Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ**

**ШИФРОВ НА ОСНОВЕ**

**ПЕРЕСТАНОВКИ СИМВОЛОВ**

Студент: Николаева Е.В.

ФИТ 3 курс 5 группа

Преподаватель:

Савельева Маргарита Геннадьевна

Минск 2023

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.

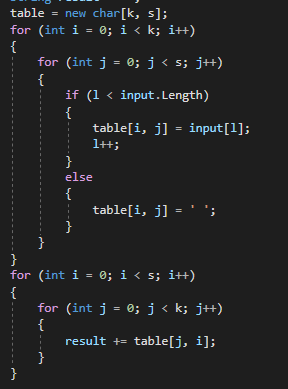


Рисунок 2.1 – Заполнение таблицы строкой пользователя

В моем варианте рассматривался алгоритм записи – по строкам, считывание – по столбцам таблицы. Функция для реализации такой перестановки представлена на рисунке 2.2.

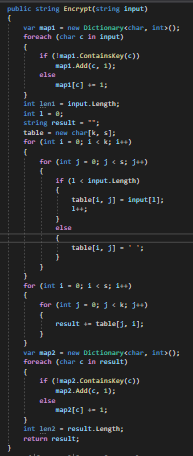


Рисунок 2.2 – Функция реализации маршрутной перестановки

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.

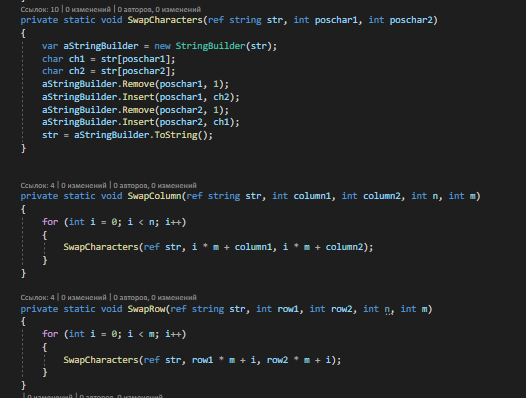


Рисунок 2.4 – Заполнение матрицы

Для выполнения множественной перестановки используется метод, который возвращает порядковый номер символа по алфавиту.

Одной из важнейших функций является заполнение ключей порядковыми номерами. Реализация данной функции представлена на рисунке 2.5.

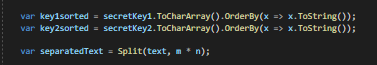


Рисунок 2.5 – Заполнение ключей порядковыми номерами

Результат работы приложения представлен на рисунке 2.7.

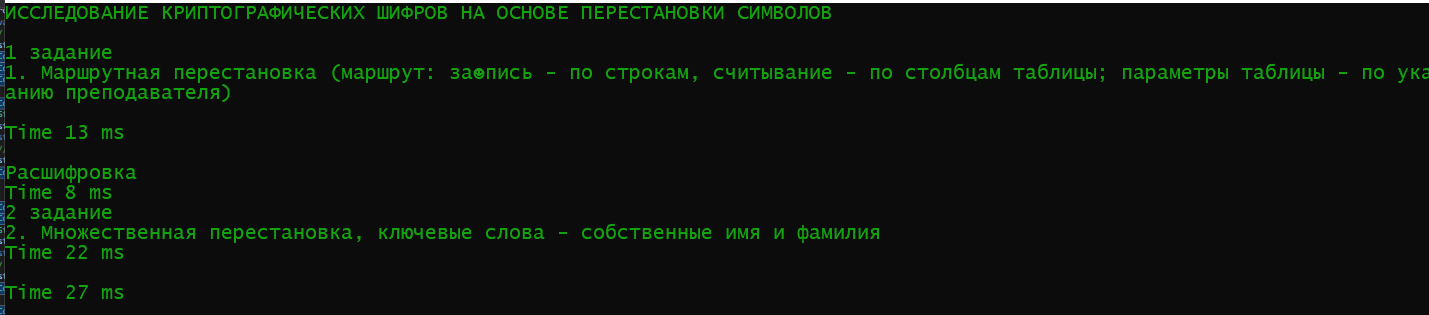


Рисунок 2.7 – Результат работы приложения

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.