Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Изучение устройства и функциональных особенностей шифровальной машины «Энигма»**

Студент: Каспер Н.В.

ФИТ 3 курс 5 группа

Преподаватель: Берников В.О.

Минск 2020

1. **Описание приложения**

Приложение написано на языке программирования C# и позволяет:

* зашифровать текст с помощью шифровальной машины «Энигма», вводя порядок следования роторов, значение рефлектора, стартовые позиции, кольцо и параметры коммутационной панели;
* расшифровать текст с помощью шифровальной машины «Энигма».

1. **Методика выполнения поставленных задач**

Для выполнения зашифрования сообщения с помощью шифровальной машины «Энигма» необходимо ввести исходный текст для зашифровки, стартовые позиции роторов, последовательность роторов, пары символов коммутационной панели, позиции кольца, тип рефлектора.

Когда все данные введены, необходимо нажать на кнопку «Зашифровать» для того, чтобы зашифровать сообщение и кнопку «Расшифровать» для того, чтобы расшифровать сообщение. Вид главного окна приложения представлен на рисунке 2.1.

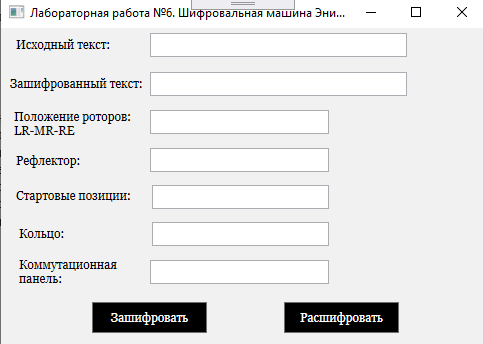


Рисунок 2.1 – Главное окно приложения

В примере, представленном на рисунке 2.2, используется исходное сообщение «natashakasperviktorovna», положение роторов «IV-III-II», рефлектор D, стартовые позиции «AAA», кольцо «AAA» и коммутационная панель «AB CD EG».

Аналогичным способом выполняется шифрование с другими параметрами роторов, рефлекторов, стартовых позиций и кольца. Также важную роль играют позиции коммутационной панели».

Результат зашифрования сообщения представлен на рисунке 2.2.

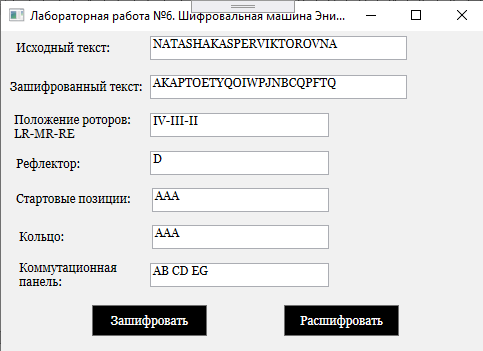


Рисунок 2.2 – Зашифрование сообщения

Обработчик кнопки «Зашифровать» представлен на рисунке 2.3.

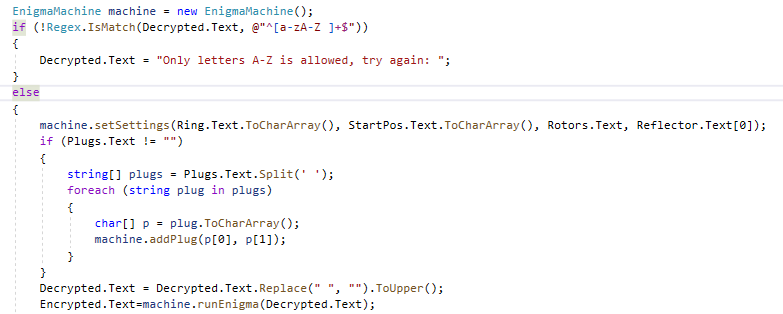


Рисунок 2.3 – Обработчик кнопки «Зашифровать»

В данной программе есть возможность установить настройки по умолчанию для шифровальной машины «Энигма», которое представлено на рисунке 2.4.

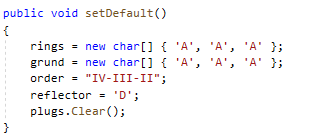


Рисунок 2.4 – Настройки по умолчанию для «Энигмы»

На рисунке 2.5 представлена функция для зашифрования и расшифрования сообщения.

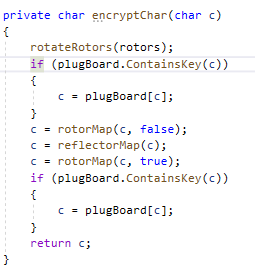


Рисунок 2.5 – Функция для зашифрования и расшифрования

Таким образом, были реализованы все поставленные задачи. Шифровальная машина «Энигма» обладает достаточной криптостойкостью за счет большого числа стартовых позиций, позиций кольца и пар на коммутационной панели.

Также, стоит отметить, что шифровальная машина «Энигма» является разновидностью динамического шифра Цезаря.

**Вывод**

В ходе лабораторной работы были приобретены навыки разработки и использования шифровальной машины «Энигма». Были изучены основные принципы работы «Энигмы».

Также было разработано приложение, на языке программирования C#, для реализации задач, связанных с шифрованием данных.