Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет к лабораторной работе №3**

**«Исследование криптографических шифров на основе перестановки символов»**

Выполнил:

студентка 3 курса 2 группы

Черноок Ю. С.

Проверил:

ассистент

Копыток Д. В.

Минск 2021

Цель: изучение и приобретение практических навыков разработки и использования приложений для реализации подстановочных шифров.

**Теоретическая часть**

Сущность перестановочного шифрования состоит в том, что исходный текст (М) и зашифрованный текст (С) основаны на использовании одного и того же алфавита, а тайной или ключевой информацией является алгоритм перестановки.

Шифры перестановки относятся к классу симметричных. Элементами текста могут быть отдельные символы (самый распространенный случай), пары, тройки букв и т. д.

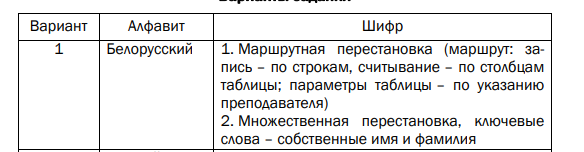
Классическими примерами перестановочных шифров являются анаграммы. Анаграмма – литературный прием, состоящий в перестановке букв (или звуков), что в результате дает другое слово или словосочетание, например: проездной – подрезной, листовка – вокалист, апельсин – спаниель. В классической криптографии шифры перестановки делятся на два подкласса:

* шифры простой, или одинарной, перестановки – при зашифровании символы открытого текста Мi перемещаются с исходных позиций в новые (в шифртексте Сi) один раз;
* шифры сложной, или множественной, перестановки – при зашифровании символы открытого текста Мi перемещаются с исходных позиций в новые (в шифртексте Сi) несколько раз.

**Практическая часть**

Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:

* выполнять зашифрование/расшифрование текстовых документов (объемом не менее 500 знаков), созданных на основе алфавита языка в соответствии с ниже следующей таблицей вариантов задания; при этом следует использовать шифры подстановки из третьего столбца данной таблицы.



* формировать гистограммы частот появления символов для исходного и зашифрованного сообщений;
* оценивать время выполнения операций зашифрования и расшифрования.

Рассмотрим реализацию маршрутной перестановки.

Программный код для шифрования сообщения данным методом представлен на рисунке 1.

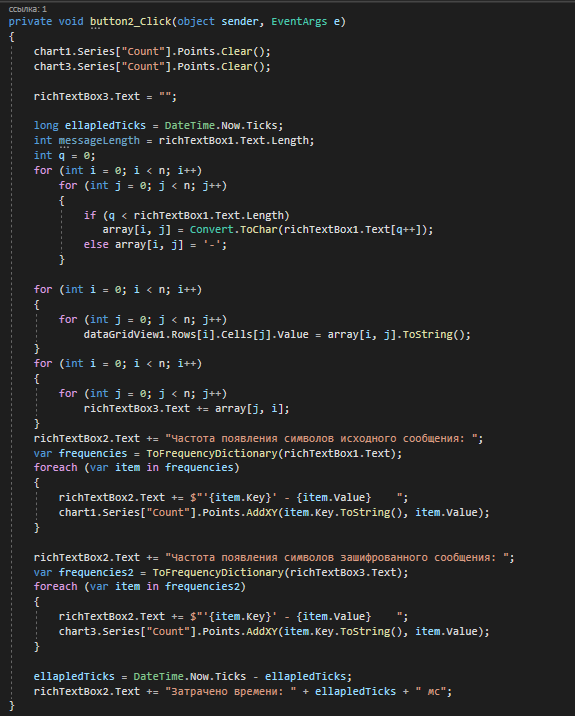


Рисунок 1 – Шифрование с помощью маршрутной перестановки

Программный код для дешифрования сообщения представлен на рисунке 2.

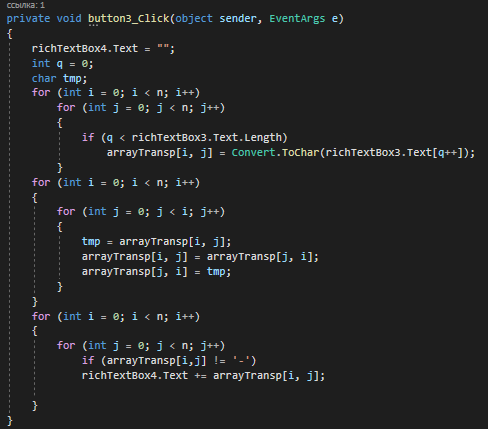


Рисунок 2 – Дешифрование с помощью маршрутной перестановки

Далее рассмотрим реализацию множественной перестановки.

Код шифрования сообщения представлен на рисунках 3.

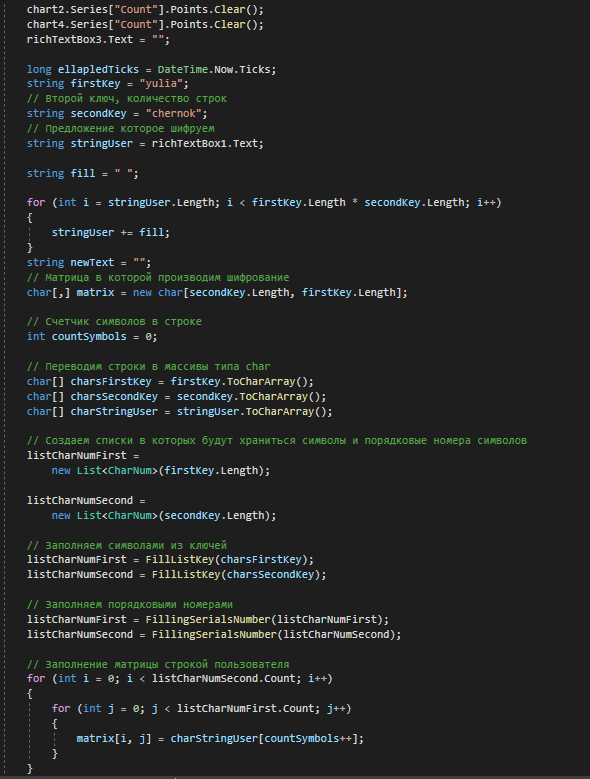


Рисунок 3 – Шифрование с помощью множественной перестановки

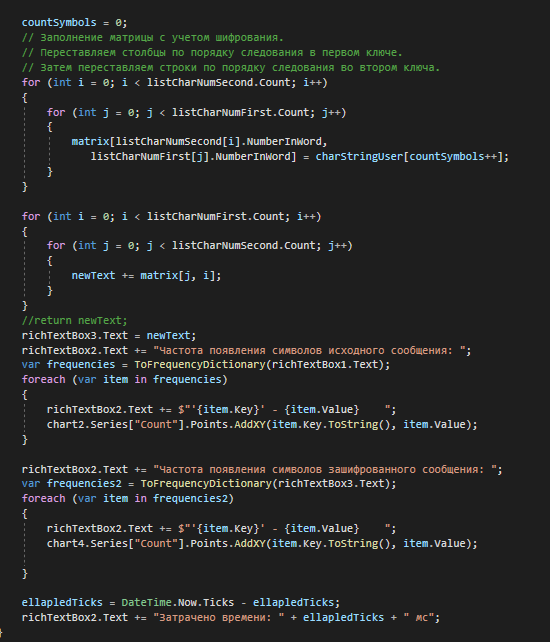


Рисунок 4 – Шифрование с помощью множественной перестановки

Реализация дешифрования множественной перестановкой представлена на рисунке 5.

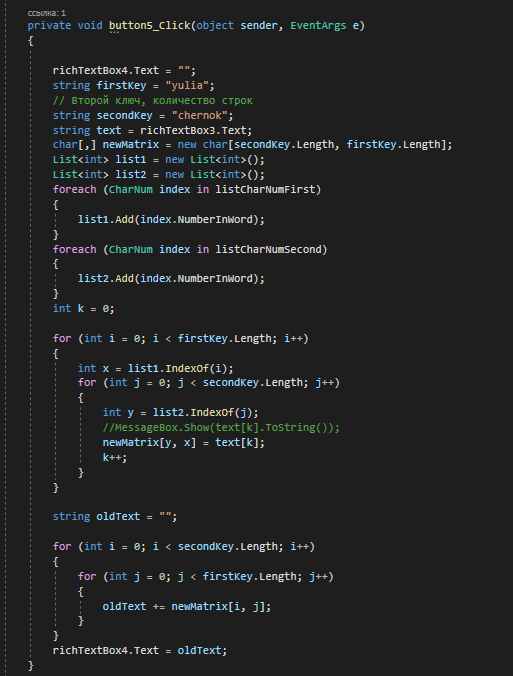


Рисунок 5 – Дешифрование с помощью множественной перестановки

Результат шифрования и расшифрования маршрутной перестановкой представлен на рисунке 6.

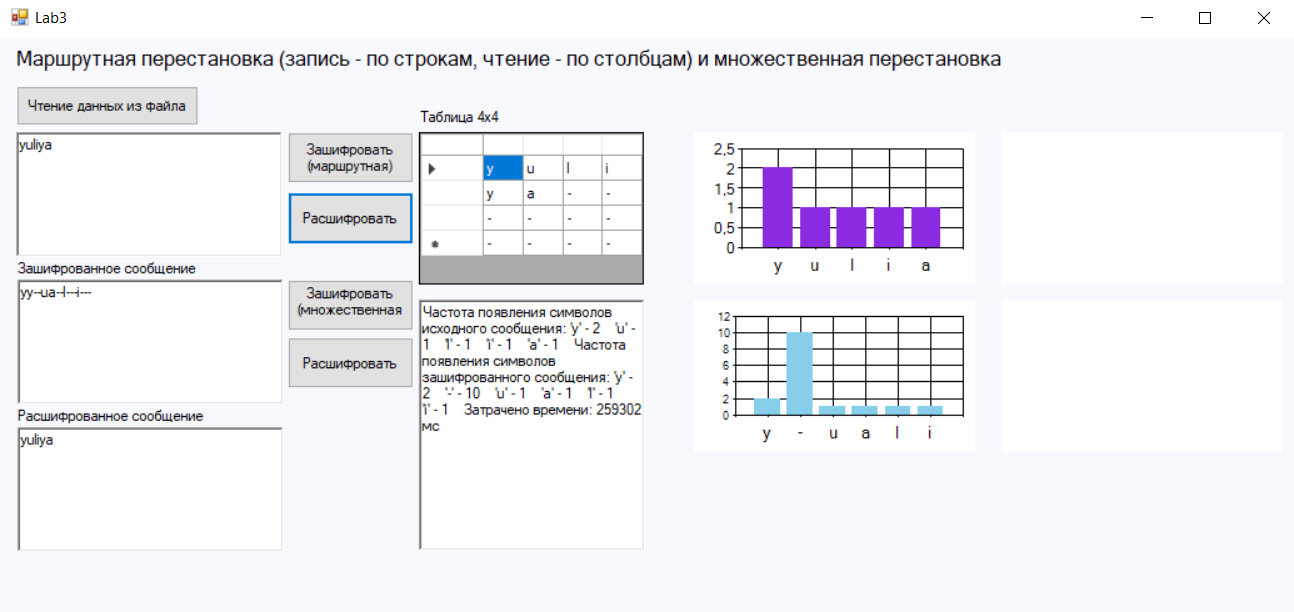


Рисунок 6 – Маршрутная перестановка

Результат шифрования и расшифрования множественной перестановкой представлен на рисунке 7.

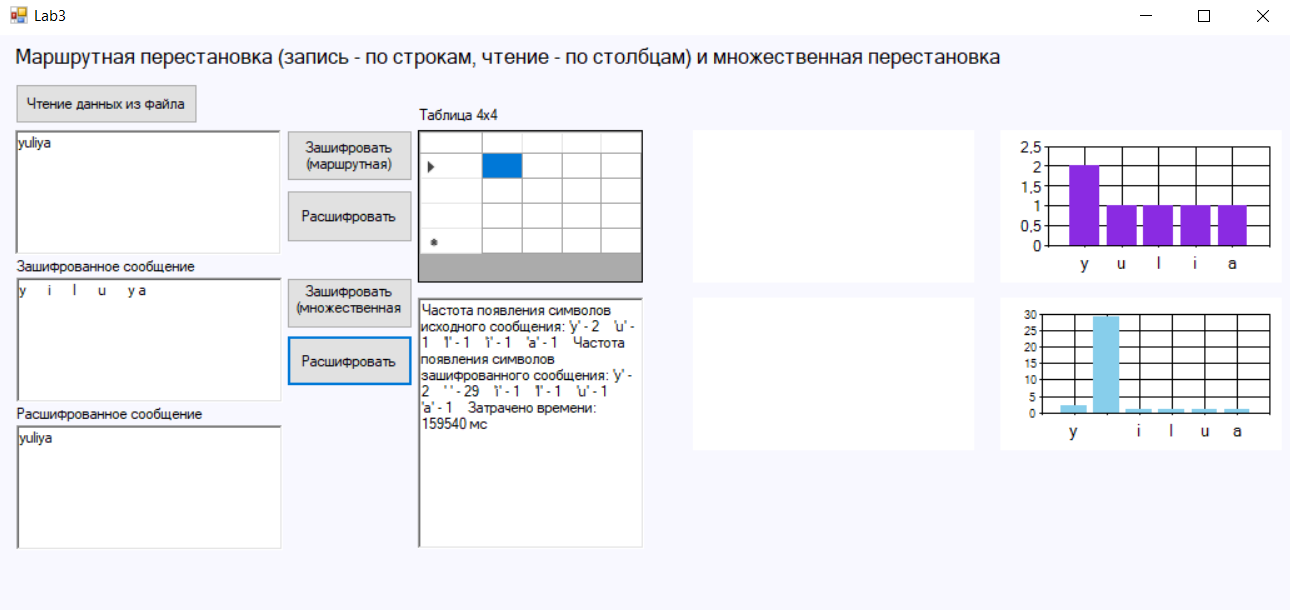


Рисунок 7 – Множественная перестановка

Вывод: я изучила и приобрела практические навыки разработки и использования приложений для реализации перестановочных шифров.