Лабораторная работа №1

Простейшие алгоритмы шифрования

Цель работы: изучить простейшие алгоритмы шифрования.

Выполнение работы.

1 ШИФРОВАНИЕ ПЕРЕСТАНОВОЧНЫМИ ШИФРАМИ

Исходный текст: Ковалёв Александр Константинович.

1.1 Шифрование простейшими перестановочными шифрами

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

КОВАЛЁВАЛЕКСАНДРКОНСТАНТИНОВИЧ.

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

КО ВА ЛЁ ВА ЛЕ КС АН ДР КО НС ТА НТ ИН ОВ ИЧ.

3.Запись слов в обратном порядке.
Результат шифрования:

ЧИВОНИТНАТСНОКРДНАСКЕЛАВЁЛАВОК.

4.Перестановка в виде матрицы 2 строки, 15 столбцов (см. таблицу 1): запись построчная, чтение по столбцам сверху вниз 1,3,5,7, 9,11,13,15,2,4, 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	15
Строки	К	О	В	А	Л	Ё	В	А	Л	Е	К	С	А	Н	Д
Строки	Р	К	О	Н	С	Т	А	Н	Т	И	Н	О	В	И	Ч

Результат шифрования:

КРВОЛСВАЛТКНАВДЧОКАНЁТАНЕИСОНИ.

1.2Шифрование шифром «железнодорожная изгородь»

Правило записи текста представлено на рисунке 1.

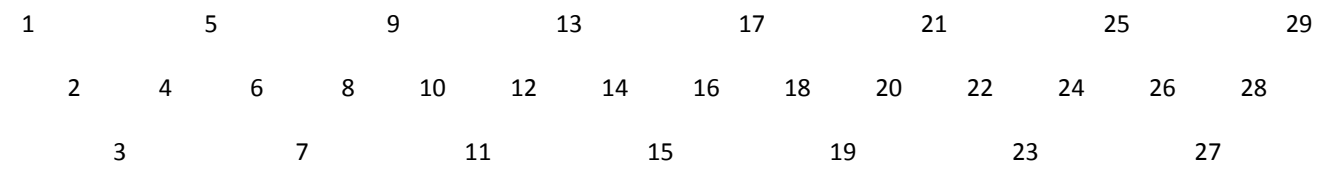

Рисунок 1 – Правило записи текста по методу «железнодорожная изгородь»

Запись исходного текста представлена на рисунке 2.

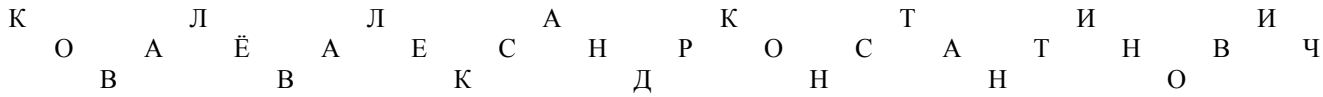

Рисунок 2 – Запись исходного текста по методу «железнодорожная изгородь»

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

КЛЛАКТИИОАЁАЕСНРОСАТНВЧВВКДННО.

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

М	**О**	**Н**	**О**	**Г**	**Р**	**А**	**Ф**	**И**	**Я**
4	**6**	**5**	**7**	**2**	**8**	**1**	**9**	**3**	**10**
К	О	В	А	Л	Ё	В	А	Л	Е
К	С	А	Н	Д	Р	К	О	Н	С
Т	А	Н	Т	И	Н	О	В	И	Ч

Результат шифрования:

ВКО ЛДИ ЛНИ ККТ ВАН ОСА АНТ ЁРН АОВ ЕСЧ.

1.4 Шифрование методом поворачивающейся решетки

По заданию размер решетки 6x6, 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 6x6 = 36 символов. Решетка – матрица (4x4), 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.

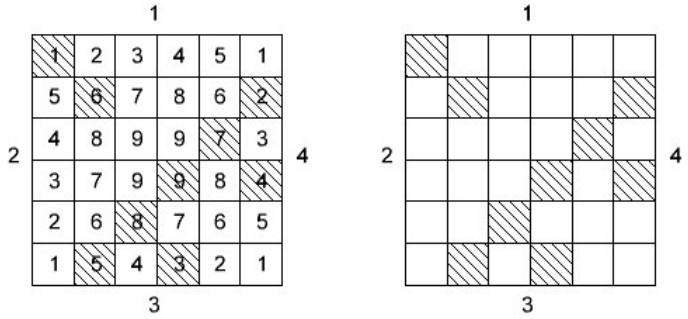

Рисунок 3 – Решетки 6x6 и количеством отверстий 9

Исходный текст:

КОВАЛЁВ АЛЕКСАНДР КОНСТАНТИНОВИЧ
ГЕОМЕТРИЯ ХИМИЯ АСТРОНОМИЯ МАТЕМАТИКА ЧЕРЧЕНИЕ

Шифрование методом поворачивающейся решетки показано на рисунке 4.

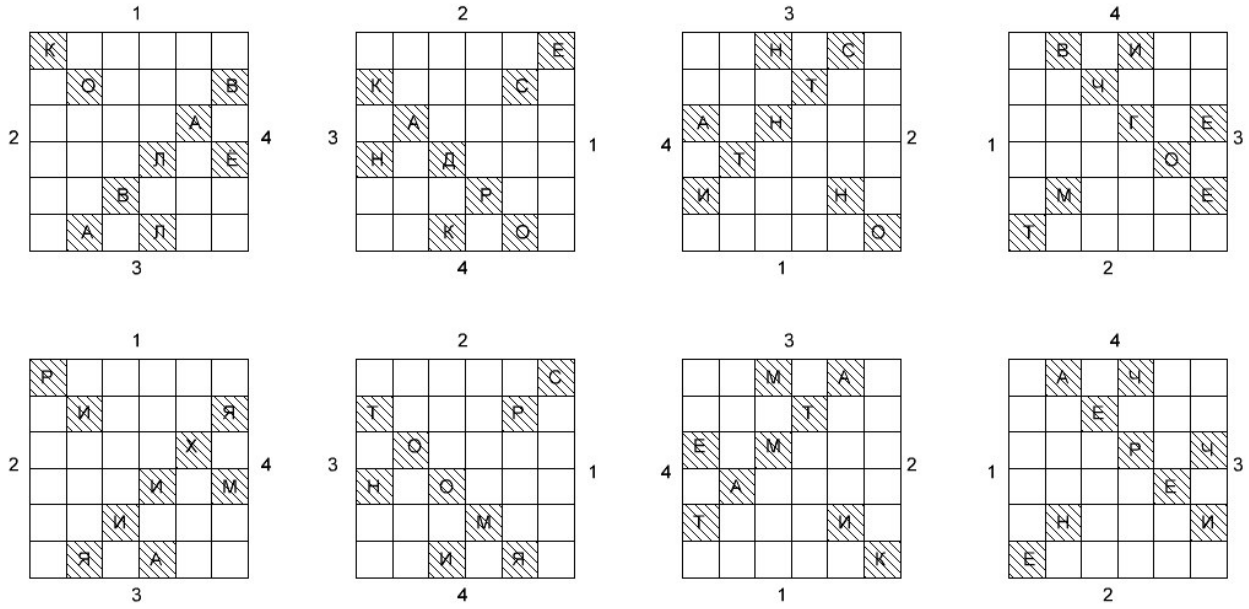

Рисунок 4 – Шифрование методом поворачивающейся решетки

Результат шифрования представлен на рисунке 5.

Первые 36 символов

К	В	Н	И	С	Е
К	О	Ч	Т	С	В
А	А	Н	Г	А	Е
Н	Т	Д	Л	О	Ё
И	М	В	Р	Н	Е
Т	А	К	Л	О	О

Остальные 36 символов

Р	А	М	Ч	А	С
Т	И	Е	Т	Р	Я
Е	О	М	Р	Х	Ч
Н	А	О	И	Е	М
Т	Н	И	М	И	И
Е	Я	И	А	Я	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 $k_1 = 6$ – номер в журнале. Так как ключ $k_1 = 6$ не удовлетворяет условию взаимной простоты, то принимаем ближайшее значение $k_1 = 7$.

Значение k_2 может быть любым, если k_1 не равно единице. Таким образом, принимаем: $k_2 = 19$.

Алгоритм шифрования следующий (см. таблицу 4):

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

2) Для каждого значения находим $(k_1 \cdot a_i + k_2) = (7 \cdot a_i + 19)$.

3) Для каждого символа возьмем остаток от деления $(7 \cdot a_i + 19)$ на 33.

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

Таблица 4 – Метод аффинного преобразования

Текст	К	О	В	А	Л	Ё	В	А	Л	Е
a_i	11	15	2	0	12	6	2	0	12	5
$k_1 \cdot a_i + k_2$	96	124	33	19	103	61	33	19	103	54
$(k_1 a_i + k_2) \bmod n$	30	25	0	19	4	28	0	19	4	21
Шифр	Э	Ш	А	Т	Д	Ы	А	Т	Д	Ф

Продолжение таблицы 4

Текст	К	С	А	Н	Д	Р	К	О	Н	С
a_i	11	18	0	14	4	17	11	15	14	18
$k_1 \cdot a_i + k_2$	96	145	19	117	47	138	96	124	117	145
$(k_1 a_i + k_2) \bmod n$	30	13	19	18	14	6	30	25	18	13
Шифр	Э	М	Т	С	Н	Ё	Э	Ш	С	М

Окончание таблицы 4

Текст	Т	А	Н	Т	И	Н	О	В	И	Ч
a_i	19	0	14	19	9	14	15	2	9	24
$k_1 \cdot a_i + k_2$	152	19	117	152	82	117	124	33	82	187
$(k_1 a_i + k_2) \bmod n$	20	19	18	20	16	18	25	0	16	22
Шифр	У	Т	С	У	П	С	Ш	А	П	Х

Результат шифрования:

ЭШАТДЫАТДФЭМТСНЁЭШСМУТСУПСШАПХ.

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 15 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

$$c_i = (k_1 \cdot a_i + k_2) \bmod n = (7 \cdot a_i + 19) \bmod 33.$$