МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

**«Отчет к лабораторной работе №6 Изучение устройства и функциональных особенностей шифровальной машины «Энигма»»**

Студент:

Септилко Анастасия Антоновна

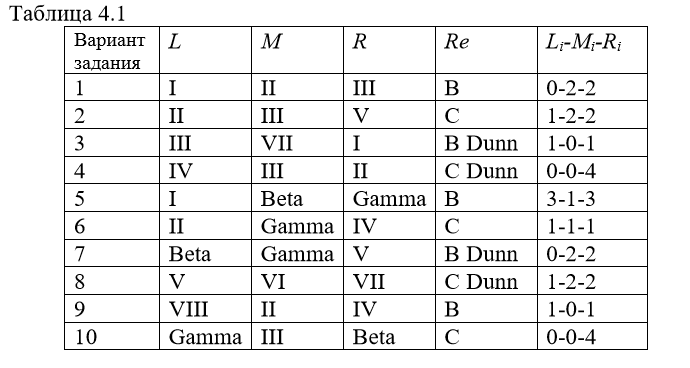
Преподаватель:

Блинова Евгения Александровна

Минск 2020

**ЗАДАНИЯ:**

1. Разработать приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя. Типы роторов (L-M-R) и отражателя Re следует выбрать из таблиц на рис. 4.5 и 4.6 в соответствии со своим вариантом, представленным в таблице 4.1. Крайний правый столбец этой таблицы показывает, на какое число шагов (букв, i) перемещается соответствующий ротор при зашифровании одного (текущего) символа; число 0 означает перемещение соответствующего ротора на один шаг при условии, что расположенный правее ротор совершит один оборот.



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).

Для начала выполнения лабораторной нужно было прописать в массивы значение дисков 5,6,7 и рефлектор C Dunn. Продемонстрировано на рисунке 1.1.

. 

Рисунок 1.1 – Создание роторов и рефлектора

Далее задаем L, M и R – обозначают действия левых, средних и правых роторов соответственно (рисунок 1.2).



Рисунок 1.2 – Сдвиг роторов

Функция реализующая данный метод шифра продемонстрирована на рисунке 1.3

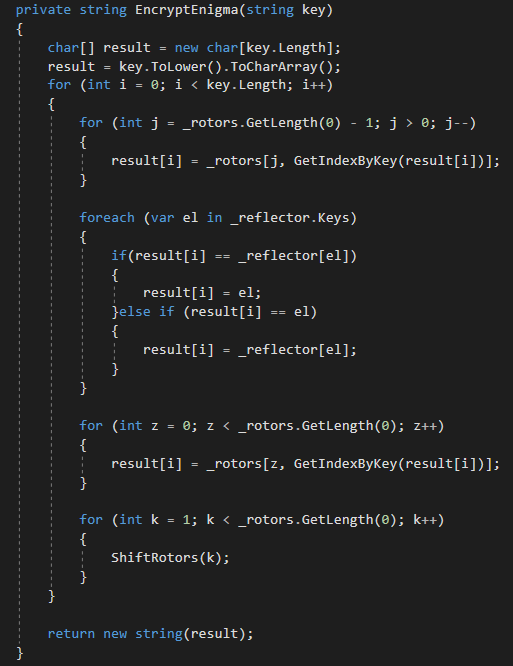


Рисунок 1.3 – Функция EncryptEnigma()

Здесь мы с помощью циклов производим все порядки действий данного шифра Энигма.

Данная функция получает индекс символа в диске (рисунок 1.4).

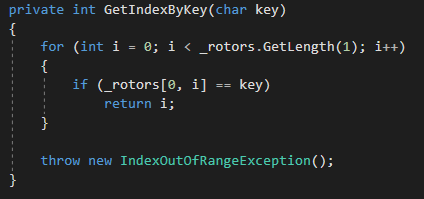


Рисунок 1.4 – Функция GetIndexByKey()

Еще есть функция, которая берет первый элемент массива из начального массива и его удаляет. Эта функция называется ShiftRotors и она показана на рисунке 1.5.

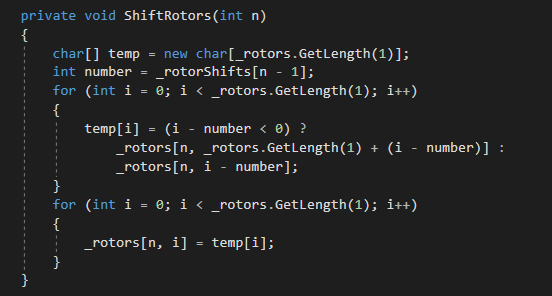


Рисунок 1.5 – Функция ShiftRotors()

Итог выполнения программы показан на рисунке 1.6:

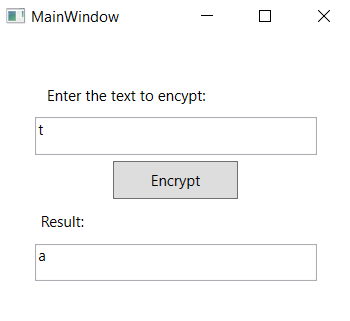


Рисунок 1.6 – Итог программы