МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

**«Отчет к лабораторной работе № 4**

**Исследование криптографических шифров на основе подстановки (замены) символов»**

Студент:

Септилко Анастасия Антоновна

Преподаватель:

Блинова Евгения Александровна

Минск 2020

**Цель**: изучение и приобретение практических навыков разработки и использования приложений для реализации подстановочных шифров. Оценивать время выполнения операций зашифрования/расшифрования (на рисунках продевонстрировано).

**Ход работы:**

1. Создан файл en.txt, объемом не менее 5 тысяч знаков, на основе алфавита английского языка. Ниже показан скриншет файла en.txt (рисунок 1.1)

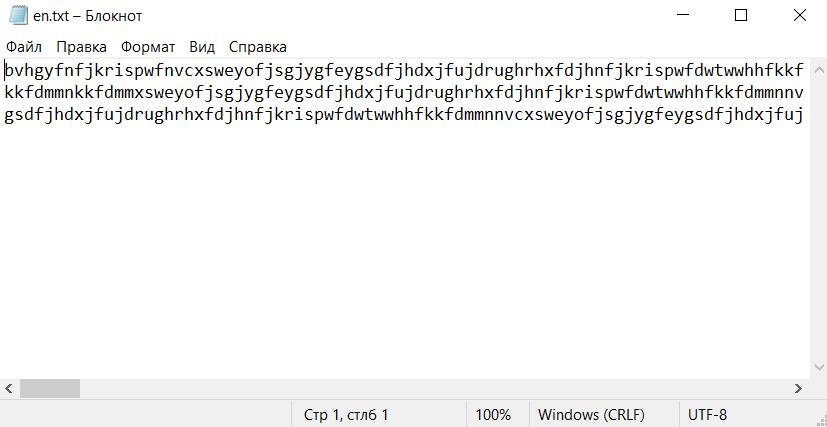


Рисунок 1.1 – Файл en.txt

1. Написана программа, реализующая алгоритм шифра Цезаря с ключевым словом, где ключевое слово – собственная фамилия («SEPTILKO»), сдвиг слова, относительно начала алфавита, а=6.

* Для зашифрования исходного текста с помощью шифра Цезаря с ключевым словом необходимо сформировать новый алфавит. Функция которая формирует новый алфавит продемонстрирована на рисунке 1.2.

Исходный алфавит приведен ниже в рамке:

private readonly char[] \_alphabet = { 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z' };

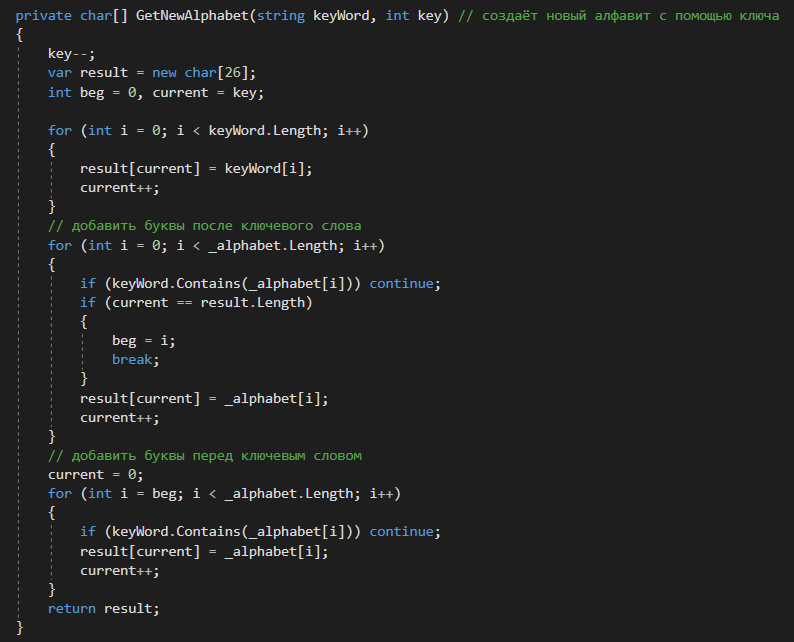


Рисунок 1.2 – Функция формирования нового алфавита

* Новый алфавит получается из исходного, путем помещения на а-ую позицию ключевого слова, буквы которого не должны повторяться.
* Далее за ключевым словом идет исходный алфавит, в котором уже исключены все символы ключевого слова, он циклически продолжается и до начала ключевого слова.

Новый алфавит: «UVWXYZSEPTILKOАBCDF'G'HJMNQR»

* Для зашифрования текста необходимо заменить символ исходного текста на символ, находящийся на той же позиции в новом алфавите, где находился этот символ в исходном алфавите.

Формула для зашифрования символа (рисунок 1.3):

y = x+k(mod N)

Формула для расшифрования символа (рисунок 1.4):

x = y – k(mod N)

В приведенных формулах х – индекс исходного символа в алфавите, у – индекс зашифрованного символа, k – ключ, N – мощность алфавита.

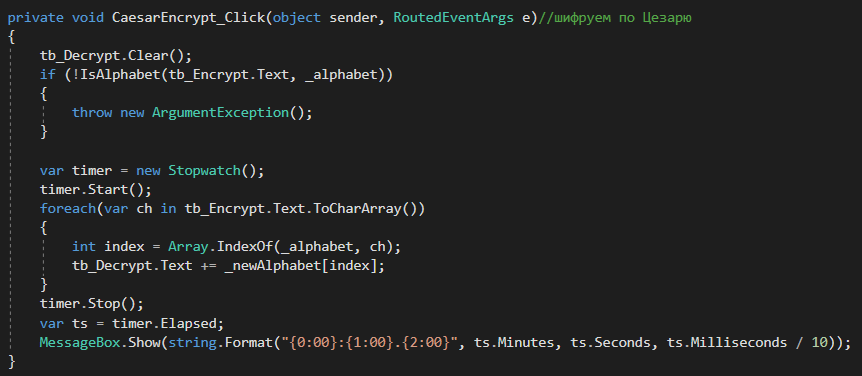


Рисунок 1.3 – Функция зашифрования по Цезарю

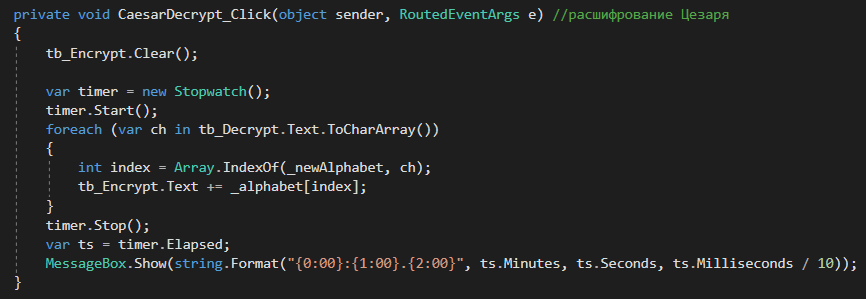


Рисунок 1.4 – Функция расшифрования по Цезарю

1. Написана программа, реализующая алгоритм шифрования с помощью таблицы Трисемуса, ключевое слово – собственное имя («NASTYA»).

* Т.к. по варианту алфавит английский, то таблица будет размерностью 5x5. Вначале пишем ключевое слово без повторяющихся букв, а затем оставшийся алфавит (рисунок 1.5):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N | A | S | T | Y |
| B | C | D | E | F |
| G | H | I | J | K |
| L | M | O | P | Q |
| R | U | V | W | X |
| Z |  |  |  |  |

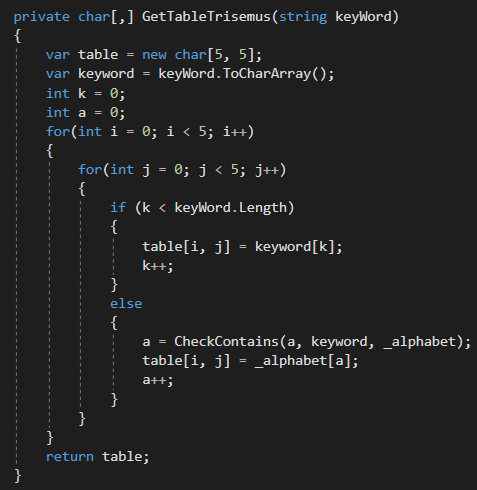


Рисунок 1.5 – Получаем таблицу Трисемуса

Шифрование происходит следующим образом:

– Символ исходного текста заменяется на символ, находящийся ниже на 1 строку, чем этот же символ в таблице Трисемуса.

– Если символ находится в последней строке, то берем символ из первой строки, находящийся в том же столбце.

Зашифровка по таблице Трисемуса показан кусочек на рисунке 1.6, расшифровка на рисунке 1.7.

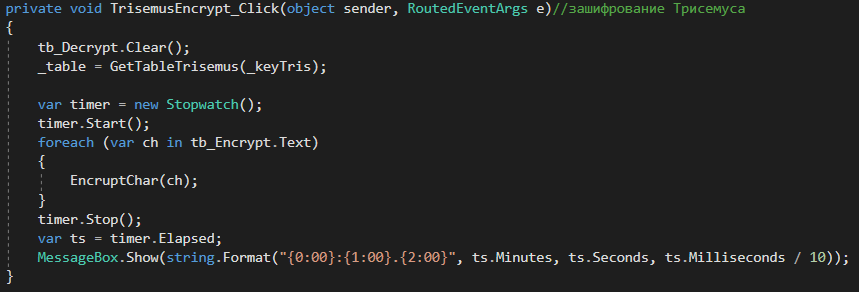


Рисунок 1.6 – Функция Функция зашифрования по Трисемусу

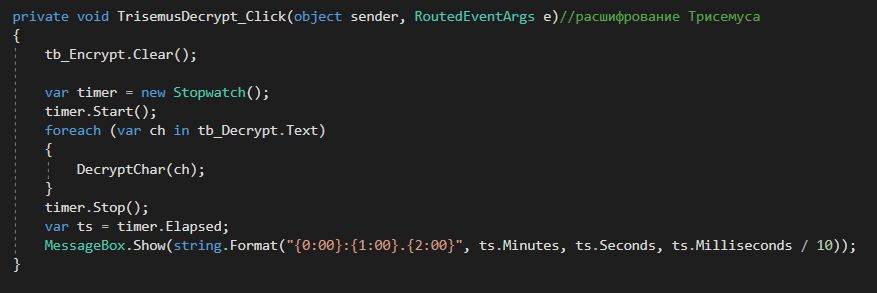


Рисунок 1.7 – Функция расшифрования по Трисемусу

Итог выполнения программы предоставлен на рисунке 1.8 ниже.

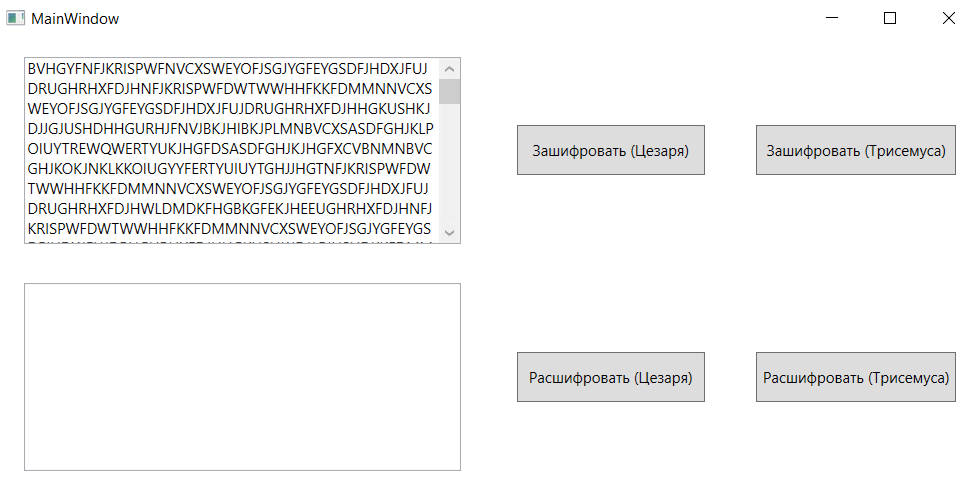


Рисунок 1.8 – Итог программы

## **Вывод**

Изучила и приобрела практические навыки разработки и использования приложений для реализации подстановочных шифров. Закрепилп теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочных шифров. Оценилп скорость зашифрования/расшифрования реализованных способов шифров.