МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №5**

**″Исследование криптографических шифров на основе перестановки 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 перестановочных шифров.

**Задачи**:

* Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости перестановочных шифров.
* Ознакомиться с особенностями реализации и свойствами различных перестановочных шифров на основе готового программного средства (L\_LUX).
* Разработать приложение для реализации указанных преподавателем методов перестановочного 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 маршрутной перестановки (запись – по строкам, считывание – по столбцам таблицы) и шифра множественной перестановки с ключевыми словами. Интерфейс разработанного программного средства представлен на рисунках 1-2.

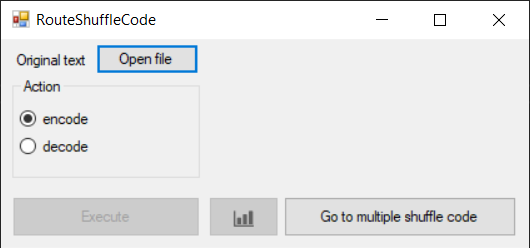


Рис. 1 – Окно программного средства для работы с шифром маршрутной перестановки

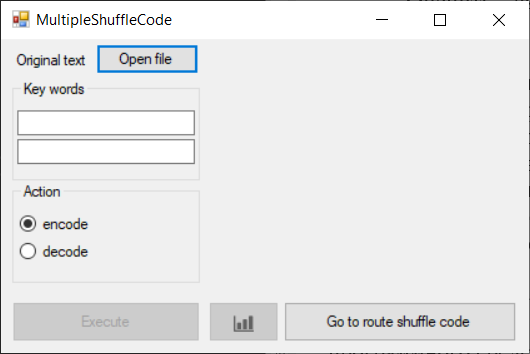


Рис. 2 – Окно программного средства для работы с шифром множественной перестановки

Рассмотрим программный код и результаты работы каждого шифра более подробно.

**Шифр маршрутной перестановки**

Шифр маршрутной перестановки основан на таблице. В такую таблицу вписывают исходное сообщение по определенному маршруту, а выписывают (получают шифрограмму) – по-другому. Для данного шифра маршруты вписывания и выписывания, а также размеры таблицы являются ключом.

Программная реализация зашифрования и дешифрования с помощью шифра маршрутной перестановки представлена на рисунках 3-5.

На рисунке 3 представлены функции для генерации таблиц, необходимых для операций зашифрования и дешифрования. В случае зашифрования запись текста в таблицу осуществляется по строкам. В случае дешифрования запись зашифрованного текста происходит по столбцам.

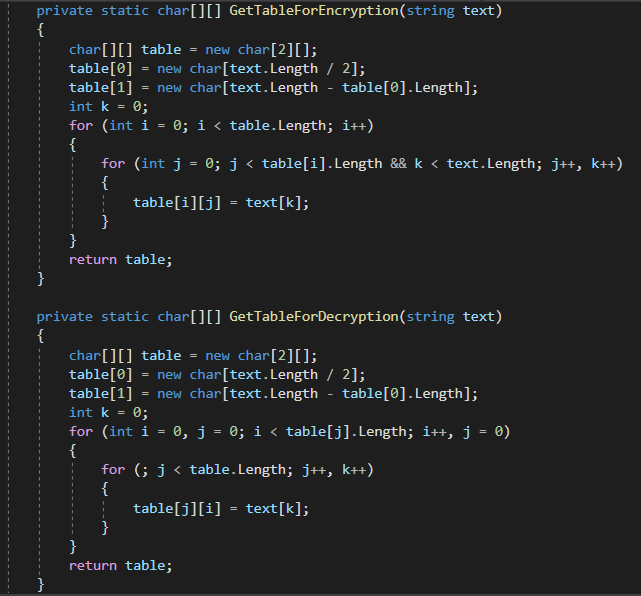


Рис. 3 – Функции для генерации таблиц для зашифрования и дешифрования

На рисунке 4 представлена функция зашифрования с помощью шифра маршрутной перестановки. В ней происходит вызов функции, представленной на рисунке 3. В результате её вызова возвращается готовая таблица для зашифрования текста. Для получения зашифрованного текста выполняется считывание этой таблицы по столбцам.

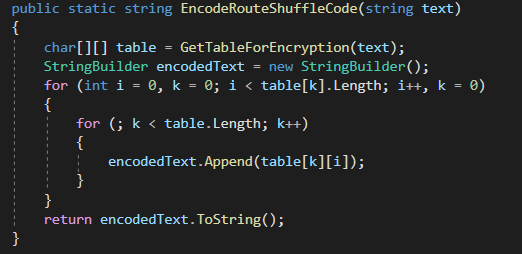


Рис. 4 – Функция зашифрования с помощью шифра маршрутной перестановки

На рисунке 5 представлена функция дешифрования с помощью шифра маршрутной перестановки. В ней происходит вызов функции, представленной на рисунке 3. В результате её вызова возвращается готовая таблица для дешифрования текста. Для получения расшифрованного текста выполняется считывание этой таблицы по строкам.

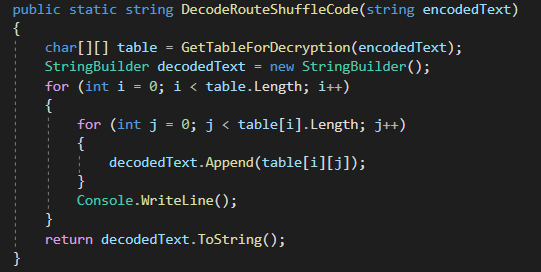


Рис. 5 – Функция дешифрования с помощью шифра маршрутной перестановки

Для тестирования разработанных функций был использован текст на белорусском языке длиной не менее 500 символов. 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 6 представлены результаты, описанных ранее операций.

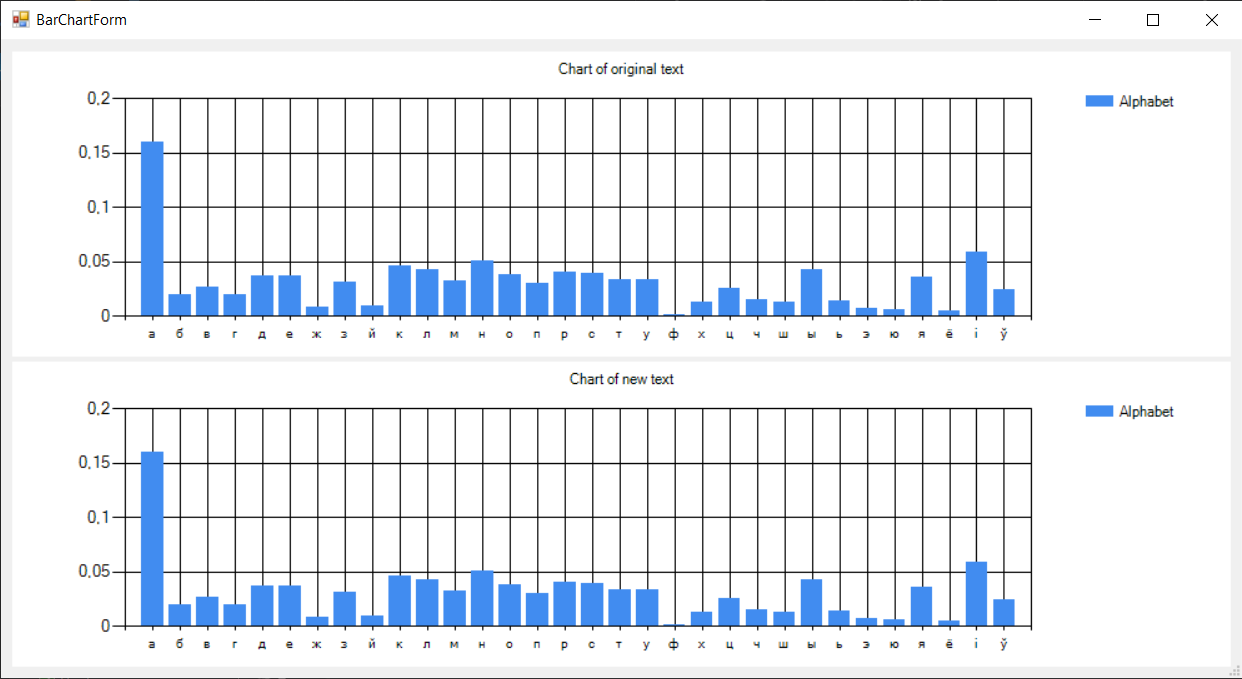


Рис. 6 – Гистограммы частот символов в текстах для шифра маршрутной перестановки

**Шифр множественной перестановки с ключевыми словами**

Особенностью шифров данного подкласса является минимум двукратная перестановка символов шифруемого сообщения. В простейшем случае это может задаваться перемешиваем не только столбцов, но и строк. Таким образом, этот случай соответствует использованию двух основных ключей: длина одного из них равна числу столбцов, другого – числу строк. К ключевой информацию мы можем относить также способы вписывания сообщения и считывания отдельных символов из текущего столбца матрицы.

Программная реализация зашифрования и дешифрования с помощью шифра множественной перестановки представлена на рисунках 7-13.

На рисунке 7 представлена функция для вычисления размеров таблицы. Размер таблицы определяется исходя из размера входного текста. Результатом работы данной функции являются количество строк и количество столбцов таблицы.

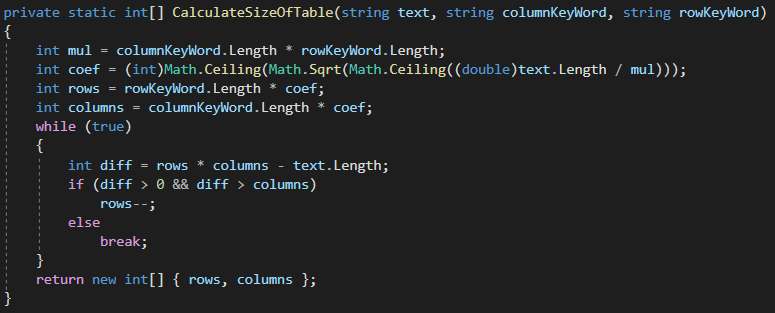


Рис. 7 – Функция для вычисления размеров таблицы

На рисунке 8 представлена функция для формирования числового массива из ключевого слова.

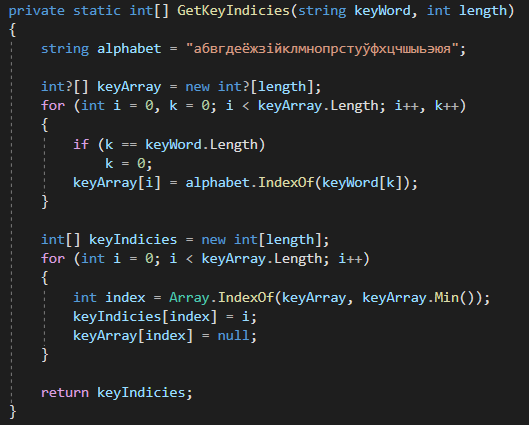


Рис. 8 – Функция для формирования числового массива из ключевого слова

На рисунке 9 представлена функция для заполнения таблицы текстом.

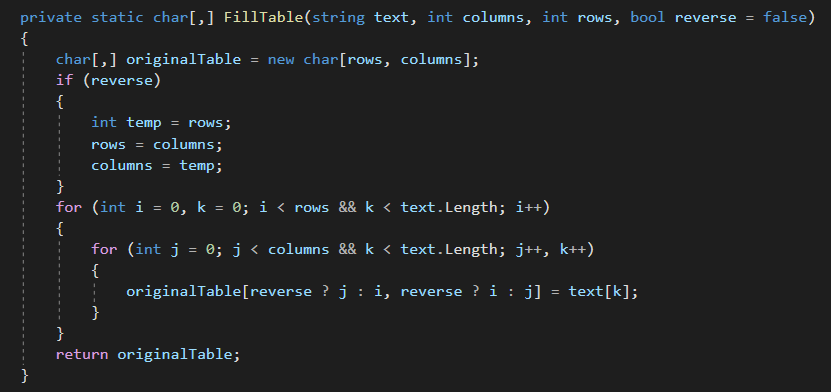


Рис. 9 – Функция для заполнения таблицы текстом

На рисунке 10 представлена функция для создания шифрующей таблицы.

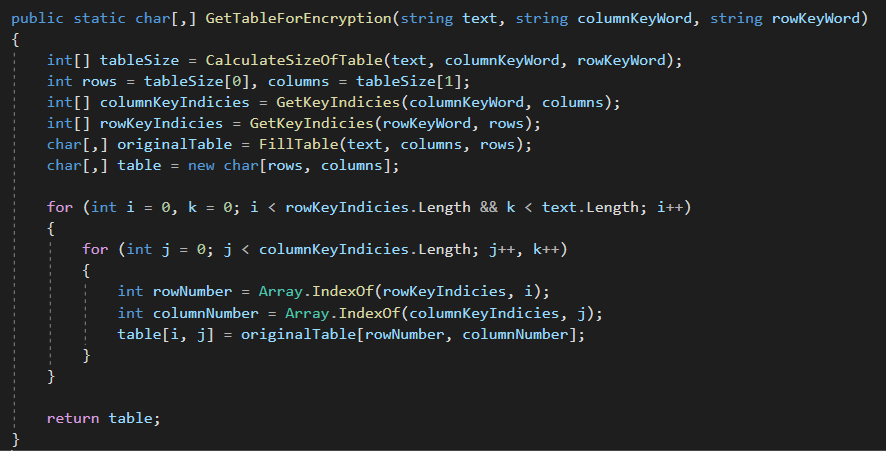


Рис. 10 – Функция для создания шифрующей таблицы

На рисунке 11 представлена функция для создания дешифрующей таблицы.

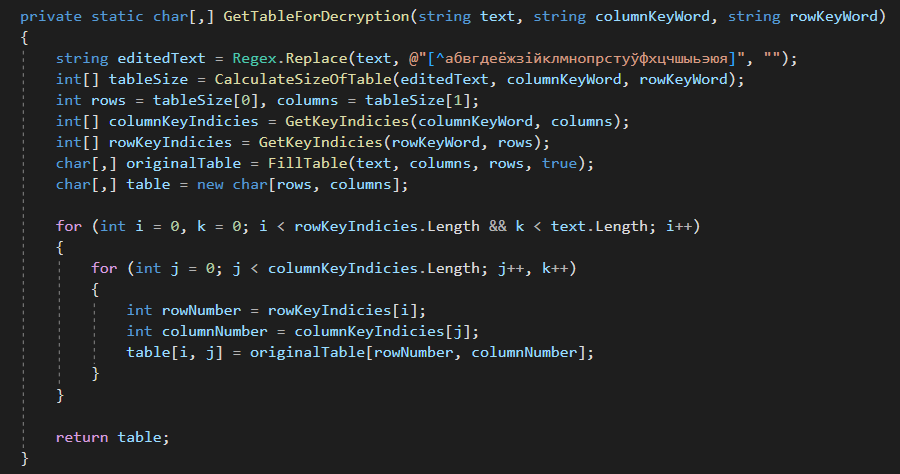


Рис. 11 – Функция для создания дешифрующей таблицы

На рисунке 12 представлена функция зашифрования с помощью шифра множественной перестановки.

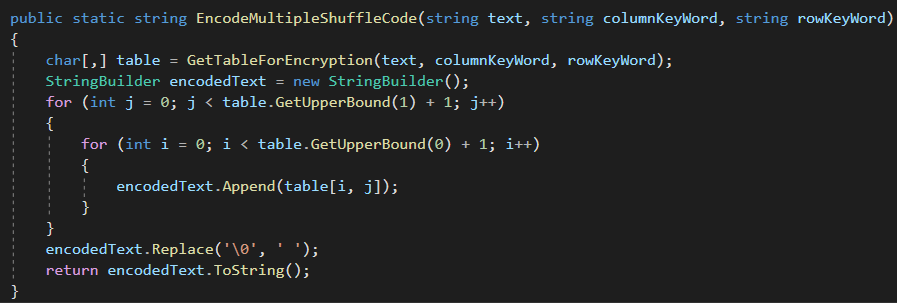


Рис. 12 – Функция зашифрования с помощью шифра множественной перестановки

На рисунке 13 представлена функция дешифрования с помощью шифра множественной перестановки.

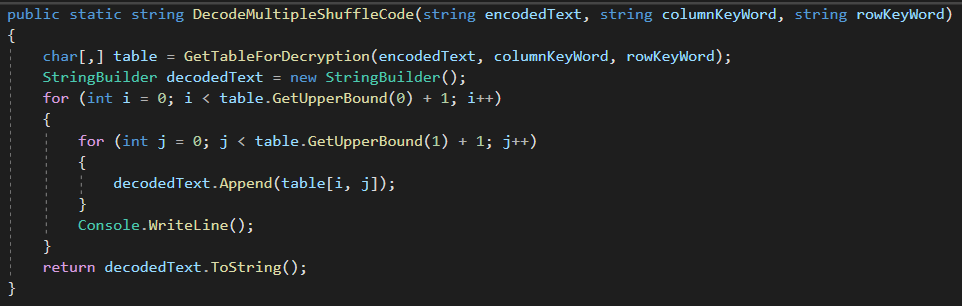


Рис. 13 – Функция дешифрования с помощью шифра множественной перестановки

Для тестирования разработанных функций был использован текст на белорусском языке длиной не менее 500 символов. 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 14 представлены результаты, описанных ранее операций.

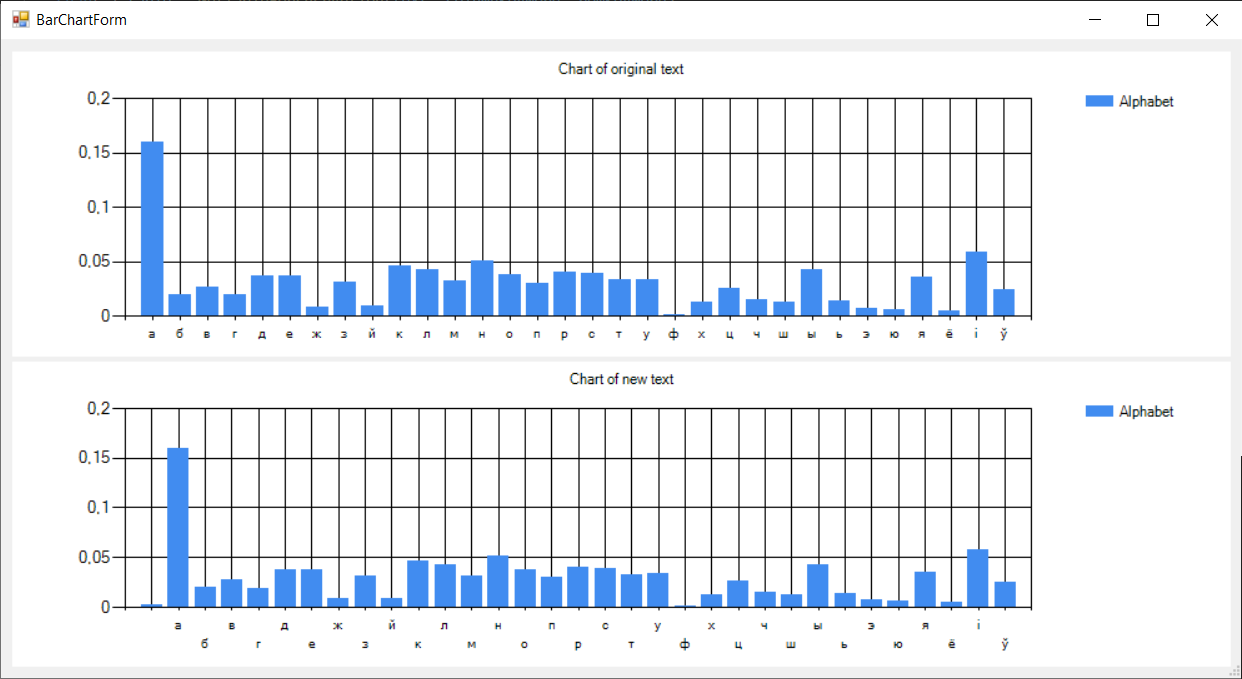


Рис. 14 – Гистограммы частот символов в текстах для шифра множественной перестановки

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