Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование криптографических шифров на основе перестановки символов**

Студент: Буданова К. А.

ФИТ 3 курс 5 группа

Преподаватель:

Савельева Маргарита Геннадьевна

1. **Цель работы**

Изучение и приобретение практических навыков разработки и использования приложений для реализации перестановочных шифров.

1. **Задание**

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 нижеследующей таблицей вариантов задания; при этом следует использовать шифры подстановки из третьего столбца данной таблицы;
2. формировать гистограммы частот появления символов для исходного и зашифрованного сообщений;
3. оценивать время выполнения операций зашифрования/расшифрования.
4. **Ход работы**

В соответствии с вариантом, алфавит выбран английский, для первого задания использовалась маршрутная перестановка (маршрут – зигзаг), для второго задания использовалась множественная перестановка, ключевые слова – собственные имя и фамилия.

Для обоих заданий следовало оценить время выполнения операций шифрования/дешифрования сообщений. Для этого был использован специальный класс Stopwatch на языке C#, который предоставляет функциональность для измерения времени выполнения операций и который представлен в директиве System.Diagnostics. Пример использования объекта данного класса представлен на рисунке 3.1.

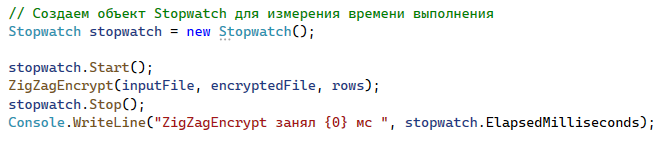


Рисунок 3.1 – Пример использования класса Stopwatch

Также, для этих заданий следовало сформировать гистограммы частот появления символов для исходного и зашифрованного сообщений. Для этой цели была разработана функция CountCharacterFrequency, представленная на рисунке 3.2.

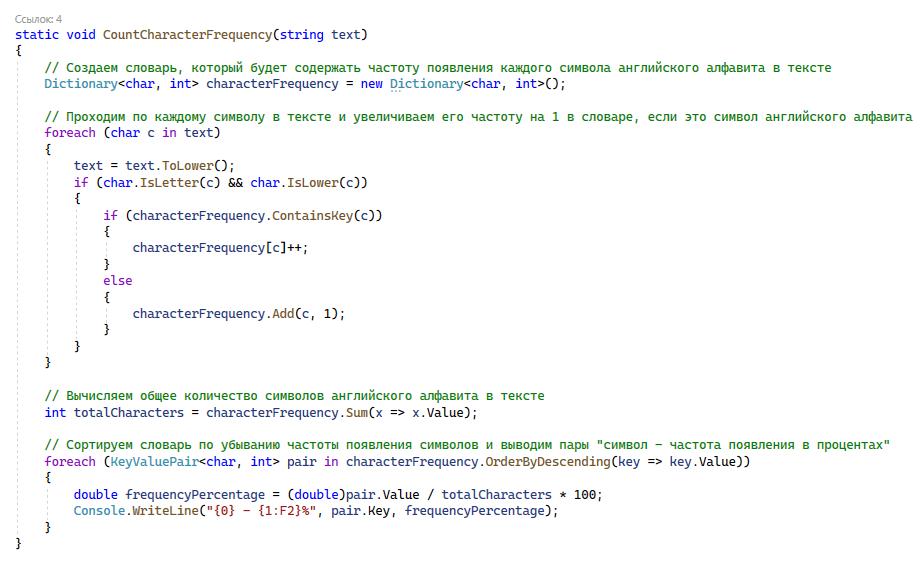


Рисунок 3.2 – Функция для определения частот появления символов

Для выполнения первого задания были разработаны функции ZigZagEncrypt и ZigZagDecrypt, которые осуществляют шифрование и дешифрование текста с использованием маршрутной перестановки. Они представлены на рисунках 3.3 и 3.4.

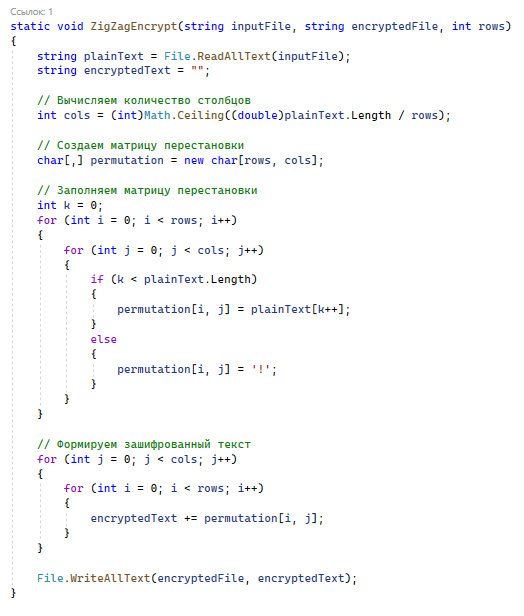


Рисунок 3.3 – Функция для шифрования текста с помощью маршрутной перестановки (маршрут – зигзаг)

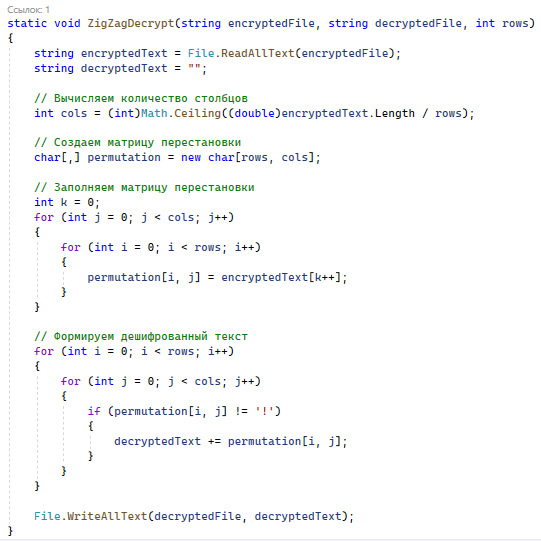


Рисунок 3.4 – Функция для дешифрования текста с помощью маршрутной перестановки (маршрут – зигзаг)

Входные данные и результаты выполнения данных функций представлены на рисунках 3.5 – 3.8.



Рисунок 3.5 – Входные данные для алгоритма маршрутной перестановки

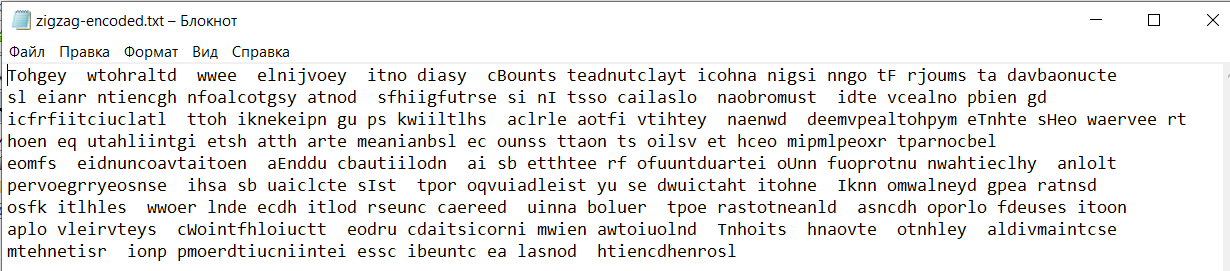


Рисунок 3.6 – Текст, зашифрованный с помощью функции ZigZagEncrypt

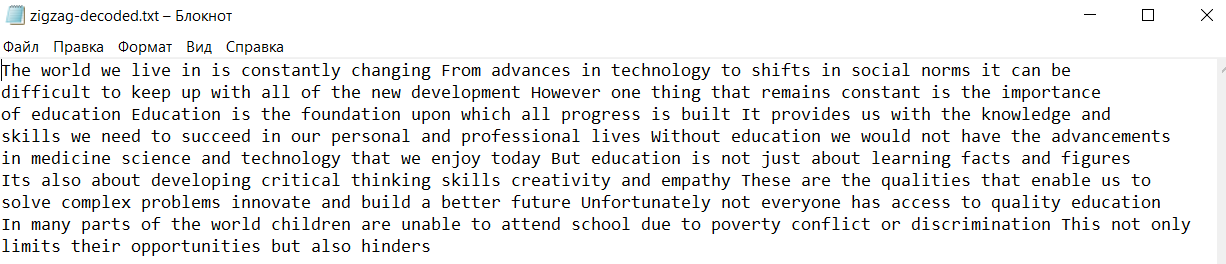


Рисунок 3.7 – Текст, расшифрованный с помощью функции ZigZagDecrypt

Рисунок 3.8 – Оценка скорости выполнения шифрования/дешифрования текста

Частота появления символов в этих текстовых файлах представлена на рисунках 3.9 и 3.10 соответственно.

Рисунок 3.9 – Гистограмма частот появления символов для зашифрованного текста

Рисунок 3.10 – Гистограмма частот появления символов для расшифрованного текста

Для выполнения второго задания были разработаны функции MultiplePermutationEncrypt и MultiplePermutationEncrypt, которые реализуют алгоритм шифрования текста с помощью алгоритма множественной перестановки (ключ – имя и фамилия). Код реализации этих функций представлен на рисунках 3.11 и 3.12.

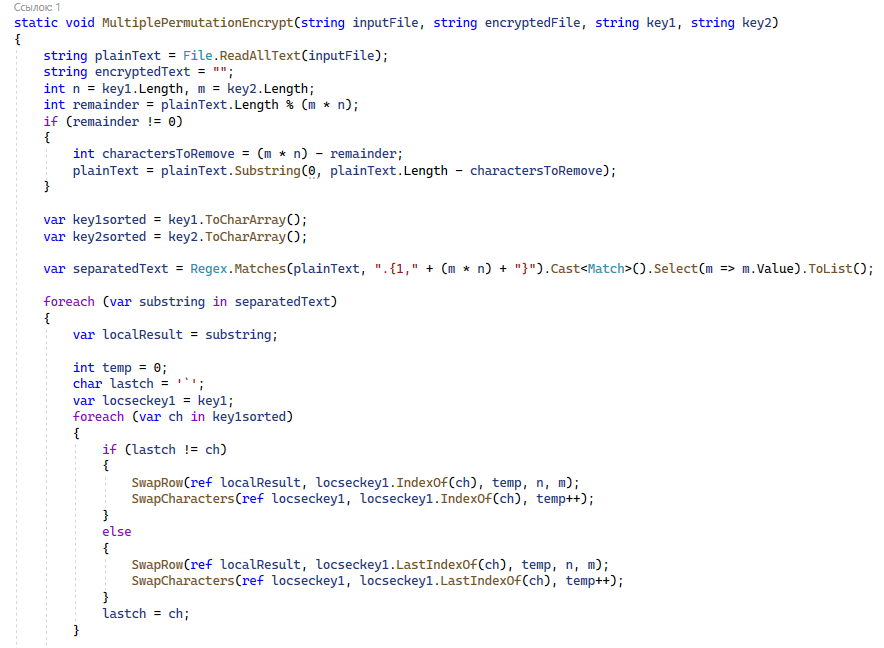


Рисунок 3.11 – Функция для шифрования текста с помощь алгоритма множественной перестановки

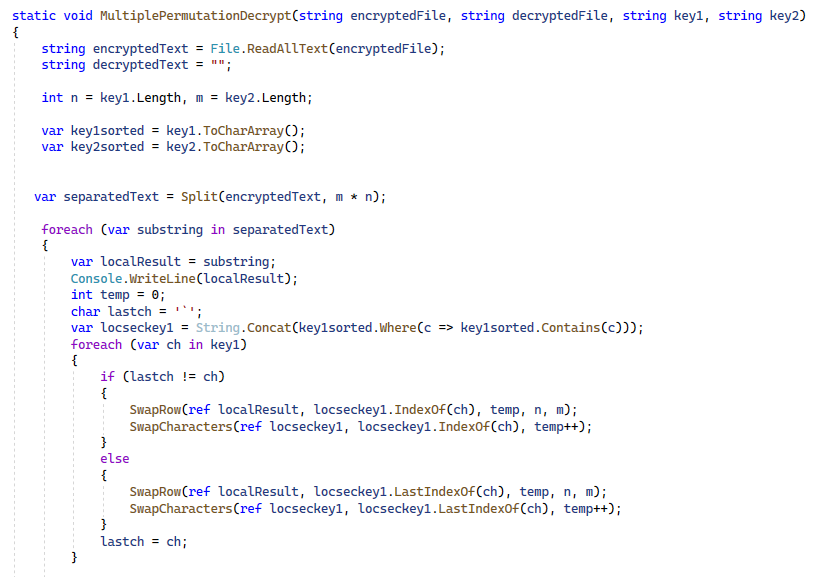




Рисунок 3.12 – Функция для дешифрования текста с помощью алгоритма множественной перестановки

В результате получаем следующие файлы и вывод, представленные на рисунках 3.13 – 3.14.

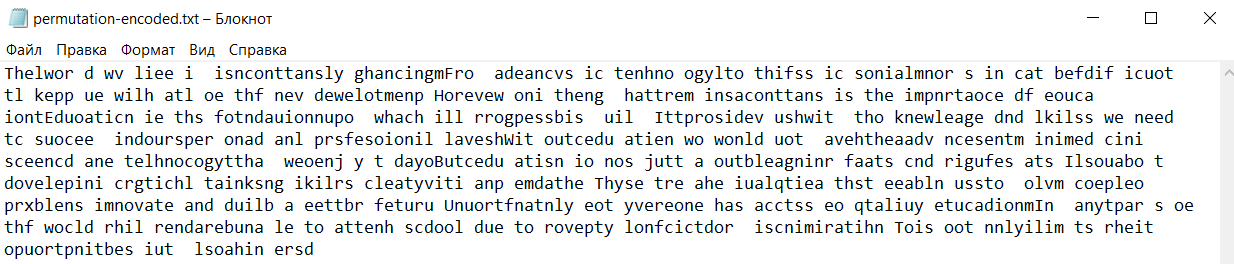


Рисунок 3.13 – Текст, зашифрованный с помощью функции MultiplePermutationEncrypt

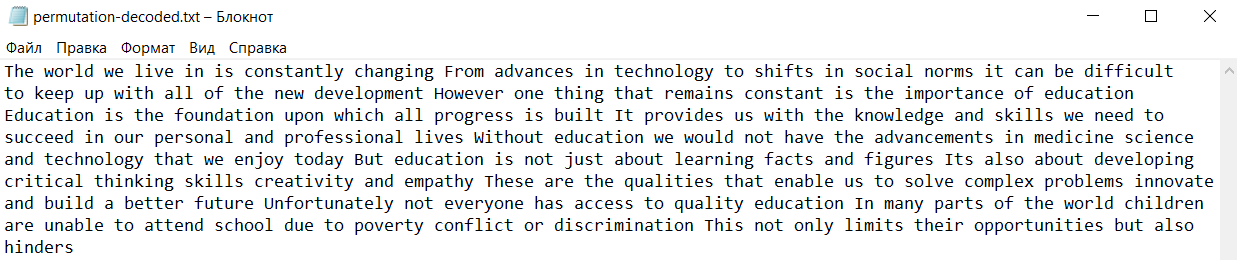


Рисунок 3.14 – Текст, расшифрованный с помощью функции MultiplePermutationDecrypt

Рисунок 3.15 – Оценка скорости выполнения шифрования/дешифрования текста

Частота появления символов в этих текстовых файлах представлена на рисунках 3.16 и 3.17 соответственно.

Рисунок 3.16 – Гистограмма частот появления символов для зашифрованного текста

Рисунок 3.17 – Гистограмма частот появления символов для расшифрованного текста

**Вывод**

В ходе лабораторной работы были изучены и приобретены практические навыки разработки и использования приложений для реализации перестановочных шифров.

Кроме того, были сформированы гистограммы появления частот на основе зашифрованных/расшифрованных сообщений. Из графиков видно, что частота символов в зашифрованном тексте вовсе не отличается от частоты символов в исходном тексте. Это обусловлено тем, что перестановочные шифры не заменяют символы открытого текста на другие символы или последовательность символов, а просто меняют порядок их следования.

Также было разработано авторское приложение в соответствии с целью лабораторной работы.