Учреждение образования

«Белорусский государственный технологический университет»

**Лабораторная работа №5**

Исследование криптографических шифров на основе перестановки символов

Выполнил:

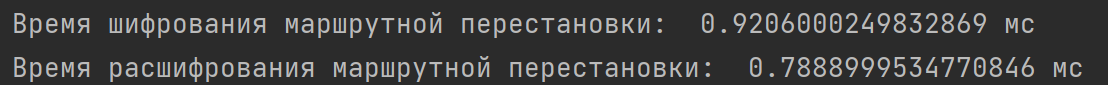
Студент 3 курса 5 группы ФИТ

Коршун Никита Игоревич

2024

Для выполнения данной лабораторной работы была разработана программа на языке Python. Язык исходного текста был выбран русский.

Для сравнения времени выполнения алгоритмов было замерено время выполнения зашифрования и расшифрования.



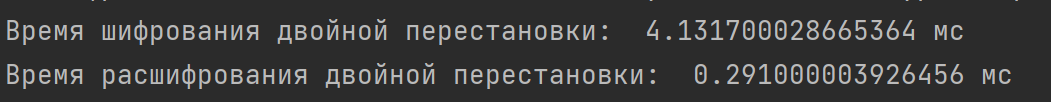


Рисунок 1 – Время выполнения алгоритмов зашифрования и расшифрования

Также были замерены частоты появления символов для исходного и зашифрованного сообщения.



Рисунок 2 – Частоты появления символов исходного сообщения

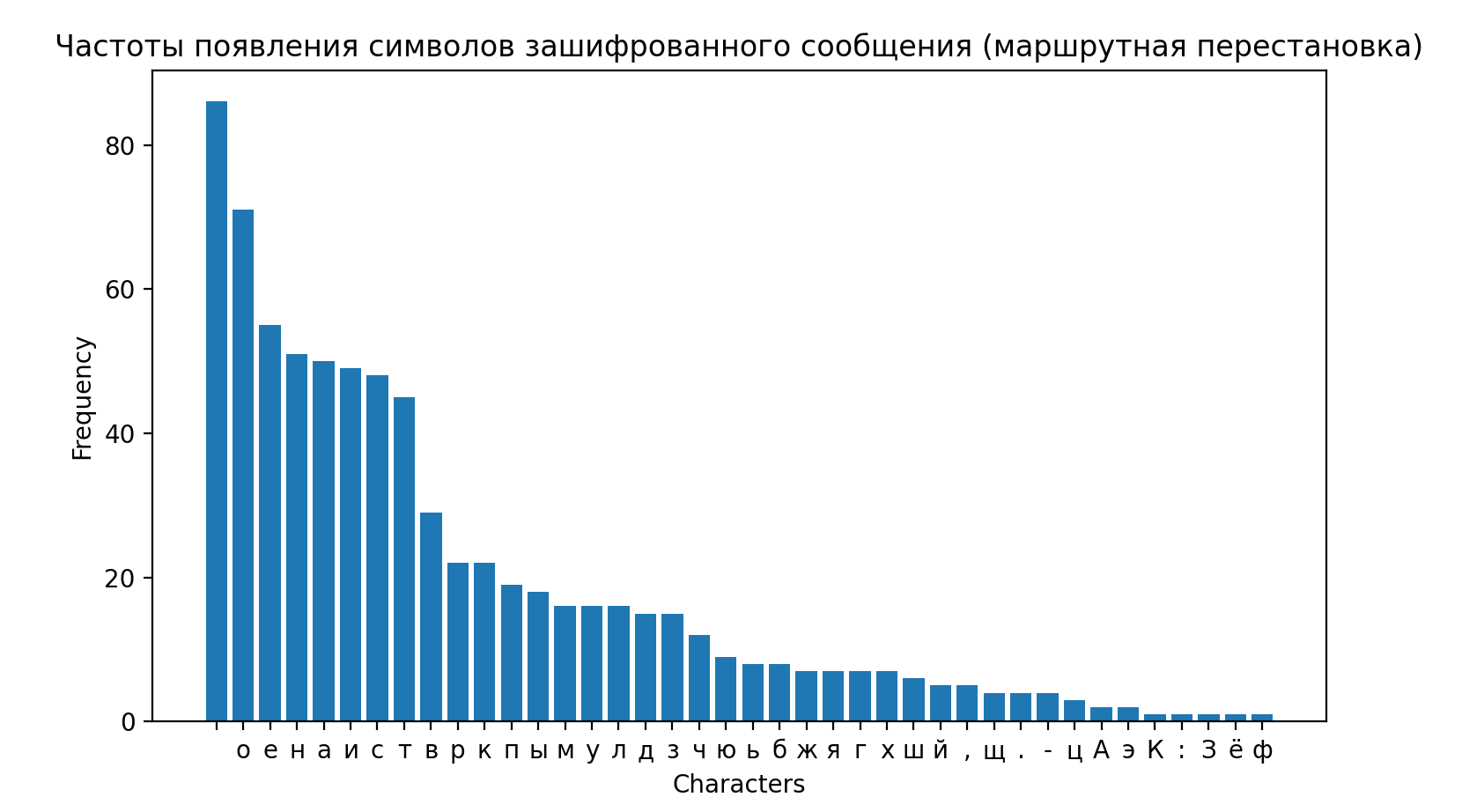


Рисунок 3 – Частоты появления символов зашифрованного сообщения с помощью маршрутной перестановки

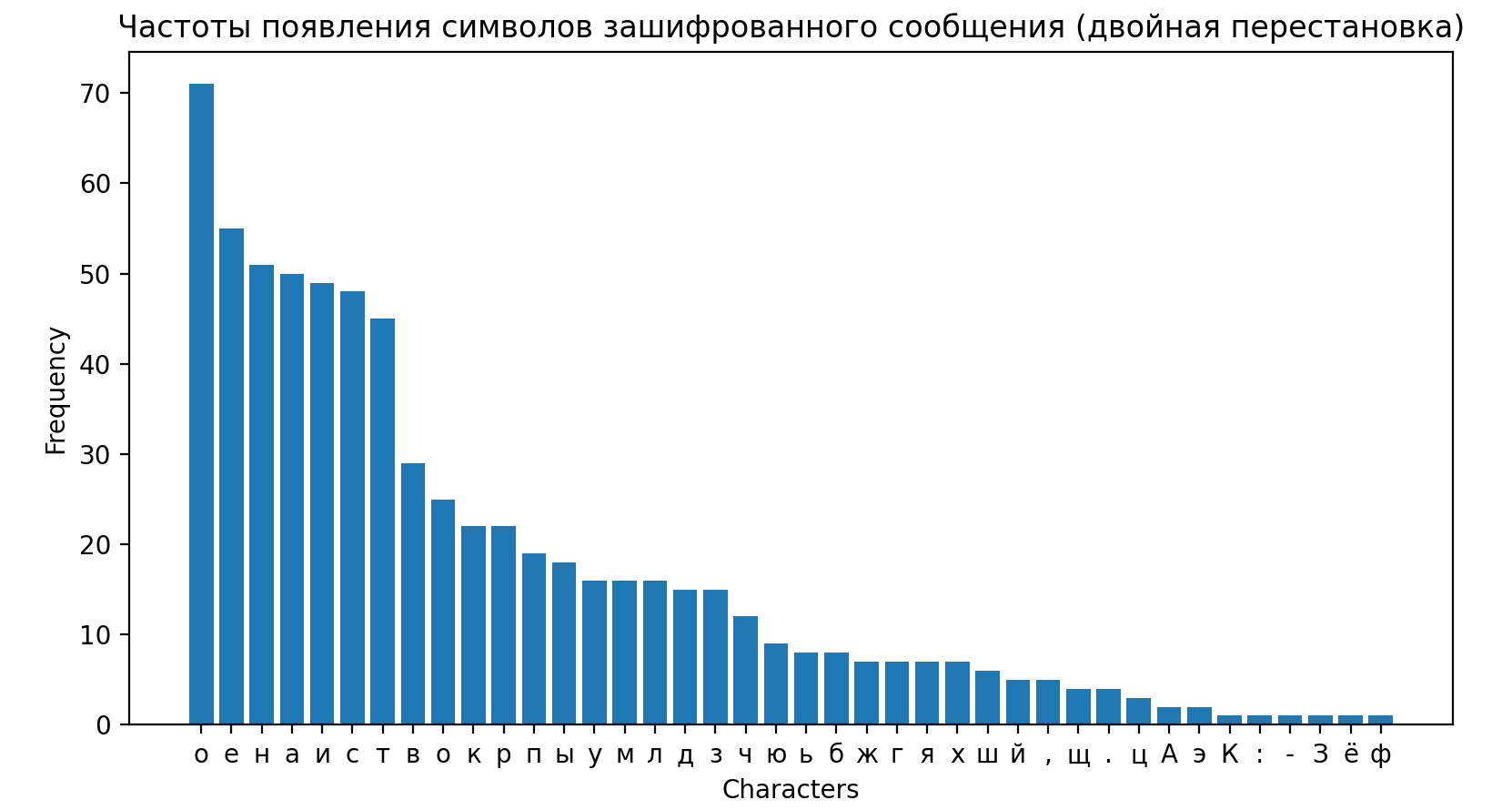


Рисунок 4 – Частоты появления символов зашифрованного сообщения с помощью множественной перестановки



Рисунок 5 – Время выполнения зашифрования с помощью маршрутной перестановки

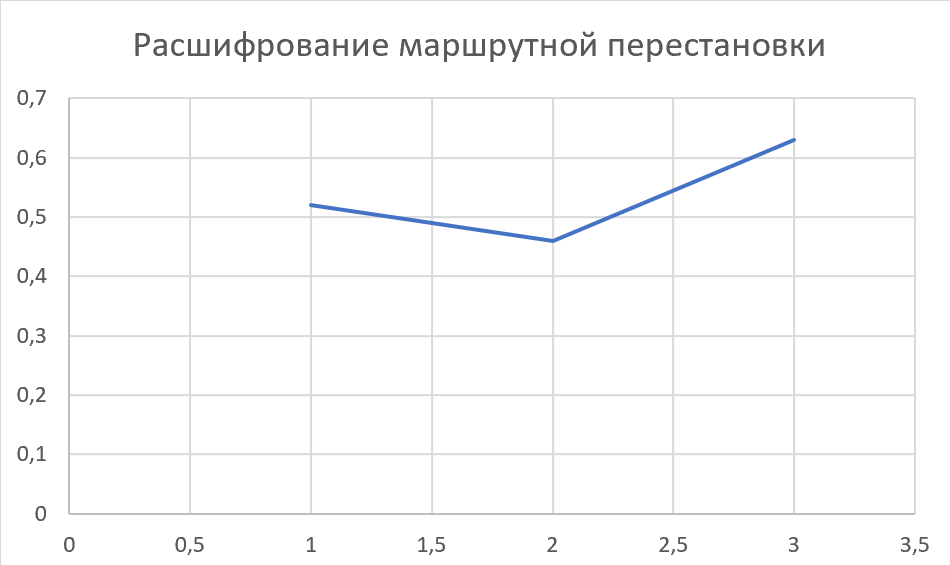


Рисунок 6 – Время выполнения расшифрования с помощью маршрутной перестановки



Рисунок 7 – Время выполнения зашифрования с помощью множественной перестановки

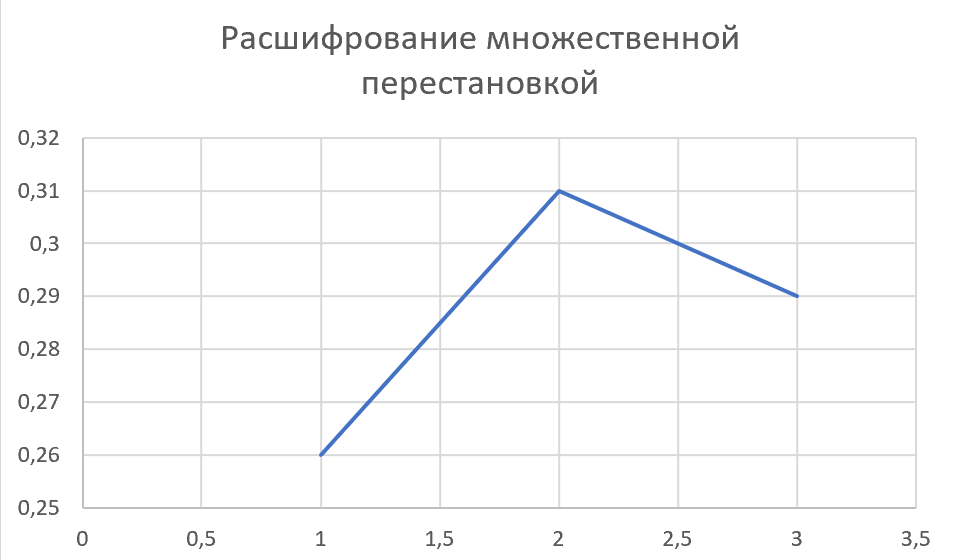


Рисунок 8 – Время выполнения расшифрования с помощью множественной перестановки

**Вывод:** В результате сравнения маршрутной перестановки и множественной перестановки, были выявлены следующие преимущества каждого метода:

Маршрутная перестановка:

Более быстрая скорость шифрования и расшифрования. В случае маршрутной перестановки время выполнения этих операций было значительно меньше, чем для множественной перестановки.

Простота реализации. Маршрутная перестановка требует меньше шагов и действий для шифрования и расшифрования, что делает ее более простой в реализации и понимании.

Множественная перестановка:

Более высокий уровень стойкости. Множественная перестановка использует несколько ключей и более сложные алгоритмы перестановки, что делает ее более устойчивой к взлому и криптоанализу.

Большая гибкость и возможность для вариации. В множественной перестановке можно использовать различные ключи и алгоритмы перестановки, что позволяет достичь различных уровней защиты и адаптировать метод под конкретные требования и ситуации.

В итоге, выбор между маршрутной перестановкой и множественной перестановкой зависит от конкретных требований и целей. Если важна скорость выполнения операций и простота реализации, то маршрутная перестановка может быть предпочтительнее. Если же требуется более высокий уровень стойкости и гибкость в настройке алгоритма, то множественная перестановка может быть более подходящим выбором.