Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование блочных шифров**

Студент: Николаева Е.В.

ФИТ 3 курс 5 группа

Преподаватель:

Савельева Маргарита Геннадьевна

Минск 2023

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.

В примере, представленном на рисунке 2.1, используется исходное сообщение «Nikolaeva Evgenia», положение роторов «Beta-VIII-I», рефлектор B Dunn.

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 2.1.

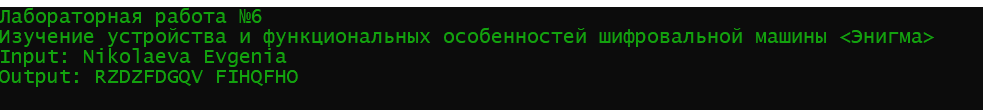


Рисунок 2.1 – Зашифрование сообщения

Функция Encrypt, что используется для шифрования представлена на рисунке 2.2.

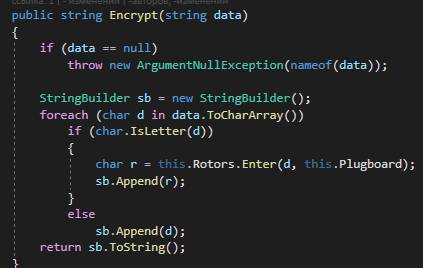


Рисунок 2.2 – Функция Encrypt

В данной программе есть возможность установить настройки для шифровальной машины «Энигма», которое представлено на рисунке 2.3.

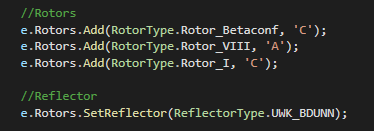


Рисунок 2.3 – Настройки по умолчанию для «Энигмы»

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.