БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

**Лабораторная работа №3**

**«Исследование криптографических шифров**

**на основе перестановки символов**»

**Выполнила:**

студентка 3 курса 1 группы

Потапейко Полина Павловна

**Проверил:**

Берников Владислав Олегович

Минск 2022

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

**Ход работы**

**Задание 1.** Разработать приложение, которое реализует операции зашифрования/расшифрования текстового документа, созданного на основе английского алфавита, методом маршрутной перестановки зигзагом и методом множественной перестановки.

Часть исходного текста (рисунок 1).

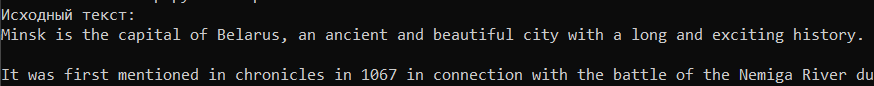


Рисунок 1 – Часть исходного текста

Часть документа, зашифрованного с помощью закодированного алфавита представлена на рисунке 2.

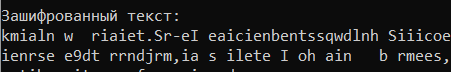


Рисунок 2 – Зашифрованный документ

Время, за которое пройден процесс зашифрования, представлено на рисунке 3.



Рисунок 3 – Время зашифрования методом маршрутной перестановки

Часть расшифрованного документа представлена на рисунке 4.

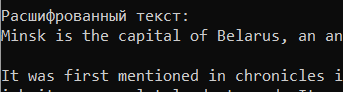


Рисунок 4 – Расшифрованный документ

Начальное состояние таблицы множественной перестановки представлено на рисунке 5 (1-й ключ – polina, 2-й ключ - potapeyko).

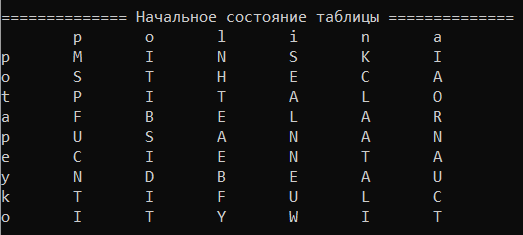


Рисунок 5 – Начальное состояние таблицы

Таблица после сортировки по строкам (рисунок 6).

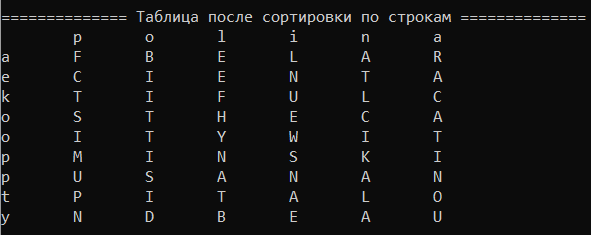


Рисунок 6 – Сортировка по строкам

Полностью отсортированная таблица представлена на рисунке 7.

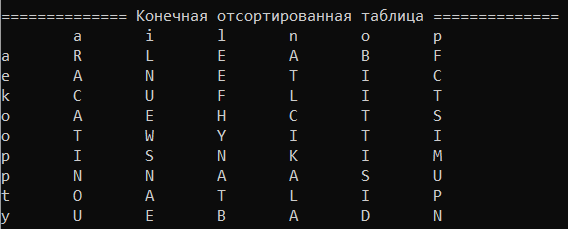


Рисунок 7 – Зашифрованный документ с помощью таблицы Трисемуса

Зашифрованное сообщение представлено на рисунке 8.



Рисунок 8 – Зашифрованное сообщение

**Вывод:** в ходе лабораторной работы были закреплены теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости перестановочных шифров, было также разработано приложение для реализации указанных методов перестановочного зашифрования/расшифрования, исследована криптостойкость шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях.