Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**Криптографические методы защиты информации**

**Лабораторная работа №5**

ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПЕРЕСТАНОВКИ СИМВОЛОВ

Вариант №6

Выполнил:

Студент 3 курса 4 группы ФИТ

Левша Марк Сергеевич

Минск 2023

**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.

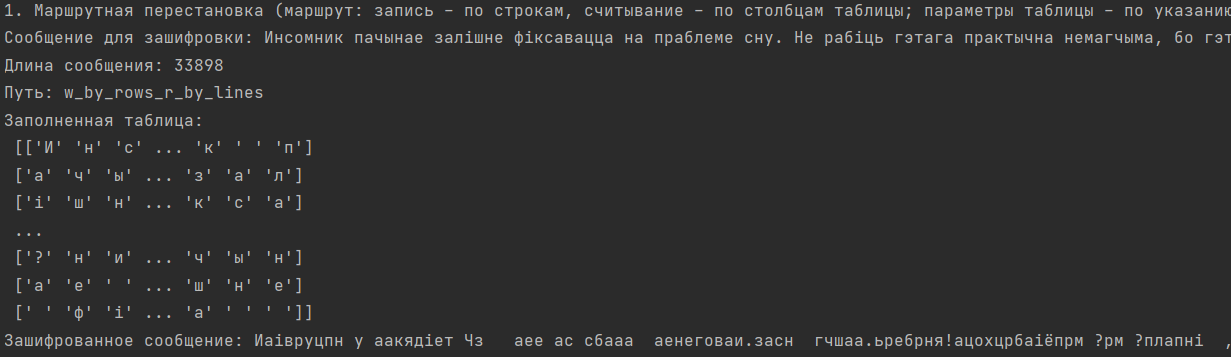
4. Выполнить исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях.

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

**Практическое задание**

Было разработано приложение для шифрования текстов на русском языке, выводящее входные данные, результат шифрования, сравнение данных и время выполнения заширования и расшифрования в консоль и гистограмму частот появления символов для исходного и зашифрованного сообщений в отдельное окно для маршрутной перестановки (маршрут –по спирали) и Множественной перестановки, где ключевые слова – собственные имя и фамилия.

На рисунках 1 и 2 представлен консольный вывод маршрутной перестановки.

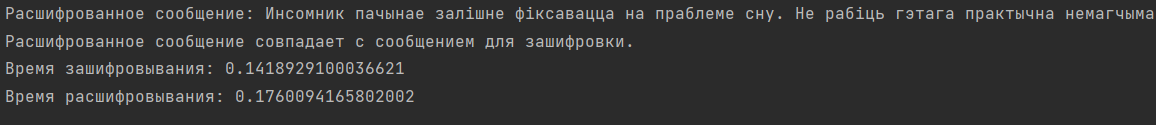
Рис. 1 – Консольный вывод подготовки к зашифрованию и шифрования методом маршрутной перестановки

Рис. 2 – Консольный вывод расшифрования маршрутной перестановки, проверки на соответствие исходного сообщения и расшифрованного сообщения и время шифрования и расшифрования

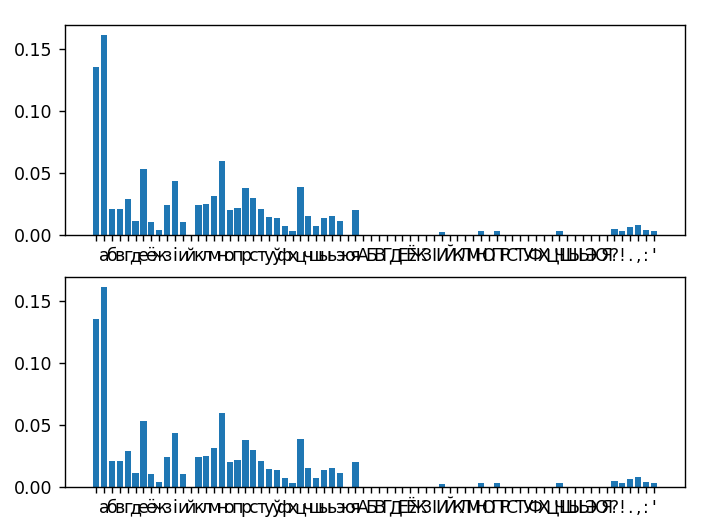
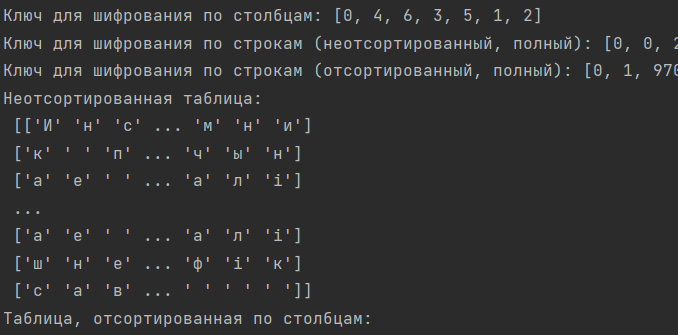
На рисунке 3 представлена гистограммы частот появления символов для исходного и зашифрованного сообщений методом маршрутной перестановки.

Рис. 3 – Гистограмма частот появления символов

Гистограммы частот появления символов в зашифрованном и исходном сообщении идентичны, так как методы перестановки не изменяют состав сообщения, только последовательность символов.

На рисунках 4 и 5 представлен консольный вывод множественной перестановки.

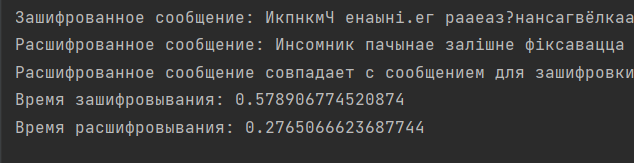
Рис. 4 – Консольный вывод подготовки матриц к зашифрованию множественной перестановки

Рис. 5 – Консольный вывод зашифрованного и зашифрованного сообщений, а также время выполнения зашифровки и расшифровки метода множественной перестановки

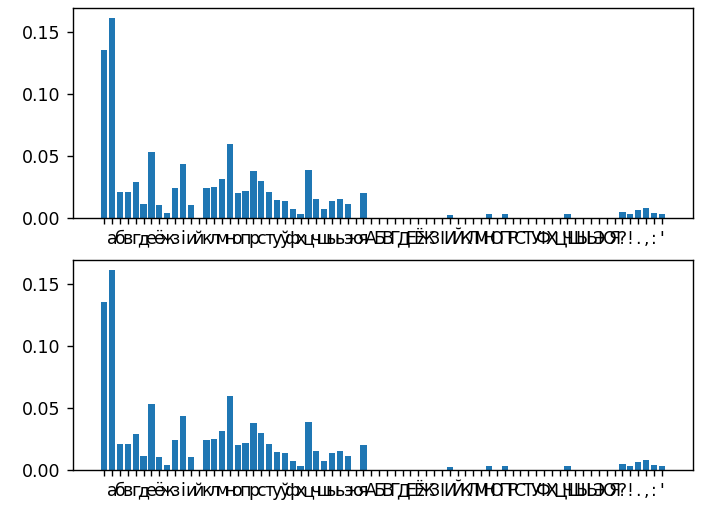
На рисунке 6 представлена гистограммы частот появления символов для исходного и зашифрованного сообщений методом множественной перестановки.

Рис. 6 – Гистограмма частот появления символов

Аналогично методу маршрутной перестановки, гистограммы частот появления символов в зашифрованном и исходном сообщении идентичны.

В программе были созданы несколько функций, такие как ***BuildHistogram*** и ***BuildHistogram2*** для построения гистограмм частот появления символов для исходного и зашифрованного сообщений, ***spiral\_Perestanovka*** и ***Multiple*** для реализации методов шифрования маршрутнойи и множественной перестановки.

Теперь исследуем время выполнения метода маршрутной перестановки при использовании разных размеров исходных сообщений, при увеличении размера исходного сообщения время шифрования и расшифрования увеличивается. Был построен график зависимости время шифрования и расшифрования от количества символов, который представлен на рисунке 7.

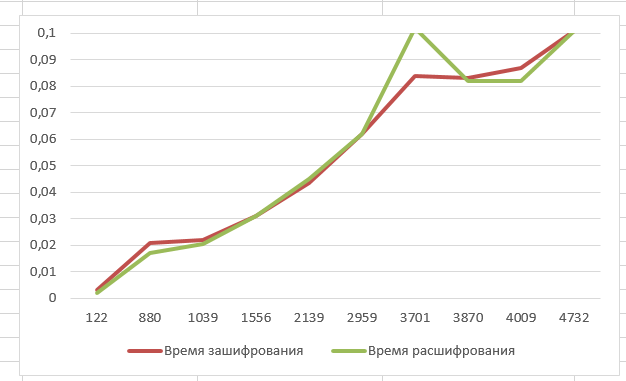


Рис. 6 – График зависимости времени зашифрования и расшифрования от количества символов в исходном сообщении

**Вывод**: в ходе лабораторной работы выли рассмотрены криптографические методы на основе перестановки символов такие, как шифры простой, блочной, маршрутной и множественной перестановки и реализованы методы маршрутной перестановки по спирали и множественной перестановки с ключевыми словами фамилией и именем.