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#* с использование технологии *WPF* 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 MainWindow()

{

original\_alphabet.ToCharArray();

InitializeComponent();

L = new Runner

{

Alphabet = new Char[] {'e', 'k', 'm', 'f', 'l', 'g', 'd', 'q', 'v',

'z', 'n', 't', 'o', 'w', 'y', 'h', 'x', 'u', 's', 'p', 'a', 'i', 'b', 'r', 'c', 'j',

},

Shift = 1

};

M = new Runner

{

Alphabet = new Char[] { 'a', 'j', 'd', 'k', 's', 'i', 'r', 'u','x',

'b', 'l', 'h', 'w', 't', 'm', 'c', 'q','g',

'z', 'n', 'p', 'y', 'f', 'v','o','e'},

Shift = 0,

};

R = new Runner

{

Alphabet = new Char[] {'b', 'd', 'f', 'h', 'j', 'l', 'c', 'r',

't', 'x', 'v', 'z', 'n', 'y', 'e', 'i', 'w', 'g', 'a', 'k', 'm', 'u', 's', 'q', 'o'},

Shift = 1,

};

reflector = new Deflector();

reflector.Alphabet = new Dictionary<char, char> { { 'a', 'y' }, { 'b', 'r' }, { 'c', 'u' }, { 'd', 'h' }, { 'e', 'q' }, { 'f', 's' }, { 'g', 'l' },

{ 'i', 'p' }, { 'j', 'x' }, { 'k', 'n' }, { 'm', 'o' }, { 't', 'z' }, { 'v', 'w' }};

}

Рисунок 1.1 – 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**

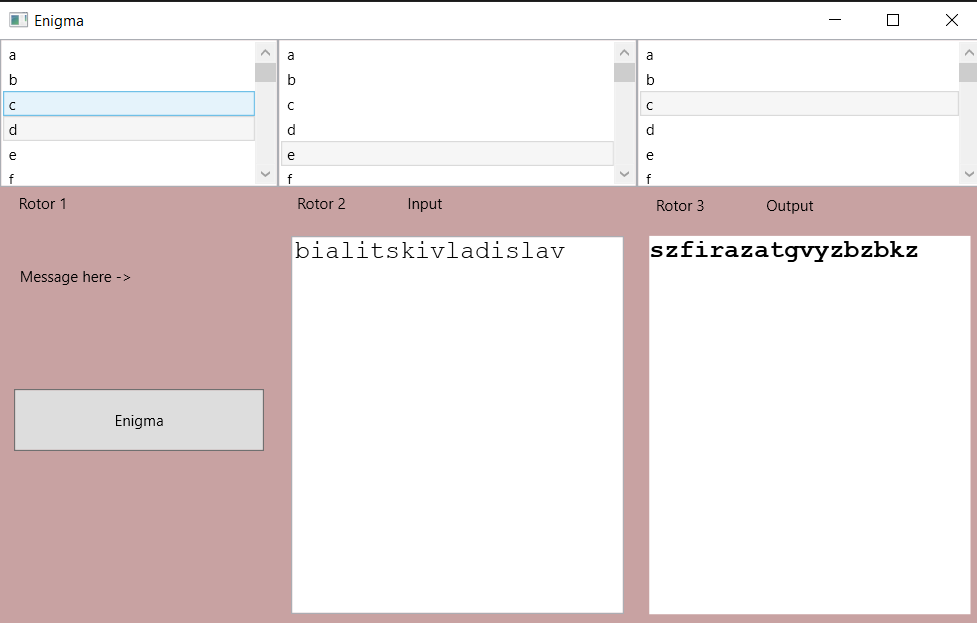


Рисунок 4.1 – результат работы приложения

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