Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**«Отчёт по лабораторной работе 5»**

“ ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПЕРЕСТАНОВКИ СИМВОЛОВ”

**Выполнила:** студентка 3 курса

4 группы специальности ПОИТ

Невар Юлия Валерьевна

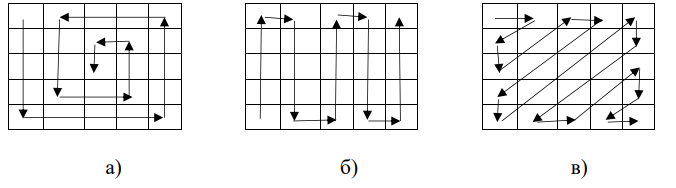
**Проверил:** преподаватель

Блинова Евгения Александровна

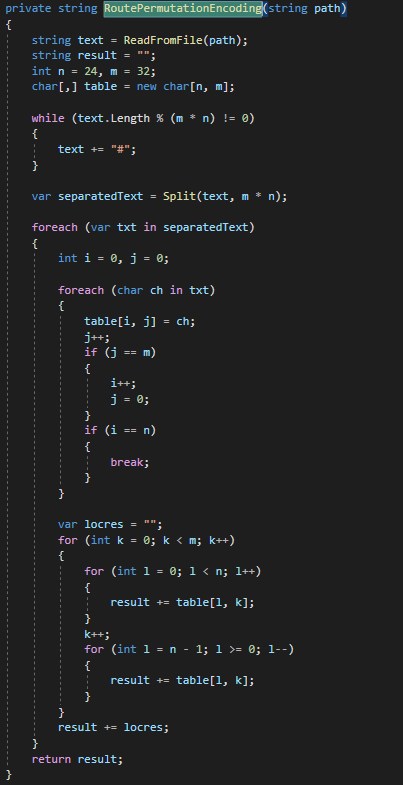
Минск 2021

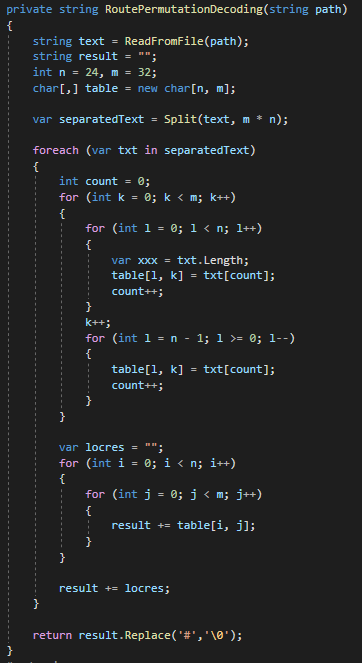
1. Маршрутная перестановка (маршрут: загзаг).

Организация маршрутной перестановки. Уже упоминавшаяся маршрутная перестановка (записываем сообщение по строкам, считываем – по столбцам матрицы) можно усложнить и считывать не по столбцам, а по спирали (рис. 3.2,а), зигзагом (рис. 3.2,б), змейкой (рис. 3.2,в) или каким-то другим способом (см. рис. 3.2). Такие способы шифрования несколько усложняют процесс, однако усиливают криптостойкость шифра.

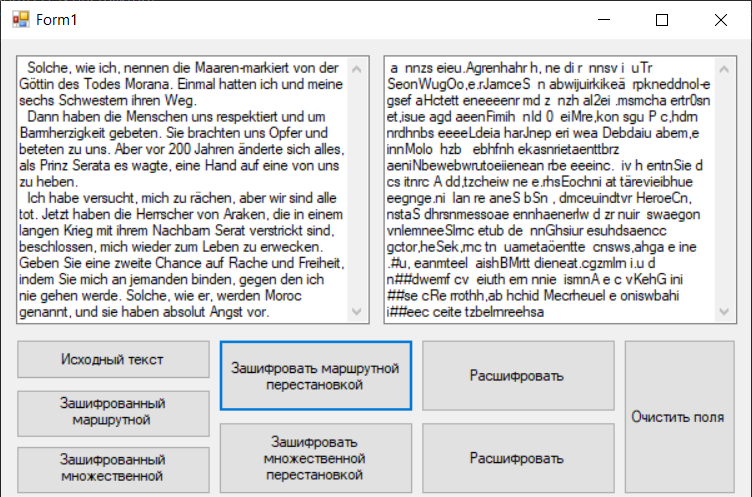


Код реализации этого шифра на языке C#:

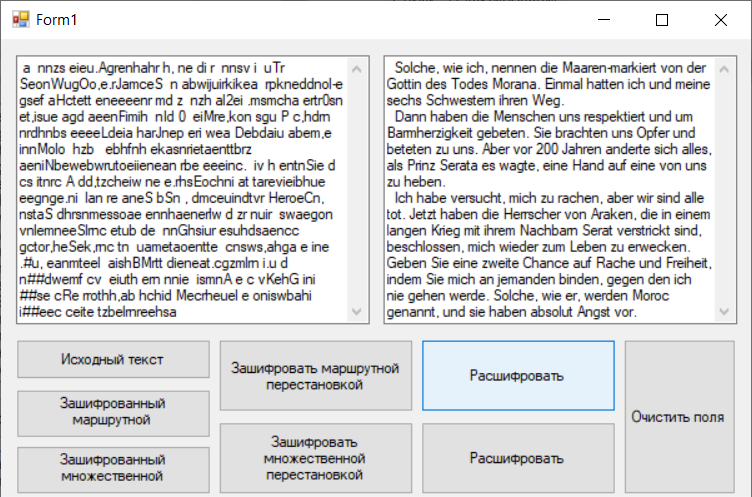




Результат выполнения шифрования:



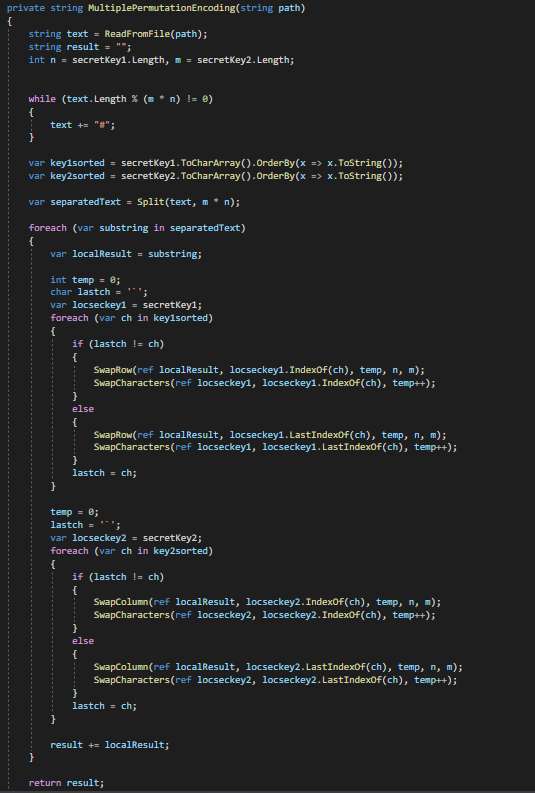
Результат выполнения расшифрования:

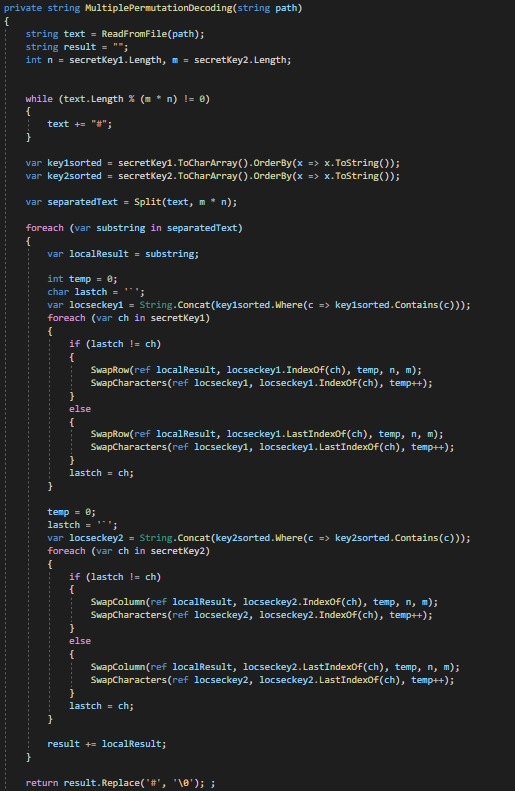


1. Множественная перестановка, ключевые слова – собственные имя и фамилия.

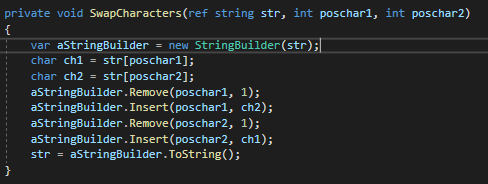
Особенностью шифров данного подкласса является минимум двукратная перестановка символов шифруемого сообщения. В простейшем случае это может задаваться перемешиваем не только столбцов (как в примере 4), но и строк. Таким образом, этот случай соответствует использованию двух основных ключей: длина одного 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#:

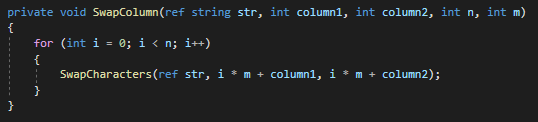




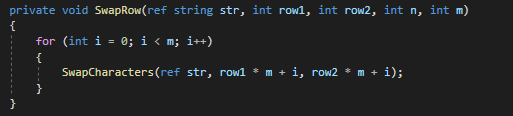
Функция для перемещения символов в слове:



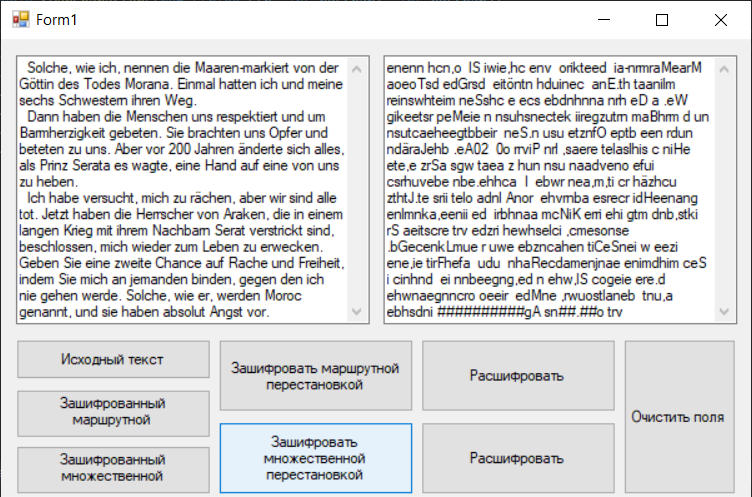
Функция для перемещения символов из одного столбца в другой:



Функция для перемещения символов из одной строки в другую:



Результат выполнения шифрования:



Результат выполнения расшифрования:

