Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа №6**

Студент: Бобрович Г.С.

ФИТ 3 курс 7 группа

Преподаватель: Савельева М.Г.

Минск 2023

**Разработать приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя.**

****

Рисунок 1.1 — Условие

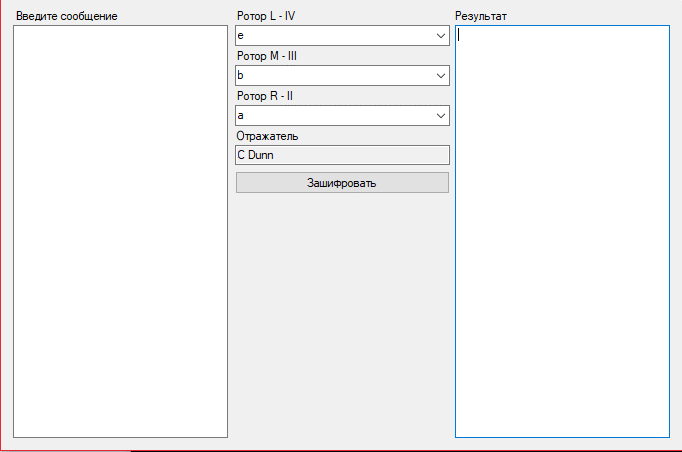
****

Рисунок 1.2 — Приложение

Для проверки работы приложения, введем какой-нибудь текст.

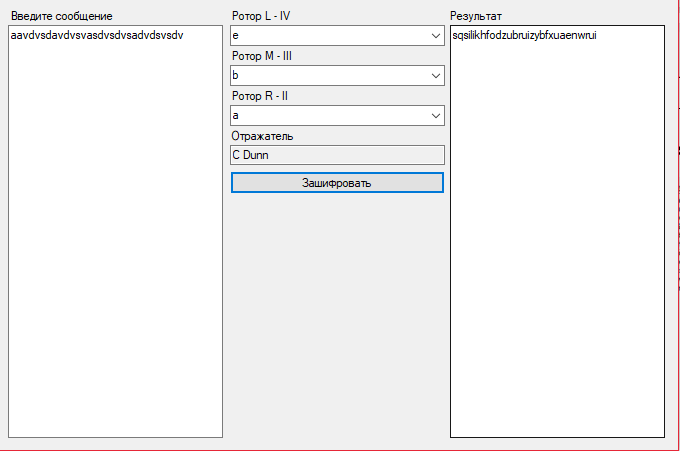


Рисунок 1.3 — Результат выполнения

**Оценка криптостойкости машины «Энигма»**

Для расчета оценки криптостойкости машины «Энигма», необходимо посчитать комбинации выбора 3-х роторов из возможных 10:

10 ∙ 9 ∙ 8 = 720

Получено 720 комбинаций. Каждый из роторов может быть установлен в 1 из 26 его положений. Тогда с 3-я роторами будет 17576 вариаций положения ротора.

26 ∙ 26 ∙ 26 = 17576

Кольцо на каждом роторе содержит маркировку ротора и выемку, которая влияет на шаг перемещения расположенного левее ротора. Каждое кольцо может быть установлено в любом из 26 положений. Поскольку слева от третьего (наиболее левого) ротора нет ротора, на расчет влияют только кольца самого правого и среднего ротора. Это дает 676 комбинаций колец:

26 ∙ 26 = 676

По условию дан рефлектор C Dunn. В нем имеется 13 пар символов. Нет разницы в порядке символов внутри пар, как и неважно то, в каком порядке расположены пары. Посчитаем число перестановок символов в рефлекторе с помощью выражения 26! / (26 – 2*n*)! · *n*! · 2*n*:

26! / (26 – 2 \* 13)! · 13! · 2 \* 13 = 2,49 \* 1015

**Вывод**

В ходе выполнения лабораторной работы были изучены и приобретены практические навыки разработки и использования приложения для реализации подстановочных шифров.