Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

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

Студент: Чистякова Ю.А.

ФИТ 3 курс 5 группа

Преподаватель: Берников В.О.

Минск 2020

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 – bezpieczeństwo;
* афинные преобразования для k=20;

Также приложение генерирует гистограммы частот появления символов для исходного и зашифрованного сообщений и оценивает время выполнения операций зашифрования и расшифрования.

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.

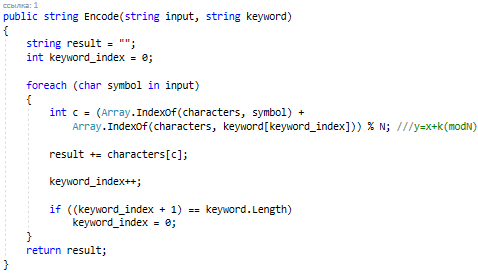


Рис. 2.1 – Реализация шифра Виженера

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.

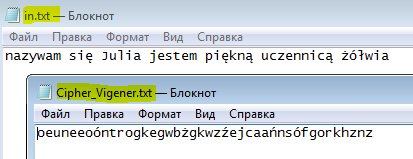


Рисунок 2.2 – Результат шифра Виженера

Для шифрования исходного текста с помощью афинных преобразований Цезаря, используется формула y = x + k (mod N), где x, y – индекс символа в алфавите, k – ключ (в нашем случае 20). Обратное преобразование осуществляется по формуле x = y – k (mod N). Реализация функции шифрования отображена на рисунке 2.3.

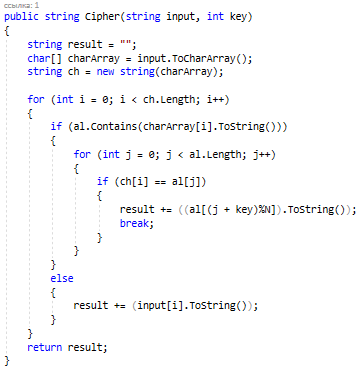


Рис. 2.3 – Реализация афинного шифра Цезаря

Также приложение оценивает скорость выполнения шифрования/дешифрования с помощью встроенной C#-структуры DateTime.Now.Ticks. Результаты вычисления скоростей представлены на рисунке 2.4. Нетрудно заметить, что афинные преобразования выполняются значительно быстрее шифра Виженера.

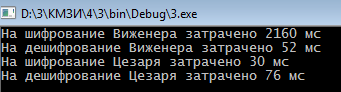


Рис. 2.4 – Скорость выполнения шифров.

Также приложение генерирует гистограммы частот появления символов в исходном и зашифрованном текстах, которые представлены на рисунках 2.5, 2.6 соответсвенно.

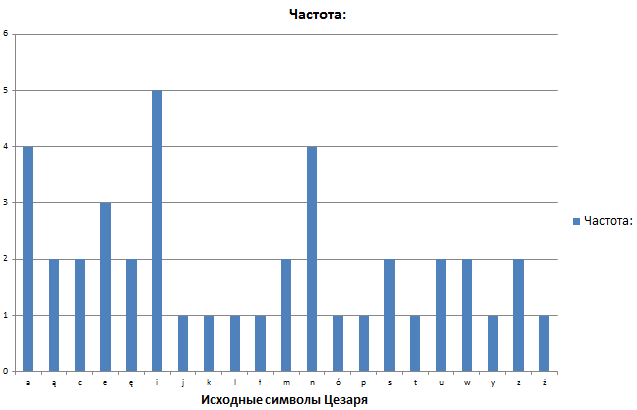


Рис. 2.5 – Гистограмма частот исходных символов

Нетрудно заметить, что после шифрования некоторые символы вовсе перестали появлятся, в то же время в зашифрованном тексте появились и новые символы. Для афинных преобразований результат аналогичен.

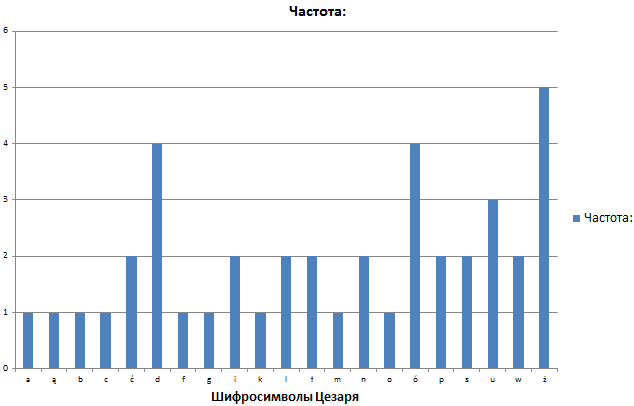


Рис. 2.6 – Гистограмма частота шифросимволов

**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.