Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ**

**ШИФРОВ НА ОСНОВЕ**

**ПЕРЕСТАНОВКИ СИМВОЛОВ**

Студент: Раченок И.А.

ФИТ 3 курс 4 группа

Преподаватель:

Сазонова Дарья Владимировна

Минск 2023

1. **Описание приложения**

Приложение написано на языке C# и выполняет следующие методы:

* метод маршрутной перестановки;
* метод множественной перестановки;
* метод подсчета количества времени выполнения операция зашифрования;
* метод обработки символов расчета частоты появлений символов.

1. **Методика выполнения поставленных задач**

Первый пункт моего задания заключался в шифрование текста при помощи маршрутной перестановки, а именно запись шла по строкам, а считывание по столбцам. Чтобы реализовать этот алгоритм следует использовать таблицу, функция которая реализует этот алгоритм, и инициализирует таблицу представлена на рисунке 2.1

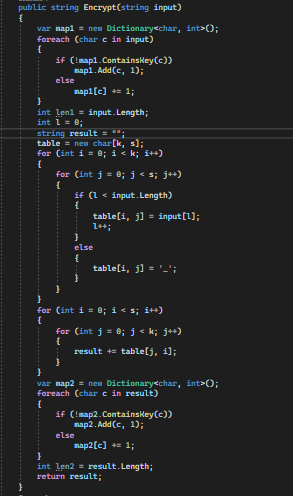


Рисунок 2.1 – Функция маршрутной перестановки(Encrypt)

Также если по заполнению таблицы будут пустые места (весь текст ввели но по размеру не хватает символов до ее полного заполнения) то они будут заполнены нижним подчеркиванием. Ниже представлена функция дешифрования, рисунок 2.2

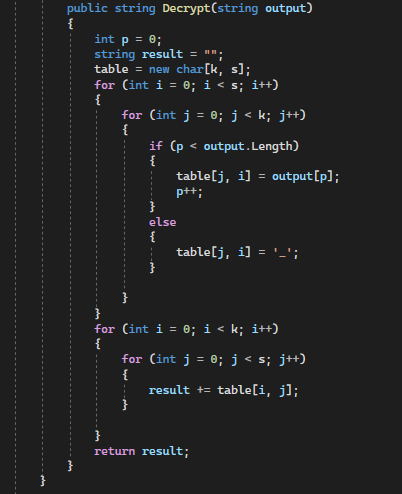


Рисунок 2.2 – Функция дешифрования

Ниже приведен пример шифрования белорусского текста и его дешифрование (рисунок 2.3).

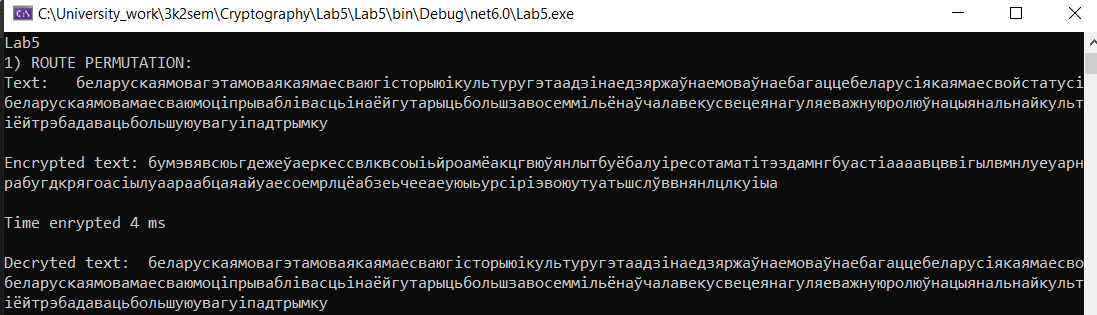


Рисунок 2.3 – Пример роботы маршрутной перестановки

Вторым заданием была множественная перестановка. Суть заключается в том, что перемешиваются столбцы и строки. Используются два ключа: длина одного из них – количество столбцов, а второго – количество строк. Символы нумеруются согласно алфавиту. Если используется две одинаковые буквы – нумеруются по порядку. Заполнение таблицы с перестановками представлено на рисунке 2.4.

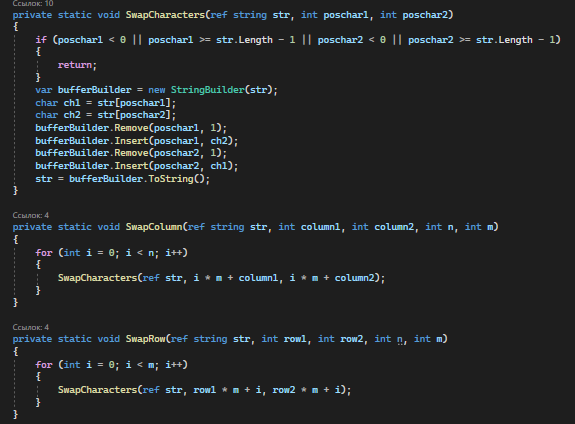


Рисунок 2.4 – Заполнение таблицы

Ниже представлены будут алгоритмы для шифрования и дешифрованя путем множественной подстановки (рисунок 2.5 и 2.6).

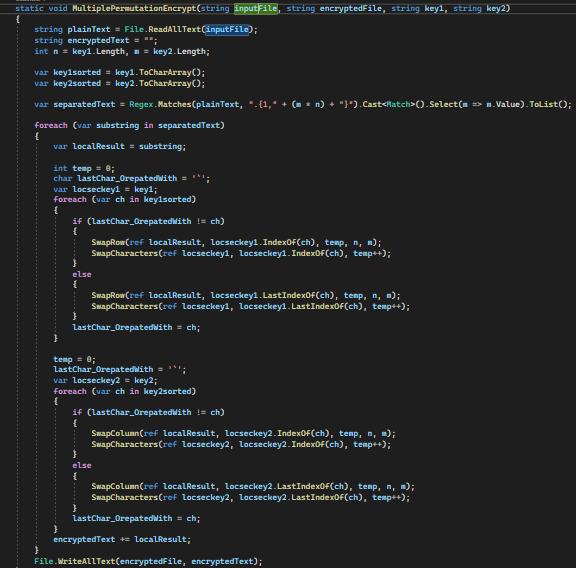


Рисунок 2.5 – Функция шифрования путем множественной перестановки

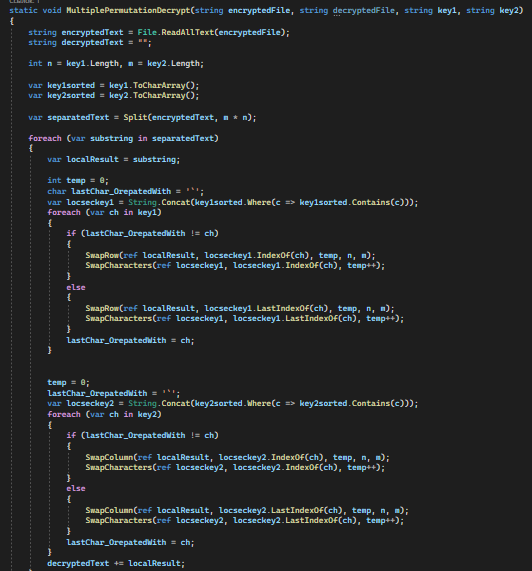


Рисунок 2.6 – Функция дешифвания сообщения

Результат работы представлен на рисунке 2.7, где слева исходный файл, а справа зашифрованный.

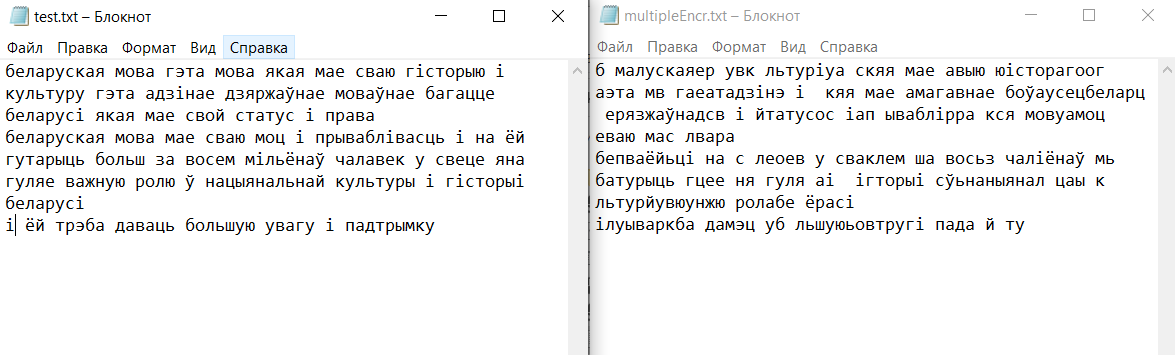


Рисунок 2.7– Функция результат работы множественной перестановки

Ниже приведен график частот появления символов в тексте, рисунок 2.8.

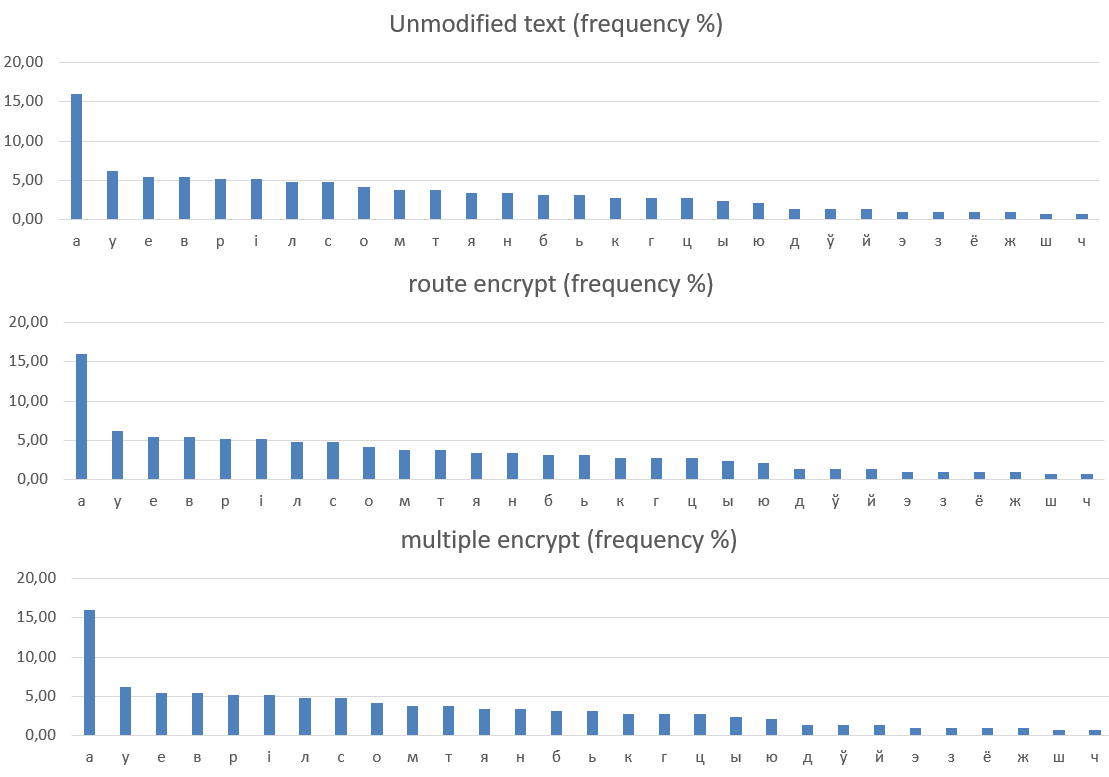


Рисунок 2.8 – Частота появления символов

И график оценки времени работы алгоритмов.

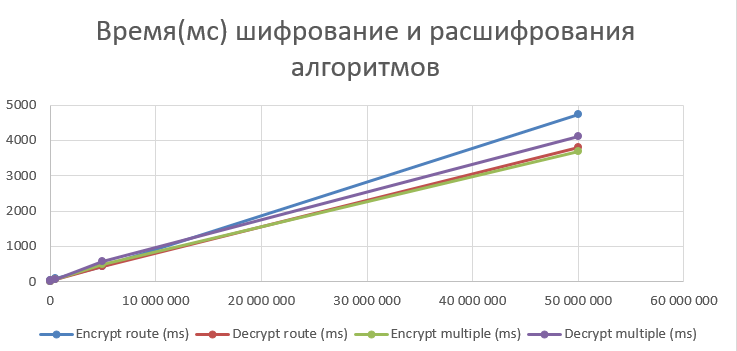


Рисунок 2.9 – Оценка времени работы алгоритмов

**Вывод**

В ходе лабораторной работы были приобретены навыки разработки и использования шифров перестановки, что каждый символ может быть только заменен (замещен) на какой-либо другой, то есть частоты графиков будут одинаковыми, идентичными.

Разработано приложение, на языке программирования C#, для реализации задач, связанных с шифрованием данных.