Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**«Отчёт по лабораторной работе 5»**

“ ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПЕРЕСТАНОВКИ СИМВОЛОВ”

**Выполнил:** студент 3 курса

4 группы специальности ПОИТ

Кравцова Диана Вячеславовна

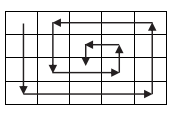
**Проверил:** преподаватель

Блинова Евгения Александровна

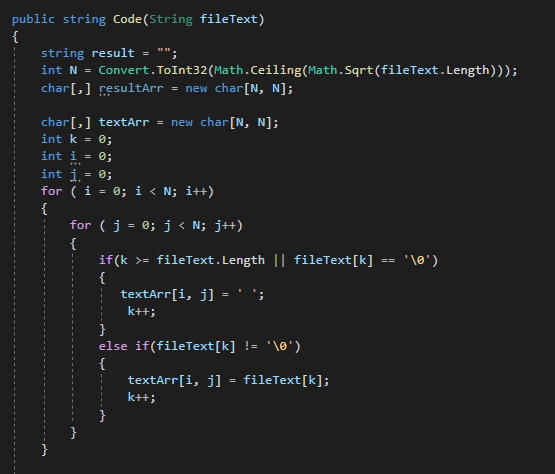
Минск 2021

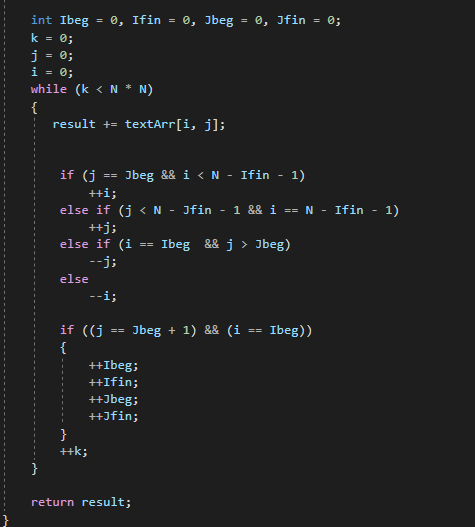
1. **Маршрутная перестановка (маршрут –по спирали, алфавит - русский)**

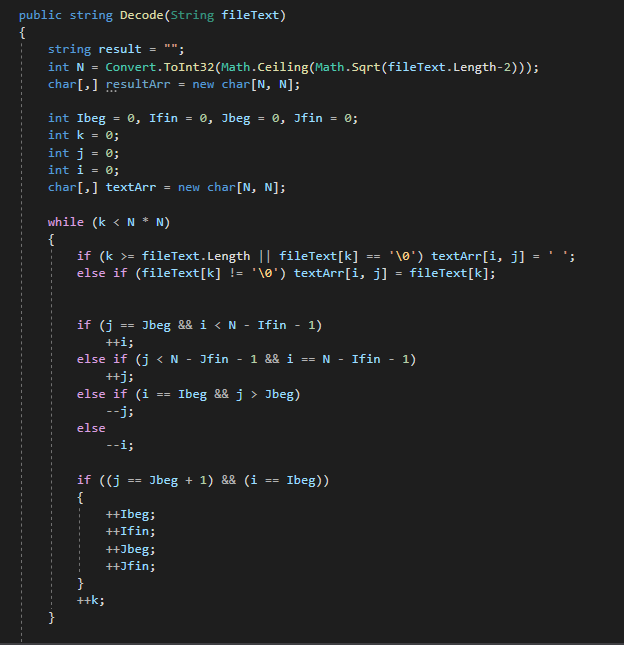
Графическое представление:

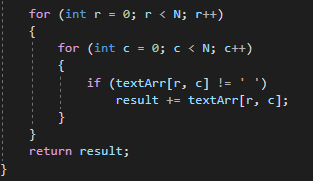
****

Код реализации этого шифра на языке C#:

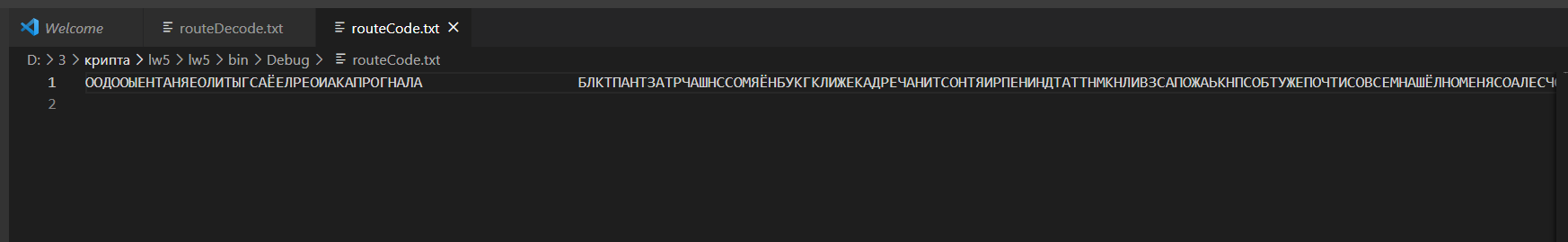
****

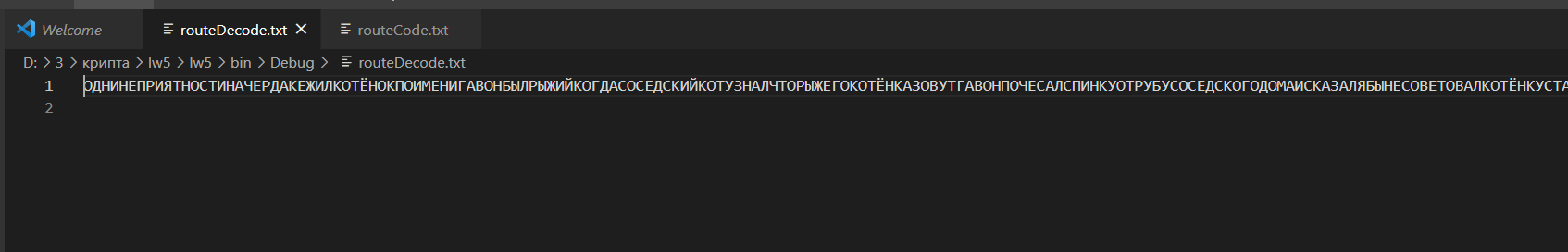
****

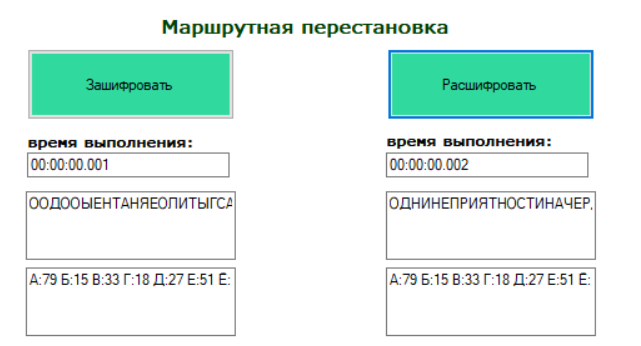
****

****

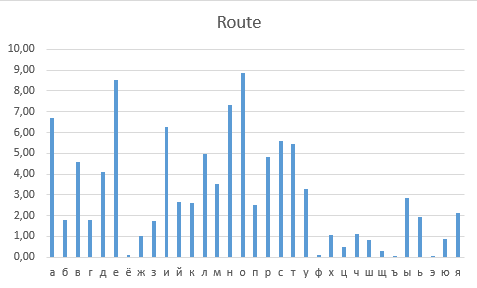
Результат выполнения программы:

****

****

****

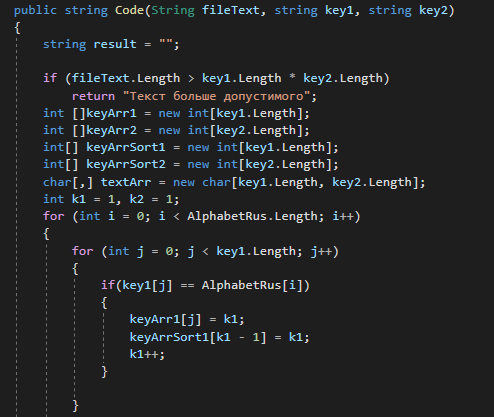
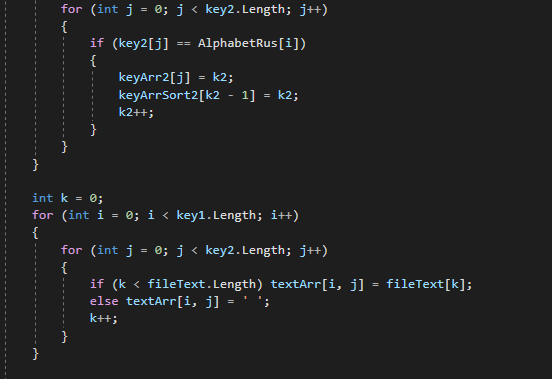
Статистические данные:

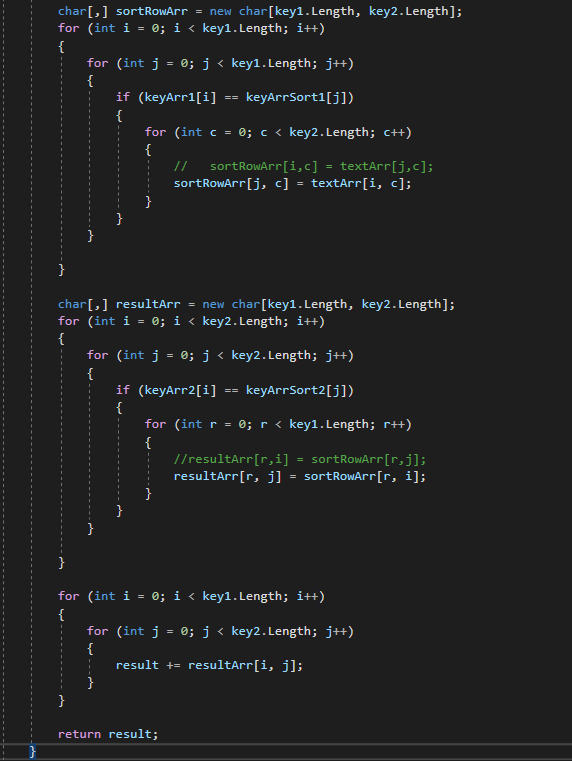


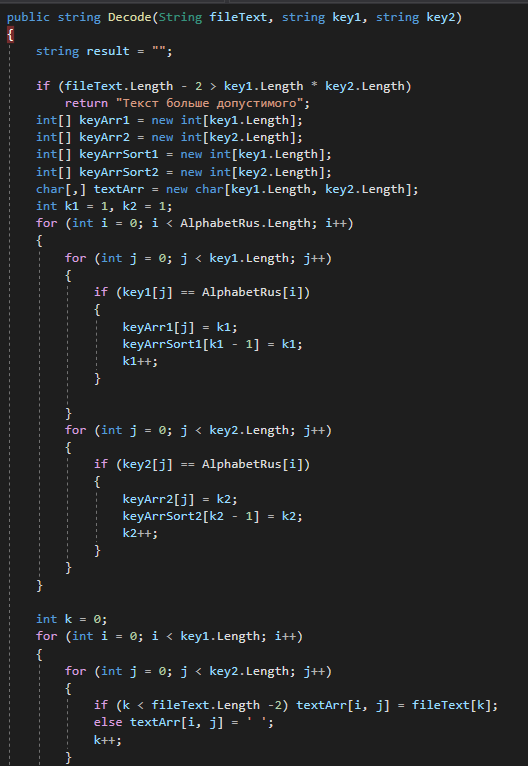
1. Множественная перестановка, ключевые слова – собственные имя и фамилия

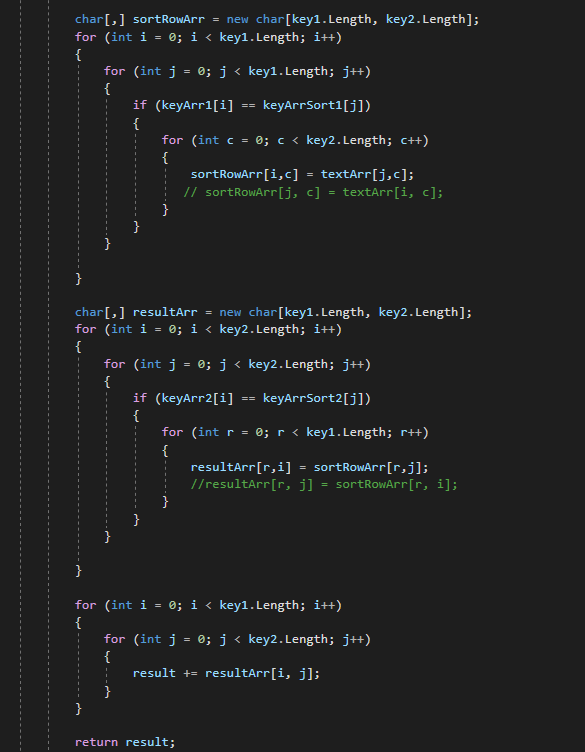
Особенностью шифров данного подкласса является минимум двукратная перестановка символов шифруемого сообщения. В простейшем случае это может задаваться перемешиванием не только столбцов (как в примере 4), но и строк. Таким образом, этот случай соответствует использованию двух основных ключей: длина одного из них равна числу столбцов, другого – числу строк. К ключевой информацию мы можем относить также способы вписывания сообщения и считывания отдельных символов из текущего столбца матрицы.

Код реализации этого шифра на языке C#:







Результат выполнения программы: