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

Невар Юлия Валерьевна

**Проверил:** преподаватель

Блинова Евгения Александровна

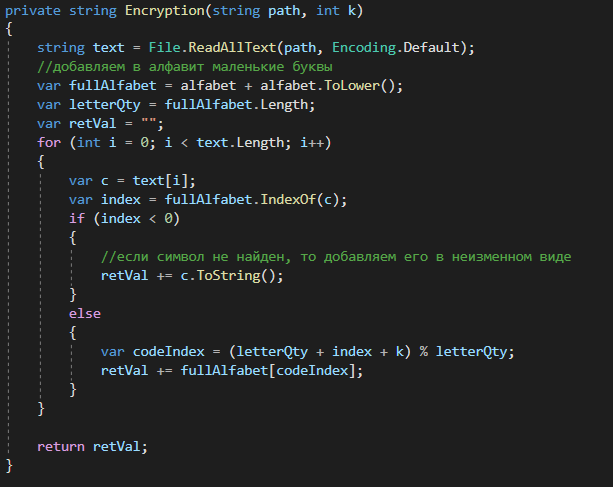
Минск 2021

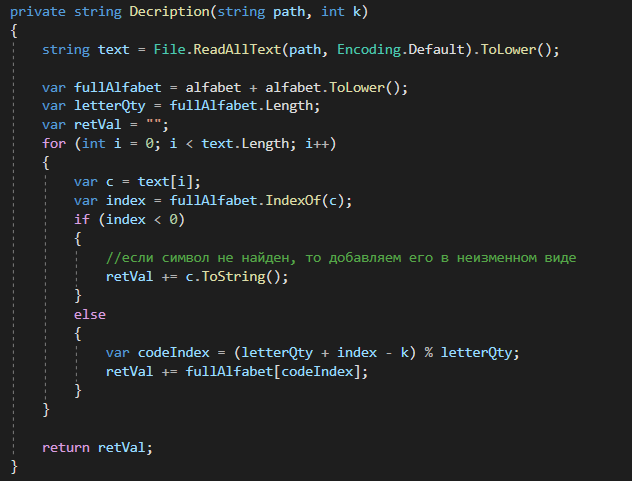
1. Шифр на основе соотношений y = x + k (mod N) и x = у – k (mod N).

Для математического описания криптографического преобразования предполагаем, что зашифрованная буква ay (ay ∈ Сi), соответствующая символу aх (aх∈ Мi), находится на позиции y ≡ x + k (mod N), где x, y – индекс (порядковый номер, начиная с 0) символа в используемом алфавите, k – ключ.

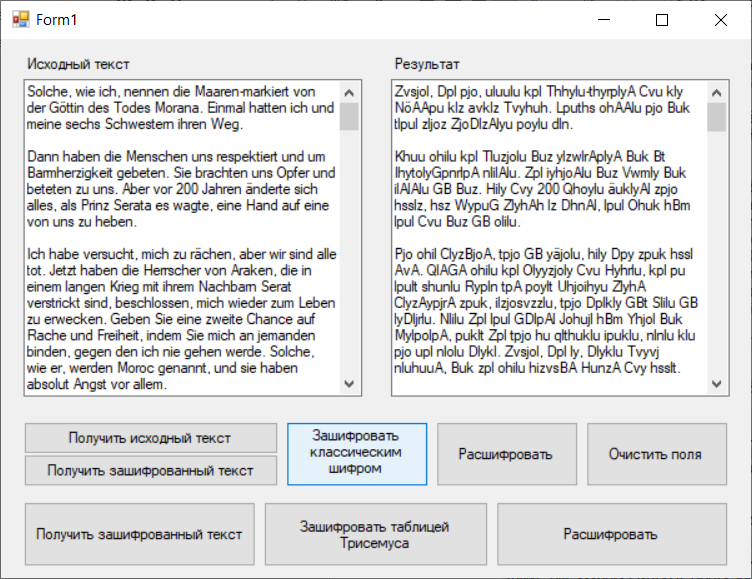
Для расшифрования сообщения Сi необходимо произвести расчеты обратные y ≡ x + k (mod N), т. е.: х ≡ у – k (mod N).

Код реализации этого шифра на языке C#:

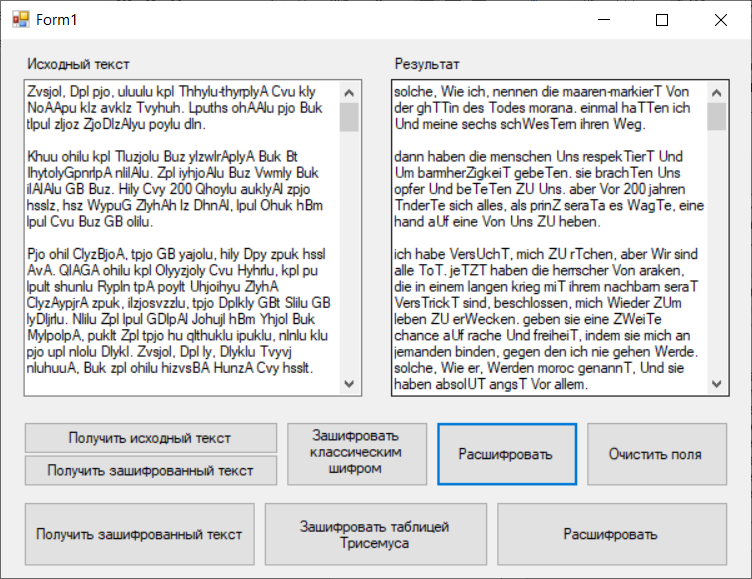




Результат выполнения шифрования:



Результат выполнения расшифрования:

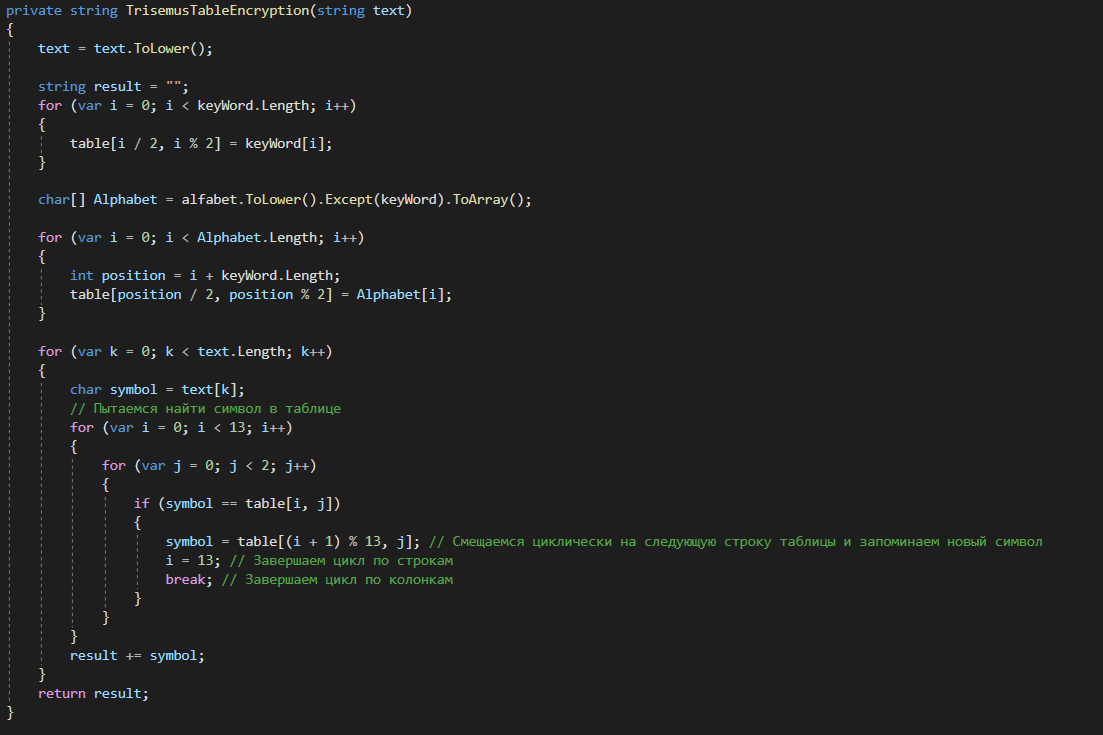


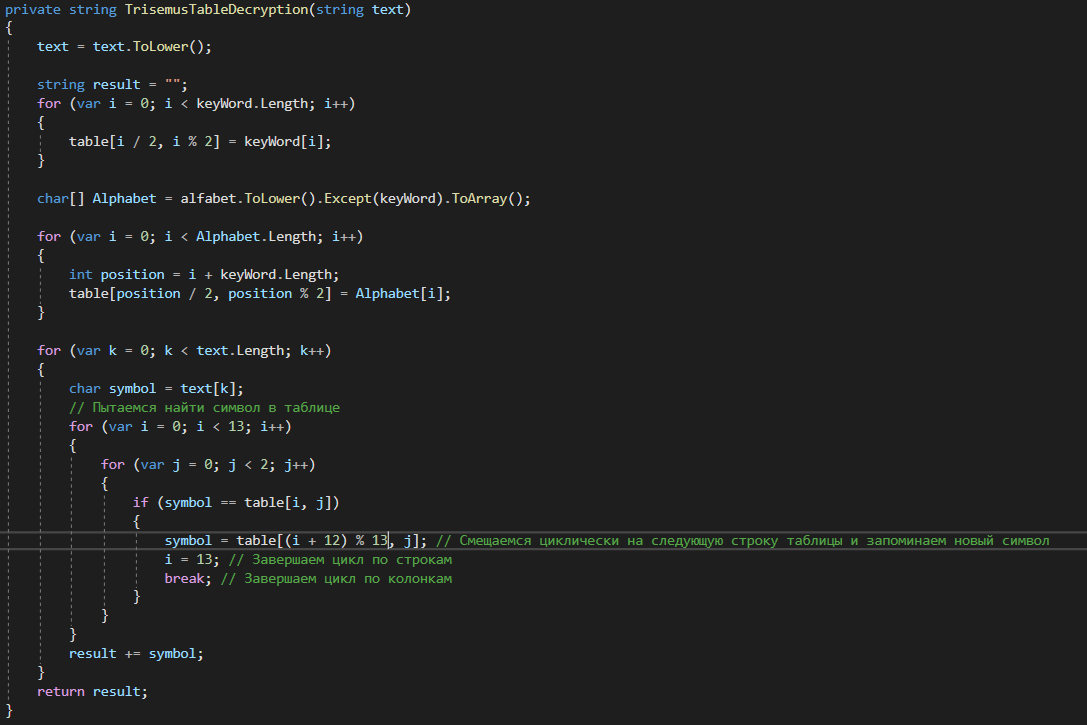
1. Таблица Трисемуса

Трисемус впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра подстановки обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). Можно найти определенную аналогию с системой шифрования Цезаря с ключевым словом. В таблицу сначала вписывалось по стрелкам ключевое слово, причем повторяющиеся буквы также отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку.

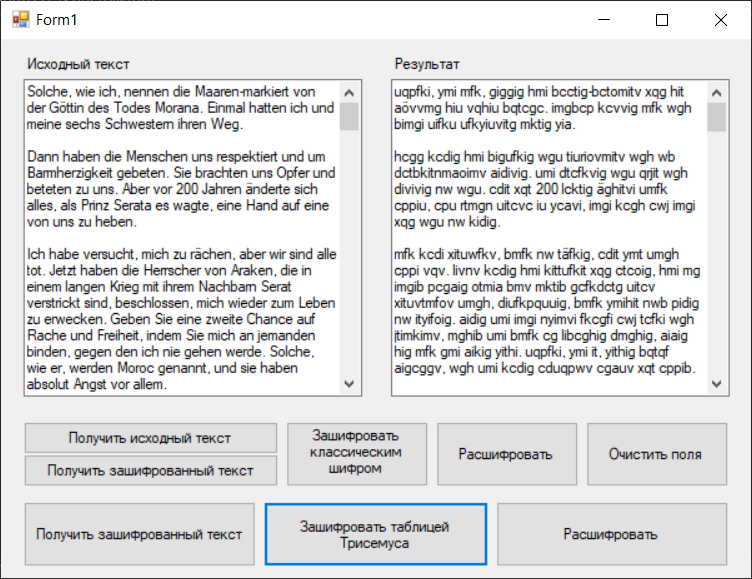
Таким образом, ключом в таблицах Трисемуса является ключевое слово и размер таблицы. При шифровании буква открытого текста заменяется буквой, расположенной ниже нее в том же столбце. Если буква текста оказывается в нижней строке таблицы, тогда для шифртекста берут самую верхнюю букву из того же столбца.

Код реализации этого шифра на языке C#:





Результат выполнения шифрования:



Результат выполнения расшифрования:

