Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование криптографических шифров на основе подстановки (замены) символов**

**Выполнил:** студент 3 курса

4 группы специальности ПОИТ

Зворыкин Дмитрий Александрович

Минск 2023

1. **Описание приложения**

Приложение написано на языке программирования TS и позволяет зашифровать и расшифровать текстовый документ на основе английского языка, используя:

* Шифр Цезаря с ключевым словом zvarykin;
* Таблица Трисемуса c ключевым словом dima;

Также приложение генерирует гистограммы частот появления символов для исходного и зашифрованного сообщений и оценивает время выполнения операций зашифрования и расшифрования.

1. **Методика выполнения поставленных задач**



Рис. 2.1 – Реализация Шифра Цезаря



Рисунок 2.2 – Результат Шифра Цезаря

Для Таблицы Трисемуса



Рис. 2.3 – Реализация Таблицы Трисемуса

Также приложение генерирует гистограммы частот появления символов в исходном и зашифрованном текстах, которые представлены на рисунках 2.5, 2.6 соответсвенно.

Рис. 2.5 – Гистограмма частот исходных символов

Рис. 2.6 – Гистограмма частота шифросимволов

**Вывод**

В ходе лабораторной работы были приобретены навыки разработки и использования приложений для реализации подстановочных шифров, а также оценены скорость зашифрования/расшифрования реализованных способов шифров.