МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6 НА ТЕМУ:**

**ИЗУЧЕНИЕ УСТРОЙСТВАИ ФУНКЦИОНАЛЬНЫХ ОСОБЕННОСТЕЙШИФРОВАЛЬНОЙ МАШИНЫ «ЭНИГМА»**

                                                                 Выполнил студент 3 курса 5 группы

Дмитрук Илья Игоревич

Минск 2024

# Задание 1.

Принцип работы машины Энигма заключается в том, что после ввода символа, сигнал подаётся на правый ротор, и в нём шифруется введёная буква. Затем зашифрованная буква подаётся на центральный ротор и там снова шифруется, затем подается на левый и тоже там шифруется. После буква преобразуется в другую букву на рефлекторе, затем шифрование проходит в обратном порядке от левого до правого ротора. Затем правый ротор сдвигается, если он прошёл полный круг, сдвигаются остальные роторы. В программе данный алгоритм реализован в функции Encrypt. Код данной функции представлен в листинге 1.1.

public string Encrypt(string text)

{

string result = "";

foreach (char item in Left.LanguageOriginalAlphabet.GetStringWithOnlyAlphabetSymbols(text.ToLower()))

{

char symbol = item;

symbol = Right.GetSymbol(symbol);

symbol = Middle.GetSymbol(symbol);

symbol = Left.GetSymbol(symbol);

symbol = Reflector.Reflect(symbol);

symbol = Left.GetSymbolReflected(symbol);

symbol = Middle.GetSymbolReflected(symbol);

symbol = Right.GetSymbolReflected(symbol);

result += symbol;

Right.Move();

if (Middle.Offset == 0)

{

if (Right.IsScrolled)

Middle.SetOffset(Middle.CurrnetOffset + 1);

}

else

Middle.Move();

if (Left.Offset == 0)

{

if (Middle.IsScrolled)

Left.SetOffset(Left.CurrnetOffset + 1);

}

else

Left.Move();

}

return result;

}

Листинг 1.1 – Функции для шифрования Энигмой



Рисунок 1.1 – Результат шифрования и расшифрования Энигмой

# Задание 2.

Количество различных перестановок роторов: всего имеется 10 роторов, из которых одномоментно может использоваться только 3, поэтому количество перестановок = 10 × 9 × 8 = 720.

На каждом роторе имеется 26 символов, поэтому общее количество перестановок букв – 26 × 26 × 26 = 17576.

Количество различных перестановок коммутаторов: всего имеется 26 букв, нам не важно, в каком порядке идут эти 13 пар, а также для каждой пары обратная пара будет той же парой («AB» = «BA»), поэтому число всех возможных перестановок 26 букв в коммутаторе будет равно:

26! / (13! x 213) = 64764752532480000 / 8192 = 7905853580625.

Таким образом, количество всевозможных состояний равно:

720 × 17576 × 7905853580625 = 100046363423806800000 ~ 1 × 1020.

Таким образом, как мы видим, число всевозможных состояний огромно, однако современные компьютеры вполне за разумный промежуток времени могут, с помощью метода перебора, подобрать нужное состояние и получить исходное сообщение из зашифрованного. Однако раньше, когда использовалась Энигма, таких технологий не было и взломать её с помощью обычного перебора было невозможно.

Вывод

В данной лабораторной работы были изучены принципы работы шифровальной машины «Энигма». Было разработано приложение, в котором можно установить определённые роторы и их сдвиги. Само приложение выполняет алгоритм шифрования «Энигмой».