МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

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

Студент: Высоцкий Я.А.

ФИТ 3 курс 5 группа

Вариант 4

Преподаватель: Савельева М. Г.

Минск 2023

**1)Разработать приложение – симулятор шифровальной машины «Энигма»**

Перед разработкой приложения нужно выделить основные части, которые требуется реализовать, для работы приложения, симулирующего шифровальную машину «Энигма». В ходе проектирования были выделены 3 объекта, требуемые программной реализации.

1. Класс эмулирующий ротор;
2. Класс эмулирующий рефлектор;
3. Класс управляющий роторами и рефлектором.

Класс Roter –программная реализацией ротора из шифровальной машины «Энигма». Класс содержит: массив символов в алфавитном порядке, массив символов, отвечающий за конкретную спецификацию ротора, начальный сдвиг ротора и шаг на который сдвигается ротор. Входные значения устанавливаются в конструкторе.

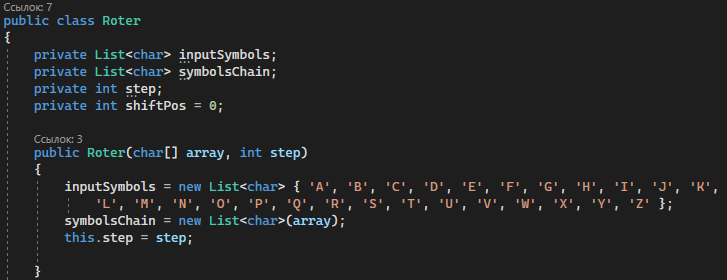


Рисунок 1.1 – Свойства класса Roter

В самом классе определенно 2 основных метода, отвечающих за получения нового символа при начальном и обратном пути.

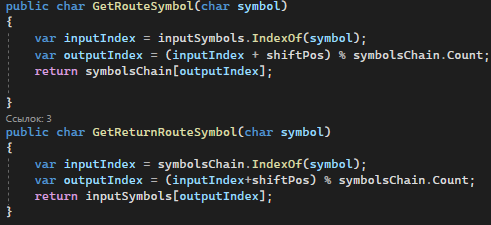


Рисунок 1.2 – Функции расчета нового символа в роторе

Класс Reflector – программная реализация рефлектора из шифровальной машины «Энигма». Класс содержит набор пар символов. В классе определен единственный метод, возвращающий символ, образующий пару для входного символа.

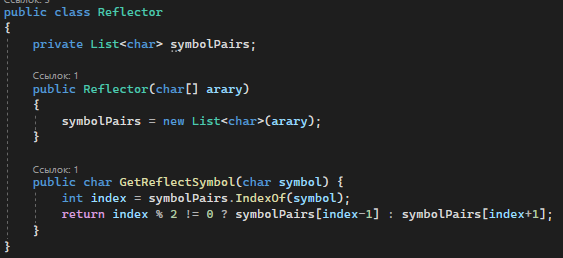


Рисунок 1.3 – Класс Reflector

Класс Enigma – класс, объединяющий роторы и рефлектор в единую сущность. Класс содержит 3 ротора и 1 рефлектор, как и шифровальная машина «Enigma». Для работы с классом требуется установить требуемые роторы и рефлектор. После установки всех компонентов и их конфигурации класс готов к шифрованию текста. За это отвечает метод   
Encrypte (string inputText). Он последовательно для каждого символа в исходном сообщении вызывает другой метод encrypteSymbol (char symbol) куда передает символ. Метод управляет всеми компонентами для получения зашифрованного результат.

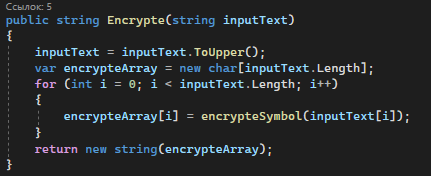


Рисунок 1.4 – Функция шифрования входного текста

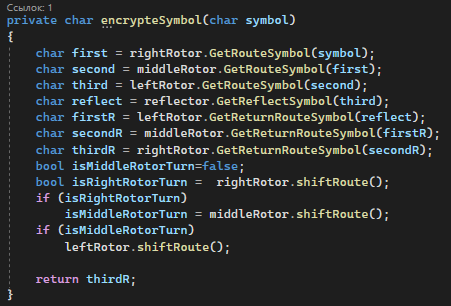


Рисунок 1.5 – Функция шифрования символа исходного текста

Результаты шифрования ФИО при разной конфигурации программы выглядит следующим образом:

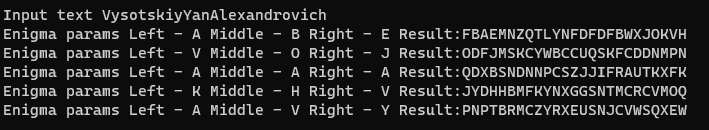


Рисунок 1.6 – Результат шифрования ФИО

**2) Оценка криптостойкости разработанной программы**

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

(1.1)

Где *L, M, R* – действия левого, среднего, правого ротора соответственно, – 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 . 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 . Умножив все между собой мы и получим ответ:

**Вывод**

При выполнении лабораторной работы были приобретены практические навыки разработки приложения для реализации перестановочных шифров. Так же были получены знания по внутреннему устройству шифровальной машины «Энигма», а также алгоритм работы с ней.