Лабораторная работа №1

Простейшие алгоритмы шифрования

Цель работы: изучить простейшие алгоритмы шифрования.

Выполнение работы.

1 ШИФРОВАНИЕ ПЕРЕСТАНОВОЧНЫМИ ШИФРАМИ

Исходный текст: Романьков Роман Александрович.

1.1 Шифрование простейшими перестановочными шифрами

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

РОМАНЬКОВРОМАНАЛЕКСАНДРОВИЧ.

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

РО МА НЬ КО ВР ОМ АН АЛ ЕК СА НД РО ВИ Ч.

3.Запись слов в обратном порядке.
Результат шифрования:

ЧИВОРДНАСКЕЛАНАМОРВОКЬНАМОР
.

4.Перестановка в виде матрицы 2 строки, 14 столбцов (см. таблицу 1): запись построчная, чтение по столбцам сверху вниз 1,3,5,7, 9,11,13,,2,4, 6,8,10,12,14.

Таблица 1 – Матрица метода перестановки

Столбцы	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Строки	Р	О	М	А	Н	Ь	К	О	В	Р	О	М	А	Н
Строки	А	Л	Е	К	С	А	Н	Д	Р	О	В	И	Ч	

Результат шифрования:

РАМЕНСКНВРОВАЧОЛАКЬАОДРОМИН.

1.2Шифрование шифром «железнодорожная изгородь»

Правило записи текста представлено на рисунке 1.

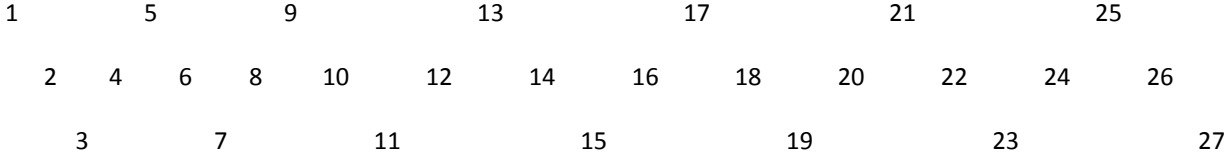

Рисунок 1 – Правило записи текста по методу «железнодорожная изгородь»

Запись исходного текста представлена на рисунке 2.

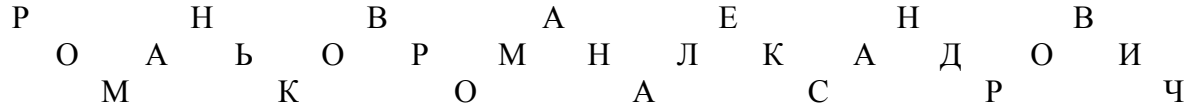

Рисунок 2 – Запись исходного текста по методу «железнодорожная изгородь»

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

РНВАЕНВОАЬОРМНЛКАДОИМКОАСРЧ.

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 ТЕПЛООБМЕН 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

Т	**Е**	**П**	**Л**	**О**	**О**	**Б**	**М**	**Е**	**Н**
10	**2**	**9**	**4**	**7**	**8**	**1**	**5**	**3**	**6**
Р	О	М	А	Н	Ь	К	О	В	Р
О	М	А	Н	А	Л	Е	К	С	А
Н	Д	Р	О	В	И	Ч			

Результат шифрования:

КЕЧ ОМД ВС АНО ОК РА НАВ ЬЛИ МАР РОН.

.

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.

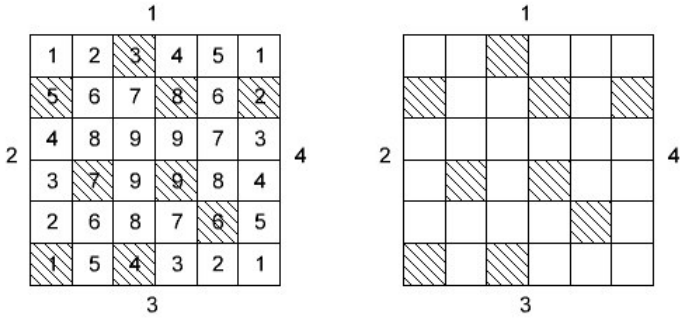

Рисунок 3 – Решетки 6х6 и количеством отверстий 9

Исходный текст:

РОМАНЬКОВ РОМАН АЛЕКСАНДРОВИЧ
ТРУД ФИЗИКА МАТЕМАТИКА АСТРОНОМИЯ ИНОСТРАННЫЙ ЯЗЫК

Шифрование методом поворачивающейся решетки показано на рисунке 4.

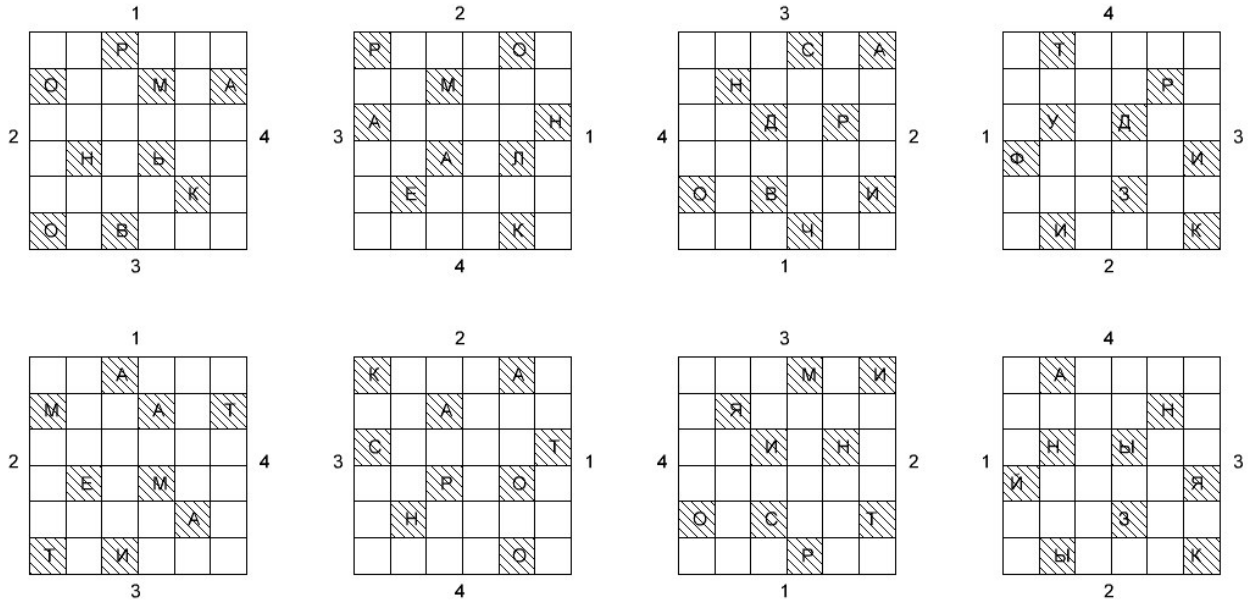

Рисунок 4 – Шифрование методом поворачивающейся решетки

Результат шифрования представлен на рисунке 5.

Первые 36 символов

Р	Т	Р	С	О	А
О	Н	М	М	Р	А
А	У	Д	Д	Р	Н
Ф	Н	А	Ь	Л	И
О	Е	В	З	К	И
О	И	В	Ч	К	К

Остальные 36 символов

К	А	А	М	А	И
М	Я	А	А	Н	Т
С	Н	И	Ы	Н	Т
Й	Е	Р	М	О	Я
О	Н	С	З	А	Т
Т	Ы	И	Р	О	К

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 $k_1 = 14$ – номер в журнале. Так как ключ $k_1 = 14$ удовлетворяет условию взаимной простоты, то принимаем $k_1 = 14$.

Значение k_2 может быть любым, если k_1 не равно единице. Таким образом, принимаем: $k_2 = 23$.

Алгоритм шифрования следующий (см. таблицу 4):

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

2) Для каждого значения находим $(k_1 \cdot a_i + k_2) = (14 \cdot a_i + 23)$.

3) Для каждого символа возьмем остаток от деления $(14 \cdot a_i + 23)$ на 33.

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

Таблица 4 – Метод аффинного преобразования

Текст	Р	О	М	А	Н	Ь	К	О	В
a_i	17	15	13	0	14	29	11	15	2
$k_1 \cdot a_i + k_2$	261	233	205	23	219	429	177	233	51
$(k_1 a_i + k_2) \bmod n$	30	2	7	23	21	0	12	2	18
Шифр	Э	В	Ж	Ц	Ф	А	Л	В	С

Продолжение таблицы 4

Текст	Р	О	М	А	Н	А	Л	Е	К
a_i	17	15	13	0	14	0	12	5	11
$k_1 \cdot a_i + k_2$	261	233	205	23	219	23	191	93	177
$(k_1 a_i + k_2) \bmod n$	30	2	7	23	21	23	26	27	12
Шифр	Э	В	Ж	Ц	Ф	Ц	Щ	Ъ	Л

Окончание таблицы 4

Текст	С	А	Н	Д	Р	О	В	И	Ч
a_i	18	0	14	4	17	15	2	9	24
$k_1 \cdot a_i + k_2$	275	23	219	79	261	233	51	149	359
$(k_1 a_i + k_2) \bmod n$	11	23	21	13	30	2	18	17	29
Шифр	К	Ц	Ф	М	Э	В	С	Р	Ь

Результат шифрования:

ЭВЖЦФАЛВСЭВЖЦФЦЩЪЛКЦФМЭВСРЬ.

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 14 столбцов, а так же шифрование шифром «железнодорожная изгородь» и шифрование с использованием ключевого слова ТЕПЛООБМЕН.

Выполнено шифрование методом поворачивающейся решетки размером 6х6 (9 отверстий) и применено шифрование подстановочным методом (аффинное преобразование) с функцией шифрования

$$c_i = (k_1 \cdot a_i + k_2) \bmod n = (14 \cdot a_i + 23) \bmod 33.$$