Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

Изучение устройства и функциональных особенностей шифровальной машины «Энигма»

Выполнил:

студент 3 курса 4 группы

специальности ПОИТ

Матюх А.А.

Минск 2020

1. **Теоретические сведения**

Машина Энигма – это электромеханическое устройство. Как и другие роторные машины, Энигма состоит из комбинации механических и электрических подсистем.

Механическая часть включает в себя клавиатуру, набор вращающихся дисков – роторов, – которые расположены вдоль вала и прилегают к нему, и ступенчатого механизма, двигающего один или несколько роторов при каждом нажатии на клавишу. Электрическая часть, в свою очередь, состояла из электрической схемы, соединяющей между собой клавиатуру, коммутационную панель, лампочки и роторы (для соединения роторов использовались скользящие контакты). На

Конкретный механизм мог быть разным, но общий принцип был таков: при каждом нажатии на клавишу самый правый ротор сдвигается на одну позицию, а при определённых условиях сдвигаются и другие роторы. Движение роторов приводит к различным криптографическим преобразованиям при каждом следующем нажатии на клавишу на клавиатуре, т.е. зашифрование/расшифрование сообщений основано на выполнении ряда замен (подстановок) одного символа другим.

Зашифрование сообщения.

1. Установить начальную стартовую позицию роторов (предположим, их 3), согласно текущей кодовой таблице (коду дня). Например, WZA.

2. Выбрать случайный ключ сообщения, например, SXT. Затем оператор устанавливал роторы в стартовую позицию WZA.

3. Зашифровывать ключ сообщения SXT. Предположим, что в результате зашифрования ключа получится UHL.

4. Далее оператор ставил ключ сообщения (SXT) как начальную позицию роторов и зашифровывал собственно сообщение. После этого он отправлял стартовую позицию (WZA) и зашифрованный ключ (UHL) вместе с сообщением.

Расшифрование сообщения.

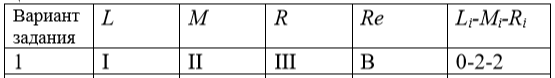
1. Установить стартовые позиции роторов в соответствии с первой трехграммой (WZA).

2. Расшифровывая вторую треграмму (UHL) и извлечь исходный ключ (SXT).

3. Далее получатель использовал этот ключ как стартовую позицию для расшифрования шифртекста. Обычно срок действия ключей составлял одни сутки.

1. **Практическая часть**

В данной лабораторной работе необходимо разработать приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя:

 Пример реализации ротора:

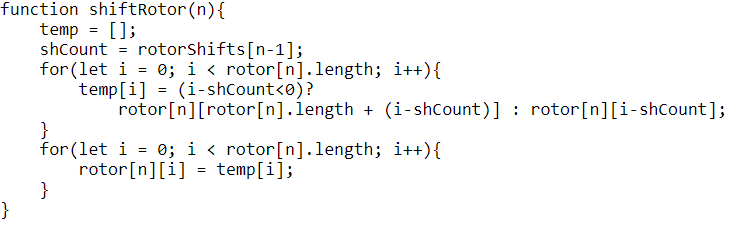


Рисунок 2.1 – Пример ротора

Пример реализации рефлектора:

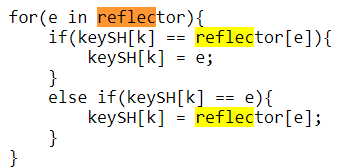


Рисунок 2.2 – Пример рефлектора

**Вывод**

В данной лабораторной работе я закрепил теоретические знания по работе с машиной Энигмы. А также, разработал приложение-симулятор шифровальной машины.