Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Криптографические методы защиты информации

Студент: Сенченя В.И.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М. Г.

Минск 2023

**Лабораторная работа №5**

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

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. Разработать приложение для реализации указанных преподавателем методов перестановочного зашифрования/расшифрования

3. Выполнить исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях.

4. Оценить скорость зашифрования/расшифрования реализованных способов шифров.

**Маршрутная перестановка**

Сущность перестановочного шифрования состоит в том, что исходный текст (*М*) и зашифрованный текст (*С*) основаны на использовании одного и того же алфавита, а тайной или ключевой информацией является алгоритм перестановки.

В маршрутной перестановке строится таблица (количество ячеек является размером секретного ключа) и на основе построенной таблицы исходное сообщение шифруется, проходя по определённому маршруту, в моём случае использовался метод зигзагом, в котором я шёл от нижнего левого угла до правого верхнего змейкой.

Для расшифровки необходимо создать таблицу на основе зашифрованного текста, при этом инвертировать размеры таблицы.

Пример кода программы для шифрования предоставлен на рисунке 1.1, а результат выполнения на 1.2, для шифрования на рисунках 1.3 и 1.4 соответственно



Рисунок 1.1 – Код программы для шифрования

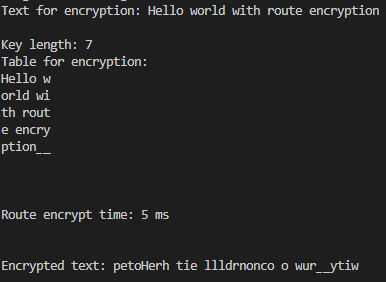


Рисунок 1.2 – Результат выполнения

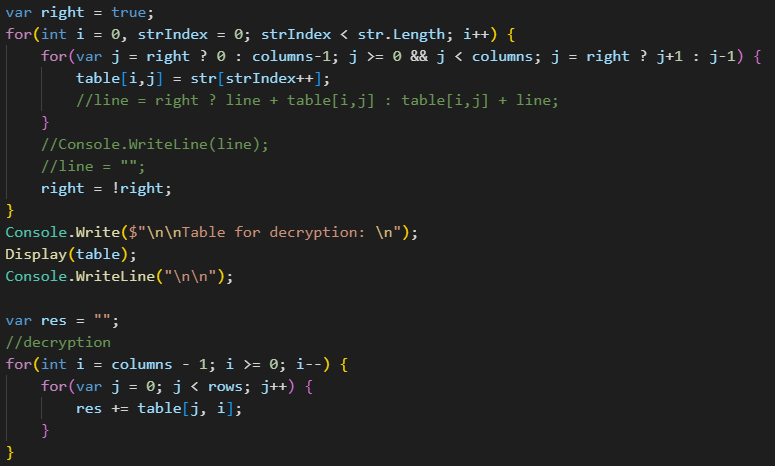


Рисунок 1.3 – Код программы для дешифрования

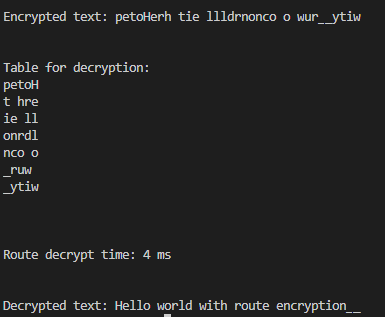


Рисунок 1.4 – Результат выполнения

Гистограммы частот появления символов при шифровании и дешифровании представлены на рисунках 1.5 и 1.6 соответственно

Рисунок 1.5 – Гистограмма появления символов при шифровании

Рисунок 1.6 – Гистограмма появления символов при дешифровании

На основе гистограмм можем сделать вывод, что они идентичные(потому что не происходит замена на другие символы), что с одной стороны хорошо, ведь данные не потерялись, а с другой стороны плохо, потому что становится проще подобрать нужные комбинации.

Скорость выполнения шифрования и дешифрования предоставления на рисунке 1.7

Рисунок 1.7 – Скорость выполнения шифрования и дешифрования

**Множественная перестановка**

Особенностью шифров данного подкласса является минимум двукратная перестановка символов шифруемого сообщения. В простейшем случае это может задаваться перемешиванием не только столбцов но и строк.

В моём случае изначально строится таблица(размеры на основе двух ключей) с помощью исходного сообщения записывая сначала в строки, потом в столбцы. Затем перемешиваются строки на основе первого ключа по алфавитному порядку, после этого перемешанная таблица снова перемешивается, но уже по столбцам. Для дешифрования всё тоже самое, только в обратном порядке.

Пример кода программы для шифрования предоставлен на рисунке 1.8, а результат выполнения на 1.9, для шифрования на рисунках 1.10 и 1.11 соответственно

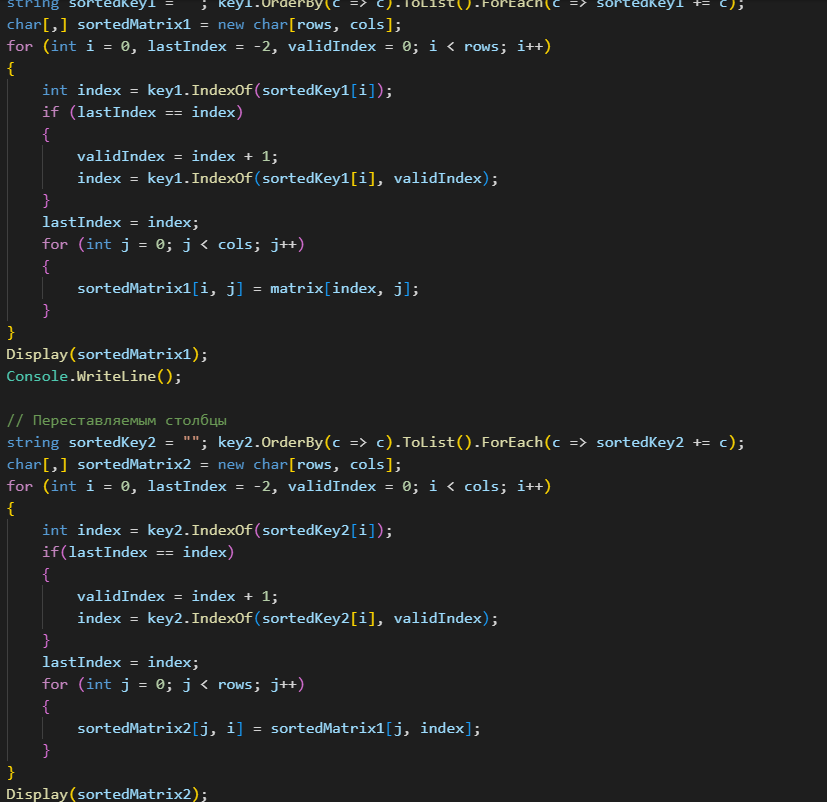


Рисунок 1.8 – Код программы для шифрования

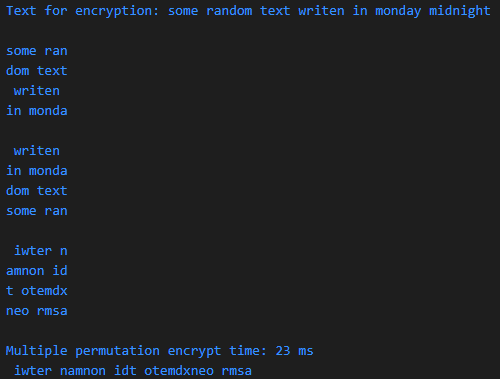


Рисунок 1.9 – Результат работы шифрования

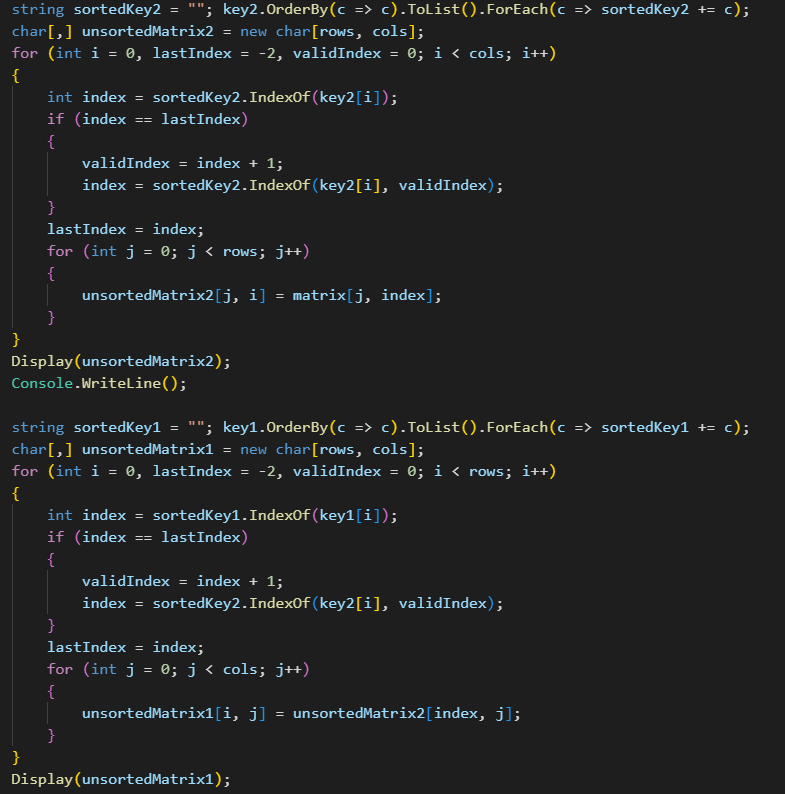


Рисунок 1.10 – Код программы для дешифрования

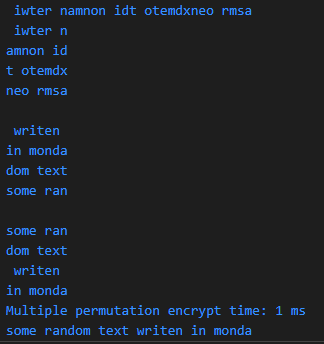


Рисунок 1.11 – Результат работы дешифрования

Гистограммы частот появления символов отображены на рисунках 1.12 и 1.13

Рисунок 1.12 – Частота появления символов исходного алфавита

Рисунок 1.13 – Частота появления символов зашифрованного алфавита

На основе гистограмм можем сделать вывод, что они идентичные, что с одной стороны хорошо, ведь данные не потерялись, а с другой стороны плохо, потому что становится проще подобрать нужные комбинации.

Скорость выполнения шифрования и дешифрования предоставления на рисунке 1.14

Рисунок 1.14 – Скорость выполнения шифрования и дешифрования

**Вывод**

В ходе выполнения лабораторной работы я приобрёл и закрепил навыки разработки приложения для реализации перестановочных шифров.