Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

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

Студент: Раченок И.А.

ФИТ 3 курс 4 группа

Преподаватель:

Сазонова Дарья Владимировна

1. **Описание приложения и заданий**

Приложение должно выполнять следующие функции:

* функция зашифрования текста с помощью шифровальной машины «Энигма;
* функция расшифрования текста с помощью шифровальной машины «Энигма».
* оценка криптостойкости варианта машины.

1. **Выполнение поставленных задач**

Алгоритм шифрования сообщения происходит строго по указанным действиям.

Конкретный механизм мог быть разным, но общий принцип был таков: при каждом нажатии на клавишу самый правый ротор сдвигался на одну позицию, а при определенных условиях сдвигались и другие роторы.

Движение роторов приводило к различным криптографическим преобразованиям при каждом следующем нажатии на клавишу на клавиатуре, т. е. зашифрование (или расшифрование) сообщений основано на выполнении ряда замен (подстановок) одного символа другим. Механические части двигались и, замыкая контакты, образовывали меняющийся электрический контур. При нажатии на клавишу клавиатуры контур замыкается, ток проходит через созданную (для зашифрования/расшифрования одного конкретного символа сообщения) цепь и в результате включает одну из набора лампочек, отображающую искомую букву шифртекста. Замыкание цепи происходило за счет рефлектора.

Зашифрование сообщения происходит с помощью шифровальной машины «Энигма». Первоначально нужно ввести текст для зашифрования, а также стартовые позиции роторов, последовательность роторов, пары символов коммутационной панели, позиции кольца, тип рефлектора.

В соответствии со своим вариантом, мы имеем следующие данные: положение роторов «II-Gamma-IV», рефлектор С. Код с установкой параметров представлен на рисунке 2.1.

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.

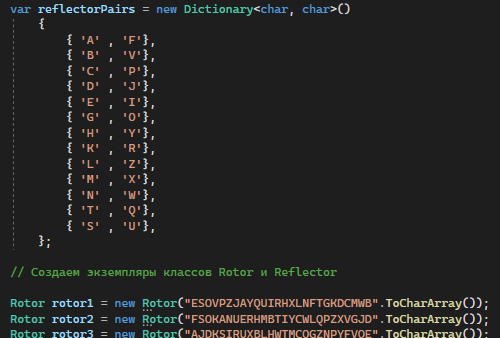


Рисунок 2.1 – Положение роторов и рефлектора

Функции Encipher, которые используются в зависимости от количества входных параметров, используемые для шифрования представлены на рисунке 2.2.

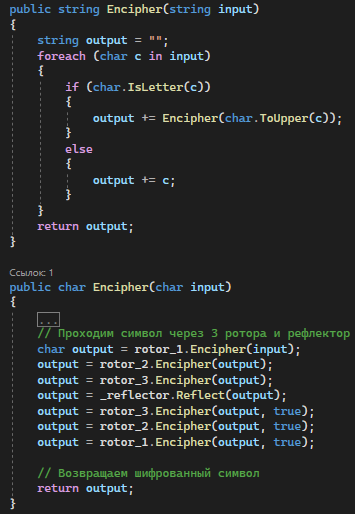


Рисунок 2.2 – Функции Encipher

Также на рисунке 2.3 видна реализация рефлектора.

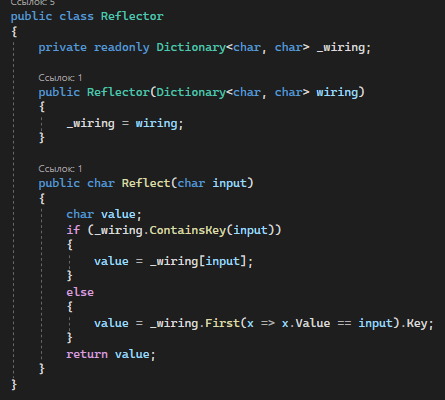


Рисунок 2.3 – Реализация рефлектора

Ниже представлена работа машины «Энигма», сначала мы вводим какое-то предложение и получаем зашифрованное, а затем, чтобы проверить правильность алгоритма, вставляем это же зашифрованное и смотрим чтобы оно расшифровало его на исходное (рисунки 2.4 и 2.5).

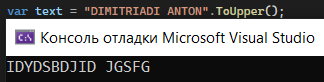


Рисунок 2.4 – Зашифрование сообщения

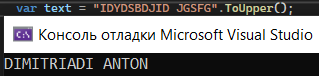


Рисунок 2.4 – Расшифрование сообщения

Также нам следует провести оценку криптостойкости нашего варианта машины.

Чтобы выбрать 3 ротора из возможных 5, существует 60 комбинаций (5 × 4 × 3). Каждый ротор может быть установлен в любом из 26 положений. С 3 роторами имеется 17 576 различных положений ротора (26 × 26 × 26). Кольцо на каждом роторе содержит маркировку ротора и выемку, которая влияет на шаг перемещения расположенного левее ротора. Каждое кольцо может быть установлено в любом из 26 положений. Поскольку слева от третьего (наиболее левого) ротора нет ротора, на расчет влияют только кольца самого правого и среднего ротора. Это дает 676 комбинаций колец (26 × 26). Для первого кабеля одна сторона может иметь любое из 26 положений, а другая сторона – любое из 25 оставшихся положений. Однако поскольку комбинация и ее обратная сторона идентичны (AB такая же, как BA), мы должны игнорировать все двойные числа во всех возможных комбинациях для одного кабеля, предоставляя (26 × 25) / (1! × 21), или 325 уникальных способов коммутаций одним кабелем. Для двух кабелей – (26 × 25) комбинаций для первого кабеля и, поскольку два разъема уже используются, то получается (24 × 23) комбинаций для второго кабеля. Следуя этой простой логике, получается (26 × 25 × 24 × 23) / (2! × 22) = 44 850 уникальных способов коммутаций с использованием двух кабелей. Для трех кабелей – (26 × 25 × 24 × 23 × 22 × 21) / (3! × 23) = 3 453 450 комбинаций. Таким образом, с использованием 10 кабелей на коммутационной панели получаются 150 738 274 937 250 различных комбинаций. Формула, где n равно количеству кабелей, равна 26! / (26 – 2*n*)! · *n*! · 2*n*. Численно это дает: 60 × 17 576 × 676 × 150 738 × 274 × 937 × 250 = 1,07 × 1023.

**Вывод**

В ходе лабораторной работы были приобретены навыки разработки и использования шифровальной машины «Энигма». Были изучены основные принципы работы «Энигмы», а также произведена оценка криптостойкости алгоритма.

Разработано приложение, на языке программирования C#, для реализации задач, связанных с шифрованием данных.