Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**«Отчёт по лабораторной работе 4»**

“ ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПОДСТАНОВКИ (ЗАМЕНЫ) СИМВОЛОВ”

**Выполнила:** студентка 3 курса

4 группы специальности ПОИТ

Кравцова Диана Вячеславовна

**Проверил:** преподаватель

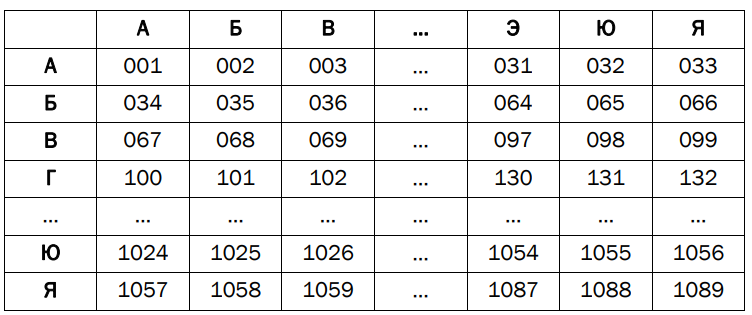
Блинова Евгения Александровна

Минск 2021

1. Шифр Порты:

Шифр представляется в виде таблицы. Наверху горизонтально и слева

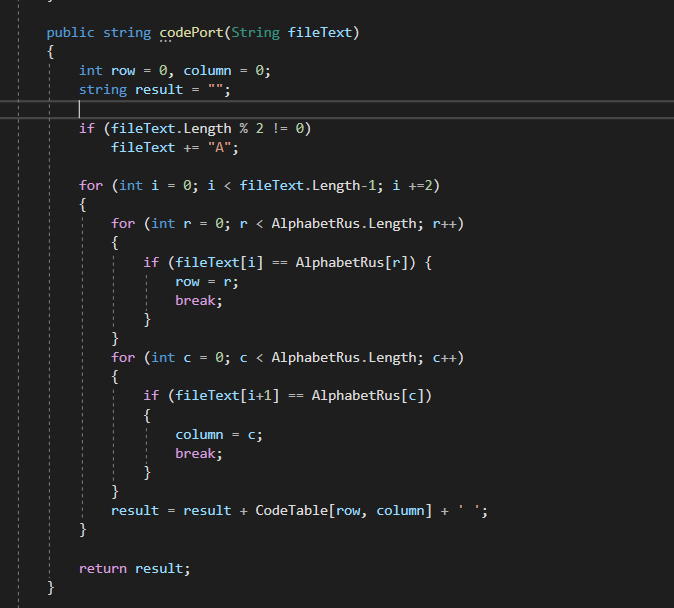
вертикально записывается стандартный алфавит. В ячейках таблицы записываются числа в определенном порядке. Фрагмет таблицы для алфавита русского показан ниже.

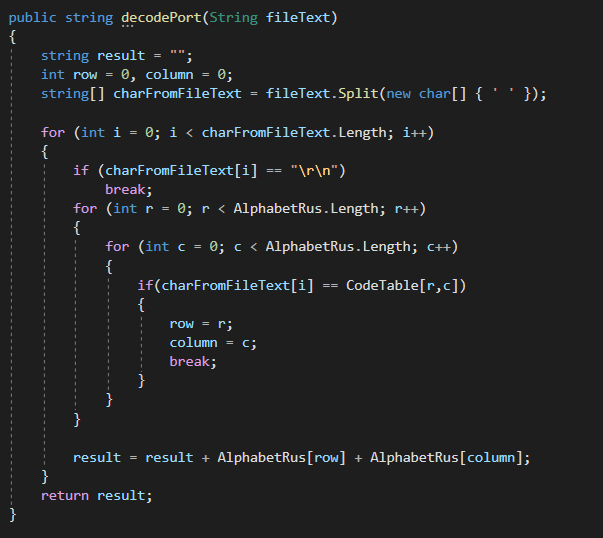
**** Шифрование выполняется парами букв исходного сообщения. Первая

буква пары указывает на строку, вторая – на столбец. В случае нечетного количества букв в сообщении Мi к нему добавляется вспомогательный символ, например «А».

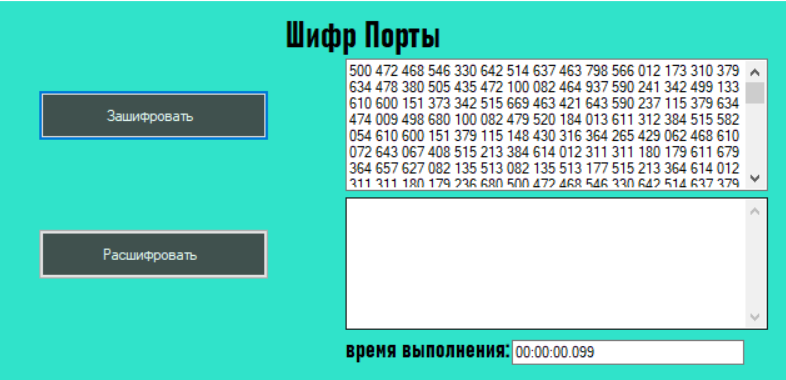
Для процедуры расшифрования используется эта же таблица. Нужно найти ячейку с вашим набором символов и сопоставить ей пару букв. Первая буква пары – строка, вторая – столбец.

Код реализации этого шифра на языке C#:

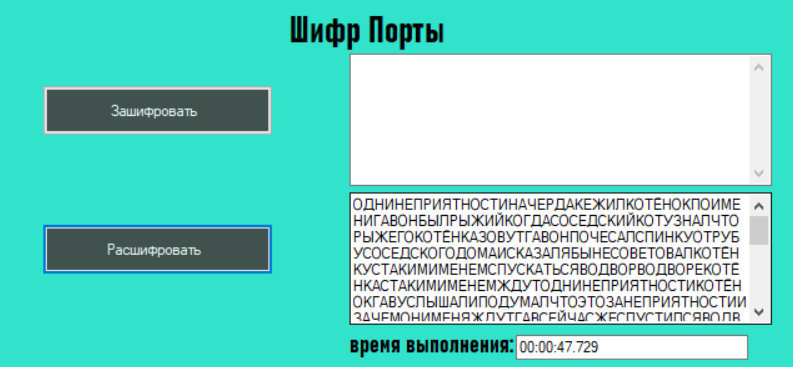




Результат выполнения шифрования:

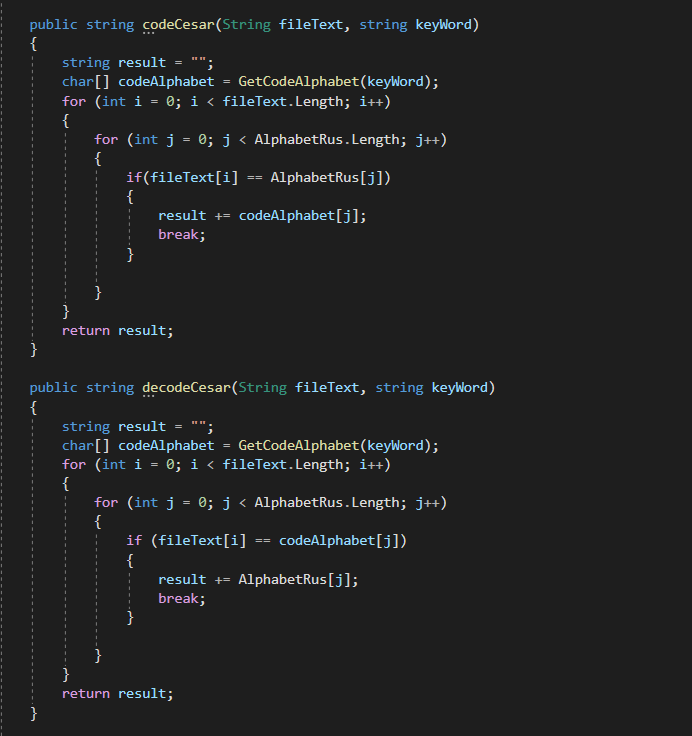


Результат выполнения расшифрования:



1. Шифр Цезаря с ключевым словом. Является одноалфавитной системой подстановки. Особенностью этой системы является использование ключевого слова (лозунга) для смещения и изменения порядка символов

в алфавите подстановки (желательно, чтобы все буквы ключевого слова были различными). Ключевое слово пишется в начале алфавита подстановки. Код реализации этого шифра на языке C#:



Результат выполнения шифрования:



Результат выполнения расшифрования:

