МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №4**

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

Выполнила студентка 3 курса 5 группы Максимчикова Ю. С.

Проверила: Блинова Е. А.

Минск 2020

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 11 был взят текст на белорусском языке, шифрование и дешифрование было произведено с помощью шифра Цезаря и таблицы Трисемуса с ключевыми словами. Рассмотрим программный код и результаты работы каждого шифра более подробно.

В качестве языка разработки программного решения был выбран язык С#. Программная реализация зашифрования и дешифрования с помощью шифра Цезаря с ключевым словом представлена на рисунках 1-3. На рисунке 1 представлена функция для генерации нового алфавита на основе ключевого слова и позиции.

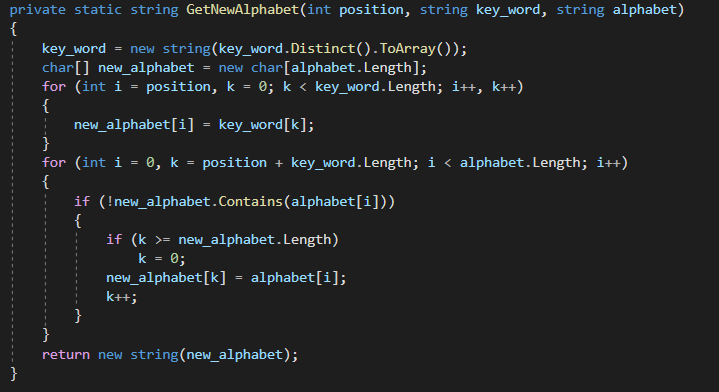


Рис. 1 – Функция для генерации нового алфавита на основе ключевого слова и позиции

На рисунке 2 представлена уже непосредственно сама функция зашифрования с помощью шифра Цезаря. В теле данной функции вызывается ранее описанная функция для генерации нового алфавита. И далее, используя полученный алфавит, генерируется зашифрованный текст.

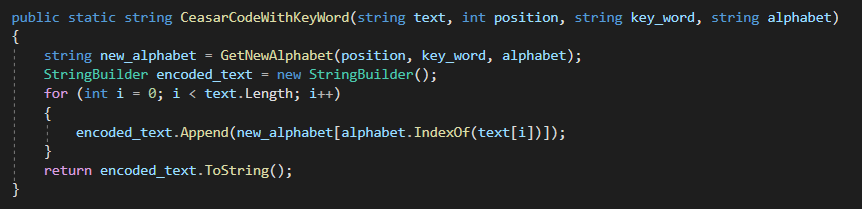


Рис. 2 – Функция зашифрования с помощью шифра Цезаря

На рисунке 3 представлена функция дешифрования с помощью шифра Цезаря. В теле данной функции вызывается ранее описанная функция для генерации нового алфавита. И далее, используя полученный алфавит, генерируется расшифрованный текст.

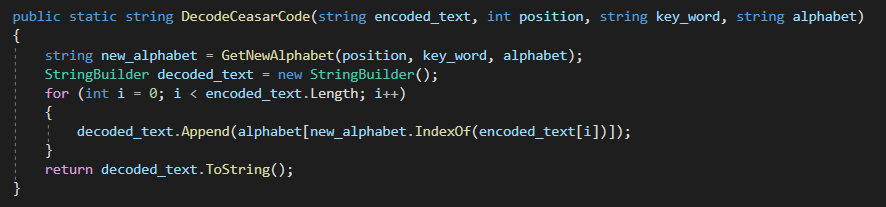


Рис. 3 – Функция дешифрования с помощью шифра Цезаря

Для тестирования разработанных функций был использован текст на белорусском языке длиной не менее 5000 символов, а в качестве ключевого слово было взято слово "інфарматыка", a = 2. 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 4 представлены результаты, описанных ранее операций.

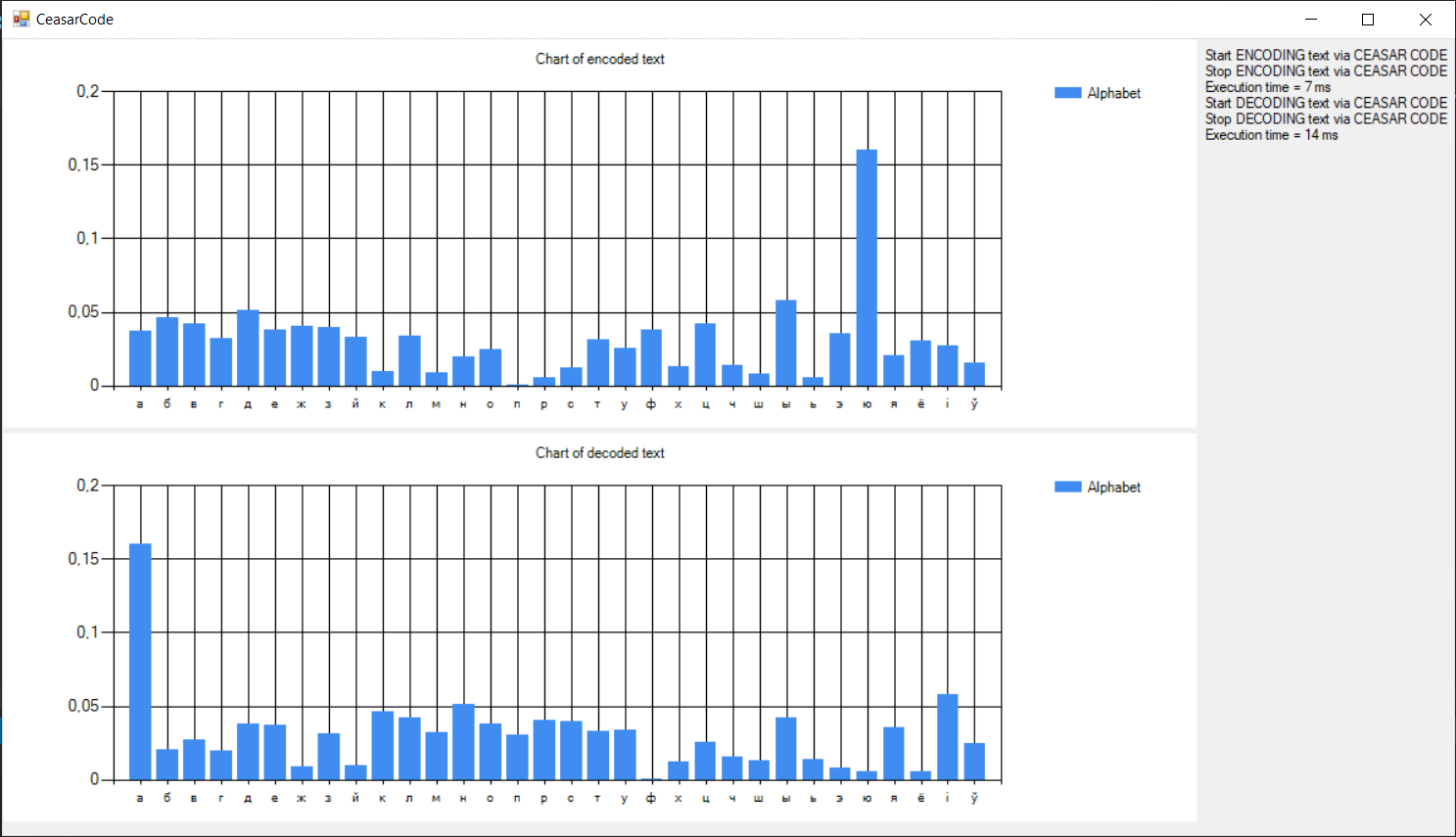


Рис. 4 – Замеры времени выполнения операций и гистограммы частот символов в текстах для шифра Цезаря

Следующим заданием данной лабораторной работы была реализация таблицы Трисемуса. Программная реализация зашифрования и дешифрования с помощью таблицы Трисемуса с ключевым словом представлена на рисунках 5-7.

На рисунке 5 представлена функция для составления таблицы Трисемуса с размерностью [8, 4], используя переданный в качестве параметра алфавит.

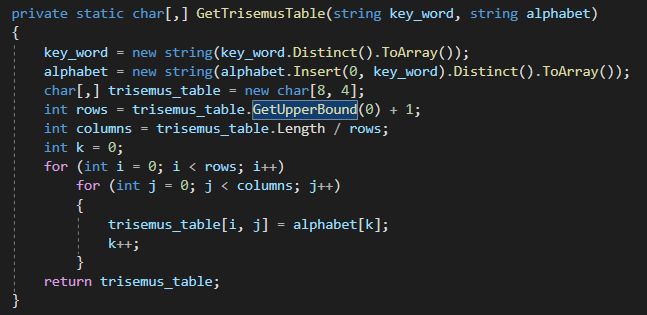


Рис. 5 – Функция для составления таблицы Трисемуса

На рисунке 6 представлена уже непосредственно сама функция зашифрования с помощью таблицы Трисемуса.

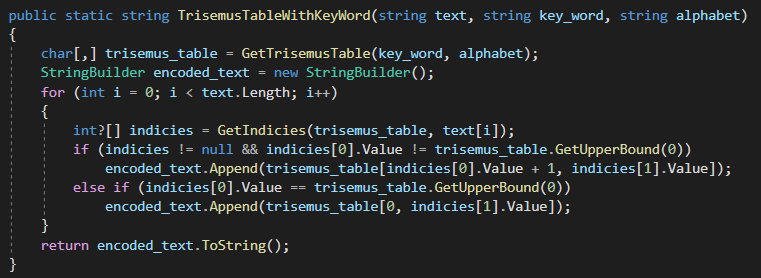


Рис. 6 – Функция зашифрования с помощью таблицы Трисемуса

На рисунке 7 представлена функция дешифрования с помощью таблицы Трисемуса.

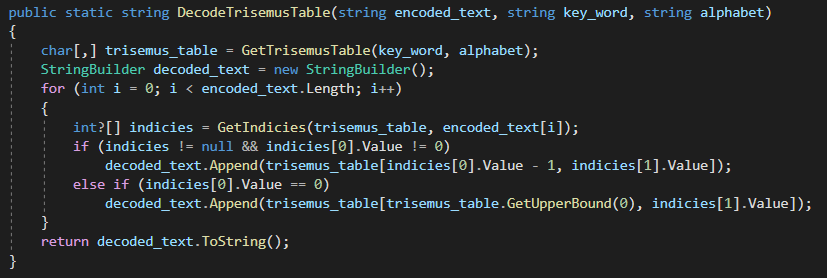


Рис. 7 – Функция дешифрования с помощью таблицы Трисемуса

Для тестирования разработанных функций был использован текст на белорусском языке длиной не менее 5000 символов, а в качестве ключевого слово было взято слово "юлія". 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 8 представлены результаты, описанных ранее операций.

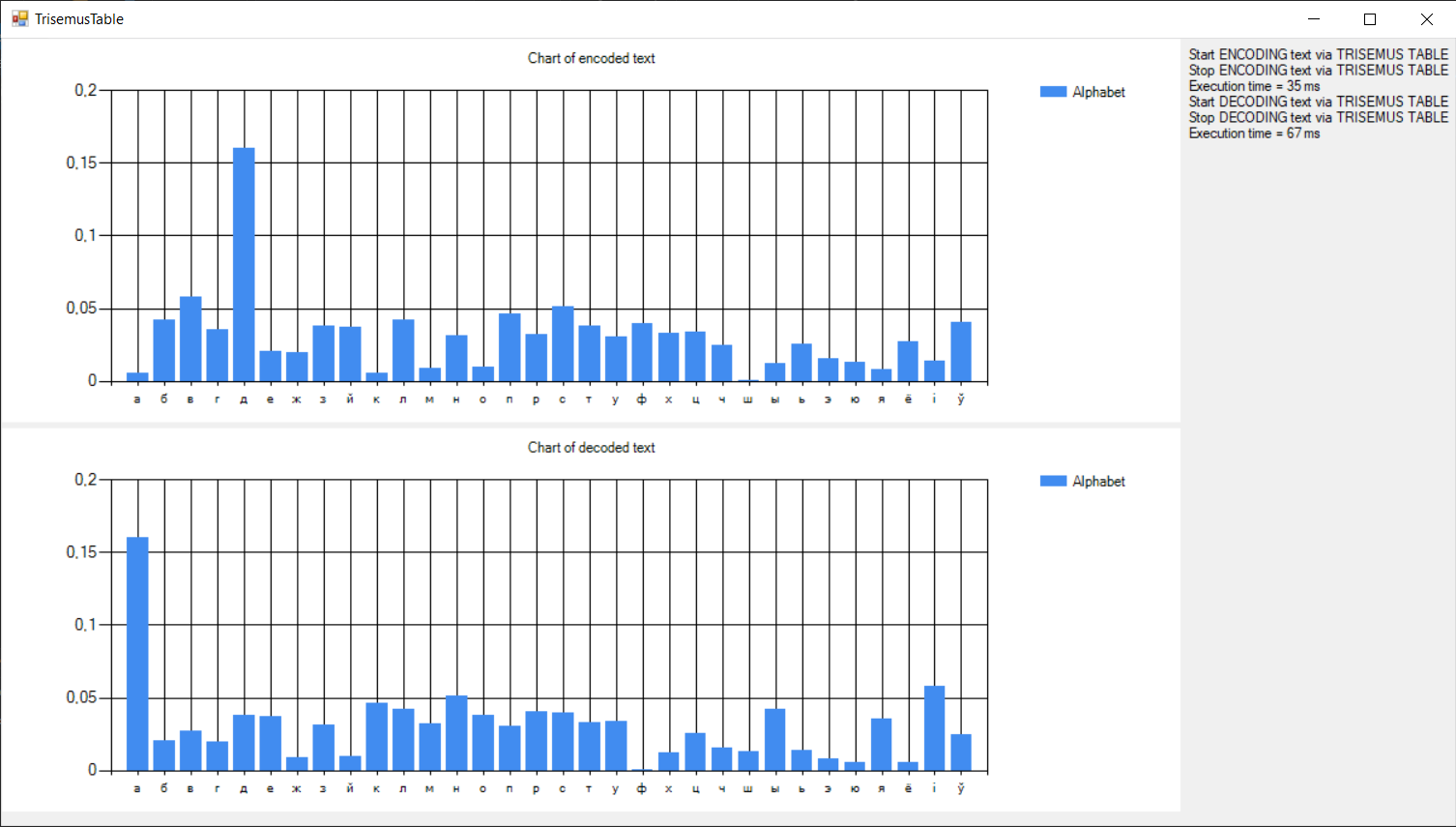


Рис. 8 – Замеры времени выполнения операций и гистограммы частот символов в текстах для таблицы Трисемуса

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

Сравнивая полученные результаты, можно заметить, что для выполнения операции зашифрования требуется больше времени, чем для операции дешифрования, независимо от используемого шифра. Также можно увидеть, что операции, связанные с таблицей Трисемуса, выполняются примерно в пять раз медленнее, чем с шифром Цезаря. Это объясняется тем, что таблица Трисемуса является усложненной версией шифра Цезаря.

Вывод: в результате данной лабораторной работы было разработано приложение для выполнения зашифрования и дешифрования текстов с помощью шифра Цезаря и таблицы Трисемуса, для вычисления времени выполнения этих операций и для построения гистограмм частоты появления символов алфавита в зашифрованном и дешифрованном текстах.