Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование криптографических шифров на основе**

**подстановки (замены) символов**

Студент: Гвоздовский К. В.

ФИТ 3 курс 6 группа

Преподаватель:

Нистюк Ольга Александровна

1. **Цель работы**

Изучение и приобретение практических навыков разработки и использования приложений для реализации подстановочных шифров.

1. **Задание**

Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:

1. выполнять зашифрование/расшифрование текстовых документов (объемом не менее 5 тысяч знаков) созданных на основе алфавита языка в соответствии с нижеследующей таблицей вариантов задания; при этом следует использовать шифры подстановки из третьего столбца данной таблицы;
2. формировать гистограммы частот появления символов для исходного и зашифрованного сообщений;
3. оценивать время выполнения операций зашифрования/расшифрования.
4. **Ход работы**

В соответствии с вариантом, алфавит выбран английский, для первого задания использовался шифр Цезаря с ключевым словом, ключевое слово – собственная фамилия, для второго задания использовалась таблица Трисемуса, ключевое слово – собственное имя.

Для обоих заданий следовало оценить время выполнения операций шифрования/дешифрования сообщений. Для этого был использован специальный класс Stopwatch на языке C#, который предоставляет функциональность для измерения времени выполнения операций и который представлен в директиве System.Diagnostics. Пример использования объекта данного класса представлен на рисунке 3.1.

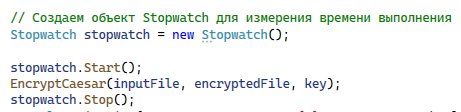


Рисунок 3.1 – Пример использования класса Stopwatch

Также, для этих заданий следовало сформировать гистограммы частот появления символов для исходного и зашифрованного сообщений. Для этой цели была разработана функция CountCharacterFrequency, представленная на рисунке 3.2.

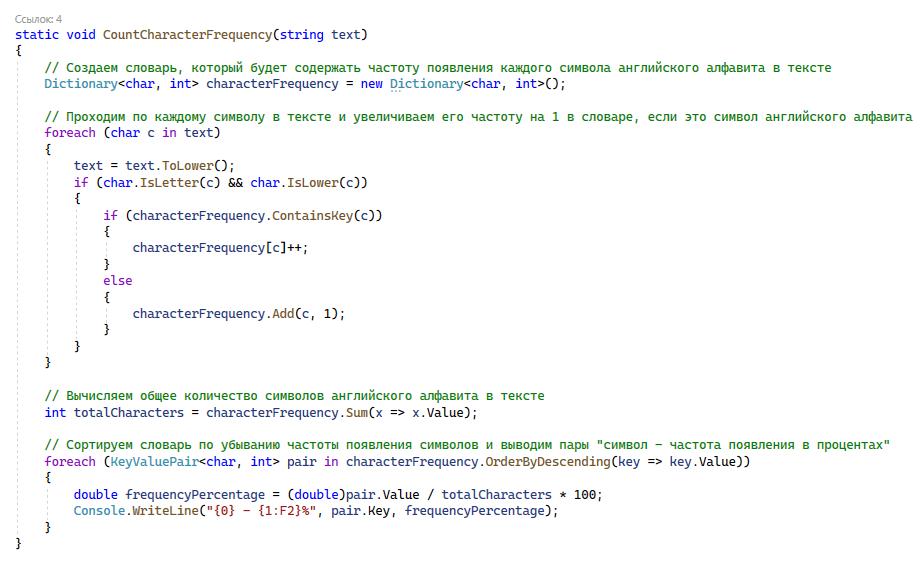


Рисунок 3.2 – Функция для определения частот появления символов

Для выполнения первого задания были разработаны функции EncryptCaesar и DecryptCaesar, которые осуществляют шифрование и дешифрование текста с использованием алгоритма Цезаря по ключу. Они представлены на рисунках 3.3 и 3.4.

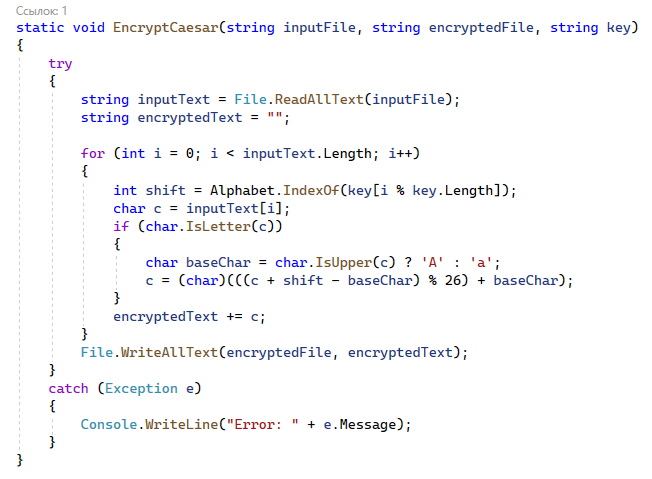


Рисунок 3.3 – Функция для шифрования текста с помощью алгоритма Цезаря по ключу

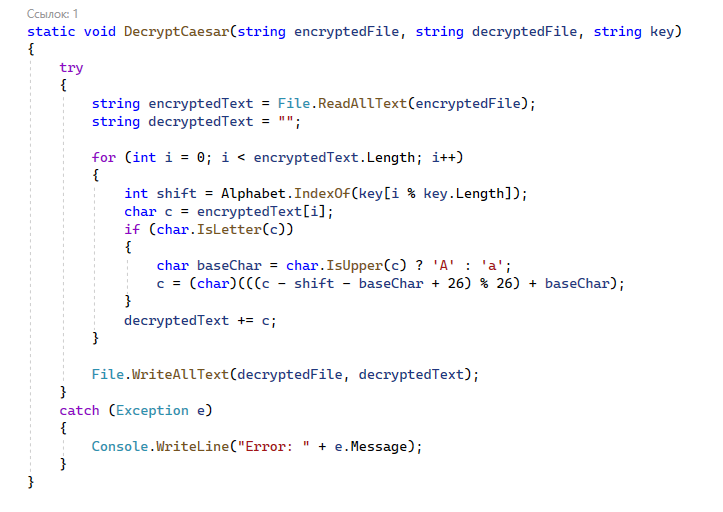


Рисунок 3.4 – Функция для дешифрования текста с помощью алгоритма Цезаря по ключу

Входные данные и результаты выполнения данных функций представлены на рисунках 3.5 – 3.8.

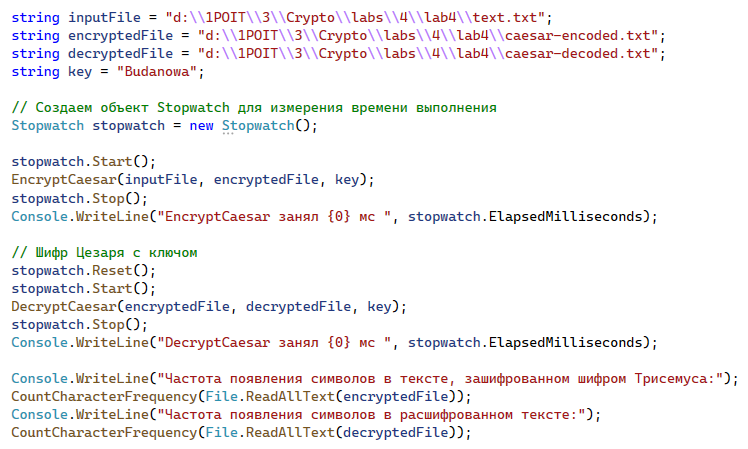


Рисунок 3.5 – Входные данные для алгоритма Цезаря

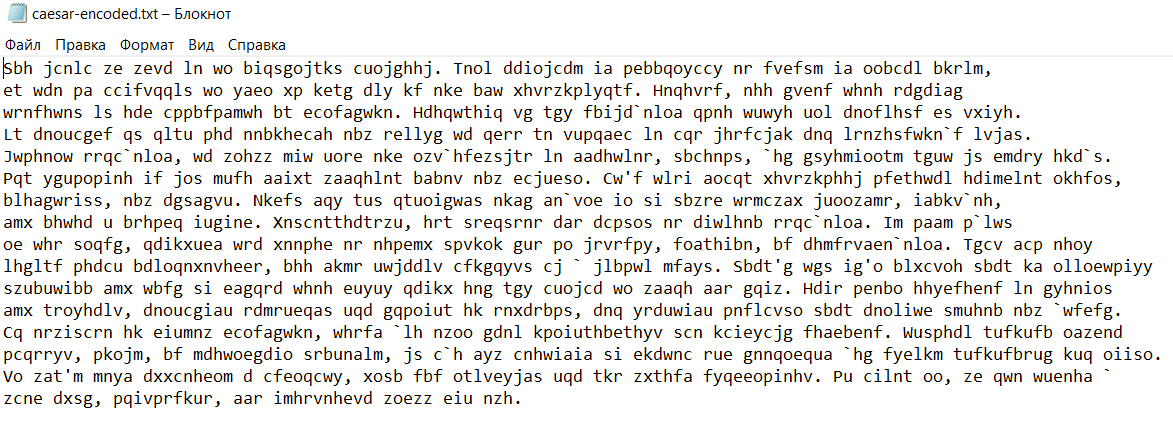


Рисунок 3.6 – Текст, зашифрованный с помощью функции EncryptCaesar

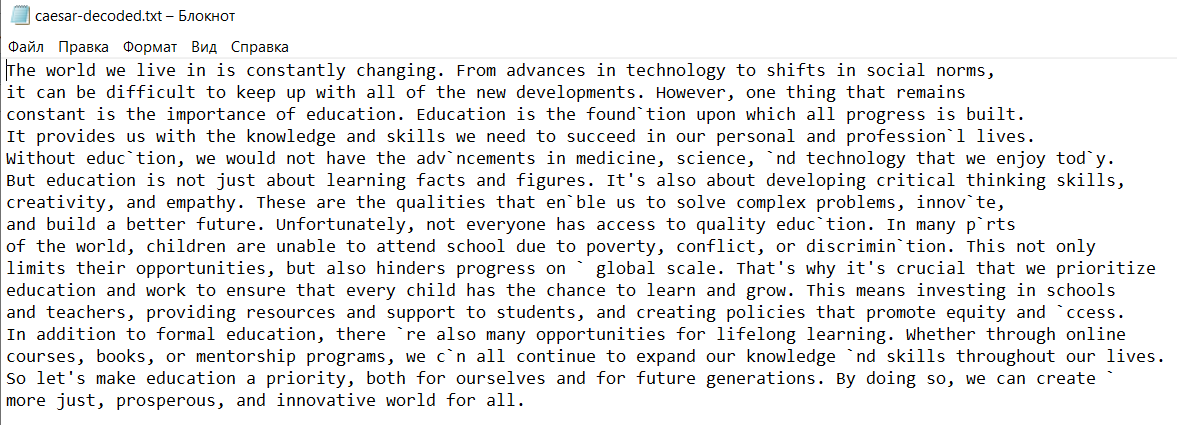


Рисунок 3.7 – Текст, расшифрованный с помощью функции DecryptCaesar

Рисунок 3.8 – Оценка скорости выполнения шифрования/дешифрования текста

Частота появления символов в этих текстовых файлах представлена на рисунках 3.9 и 3.10 соответственно.

Рисунок 3.9– Гистограмма частот появления символов для зашифрованного текста

Рисунок 3.10 – Гистограмма частот появления символов для расшифрованного текста

Для выполнения второго задания были разработаны функции EncryptTrisemus, DecryptTrisemus и TrisemusTable, которые реализуют алгоритм шифрования текста с помощью таблицы Трисемуса. Код реализации этих функций представлен на рисунках 3.11 – 3.13.

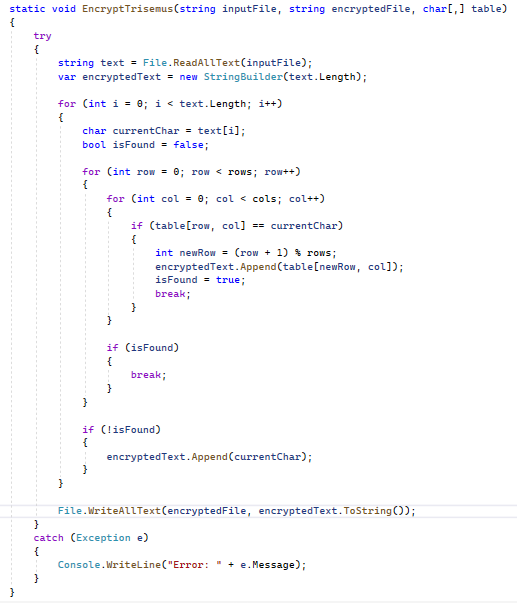


Рисунок 3.11 – Функция для шифрования текста с помощью таблицы Трисемуса

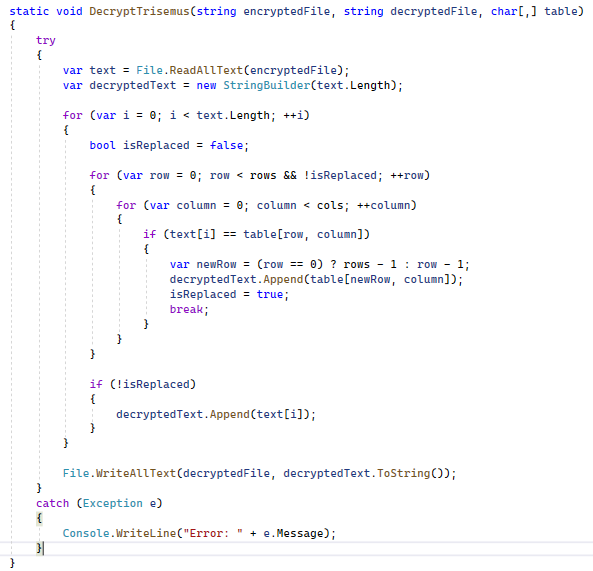


Рисунок 3.12 – Функция для дешифрования текста с помощью таблицы Трисемуса

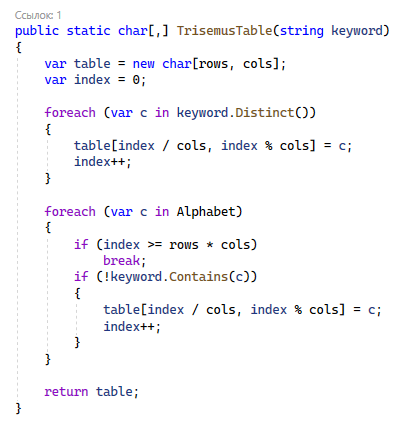


Рисунок 3.13 – Функция для заполнения таблицы Трисемуса

В результате получаем следующие файлы и вывод, представленные на рисунках 3.14 – 3.16.

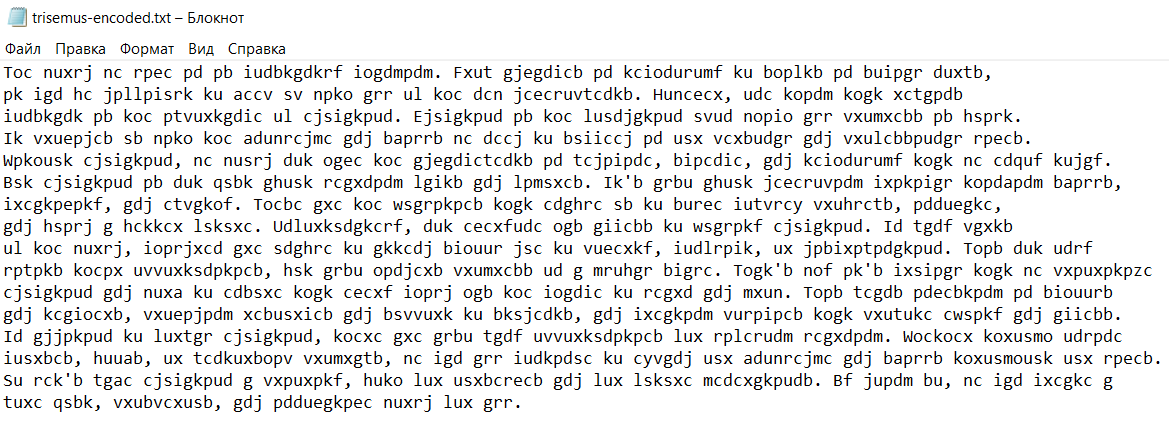


Рисунок 3.14 – Текст, зашифрованный с помощью функции EncryptTrisemus

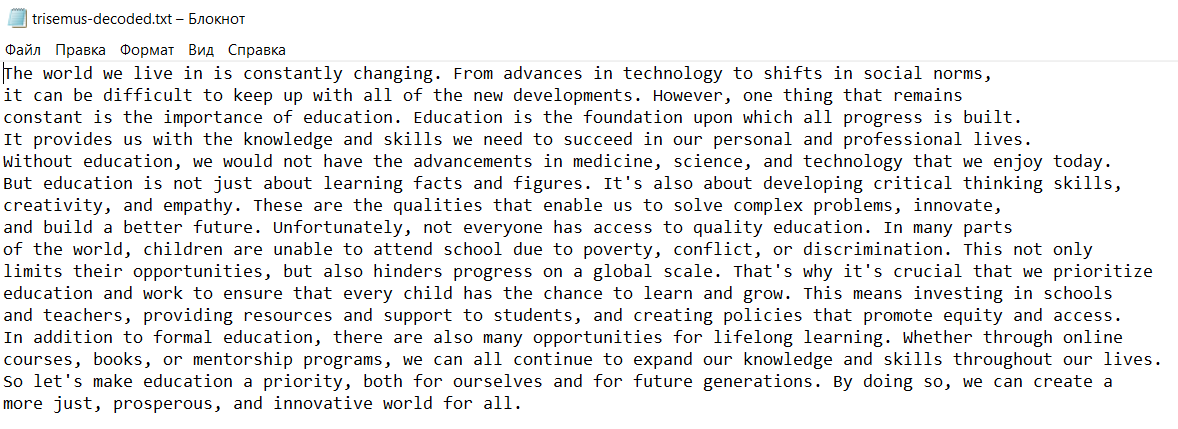


Рисунок 3.15 – Текст, расшифрованный с помощью функции DecryptTrisemus

Рисунок 3.16 – Оценка скорости выполнения шифрования/дешифрования текста

Частота появления символов в этих текстовых файлах представлена на рисунках 3.17 и 3.18 соответственно.

Рисунок 3.17– Гистограмма частот появления символов для зашифрованного текста

Рисунок 3.18– Гистограмма частот появления символов для расшифрованного текста

**Вывод**

В ходе лабораторной работы были изучены и приобретены практические навыки разработки и использования приложений для реализации подстановочных шифров.

Кроме того, были сформированы гистограммы появления частот на основе зашифрованных/расшифрованных сообщений. Из графиков видно, что частота символов в зашифрованном тексте существенно отличается от частоты символов в исходном тексте. Это обусловлено тем, что подстановочные шифры заменяют каждый символ открытого текста на другой символ или последовательность символов в зашифрованном тексте. Так как подстановка была случайной и не учитывала частоту появления символов в открытом тексте, то частотный анализ зашифрованного текста сильно отличается от анализа открытого текста.

Также было разработано авторское приложение в соответствии с целью лабораторной работы.