МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

**«**ИЗУЧЕНИЕ УСТРОЙСТВА И ФУНКЦИОНАЛЬНЫХ ОСОБЕННОСТЕЙ ШИФРОВАЛЬНОЙ МАШИНЫ «ЭНИГМА»**»**

Студент: Бутурля Р.А.

ФИТ 3 курс 5 группа

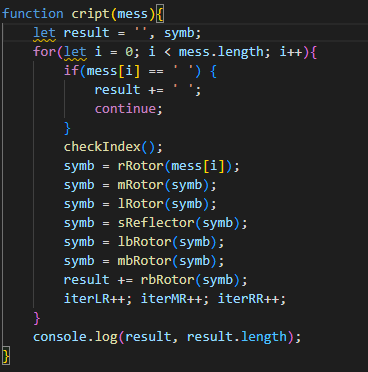
Вариант 3

Преподаватель: Савельева М. Г.

Минск 2023

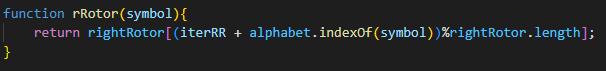
1. Разработать приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя.

Для выполнения шифрования был разработан метод cript(mess). Метод последовательно вызывает методы для шифровки каждого символа. Параметр mess содержит в себе сообщение для зашифровки.



Листинг 1– Метод cript(mess)

Метод rRotor(symbol) шифрует пришедший символ, хранящийся в параметре symbol. Для зашифровки используется схема правого ротора и его сдвиг.

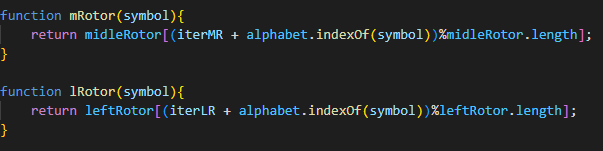


Листинг 2 – Метод rRotor(symbol)



Рисунок 1 – Схема правого ротора

Методы mRotor(symbol) и lRotor(symbol) аналогичны методу rRotor(symbol), но используют схемы среднего и левого ротора соответственно.

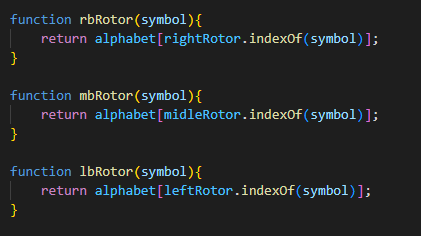


Листинг 3 – Методы mRotor(symbol) и lRotor(symbol)



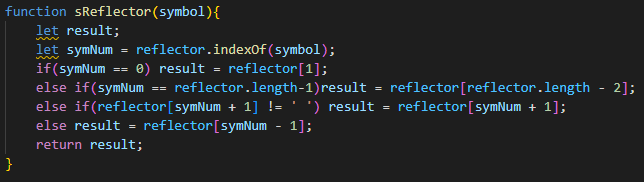
Рисунок 2 – Схемы левого и среднего роторов

Методы rbRotor(symbol), lbRotor(symbol) и mbRotor(symbol) предназначены для выполнения задачи методов rRotor(symbol), lRotor(symbol) и mRotor(symbol) в обратном порядке.



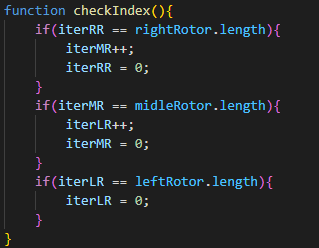
Листинг 4 – Методы rbRotor(symbol), lbRotor(symbol) и mbRotor(symbol)

Метод sReflector(symbol) шифрует символ как рефлектор машины «Энигма».

****

Листинг 5 – Метод sReflector(symbol)

Метод checkIndex() предназначен для изменения счетчика сдвига каждого из роторов.



Листинг 6 – Метод checkIndex()

Результаты шифрования сообщения «buturlia roman» с различными настройками роторов (R/M/L):

* 0/0/0: ktakwbpv ifmoi
* 1/0/1: eyxgftgo xmxwh
* 5/8/0: fjfrqlhb siryd
* 10/10/10: orsaduyh uoxeu
* 25/25/25: mtxnlwbc tuqhw

1. Оценка криптостойкости разработанной программы

Чтобы оценить криптостойкость программы, нужно учитываться все возможные настройки машины. Формула оценки криптостойкости выглядит следующим образом.

*Ek* = *f*(*B*, *Re*, *L*, *M*, *R*)(*1.1*)

Где *L, M, R* – действия левого, среднего, правого ротора соответственно, *Re* – действия рефлектора, B – кол-во возможных начальных положений ротора.

Так как по заданию у нас выбор из трёх роторов, то количество возможных комбинаций при выборе порядка роторов равно 6. Так как в исходном алфавите у нас 26 символов, то количество возможных комбинаций начальных позиций равна 263=17576. Так как кольцо влияет на сдвиг последующего ротора, то нам требуется посчитать кол-во возможных вариаций установок кольца. Так как 3 кольцо является последним и не влияет ни на что, то его при расчетах мы не учитываем. Тогда кол-во возможных перестановок будет равно 26×26=676. Умножив все между собой мы и получим ответ: 6×17576×676=71288256 ~ 226

**Вывод**

Применил практические навыки разработки и использования приложений для реализации перестановочных шифров.