БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

**Лабораторная работа №2**

**«Исследование криптографических шифров**

**на основе подстановки (замены) 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 подстановочных шифров.

**Ход работы**

**Задание 1.** Разработать приложение, которое реализует операции зашифрования/расшифрования текстового документа, созданного на основе английского алфавита шифром Цезаря с ключевым словом и с помощью таблиц Трисемуса. Оценить время выполнения операций зашифрования/расшифрования

Создание зашифрованного алфавита для шифра Цезаря с ключевым словом (рисунок 1).

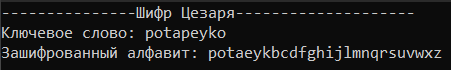


Рисунок 1 – Зашифрованный алфавит

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

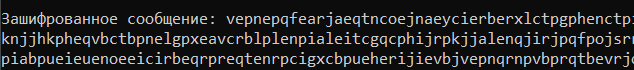


Рисунок 2 – Зашифрованный документ с помощью шифра Цезаря

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



Рисунок 3 – Время зашифрования шифром Цезаря

Часть расшифрованного документа представлена на рисунке 4.

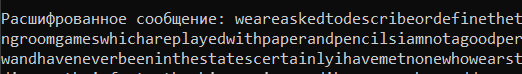


Рисунок 4 – Расшифрованный документ

Время, за которое пройден процесс расшифрования, представлено на рисунке 5.

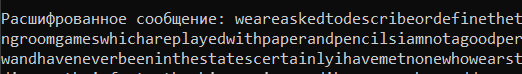


Рисунок 5 – Время расшифрования документа

Составление таблицы Трисемуса с ключом polina (рисунок 6).

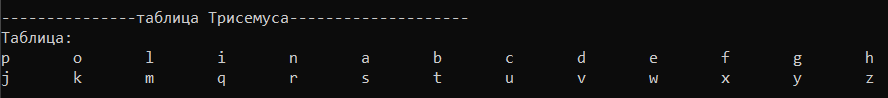


Рисунок 6 – Таблица Трисемуса

Часть документа, зашифрованного с помощью таблицы Трисемуса, представлена на рисунке 7.

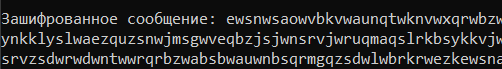


Рисунок 7 – Зашифрованный документ с помощью таблицы Трисемуса

Время, за которое пройден процесс зашифрования, представлено на рисунке 8.



Рисунок 8 – Время зашифрования с помощью таблицы Трисемуса

Часть расшифрованного документа представлена на рисунке 9.

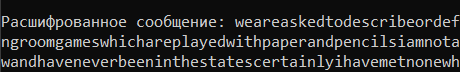


Рисунок 9 – Расшифрованный документ

Время, за которое пройден процесс расшифрования, представлено на рисунке 10.



Рисунок 10 – Время расшифрования документа

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