МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных Технологий

Кафедра Информационных систем и технологий

Специальность 1-40 01 01 Программное обеспечение информационных технологий

Направление специальности 1-40 01 01 10 Программирование интернет-приложений

**ОТЧЁТ К ЛАБОРАТОРНОЙ РАБОТЕ №5:**

по дисциплине «Криптографические методы защиты информации»

Исполнитель

студентка 3 курса группы 5 Шкода Кристина Михайловна

(Ф.И.О.)

Руководитель работы преподаватель Савельева М. Г.

(учен. степень, звание, должность, подпись, Ф.И.О.)

Минск 2023

**Исследование криптографических шифров на основе перестановки символов**

**Цель**: изучение и приобретение практических навыков разработки и использования приложений для реализации перестановочных шифров (работа рассчитана на 4 часа аудиторных занятий).

**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

**Ход работы**

Приложение разработано на NodeJS.

Задание №1

В первом задании надо было реализовать шифр маршрутной перестановки (маршрут – зигзагом). Код реализации данного шифра представлен на рисунке 1. При маршрутной перестановки записываем сообщение по строкам, считываем – зигзагом как представлено на рисунке 2.

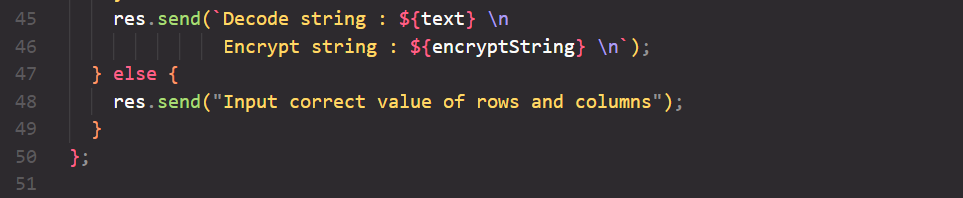


Рисунок 1 – Реализация шифр маршрутной перестановки

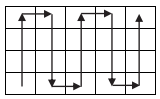


Рисунок 2 – Считывание зигзагом

Для выполнения шифрования необходимо ввести количество строк и столбцов и строку как показано на рисунке 3.

Рисунок 3 – Пример работы шифратора

Задание №2

В данном задании надо было реализовать дешифратор маршрутной перестановки (маршрут – зигзагом). Код реализации данного шифра представлен на рисунке 4.

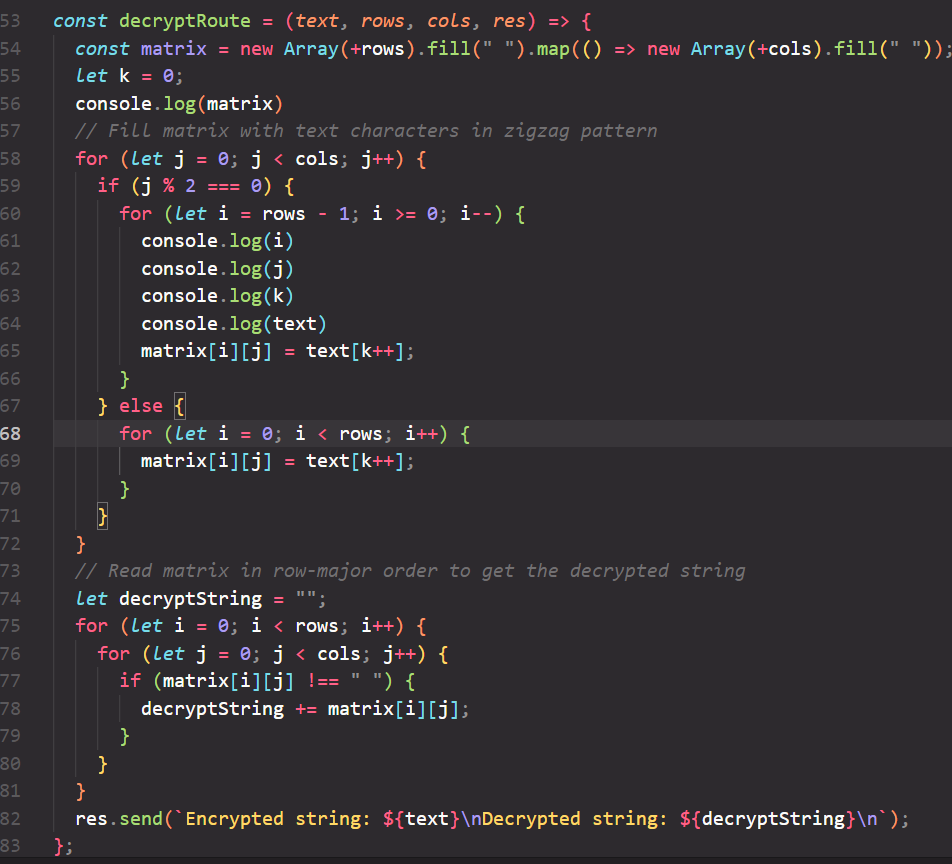


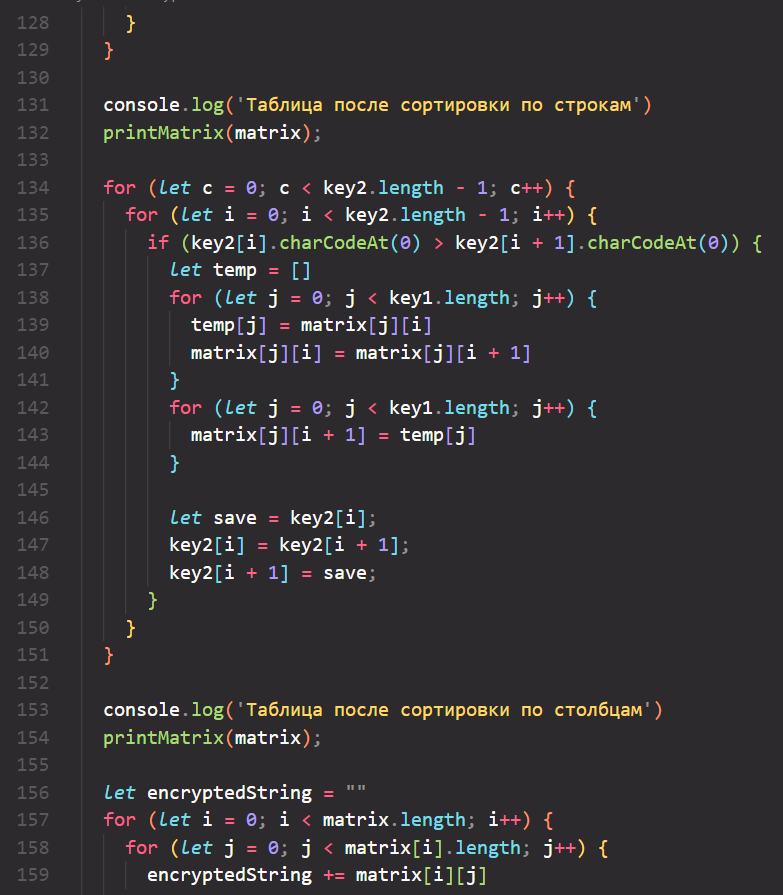
Рисунок 4 – Реализация дешифратора маршрутной перестановки

Рисунок 5 – Пример работы дешифратора

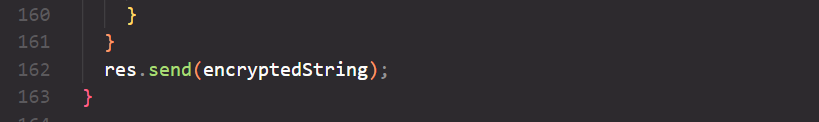
Задание №3

Далее необходимо было разработать функцию для шифра множественных перестановок, где ключевые слова имя и фамилия (Шкода Кристина). Сначала сортируются строки, после них столбцы. Функция представлена на рисунке 6 а, б, в.

б

а



в

Рисунок 6 – Реализация шифра множественных перестановок

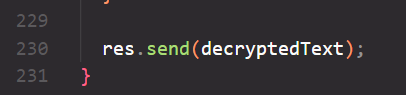
Так же надо было реализовать для данного шифра дешифратор. Код представлен на рисунке 7 а, б, в.

На рисунках 8, 9 показано, как данным шифратором и дешифратором можно воспользоваться, а так же его работа.

б

а



в

Рисунок 7 – Реализация дешифратора шифра множественных перестановок

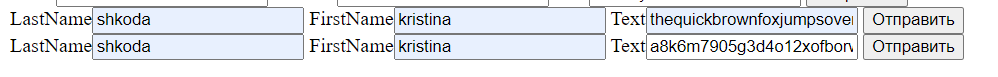
 Рисунок 8 – Способ заполнения полей

Рисунок 9 – Работа шифратора и дешифратора



Рисунок 10 – Частота появления символов



Рисунок 11 – Частота появления символов

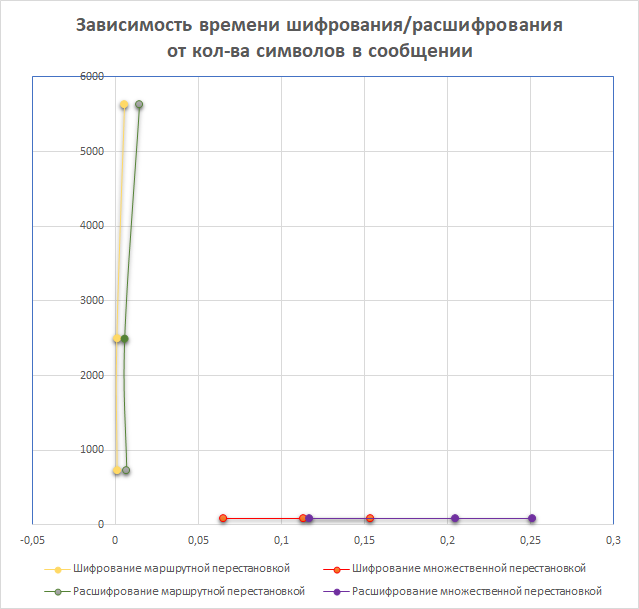


Рисунок 12 – Зависимость времени от количества символов