Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

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

Студент: Яшный Н. С.

ФИТ 3 курс 4 группа

Минск 2024

1. **Описание приложения**

Приложение написано на языке программирования C# и позволяет зашифровать и расшифровать текстовый документ на основе польского языка, используя:

* шифр Виженера с ключевым словом – yashny;
* шифр Порты.

1. **Методика выполнения поставленных задач**

При шифровании исходного текста шифром Виженера каждый символ входного сообщения последовательно замещается на символ, находящийся на (x+k(mod N)) позиции в польском алфавите, где x – позиция исходного символа, k – позиция текущего символа ключевого слова в алфавите, N – мощность алфавита. Реализация функции шифрования приведена на рисунке 2.1.

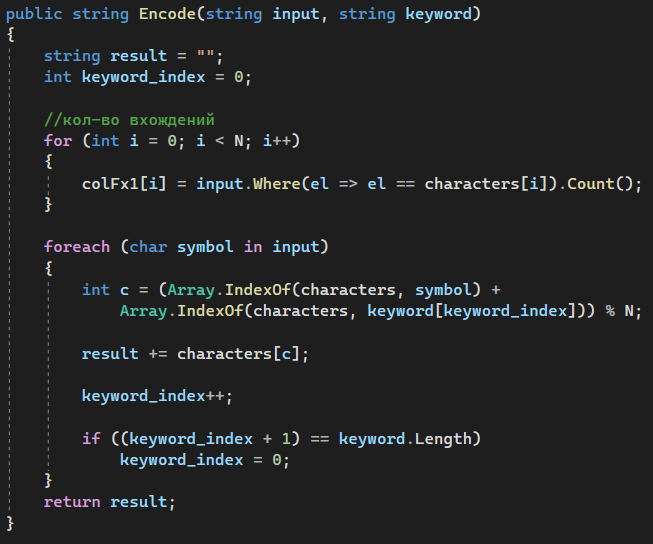


Рис. 2.1 – Реализация шифра Виженера

Расшифрование выполняется путем вычисления новой позиций в алфавите каждого символа после расшифровки по формуле (y–k(modN)), где y – позиция в алфавите текущего зашифрованного символа. Результат шифрования Виженера а также исходный текст представлены на рисунке 2.2.

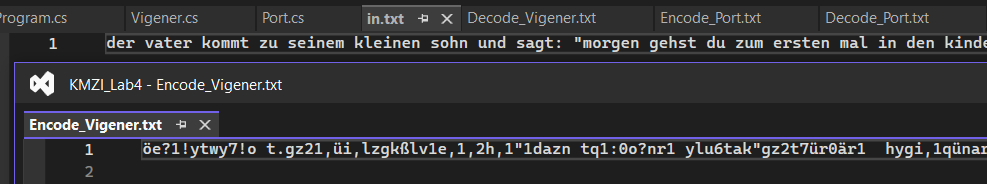


Рисунок 2.2 – Результат шифра Виженера

Для шифрования исходного текста с помощью шифра Порты, используется таблица N x N, где N – количество символов алфавита. Комбинаций пар символов представляются числами. Реализация функции шифрования отображена на рисунке 2.3.

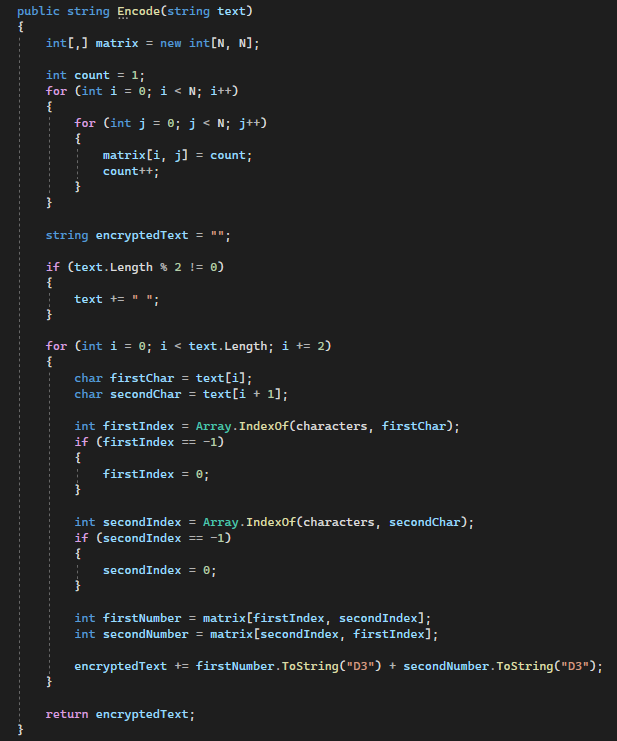


Рис. 2.3 – Реализация шифра Порты

Также приложение оценивает скорость выполнения шифрования/дешифрования с помощью встроенной C#-структуры DateTime.Now.Ticks. Результаты вычисления скоростей представлены на рисунке 2.4. Можно заметить, что оба шифра выполняются с примерно одинаковой скоростью.

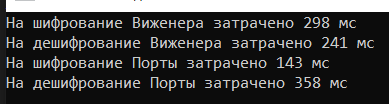


Рис. 2.4 – Скорость выполнения шифров.

Гистограммы частот появления символов в исходном и зашифрованном текстах, представлены на рисунке 2.5.

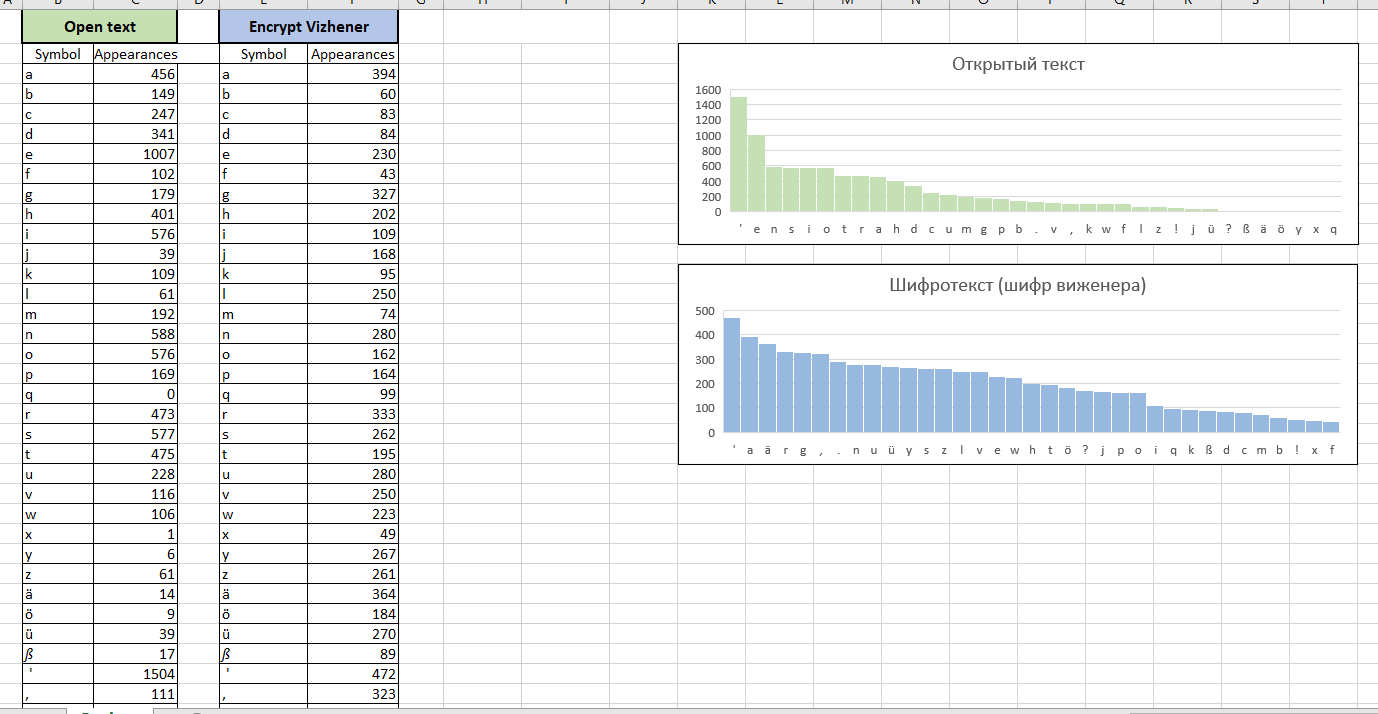


Рис. 2.5 – Гистограммы частот

Можно четко проследить, что распределение символов после кодирования шифром виженера стало намного равномернее.

**Вывод**

В ходе лабораторной работы были приобретены навыки разработки и использования приложений для реализации подстановочных шифров, а также оценены скорость зашифрования/расшифрования реализованных способов шифров.