БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

**Лабораторная работа №4**

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

Выполнила:

студентка 3 курса 5 группы

Почиковская Юлия Сергеевна

Вариант 10

Проверил:

Берников В. О.

Минск 2022

1. **Маршрутная перестановка**

Для зашифрования исходного текста использована простая маршрутная перестановка. Сначала исходная строка разбивается на подстроки длиной k (ключ), после чего последовательно считываются первый символ каждой подстроки, затем второй и т.д. по возрастанию. Реализация данного алгоритма представлена на рисунке 1.1.

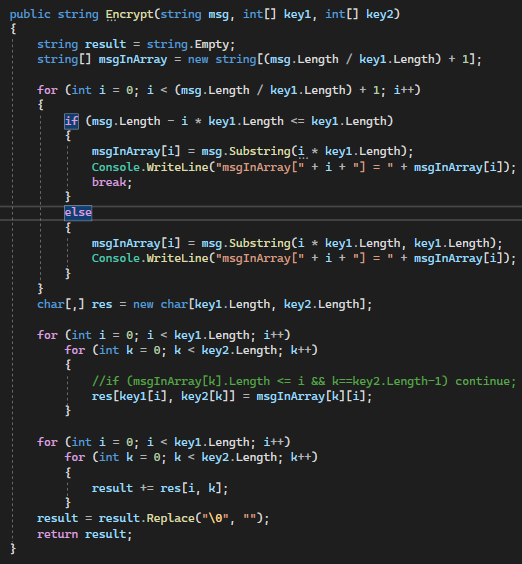


Рисунок 1.1 – Реализация маршрутной перестановки

1. **Множественная перестановка**

Для множественной перестановки используются ключи «Юлия» и «Почиковская», то есть соответствующие им порядки расположения символов в алфавите – «0321» и «837512046». Сначала исходная строка разбивается на подстроки длиной 4 (длина первого ключа), которые выводятся на консоль. Затем каждый символ a[ij] образовавшейся таблицы ставится в позицию [k1[i] k2[j]] соответствующего значения элемента ключа. Считывания производится по строкам. Реализация функции шифрования представлена на рисунке 2.1.

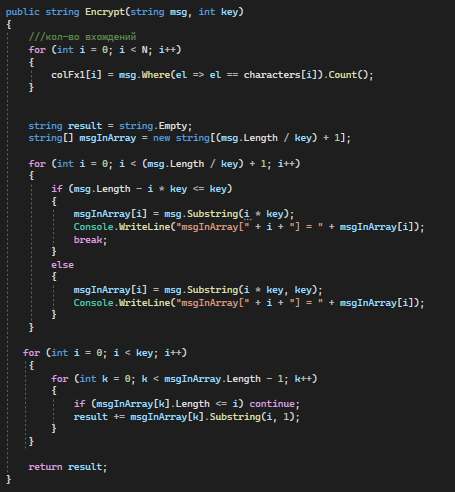


Рисунок 2.1 – Реализация множественной перестановки

Промежуточные результаты разбивания исходной строки на подстроки а также конечные результаты зашифрования и затраченное время выводятся на консоль, представленную на рисунке 2.2.

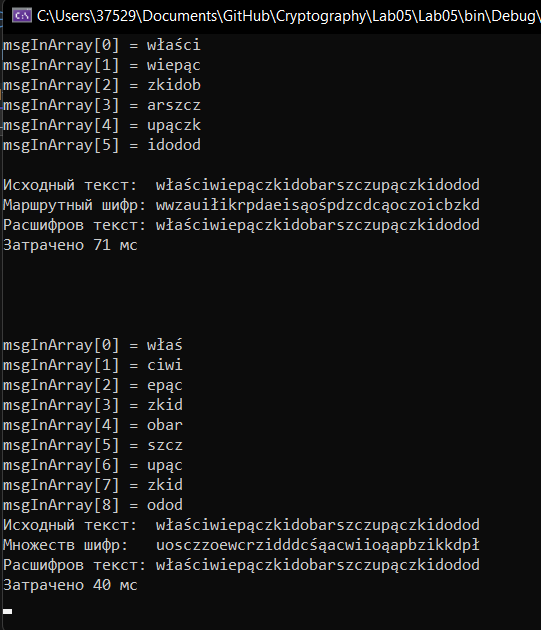


Рисунок 2.2 - Результаты выполнения функций

1. **Генерация гистограммы**

Приложение генерирует гистограммы появления частот символов в исходном и зашифрованном тексте. Поскольку используется шифр перестановки, а не замены, то частоты появления символов остаются неизменными после зашифрования. Полученная гистограмма представлена на рисунке 3.1.

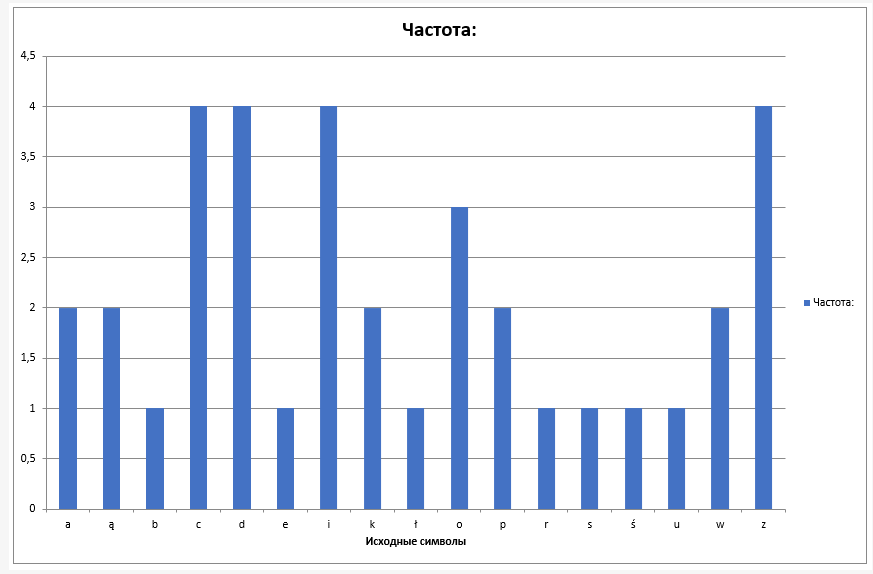


Рисунок 3.1 – Гистограмма частот символов