МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №5**

**«Исследование криптографических шифров на основе перестановки символов»**

Выполнил студент

3 курса 5 группы

Храмых В.О.

Проверила: Блинова Е. А.

Минск 2020

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

**Задачи**:

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

**Основное задание:**

Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:

* выполнять зашифрование/расшифрование текстовых документов (объемом не менее 500 знаков) созданных на основе алфавита языка в соответствии с нижеследующей таблицей вариантов задания;
* формировать гистограммы частот появления символов для исходного и зашифрованного сообщений;
* оценивать время выполнения операций зашифрования/расшифрования.

Исходя из варианта 2:

* используемый алфавит – русский;
* маршрутная перестановка (маршрут: по спирали (сторона спирали не была указана, поэтому я использовал запись против часовой стрелке); параметры таблицы – по указанию преподавателя);
* множественная перестановка, ключевые слова – собственные имя и фамилия.

**Маршрутная перестановка:**

Код функции шифрования представлен на рисунках 1.1 – 1.3.

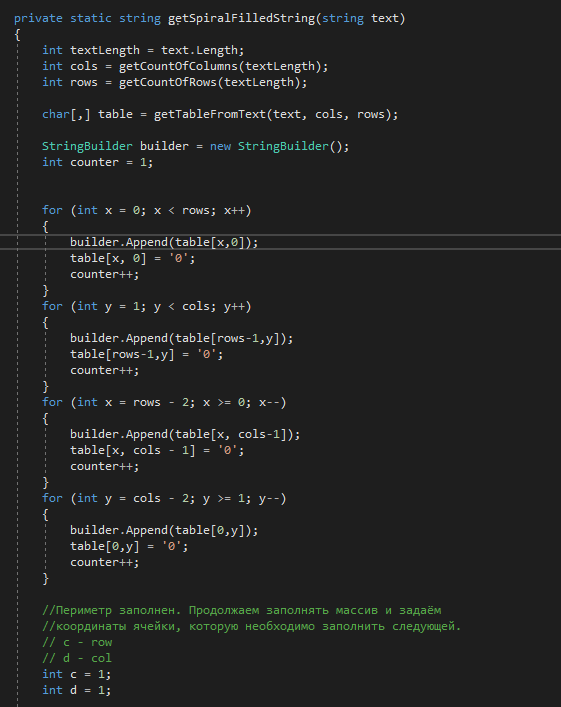


Рисунок 1.1 – часть функции шифрования

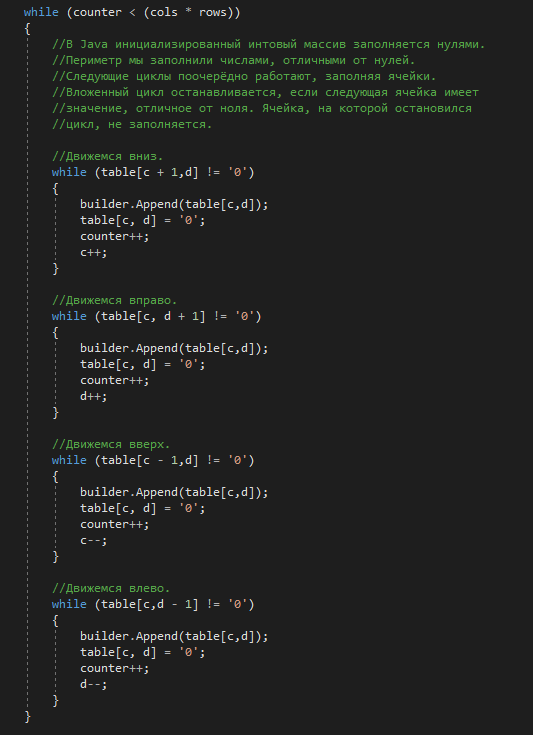


Рисунок 1.2 – вторая часть функции шифрования

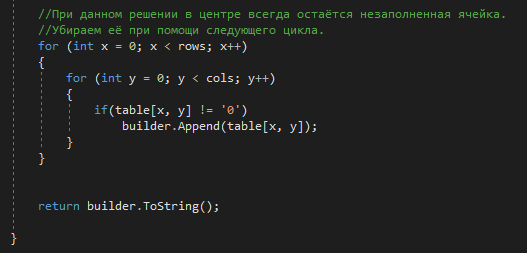


Рисунок 1.3 –третья часть функции шифрования.

Результат выполнения можно увидеть в правом текстовом поле. В первом находится текст, который нужно зашифровать. Время выполнения указано в нижнем правом углу (рисунок 2).

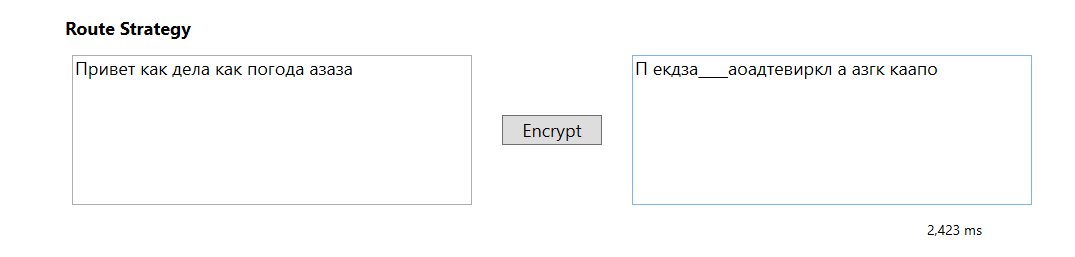


Рисунок 2 – Результат выполнения шифрования.

Код функции расшифрования маршрутного шифра по спирали против часовой стрелки, представлен на рисунках 3.1 - 3.3.

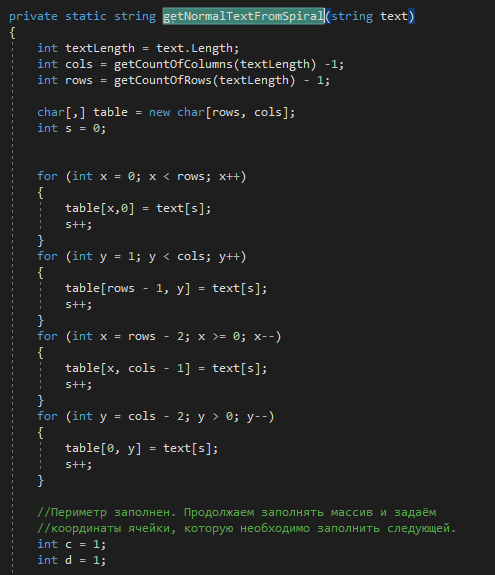


Рисунок 3.1 – первая часть функции расшифрования.

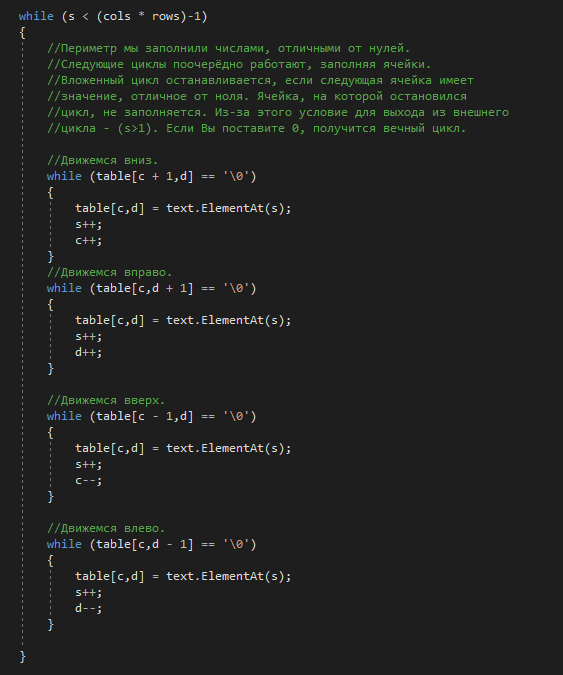


Рисунок 3.1 – вторая часть функции расшифрования.

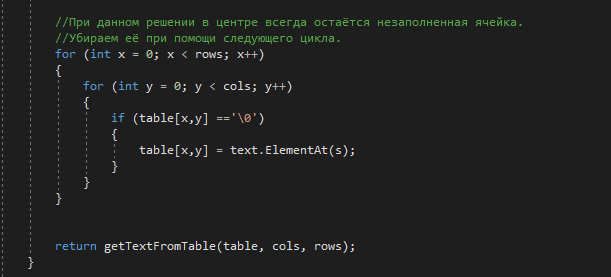


Рисунок 3.3 –третья часть функции расшифрования.

На рисунке 4 представлен результат выполнения расшифрования и сверка результат с исходным текстом. Время выполнения указано в нижнем правом углу.

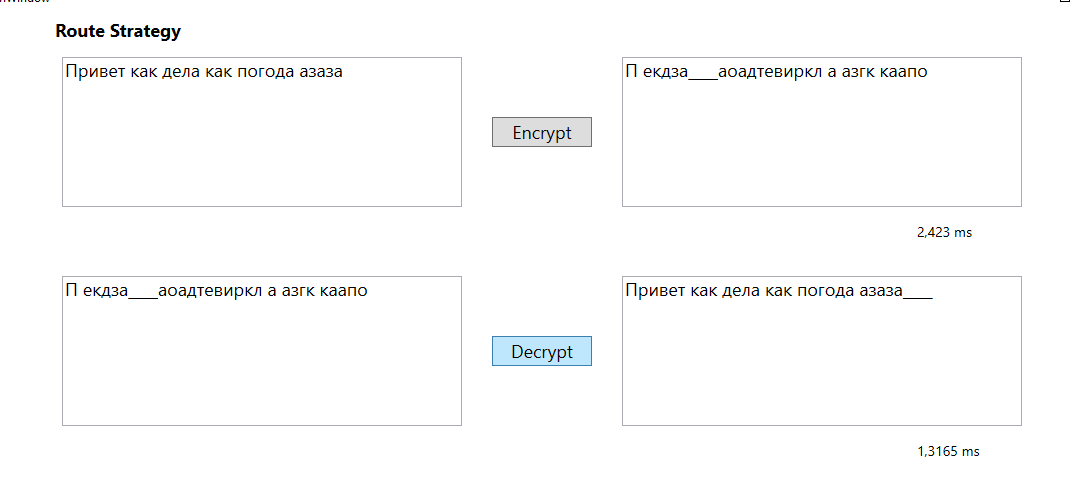


Рисунок 4 –результат выполнения расшифрования.

**Множественная перестановка:**

Код для зашифрования сообщения представлен на рисунке 5

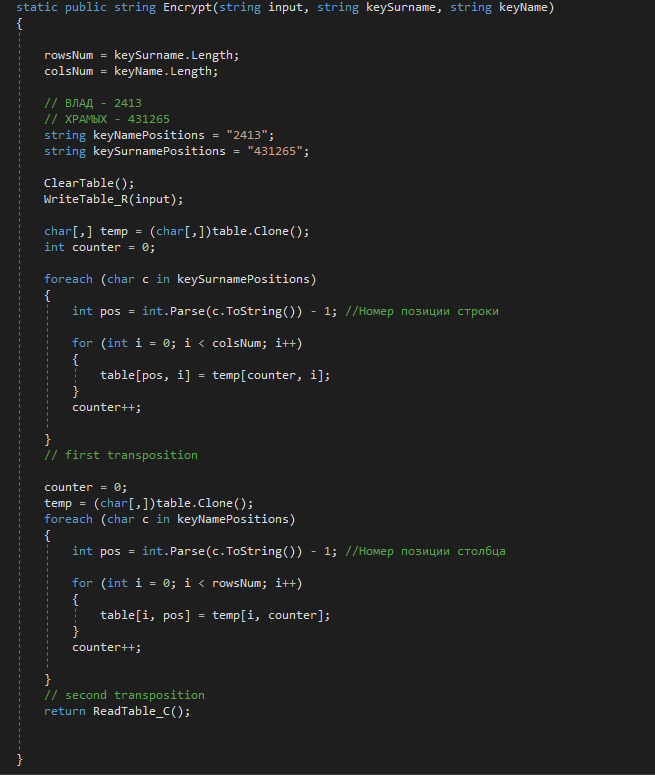


Рисунок 5 – код для зашифрования.

Сообщение записывается в таблицу по строкам.

Параметры keySurname и keyName представляют собой ключи. В данном случае, ХРАМЫХ – 431265, ВЛАД– 2413. Размерность таблицы 6 на 4. Количество символов – 24. Входное сообщение: [текст, длиной до 24 символов].

Код для расшифрования сообщения представлен на рисунке 6.

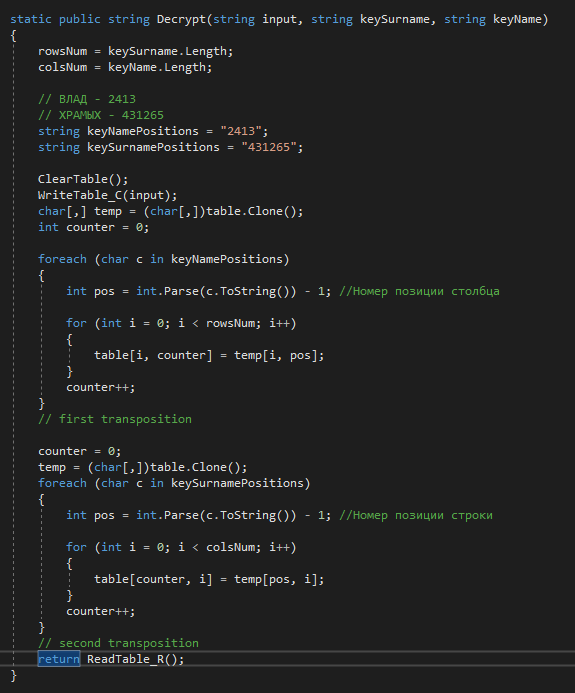


Рисунок 6 – код для расшифрования.

Сообщение записывается в таблицу по столбцам.

Пример работы алгоритма приведен на рисунке 7.

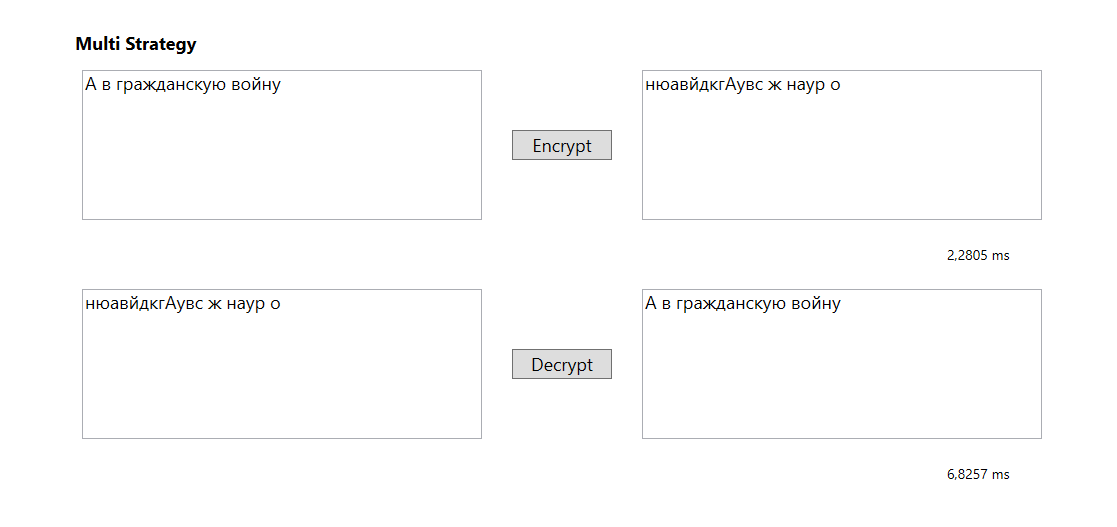


Рисунок 8 – пример работы алгоритма.

На рисунке видно, что результат зашифрования в расшифрованном виде совпадает с исходным текстом. Время выполнения указано в правом углу.

**Вывод**: в ходе выполнения данной лабораторной работы было создано приложение, реализующее указанные условием задания. Изучены и приобретены практические навыки разработки и использования приложений для реализации перестановочных шифров.

Частота появления символов для исходного и зашифрованного сообщений идентичны в обоих случаях, так как происходит лишь перестановка символов между собой.