Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

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

Студент: Плотников Д.А.

ФИТ 3 курс 5 группа

Преподаватель: Берников В.О.

Минск 2020

1. **Описание приложения**

В соответствии с целями лабораторной работы было создано приложение, обладающее следующим функционалом: шифрование и дешифрование текста на немецком языке на основе соотношений, шифрование и дешифрование текста на немецком языке на основе таблицы Трисемуса с ключевым словом «enigma».

Приложение написано на основе .NET Framework с использованием языке C#, оконная подсистема основана на WPF. Разработано и исполняется на операционной системе Windows 10. Вид главного окна приложения представлен на рисунке 1.1.

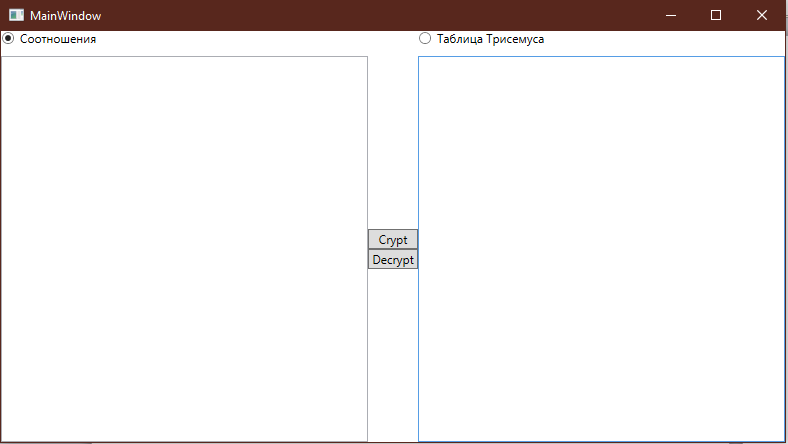


Рисунок 1.1 – Главное окно приложения.

Исходный текст на немецком языке, располагается рядом с проектом в файле с именем text.txt. Достаточно вставить содержимое файла в текстовое поле главного окна приложения и появляется возможность протестировать его работу. В верхней части окна находятся маркеры, предоставляющие возможность выбрать желаемый алгоритм шифрования исходного текста. Две кнопке посреди экрана отвечают за то, в какую сторону будет выполняться шифрование, т.е. прямо или в обратную.

По окончанию шифрования в отдельном окне отображается количество миллисекунд, которое было потрачено на шифрование выбранного текста, что представлено на рисунке 1.2.

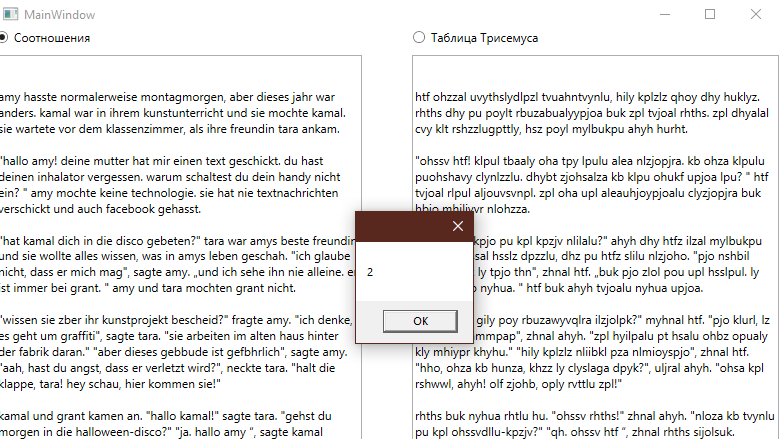
\

Рисунок 1.2 – Отображение времени, затраченного на шифрование.

Как видно из рисунка, много времени на шифрование не требуется, потому что алгоритмы очень простые и алгоритмическая сложность на каждый символ исходного текста составляет O(1).

В результате работы приложения формируются два файла с именами result.csv и source.csv. В файле source.csv приводятся количества встречаемости символов в исходном тексте, а в файле result.csv соответственно количества встречаемости в зашифрованном. Содержимое файла source.csv показано на рисунке 1.3, а файла result.csv на рисунке 1.4.

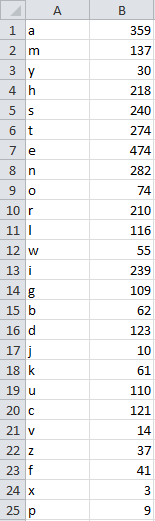


Рисунок 1.3 – Содержимое файла source.csv.

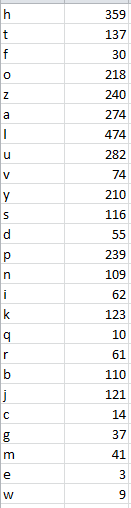


Рисунок 1.4 – Содержимое файла result.csv.

По данным, приведенных выше изображений появляется возможность построить гистограммы символов до и после шифрования. Обе гистограммы приведены на рисунке 1.5.

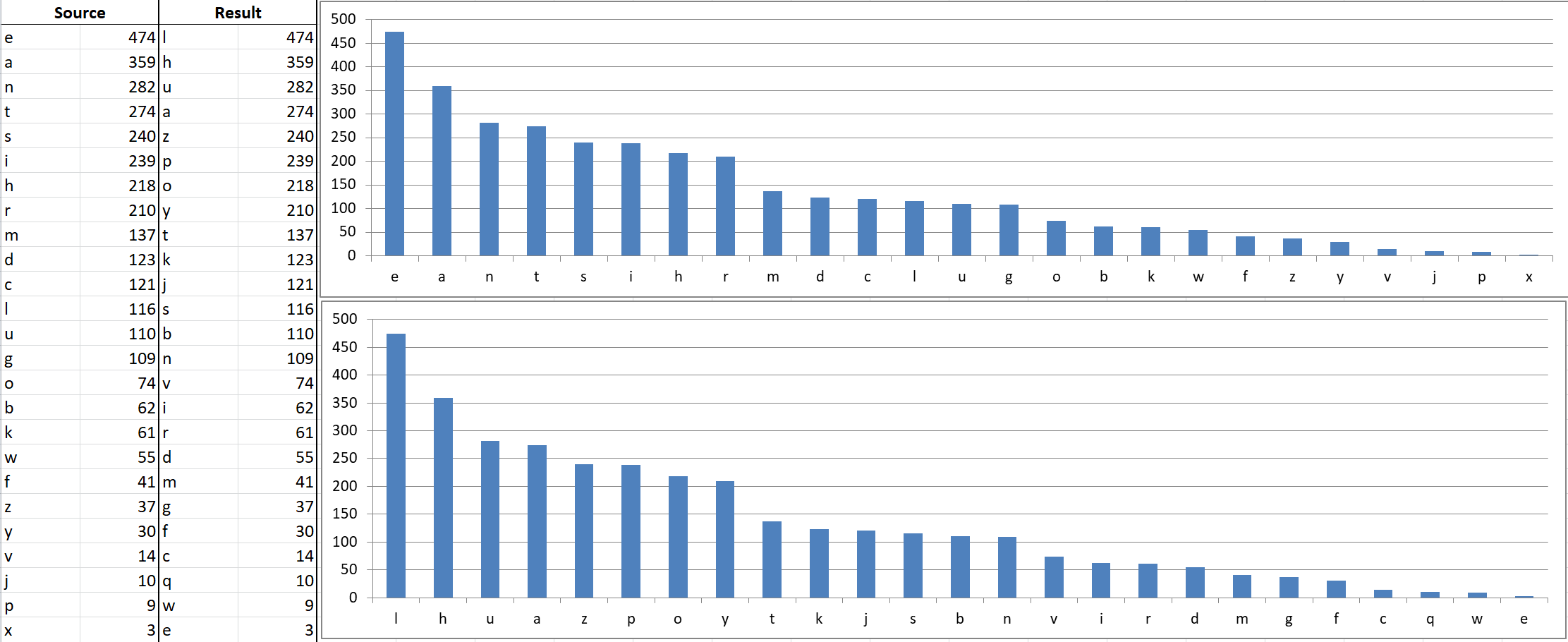


Рисунок 1.5 – Гистограммы, демонстрирующую частоту символов.

Таким образом видно, что гистограммы одинаковы, изменились лишь подписи к ним, что говорит о том, что подстановочные шифры являются самыми уязвимыми к частотному криптографическому анализу.

**Вывод**

В ходе этой работы были изучены и приобретены практические навыки разработки и использования приложений для реализации подстановочных шифров. Разработано приложения на языке программирования С#, позволяющее выполнять шифрование и дешифрование на основе соотношений и на основе алгоритма Трисемуса. Измерено и оценено время выполнения всех операций, а так же построены графики появления символов для исходного и зашифрованного текстов.