Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование криптографических шифров на основе перестановки символов**

Студент: Сергеев С.А.

ФИТ 3 курс 5 группа

Преподаватель: Берников В.О.

Минск 2022

1. **Описание приложения**

Приложение написано на языке программирования C# и позволяет:

* осуществлять маршрутную перестановку;
* осуществлять множественную перестановку;
* оценивать время выполнения операция зашифрования.

1. **Методика выполнения поставленных задач**

Для выполнения зашифрования сообщения при помощи маршрутной перестановки используется таблица, заполнение которой представлено на рисунке 2.1. Смысл таких шифров заключается в том, что в качестве таблицы предусматривается какая-то геометрическая фигура, по которой мы будем шифровать сообщение по определенному маршруту.

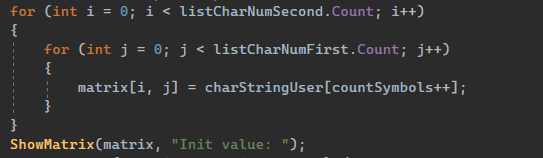


Рисунок 2.1 – Заполнение таблицы строкой пользователя

Функция для отображения таблицы представлена на рисунке 2.2.

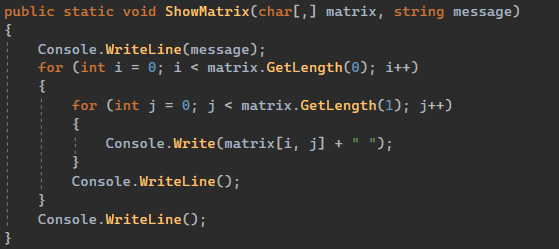


Рисунок 2.2 – Функция отображения таблицы

В моем варианте рассматривался алгоритм змейки. Таким образом, читается первая строка слева направо, затем вторая строка справа налево и так далее. Функция для реализации такой перестановки представлена на рисунке 2.3.

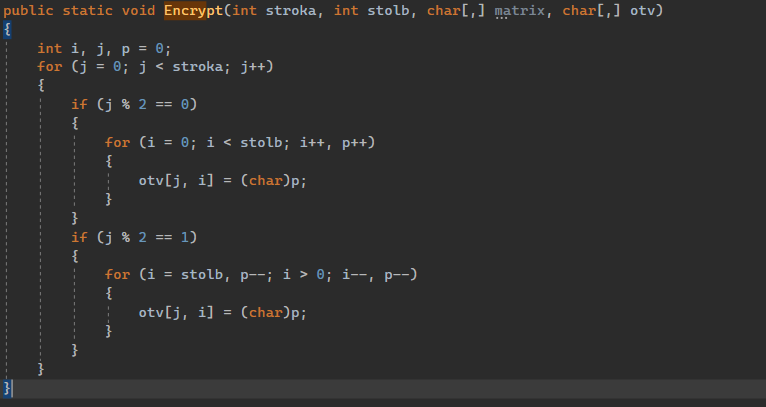


Рисунок 2.3 – Функция реализации маршрутной перестановки

Также необходимо было реализовать множественную перестановку. Суть такой перестановки заключается в том, что перемешиваются столбцы и строки. При этом 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.

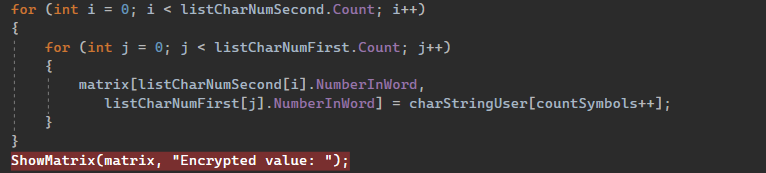


Рисунок 2.4 – Заполнение матрицы

Для выполнения множественной перестановки используется метод, который возвращает порядковый номер символа по алфавиту. Реализация данного метода представлена на рисунке 2.5.

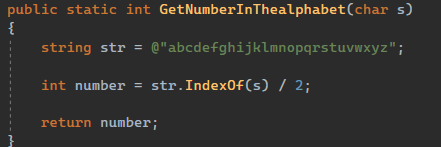


Рисунок 2.5 – Функция для зашифрования и расшифрования

Одной из важнейших функций является заполнение ключей порядковыми номерами. Реализация данной функции представлена на рисунке 2.6.

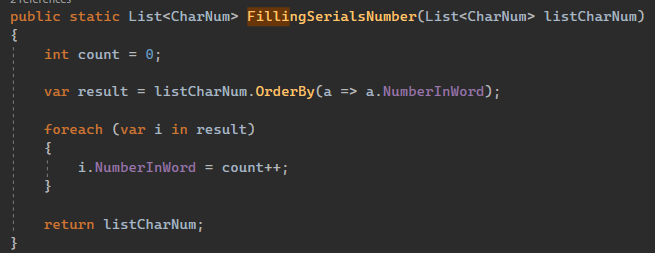


Рисунок 2.6 – Заполнение ключей порядковыми номерами

Результат работы приложения для множественной перестановки представлен на рисунке 2.7.

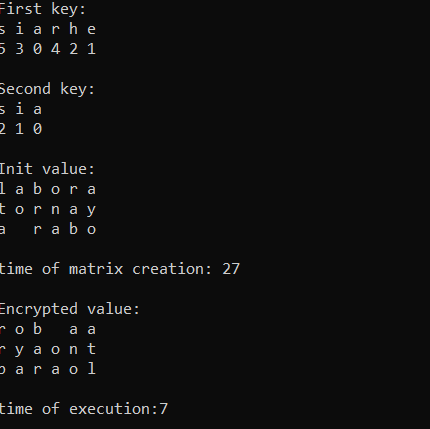


Рисунок 2.7 – Результат работы приложения

Результат работы приложения для маршрутной перестановки представлен на рисунке 2.8.

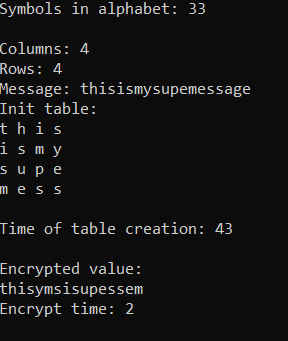


Рисунок 2.8 – Результат работы приложения

Таким образом, были реализованы все поставленные задачи.

**Вывод**

В ходе лабораторной работы были приобретены навыки разработки и использования шифров перестановки.

Также было разработано приложение, на языке программирования C#, для реализации задач, связанных с шифрованием данных.