Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

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

Студент: Плотников Д.А.

ФИТ 3 курс 5 группа

Преподаватель: Берников В.О.

Минск 2020

1. **Постановка задачи**

В соответствии с целями лабораторной работы было создано приложение, обладающее следующим функционалом: шифрование и дешифрование текста так, как это делает машина «Енигма» с заданными начальными положениями роторов, их последовательностью а так же рефлектором в соответствии со своим вариантом (в данном случае 9).

В соответствии с требованиями по варианту требовалось взять исходные параметры для машины из таблицы, часть снимка которой приведено на рисунке 1.



Рисунок 1 – Условия задания по варианту.

Здесь видно, что будут использоваться три ротора (VIII, II, IV) и один рефлектор (B), положение роторов будет 1-0-1. Последовательности берутся из таблицы, показанной на рисунке 2 и рисунке 3.



Рисунок 2 – Таблица типов роторов с именами.

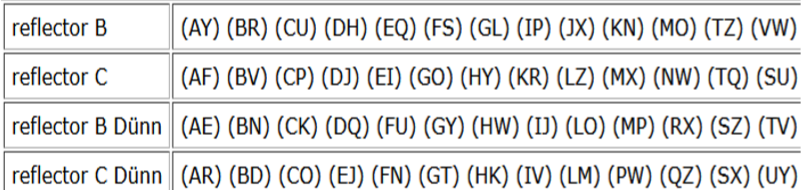


Рисунок 3 – Таблица типа рефлекторов с названиями.

Выбранный вариант выглядит в коде как на рисунке 4.

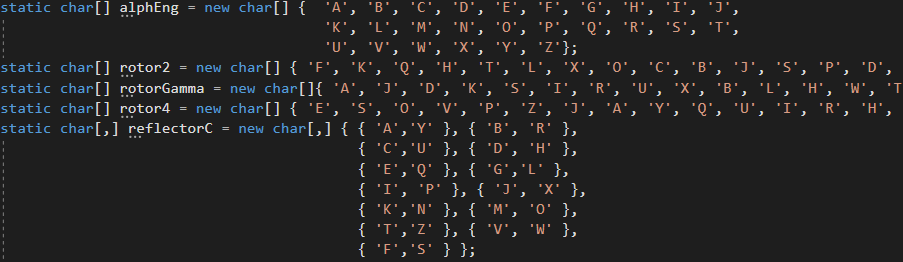


Рисунок 4 – Часть программы, демонстрирующая настройку енигмы.

Таким образом нужно разработать приложение, позволяющее шифровать и дешифровать текст шифром енигмы.

# 2. Описание приложения

Приложение представляет собой windows-приложение, написанное на языке программирования С# с использованием WPF. Главное окно приложения приведено на рисунке 5.

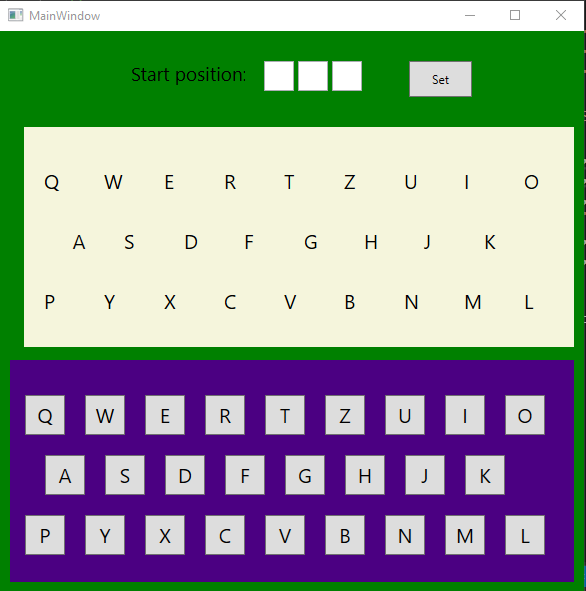


Рисунок 5 – Главное окно разработанного приложения.

Три текстовых поля посредине верхней части окна позволяют задать положение роторов енигмы. Применяются значения нажатием кнопки set. Сами роторы, а так же рефлектор строго заданы вариантом и поэтому не имеют возможности конфигурирования.

После установки начального положения роторов можно нажимать на кнопки, расположенные на окне. По нажатию кнопки, соответствующая ей буква подсвечивается на клавиатуре выше, как показано на рисунке 6.

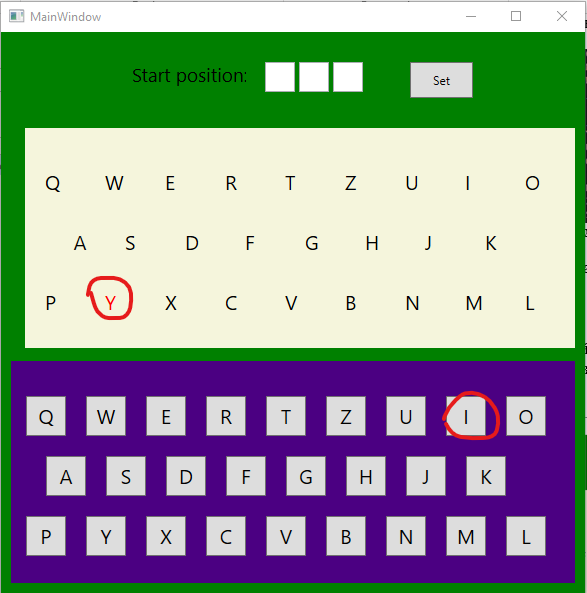


Рисунок 6 – Подсветка соответствующих символов енигмы.

Так как каждая буква соответствует каждой какой-либо другой, то процесс шифрования и расшифрования идентичен. Одной из главных особенностей енигмы, что одновременно и является ее слабостью является то, что исходный символ не может быть зашифрован сам в себя, это снижает криптостойкость системы.

**Вывод**

В ходе этой работы были изучены и приобретены практические навыки разработки и использования функциональных возможностей и особенностей машины «Енигма». Разработано приложения на языке программирования С#, позволяющее выполнять шифрование и дешифрование текста с помощью программно созданной машины «Енигма» в соответствии со своим вариантом.