
Результат шифрования:

ТУ ПА ЛЬ СК ИЙ МА РК ЕВ ГЕ НЬ ЕВ ИЧ.

3) Запись слов в обратном порядке.
Результат шифрования:

ЧИВЕЬНЕГВЕКРАМЙИКСЬЛАПУТ.

4) Перестановка в виде матрицы 2 строки, 12 столбцов (см. таблицу 1): запись построчная, чтение по столбцам сверху вниз 1,3,5,7, 9,11,2,4, 6,8,10,12.

Таблица 1 – Матрица метода перестановки

Столбцы	1	2	3	4	5	6	7	8	9	10	11	12
Строки	Т	У	П	А	Л	Ь	С	К	И	Й	М	А
Строки	Р	К	Е	В	Г	Е	Н	Ь	Е	В	И	Ч

Результат шифрования:

ТРПЕЛГСНИЕМИУКАВЬЕКЬЙВАЧ.

1.2Шифрование шифром «железнодорожная изгородь»

Правила записи текста представлено на рисунке 1.

1 5 9 13 17 21
2 4 6 8 10 12 14 16 18 20 22 24
3 7 11 15 19 23

Рисунок 1 – Правили записи текста по методу «железнодорожная изгородь»

Запись исходного текста представлена на рисунке 2.

Т Л И Р Г Е
У А Ь К Й А К В Е Ь В Ч
П С М Е Н И

Рисунок 2 – Запись исходного текста по методу «железнодорожная изгородь»

Правило чтения – по строкам слева направо начиная с первой строки.
Результат шифрования:

ТЛИРГЕУАЬКЙАКВЕЬВЧПСМЕНИ.

1.3 Шифрование с использованием ключевого слова

Метод использования ключевого слова или фразы в качестве правила перестановки столбцов.

Буквам ключевого слова назначаются номера, начиная с первого в соответствии с русским алфавитом. Если буква встречается несколько раз, то нумерация определяется порядком следования повторяющейся буквы в ключевом слове.

Ключевое слово ЭЛЕКТРОЛИЗ определяет количество столбцов – 10 столбцов для записи исходных текстов, а буквы этого слова определяют порядок чтения столбцов текста – запись построчно, чтение по столбцам, начиная с первого столбца, см. таблицу 2.

Таблица 2 – Метод использование ключевого слова

Э	**Л**	**Е**	**К**	**Т**	**Р**	**О**	**Л**	**И**	**З**
10	**5**	**1**	**4**	**9**	**8**	**7**	**6**	**3**	**2**
Т	У	П	А	Л	Ь	С	К	И	Й
М	А	Р	К	Е	В	Г	Е	Н	Ь
Е	В	И	Ч						

Результат шифрования:

ПРИ ЙЬ ИН АКЧ УАВ КЕ СГ ЬВ ЛЕ ТМЕ.

1.4 Шифрование методом поворачивающейся решетки

По заданию размер решетки 6х6, а вырезаемые отверстия в количестве 9 выбираются на основе алгоритма: исходный текст записывается через отверстия в решетке, которая по мере заполнения поворачивается на 90º.

Предварительно текст разбивается на блоки 6х6 = 36 символов. Решетка – матрица (4х4), для которой ячейки, которые при повороте матрицы на 90º занимают одинаковое положение, нумеруются одинаково, см. рисунок 3. При использовании вырезается один из квадратов с одинаковым номером.

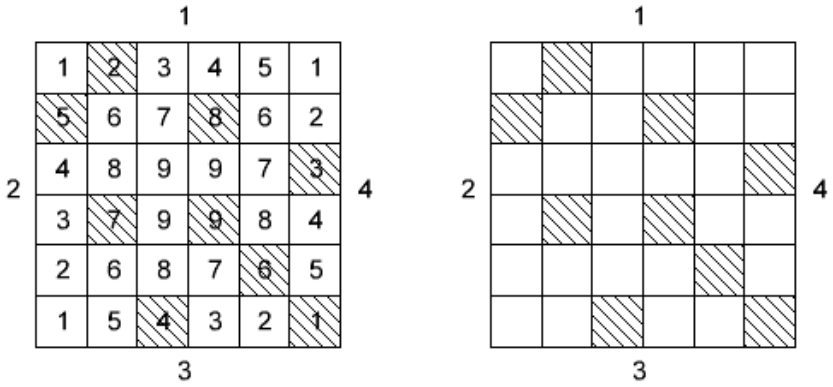

Рисунок 3 – Решетки 6х6 и количеством отверстий 9

Исходный текст:

ТУПАЛЬСКИЙ МАРК ЕВГЕНЬЕВИЧ
ОБЖ ТРУД ХИМИЯ

Шифрование методом поворачивающейся решетки показано на рисунке 4.

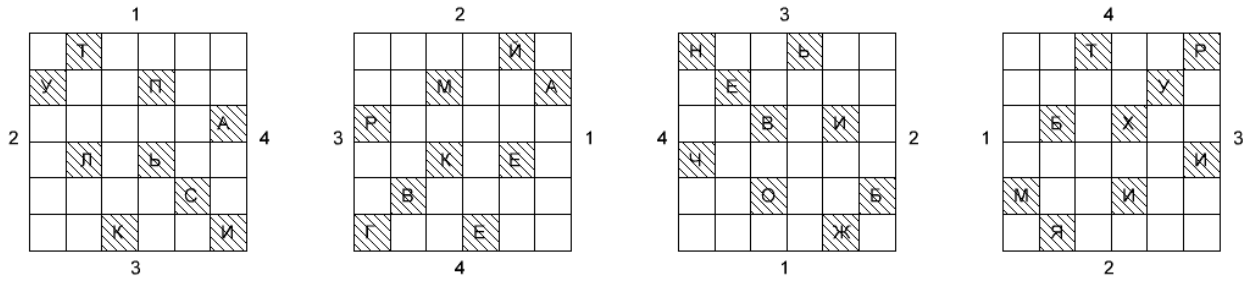

Рисунок 4 – Шифрование методом поворачивающейся решетки

Результат шифрования представлен на рисунке 5.

Н	Т	Т	Ь	Й	Р
У	Е	М	П	У	А
Р	Б	В	Х	И	А
Ч	Л	К	Ь	Е	И
М	В	О	И	С	Б
Г	Я	К	Е	Ж	И

Рисунок 5 – Результат шифрования методом поворачивающейся решетки

2 ШИФРОВАНИЕ ПОДСТАНОВОЧНЫМ МЕТОДОМ

Подстановочный метод – аффинное преобразование определяется функцией шифрования

$$c_i = (k_1 \cdot a_i + k_2) \bmod n,$$

где c_i – символ текста шифра;

a_i – число соответствующее букве исходного текста;

k_1, k_2 – первый и второй ключ;

n – мощность алфавита.

В русском алфавите 33 буквы, т.е. n = 33 (3·11 = 33), см. таблицу 3.

Таблица 3 – Соответствие букв русского алфавита

Буква	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й
Цифра	0	1	2	3	4	5	6	7	8	9	10

Продолжение таблицы 3

Буква	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Цифра	11	12	13	14	15	16	17	18	19	20	21

Окончание таблицы 3

Буква	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Цифра	22	23	24	25	26	27	28	29	30	31	32

Ключ k_1 должен быть взаимно простым с 33. Возможные значения:
1, 2, 4, 5, 7, 8, 10, 13, 14, 16, 17, 19, 20, 23, 25, 26, 28, 29, 31, 32.

По условию $k_1 = 20$ – номер в журнале. Ключ $k_1 = 20$ удовлетворяет условию взаимной простоты, принимаем $k_1 = 20$. Значение k_2 может быть любым, если k_1 не равно единице. Таким образом, принимаем: $k_2 = 17$.

Алгоритм шифрования следующий (см. таблицу 4):

1) Первый шаг шифрования – запись чисел a_i , соответствующих каждой букве текста шифрования.

2) Для каждого значения находим $(k_1 \cdot a_i + k_2) = (20 \cdot a_i + 17)$.

3) Для каждого символа возьмем остаток от деления $(20 \cdot a_i + 17)$ на 33.

4) Подстановка вместо каждого числа соответствующей ему буквы из таблицы 3.

Таблица 4 – Метод аффинного преобразования

Текст	Т	У	П	А	Л	Ь	С	К	И	Й	М	А
a_i	19	20	16	0	12	29	18	11	9	10	13	0
$k_1 \cdot a_i + k_2$	397	417	337	17	257	597	377	237	197	217	277	17
$(k_1 a_i + k_2) \bmod n$	1	21	7	17	26	3	14	6	32	19	13	17
Шифр	Б	Ф	Ж	Р	Щ	Г	Н	Ё	Я	Т	М	Р

Продолжение таблицы 4

Текст	Р	К	Е	В	Г	Е	Н	Ь	Е	В	И	Ч
a_i	17	11	5	2	3	5	14	29	5	2	9	24
$k_1 \cdot a_i + k_2$	357	237	117	57	77	117	297	597	117	57	197	497
$(k_1 a_i + k_2) \bmod n$	27	6	18	24	11	18	0	3	18	24	32	2
Шифр	Ъ	Ё	С	Ч	К	С	А	Г	С	Ч	Я	В

Результат шифрования:

БФЖРЩГНЁЯТМРЪЁСЧКСАГСЧЯВ.

Выводы.

В результате выполнения работы изучены методы шифрования простейшими перестановочными шифрами, такими как разбиение текста на блоки по 2, запись слов в обратном порядке, перестановка в виде матрицы 2 строки и 12 столбцов, а так же шифрование шифром «железнодорожная изгородь» и шифрование с использованием ключевого слова ЭЛЕКТРОЛИЗ.

Выполнено шифрование методом поворачивающейся решетки размером 6x6 (9 отверстий) и применено шифрование подстановочным методом **(**аффинное преобразование) с функцией шифрования

$$c_i = (k_1 \cdot a_i + k_2) \bmod n = (20 \cdot a_i + 17) \bmod 33.$$