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»»

Выполнил:

Студент: Белицкий В.Д.

ФИТ 2 курс 5 группа

Преподаватель: Савельева М.Г.

Минск 2023

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

1. **Описание приложения**

Приложение написано на языке программирования *C#* и позволяет:

* Зашифровать и расшифровать сообщение приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя
* Согласно первому варианту использованы первые три ротара.
* Выбирать исходную позицию для каждого ротара.

1. **Методика выполнения расчетов**

public EnigmaMachine()

{

// Инициализация алфавита

alphabet = "ABCDEFGHIJKLMNOPQRSTUVWXYZ".ToCharArray();

// Инициализация роторов

rotorL = "EKMFLGDQVZNTOWYHXUSPAIBRCJ".ToCharArray();

rotorM = "AJDKSIRUXBLHWTMCQGZNPYFVOE".ToCharArray();

rotorR = "BDFHJLCPRTXVZNYEIWGAKMUSQO".ToCharArray();

// Инициализация рефлектора

reflector = "YRUHQSLDPXNGOKMIEBFZCWVJAT".ToCharArray();

}

Рисунок 2.1 – настройка Энигмы в коде

1. **Оценка криптостойкость машины**

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)

1. **Результаты работы приложения**

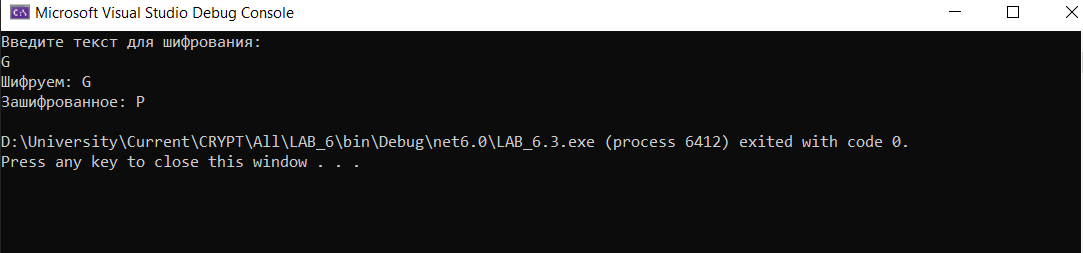


Рисунок 4.1 – результат работы приложения

**Вывод**: в ходе лабораторной работы разработано приложение для реализации перестановочных шифров на базе «Энигма».