Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Изучение устройства и функциональных особенностей шифровальной машины «Энигма»

Студент: Голодок А. Ю.

ФИТ 3 курс 4 группа

Преподаватель: Сазонова Д. В.

Минск 2024

1. **Теоретическая часть**

Первая шифровальная машина, «Enigma A», появилась в 1923 году и весила около 50 кг. Вскоре была представлена «Enigma B», похожая на первую модель, но обе оказались слишком громоздкими для военного использования. Во время Второй мировой войны было произведено более 100 тысяч таких машин.

«Энигма» – это электромеханическое устройство, состоящее из механической и электрической частей. Механическая часть включает клавиатуру, роторы и ступенчатый механизм, который поворачивает роторы при каждом нажатии клавиши. Электрическая часть включает клавиатуру, коммутационную панель, лампочки и роторы.

Основные блоки «Энигмы»:

* Панель механических клавиш, дающая сигнал для поворота роторов.
* Три или более роторных дисков, каждый с 26 контактами, коммутируемыми в случайном порядке.
* Рефлектор, соединенный с крайним левым ротором.
* Коммутационная панель для изменения электрических соединений двух букв.
* Панель с электрическими лампочками, показывающими выходную букву.

При каждом нажатии клавиши самый правый ротор сдвигается на одну позицию, а при определенных условиях сдвигаются и другие роторы. Это приводит к различным криптографическим преобразованиям, заменяя один символ другим. Механические части замыкают контакты, создавая электрический контур. При нажатии клавиши контур замыкается, ток проходит через цепь и включает лампочку, показывая букву шифртекста. Рефлектор замыкает цепь, возвращая ток по другому пути и зажигая лампочку.

EK = f (m, В, Re, L, M, R).

Чтобы оценить криптостойкость шифра, нужно учитывать все

возможные настройки машины. Для этого необходимо рассмотреть

следующие свойства «Энигмы»:

• выбор и порядок роторов;

• разводку (коммутацию) роторов;

• настройку колец на каждом из роторов;

• начальное положение роторов в начале сообщения;

• отражатель;

• настройки коммутационной панели.

1. **Практическая часть**

Приложение состоит из двух частей, код для роторов, и код для шифрования и дешифрования. Первая часть представлена на рисунке 2.1.

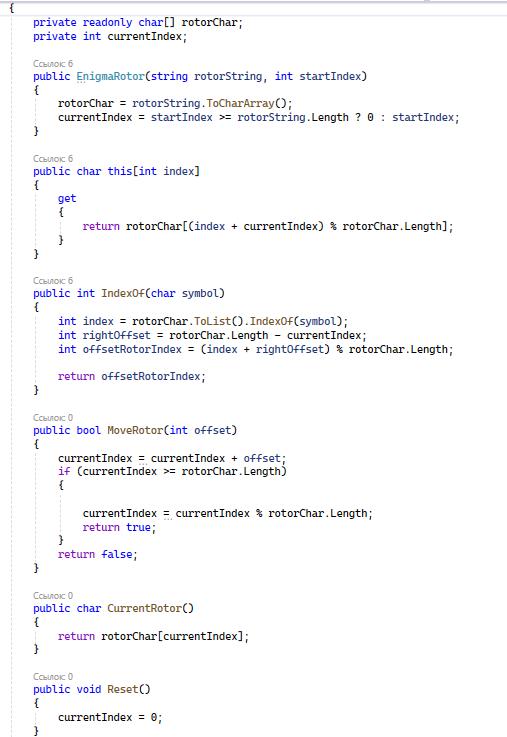


Рисунок 2.1 – код класса EnigmaRotor

Класс EnigmaRotor представляет ротор шифровальной машины «Энигма» и реализует следующие функции. Конструктор инициализирует ротор символами из строки rotorString и устанавливает начальный индекс currentIndex. Индексатор возвращает символ ротора с учётом текущего смещения. Метод IndexOf находит индекс символа в роторе, учитывая текущее смещение. Метод MoveRotor перемещает ротор на заданное количество позиций и возвращает true, если произошёл полный оборот ротора. Метод CurrentRotor возвращает текущий символ ротора. Метод Reset сбрасывает ротор в начальное положение.

Вторая часть представлена на рисунке 2.2.



Рисунок 2.2 – код класса EnigmaMachine

Класс EnigmaMachine моделирует работу шифровальной машины «Энигма». В нём определены статические строки, представляющие алфавит и три ротора. Также определён массив строк, представляющий рефлектор.

Метод Encrypt шифрует входной текст. Он принимает текст и начальные позиции трёх роторов. Для каждого символа текста он проходит через три ротора, рефлектор и снова через три ротора в обратном порядке, затем добавляет зашифрованный символ в результат.

Метод Decrypt выполняет обратную операцию. Он также принимает текст и начальные позиции роторов. Для каждого символа текста он проходит через роторы и рефлектор в обратном порядке, а затем в прямом порядке, добавляя расшифрованный символ в результат.