МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №2**

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

Выполнила:

Cтудентка 3 курса 2 группы

Бобрик В.С.

Проверила: Копыток Д.В.

Минск 2021

Цель: изучение и приобретение практических навыков разработки и использования приложений для реализации подстановочных шифров.

Задачи:

* Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочных шифров.
* Ознакомиться с особенностями реализации и свойствами различных подстановочных шифров на основе готового программного средства (L\_LUX).
* Разработать приложение для реализации указанных преподавателем методов подстановочного зашифрования/расшифрования.
* Выполнить исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях.
* Оценить скорость зашифрования/расшифрования реализованных способов шифров.
* Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

В данной лабораторной работе необходимо было создать программное средство для выполнения операций зашифрования и дешифрования текстовых документов, созданных на основе алфавита определенного языка с использованием шифров в соответствии с вариантом задания. Для варианта номер 1 был взят текст на белорусском языке, шифрование и дешифрование было произведено на основе соотношений (2.1) и (2.2); k = 5 и Виженера, ключевое слово – собственная фамилия.

В качестве языка разработки программного решения был выбран язык С#. Программная реализация зашифрования и дешифрования с помощью на основе соотношений (2.1) и (2.2) представлена на рисунках 1-2. На рисунке 1 представлена функция для шифрования на основе соотношения 2.1.

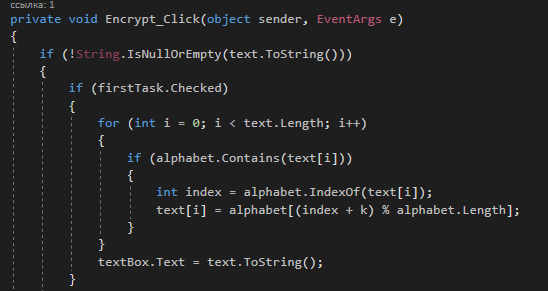


Рис. 1 – Функция для шифрования на основе соотношения 2.1

На рисунке 2 представлена функция дешифрования для шифрования на основе соотношения 2.2. В теле данной функции используется данное соотношение. И далее, используя алфавит, генерируется расшифрованный текст.

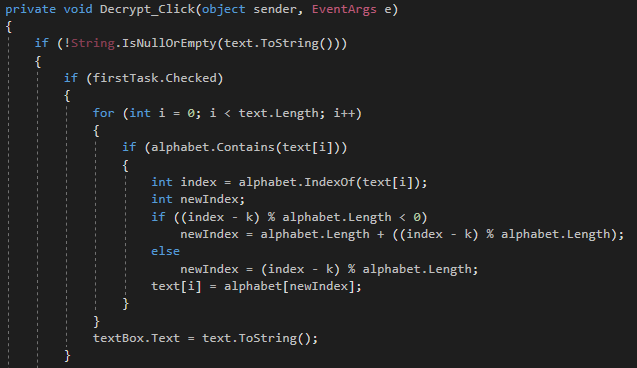


Рис. 3 – Функция на основе соотношения 2.2

Для тестирования разработанных функций был использован текст на белорусском языке, а в качестве ключевого слово было взято слово "бобрык", k = 5. Кроме зашифрования и дешифрования исходного текста были произведены замеры времени работы данных операций и построены гистограммы частот появления символов алфавита в зашифрованном и дешифрованном тексте. На рисунке 3 представлены результаты, описанных ранее операций.

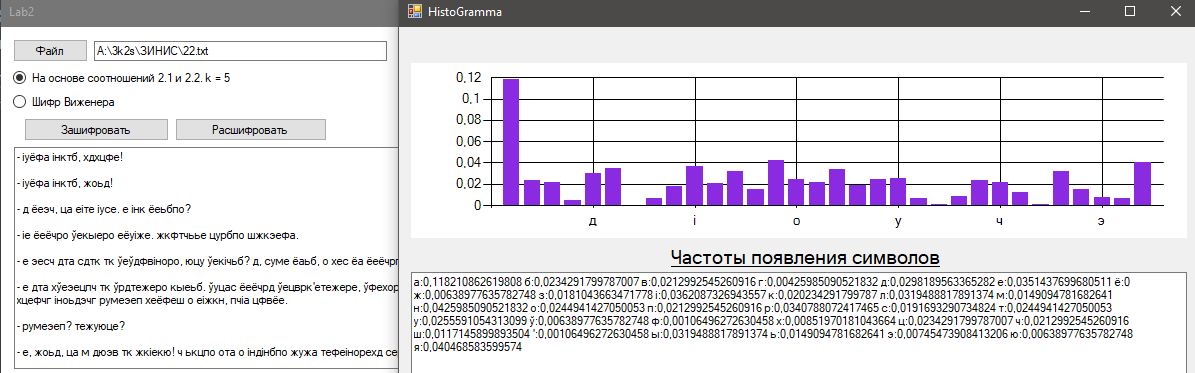


Рис. 4 – Замеры времени выполнения операций и гистограммы частот символов в текстах

Следующим заданием данной лабораторной работы была реализация шифра Виженера. Программная реализация зашифрования и дешифрования с помощью данного шифра с ключевым словом представлена на рисунках 5-6.

На рисунке 5 представлена функция для реализации шифрования методом Виженера, используя переданный в качестве параметра алфавит.

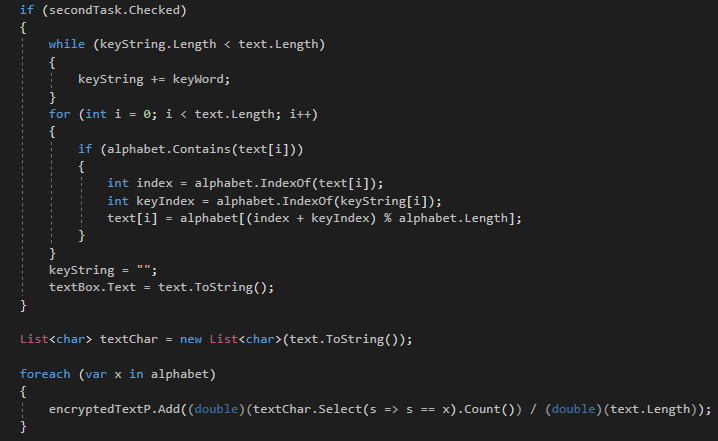


Рис. 5 – Функция шифрования Виженером

На рисунке 7 представлена функция дешифрования с помощью Виженера.

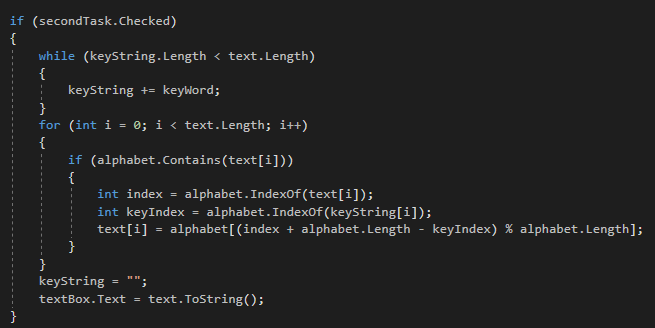


Рис. 6 – Функция дешифрования с помощью Виженера

Для тестирования разработанных функций был использован текст на белорусском языке, а в качестве ключевого слово было взято слово "бобрык". Кроме зашифрования и дешифрования исходного текста были произведены замеры времени работы данных операций и построены гистограммы частот появления символов алфавита в зашифрованном и дешифрованном тексте. На рисунке 7 представлены результаты, описанных ранее операций.

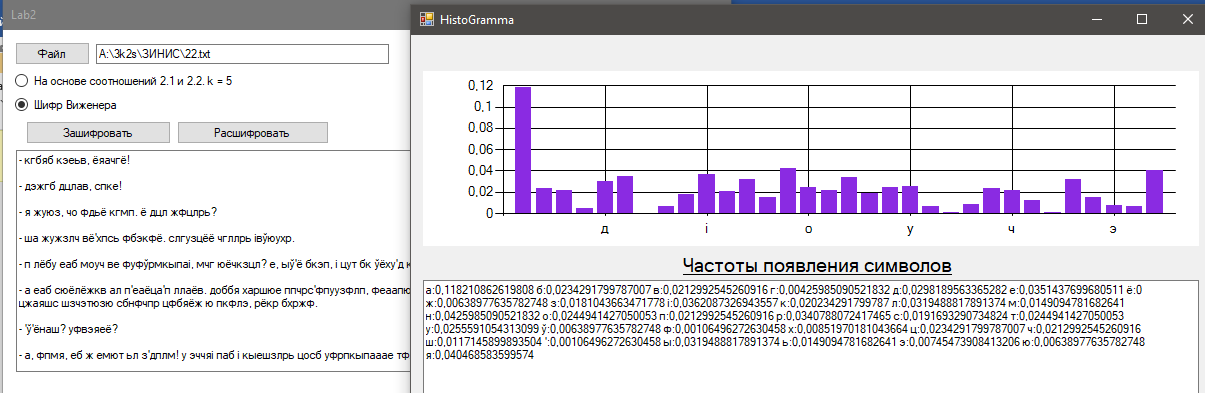


Рис. 7 – Замеры времени выполнения операций и гистограммы частот символов в текстах для шифра Виженера

С помощью полученных гистограмм можно дешифровать зашифрованный текст, сопоставив частоты появления символов алфавита в зашифрованном тексте с частотами в исходном незашифрованным текстом.

Вывод: в результате данной лабораторной работы было разработано приложение для выполнения зашифрования и дешифрования текстов на основе соотношений 2.1 и 2.2 и метода Виженера, для вычисления времени выполнения этих операций и для построения гистограмм частоты появления символов алфавита в зашифрованном и дешифрованном текстах.