Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Лабораторная работа № 6**

«Изучение устройства и функциональных особенностей шифровальной машины Энигма»

Студент: Шулаков А.А.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М.Г.

Минск 2023

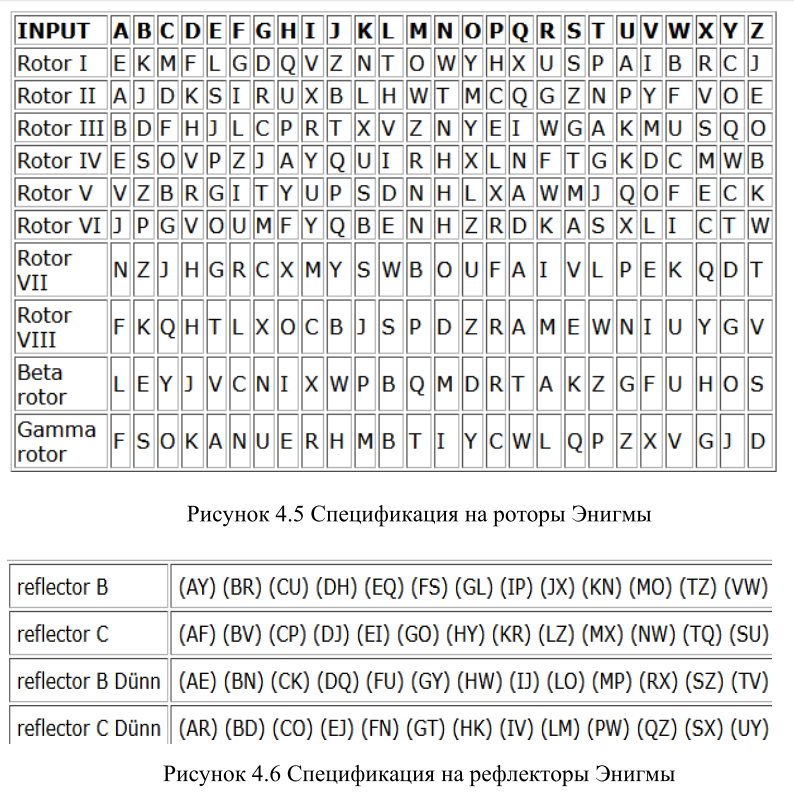
**Цель**: изучение и приобретение практических навыков разработки и использования приложений для реализации перестановочных шифров.

**Ход работы:**

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. 1 в соответствии со своим вариантом, представленным в таблице 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.

Таблица 1.1 – Данные варианта

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Вариант задания | L | M | R | Re | Li-Mi-Ri |
| 14 | II | Beta | VIII | C | 0-2-2 |



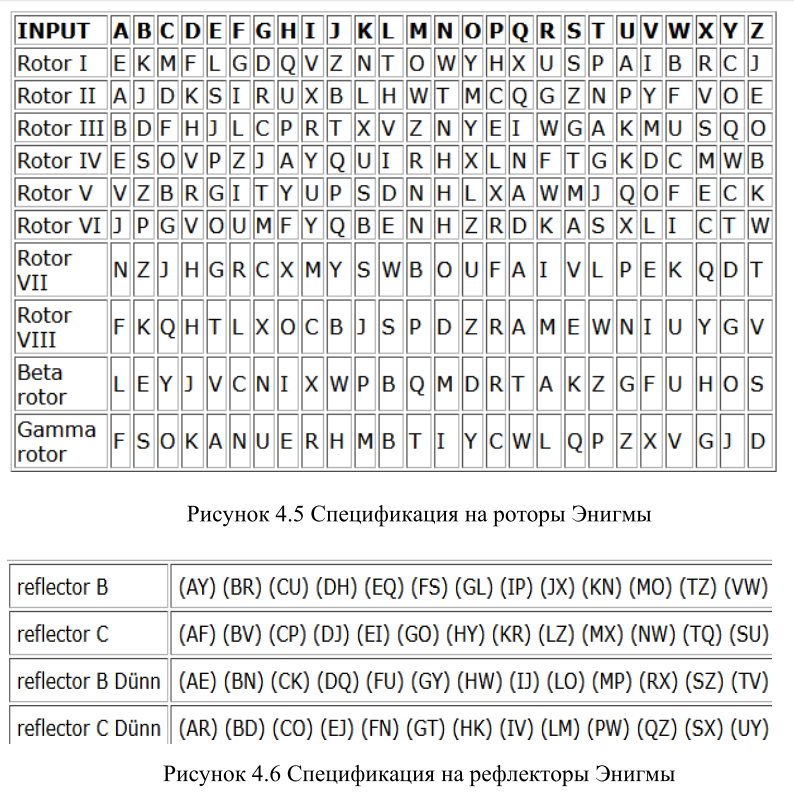


Рисунок 1.1 – спецификация для выполнения задания

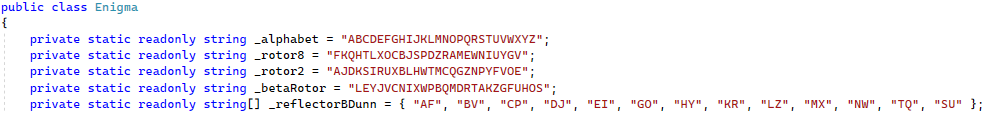


Рисунок 1.2 – настройка Энигмы в коде

1. С помощью разработанного приложения зашифровать сообщение (собственные имя, фамилия), применив не менее 5 вариантов начальных установок роторов.

Результат представлен на рисунке 1.3.

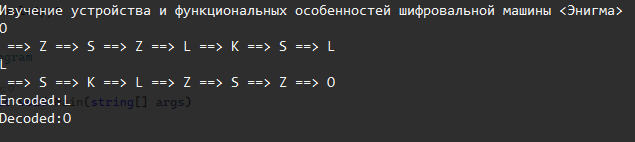


Рисунок 1.3 – результат работы приложения

5×4×3=60 (количество возможных комбинаций роторов)

26×26×26=17576 (возможные положения роторов)

26×26=676 (начальные положения роторов)

26! / (26-2×10) ×10! × 210=1,5 ×1014 (коммутация панели)

60×17576×676×1,5×1014 =1,07×1023

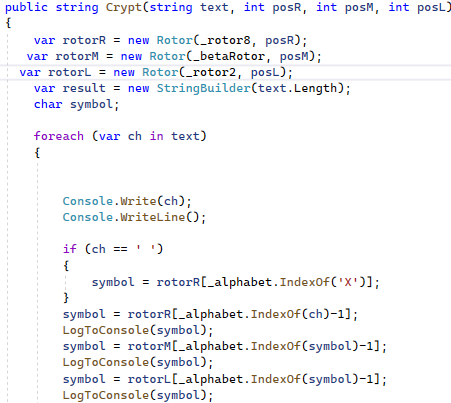


Рисунок 1.4 – Реализация

**Вывод**: в ходе лабораторной работы была разработана реализация шифровальной машины Энигма. Также установлено, что криптостойкость машины составляет 1,07×1023 комбинаций.