МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

**«ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПЕРЕСТАНОВКИ СИМВОЛОВ»**

Студент: Бутурля Р.А.

ФИТ 3 курс 5 группа

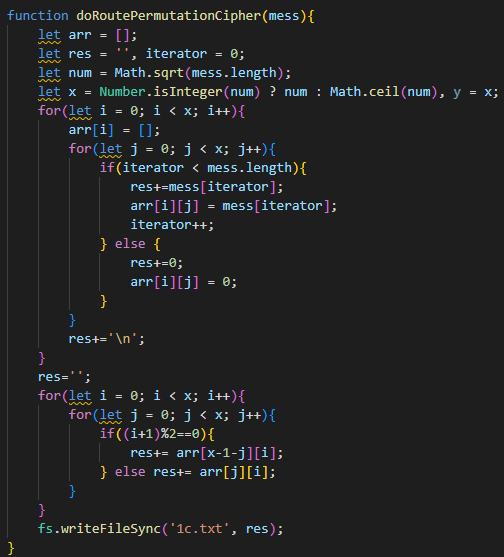
Вариант 3

Преподаватель: Савельева М. Г.

Минск 2023

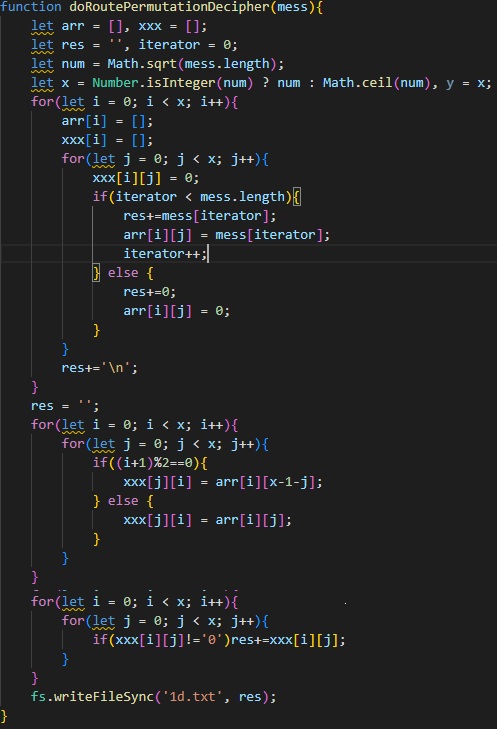
1. Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:
   1. выполнять зашифрование/расшифрование текстовых документов (объемом не менее 500 знаков), созданных на основе алфавита языка в соответствии с таблицей вариантов задания:

Метод doRoutePermutationCipher(mess) реализует шифр маршрутной перестановки зиг­зага. В первом цикле все символы сообщения записываются в двумерный массив. Во втором цикле данные двумерного массива считываются согласно маршруту – зигзаг.



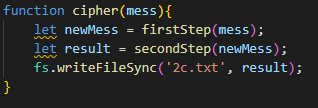
Листинг 1– Метод doRoutePermutationCipher(mess)

Метод doRoutePermutationDecipher(mess) расшифрует входящее зашифрованное методом маршрутной перестановки(зигзаг) сообщение. Сперва требуется считать входящее сообщение в двумерный массив, а следом считать массив так же, как и при шифровании, но сменив ось.



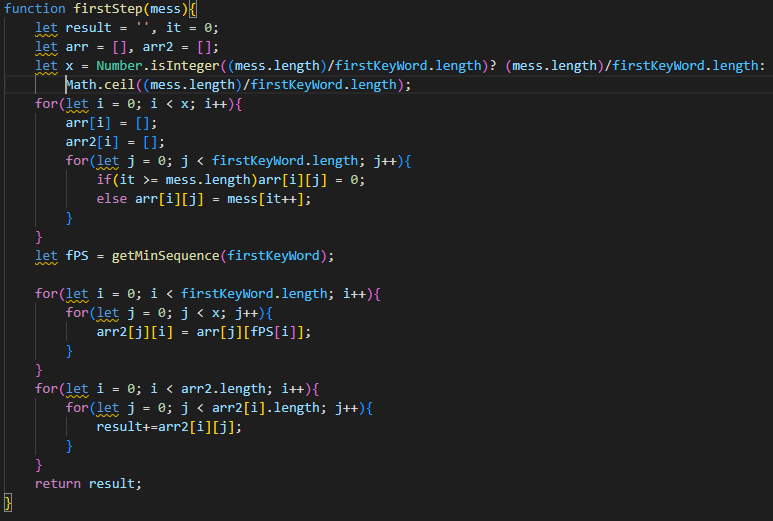
Листинг 2 – Метод doRoutePermutationDecipher (mess)

Метод cipher(mess) разработан для шифрования сообщения методом множественной перестановки(ключевые слова – имя и фамилия). Задача метода – управление побочными методами.

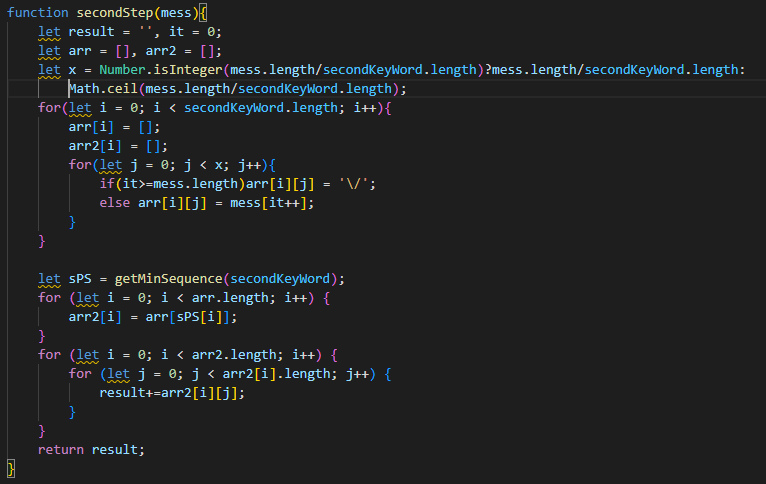


Листинг 3 – Метод cipher(mess)

Метод firstStep(mess) предназначен для шифрования сообщения следующим способом: запись сообщения в массив, а после перестановка столбцов массива по ключу.

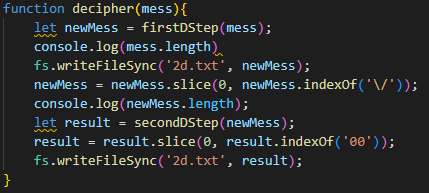
****

Листинг 4 – Метод firstStep(mess)

Метод secondStep(mess) предназначен для шифрования сообщения следующим способом: запись сообщения в массив, а после перестановка строк массива по ключу.

Листинг 5 – Метода secondStep(mess)

Метод decipher(mess) разработан для расшифровки сообщения, зашифрованное методом множественной перестановки(ключевые слова – имя и фамилия). Задача метода – управление побочными методами.



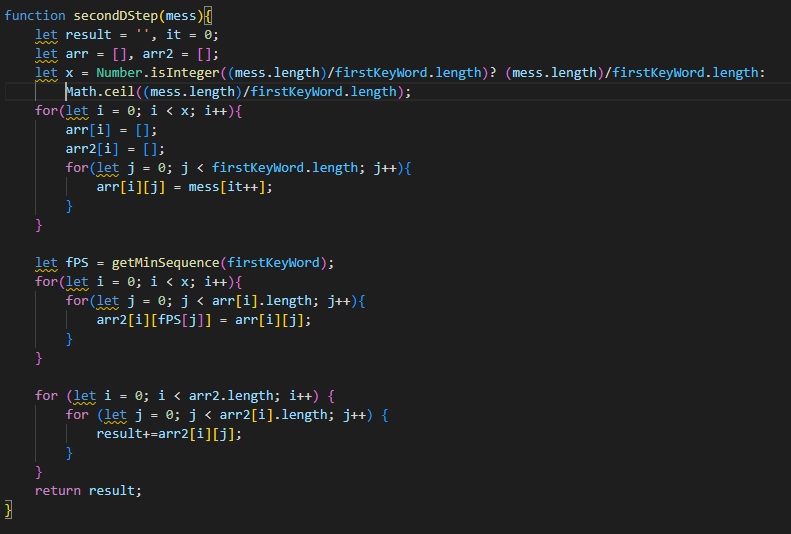
Листинг 6 – Метод decipher(mess)

Метод firstDStep(mess) предназначен для расшифровки сообщения следующим способом: запись сообщения в массив, а после перестановка строк массива в соответствии с ключом.

****

Листинг 7 – Метод firstDStep(mess)

Метод secondDStep(mess) предназначен для расшифрования сообщения следующим способом: запись сообщения в массив, а после перестановка столбцов массива в соответствии с ключом.



Листинг 8 – Метод secondDStep(mess)

* 1. Формировать гистограммы частот появления символов для исходного и зашифрованного сообщений:

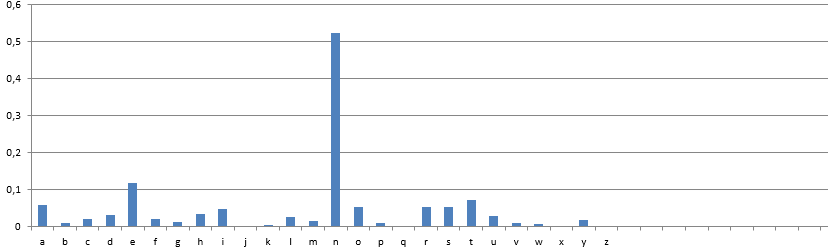


Рисунок 1 – Гистограмма частот появления символов входящего сообщения



Рисунок 2 – Гистограмма частот появления символов зашифрованного сообщения методом маршрутной перестановки

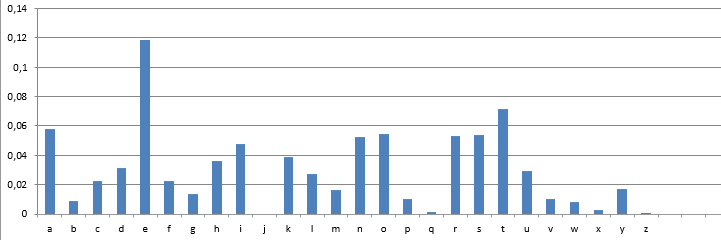


Рисунок 3 – Гистограмма частот появления символов зашифрованного сообщения методом множественной перестановки

* 1. Оценивать время выполнения операций зашифрования/расшифрования:

Результаты работы функции(количество символов – 1172/1525/3050):

* шифровка маршрутной перестановкой(rC) – 1,75 / 1,91 / 1,99;
* расшифровка маршрутной перестановкой(rD) – 2,96 / 2,53 / 3, 89;
* шифровка множественной перестановкой(C) – 1,95 / 2,68 / 3,13;
* расшифрока множественной перестановкой(D) – 5,39 / 4,28 / 8, 29.

Рисунок 4 ­­­– Графики затраченного времени

**Вывод**

Изучил и приобрел практические навыки разработки и использования приложений для реализации шифров на основе перестановки символов.