Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование криптографических шифров на основе перестановки символов

Студент: Чёрная Я.Р.

ФИТ 3 курс 4 группа

Преподаватель: Нистюк О.А,

Минск 2025

**Задание 1**

Язык - Немецкий

1. Маршрутная перестановка (маршрут змейкой; параметры таблицы – по указанию преподавателя)

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

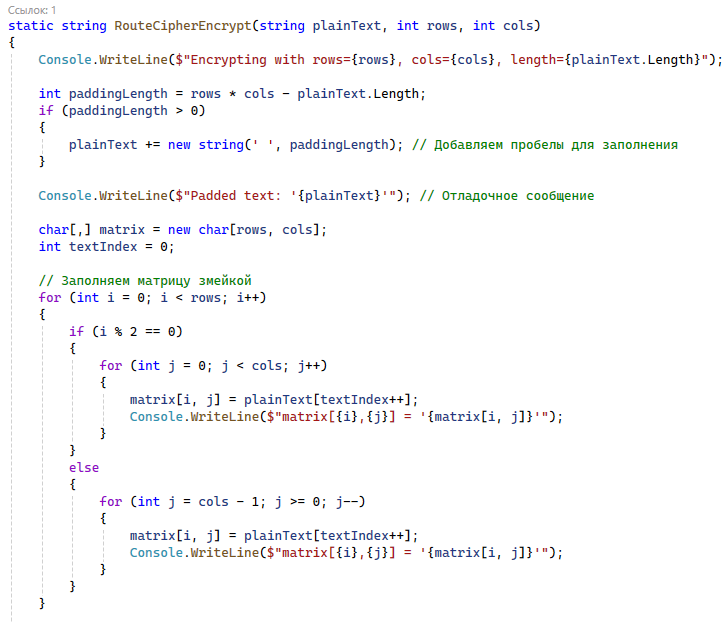


Рисунок 1 – Функция зашифрования маршрутное перестановкой

(змейкой)

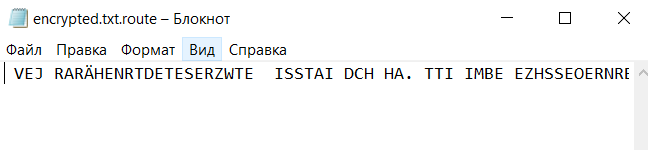


Рисунок 2 – зашифрованный текст

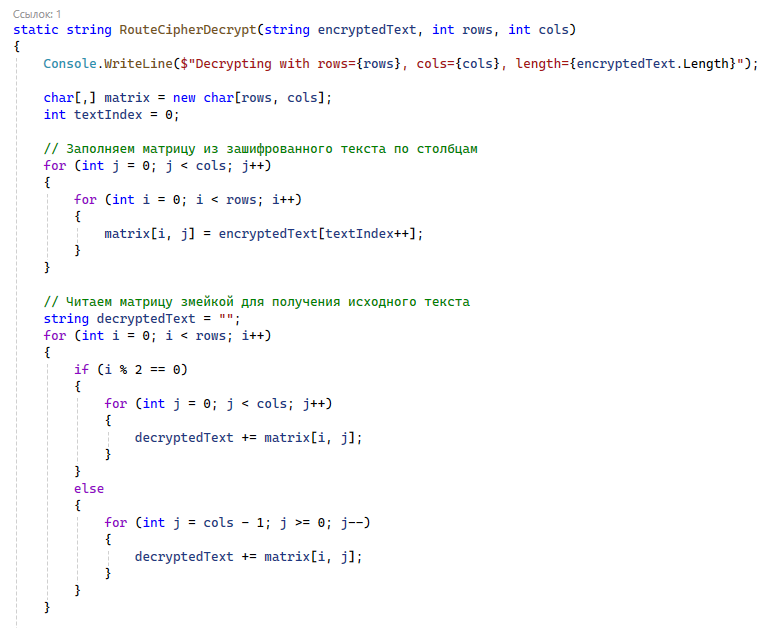


Рисунок 3 – функция расшифрования метода маршрутной перестановки

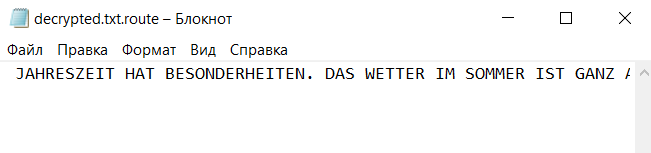


Рисунок 4 – расшифрованный текст

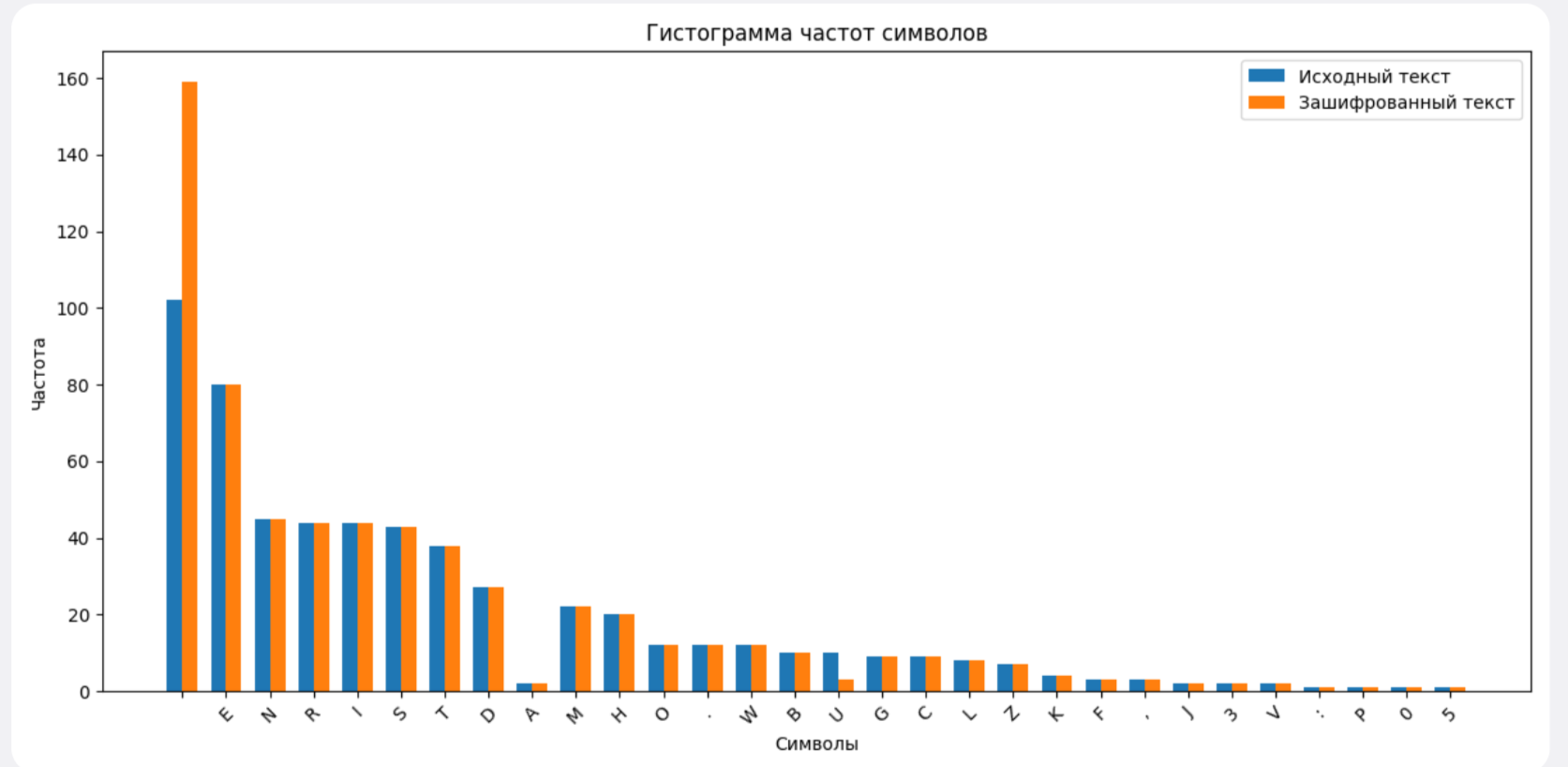


Рисунок 5 – гистограмма частот символов до и после шифрования

Количество символов не изменилось. Пробелов стало больше поскольку при создании таблицы для данного метода была взята таблица, размер кооторый превышает количество символов в тексте, следовательно все пустые ячейки были заполнены пробелом.

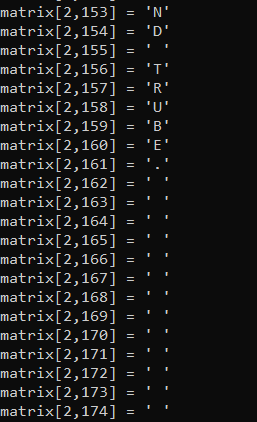


Рисунок 6 – заполнение пустых клеток символом пробела

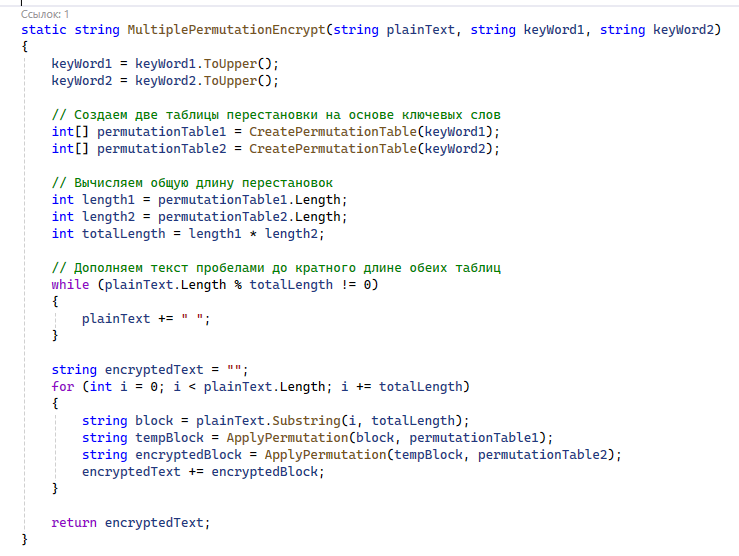


Рисунок 7 – зашифрование множественной перестановкой

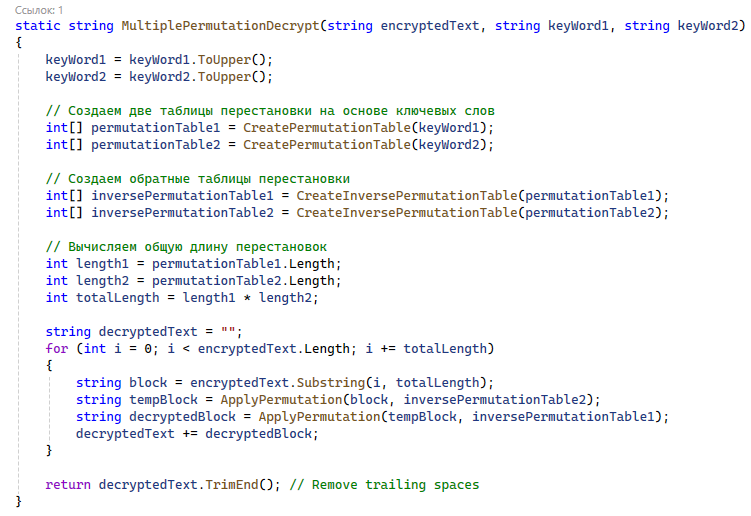


Рисунок 8 – расшифрование множественной перестановки

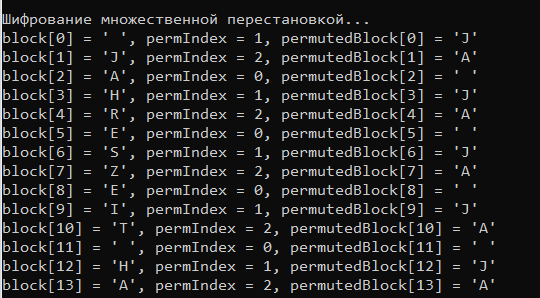


Рисунок 9 – процесс зашифрования

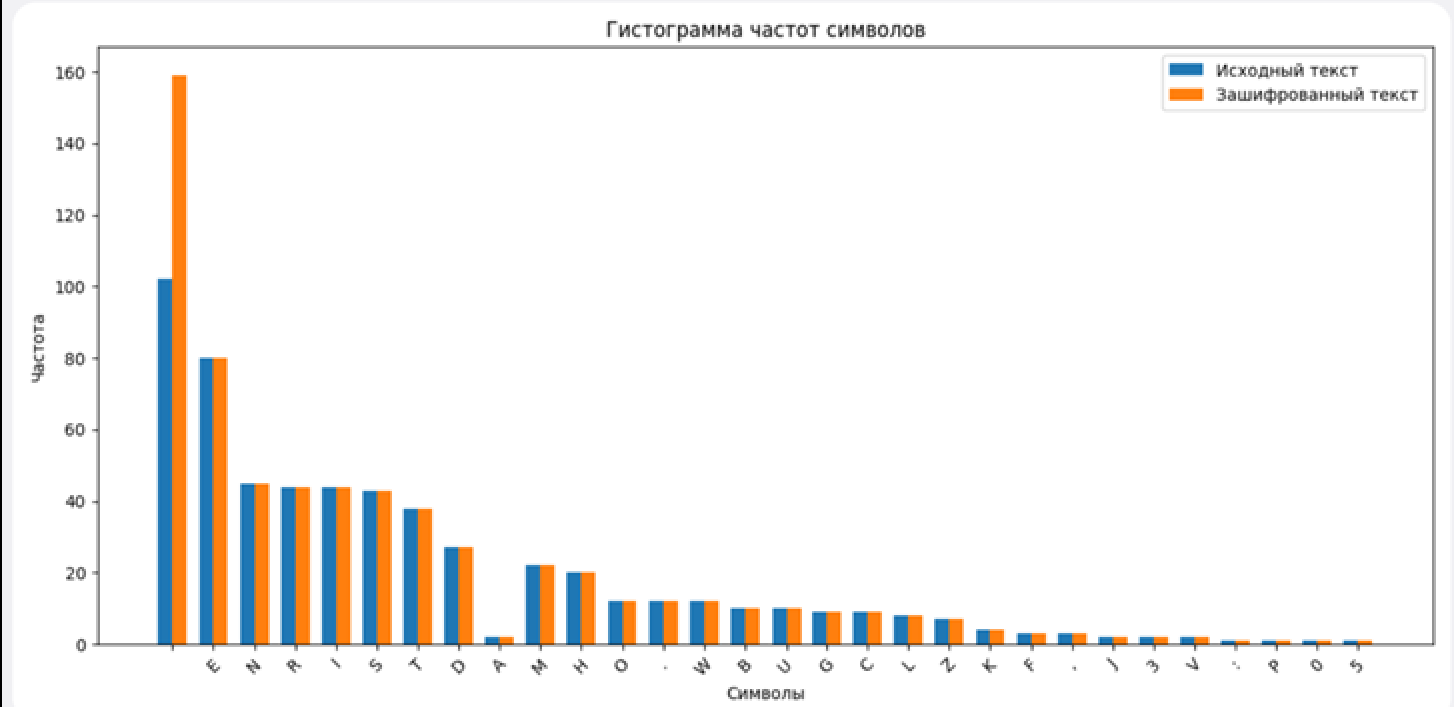


Рисунок 10 – Гистограмма символов

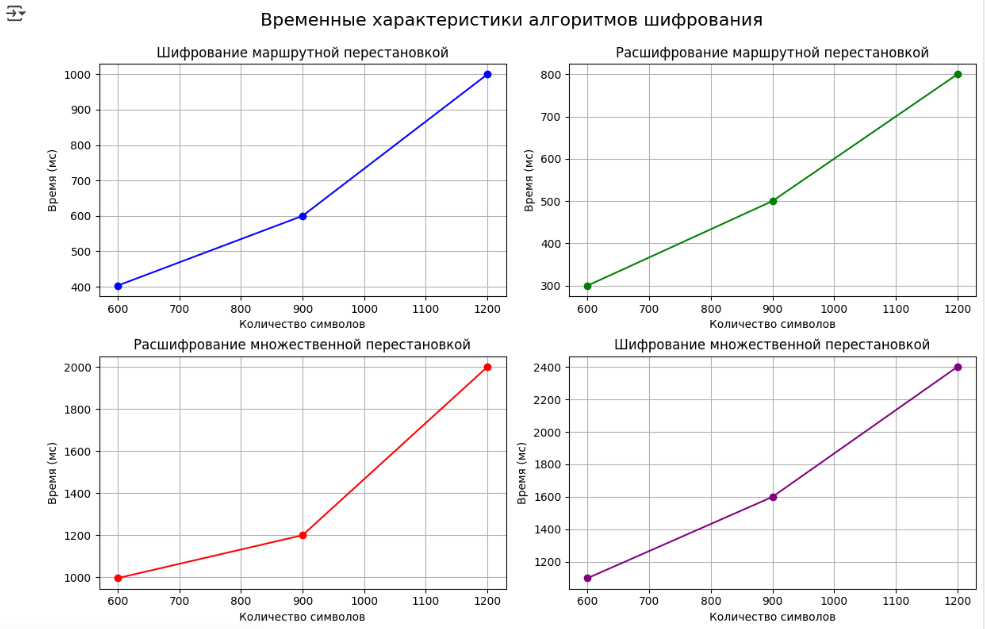


Рисунок 11 – Графики зависимости времени от количества символов

Вывод: изучили и приобрели практические навыки разработки и использования приложений для реализации перестановочных шифров.