Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Изучение устройства и функциональных особенностей шифровальной машины «Энигма»**

Студент: Сергеев С.А.

ФИТ 3 курс 5 группа

Преподаватель: Берников В.О.

Минск 2022

1. **Описание приложения**

Приложение написано на языке программирования python и позволяет:

* зашифровать текст с помощью шифровальной машины «Энигма», вводя порядок следования роторов, значение рефлектора, стартовые позиции, кольцо и параметры коммутационной панели;
* расшифровать текст с помощью шифровальной машины «Энигма».

1. **Методика выполнения поставленных задач**

Для выполнения зашифрования сообщения с помощью шифровальной машины «Энигма» необходимо указать исходный текст для зашифровки, стартовые позиции роторов, последовательность роторов, пары символов коммутационной панели, позиции кольца, тип рефлектора.

В примере, представленном на рисунке 2.1, используется исходное сообщение «SIARHEIXSIARHEYEU», положение роторов «II-III-V», рефлектор C, стартовые позиции роторов и настройки коммутационной модели «AV BS CG DL FU HZ IN KM OW RX».

Аналогичным способом выполняется шифрование с другими параметрами роторов, рефлекторов, стартовых позиций и кольца. Также важную роль играют позиции коммутационной панели.

Результат зашифрования сообщения представлен на рисунке 2.2.

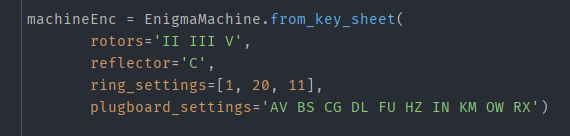


Рисунок 2.1 – Настройки машины

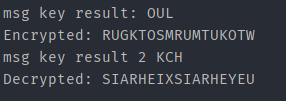


Рисунок 2.2 – Результат работы программы

Таким образом, были реализованы все поставленные задачи. Шифровальная машина «Энигма» обладает достаточной криптостойкостью за счет большого числа стартовых позиций, позиций кольца и пар на коммутационной панели.

Также, стоит отметить, что шифровальная машина «Энигма» является разновидностью динамического шифра Цезаря.

**Вывод**

В ходе лабораторной работы были приобретены навыки разработки и использования шифровальной машины «Энигма». Были изучены основные принципы работы «Энигмы».

Также было разработано приложение, на языке программирования Python, для реализации задач, связанных с шифрованием данных.