Учреждение образования

«Белорусский государственный технологический университет»

**Лабораторная работа № 5**

Исследование криптографических шифров

на основе перестановки символов

Выполнила:

Студентка 3 курса 6 группы ФИТ

Булавский Кирилл

**2023 г.**

1. **Теоретические сведения**

Среди шифров рассматриваемого подкласса иногда выделяют шифры простой перестановки (или перестановки без ключа). Символы открытого текста Мi перемешиваются по каким-либо правилам. Формально каждое из таких правил может рассматриваться в качестве ключа.

Для использования шифров **одинарной перестановки** используется таблица, состоящая из двух строк: в первой строке записываются буквы, во второй – цифры J. Строки состоят из n столбцов. Буквы составляют шифруемое сообщение. Цифры J = j1, j2, …, jn, где j1 – номер позиции в зашифрованном сообщении первого символа открытого текста, где j2 – номер позиции в зашифрованном сообщении второго символа открытого текста и т. д. Таким образом, порядок следования цифр определяется используемым правилом (ключом) перестановки символов открытого текста для получения шифрограммы.

Шифры **простой блочной перестановки**. Блок должен состоять из 2-х или более символов. Если общее число таких символов в сообщении не кратно длине сообщения, то последний блок можно дополнить произвольными знаками.

Шифры **маршрутной перестановки**. Основой рассматриваемого типа является геометрическая фигура. Обычно прямоугольник или прямоугольная матрица. В ячейки этой фигуры по определенному маршруту записывается открытый текст.

Шифр **Скитала** (Сцитала). Известно, что в V веке до н. э. в Спарте существовала хорошо отработанная система секретной военной связи. Для этого использовался специальный жезл «скитала» (греч. σκυτάλη – первое, вероятно, простейшее криптографическое устройство, реализующее метод перестановки

**Организация маршрутной перестановки**. Уже упоминавшаяся маршрутная перестановка (записываем сообщение по строкам, считываем – по столбцам матрицы) можно усложнить и считывать не по столбцам, а по спирали, зигзагом, змейкой или каким-то другим способом.

Шифр **вертикальной перестановки.** Данный шифр является разновидностью шифра маршрутной перестановки. К особенностям вертикального шифра можно отнести следующие:

* количество столбцов в таблице фиксируется и определяется длиной ключа;
* маршрут вписывания: слева-направо, сверху-вниз;
* шифрограмма выписывается по столбцам в соответствии с их нумерацией (ключом).

Шифры **множественной перестановки.** Особенностью шифров данного подкласса является минимум двукратная перестановка символов шифруемого сообщения. В простейшем случае это может задаваться перемешиваем не только столбцов (как в примере 4), но и строк. Таким образом, этот случай соответствует использованию двух основных ключей: длина одного из них равна числу столбцов, другого – числу строк. К ключевой информацию мы можем относить также способы вписывания сообщения и считывания отдельных символов из текущего столбца матрицы.

1. **Практическая часть**

В данной лабораторной работе необходимо разработать авторское приложение для шифрования с использованием русского алфавита:

• Маршрутная перестановка (маршрут: змейка);

• Множественная перестановка, ключевые слова – собственные имя и фамилия.

Наглядно маршрутную перестановку змейкой можно представить так, как на рисунке 2.1.

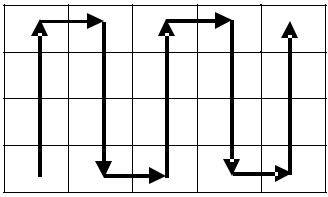


Рисунок 2.1 – Графический вид маршрутной перестановки змейкой

Для реализации данной перестановки был написан следующий программный алгоритм, представленный на рисунке 2.2.



Рисунок 2.2 – Программная реализация маршрутной перестановки зигзагом

В ходе алгоритма из исходной матрицы текста путем ее обхода по спирали создается новая матрица encryptMess, в которой элементы расположены нужным образом. Таким образом, превратив эту матрицу в строку (одномерный массив), получим зашифрованное сообщение. Вид программного средства можно увидеть на рисунке 2.3.



Рисунок 2.3 – Интерфейс программного средства

Слева расположена матрица исходного текста. Справа – зашифрованный текст путем обхода исходной матрицы зигзагом. Также там можно увидеть время выполнения функции. Расшифровать сообщение помогает обратный обход матрицы зашифрованного сообщения, код которого представлен в листинге 2.1.

|  |
| --- |
| function decrypt(*encryptText*) {      let decryptArr = [];      for (let i = 0; i < ROWS; i++) {          decryptArr[i] = [];      }      let even = true,          odd = false,          encryptIndex = 0;      let timeStart = performance.now();  *///////////////////////     START     ///////////////////////*      for (let i = 0; i < COLUMS; i++) {          if (even) {              for (let j = 0; j < ROWS; j++) {                  decryptArr[j][i] = *encryptText*[encryptIndex++];              }              if (*encryptText* != *encryptText*.length) {                  even = false;                  odd = true;                  continue;              } else {                  break;              }          }          if (odd) {              for (let j = ROWS - 1; j >= 0; j--) {                  decryptArr[j][i] = *encryptText*[encryptIndex++];              }              if (*encryptText* != *encryptText*.length) {                  even = true;                  odd = false;                  continue;              } else {                  break;              }          }      }  *///////////////////////     FINISH     ///////////////////////*      let timeFinish = performance.now();      return decryptArr;  } |

Листинг 2.1 – Расшифровка сообщения

Расшифрованное сообщение представлено на рисунке 2.4.

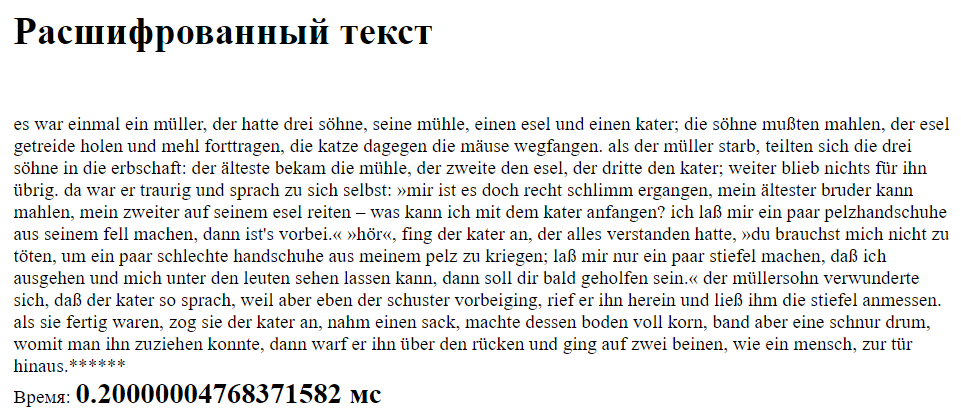


Рисунок 2.3 – Расшифрованное сообщение

Гистограммы полученных сообщений (рисунок 2.4):

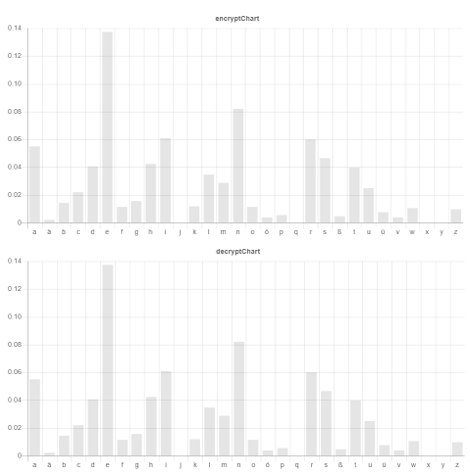


Рисунок 2.4 – Гистограммы сообщений

Как видно из гистограмм, частоты появления символов алфавита не изменились, так как расшифрованное и зашифрованное сообщения состоят из одних и тех же символов.

Для реализации шифра с множественными перестановками было разработано следующее приложение (рисунок 2.5).



Рисунок 2.5 – Приложение реализации шифра множественных перестановок

Функция шифрования представлена на рисунке 2.6.



Рисунок 2.6 –Функция шифрования множественных перестановок

Выполняется двукратная перестановка символов шифруемого сообщения. В алгоритме происходит перемешивание не только столбцов, но и строк.

В данном случае длина шифруемого сообщения ограничена произведением длины ключевых слов, а именно длиной имени (Valeria – 7) и фамилии (Troshko – 7). То есть максимальная длина сообщения 7\*7=49 символа.

Для расшифрования выполняется обратная перестановка, алгоритм представлен на рисунке 2.7.



Рисунок 2.7 –Функция шифрования множественных перестановок

Гистограммы двух сообщений, как и в случае маршрутной перестановки, не отличаются друг от друга (рисунок 2.8).

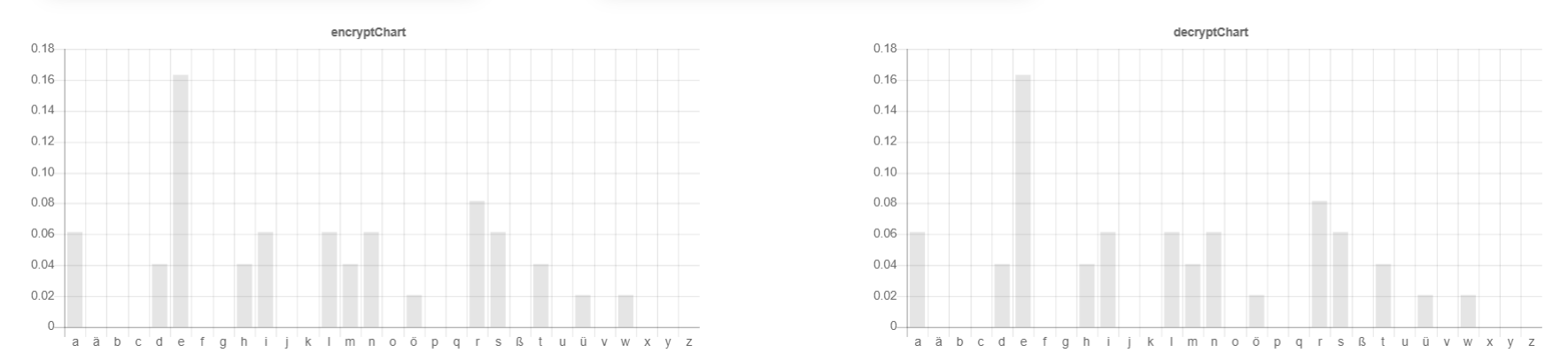


Рисунок 2.8 – Гистограммы сообщений

**Вывод:** таким образом, в данной лабораторной работе я закрепила теоретические знания по перестановочным шифрам, а также, разработала приложение для работы с множественной и маршрутной перестановками.