МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №5 НА ТЕМУ:**

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

Выполнила студентка 3 курса 5 группы

Авсюкевич Полина

Минск 2024

**Задание 1:** Разработать приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя. Левый ротор – первый, средний – второй, правый – третий. Рефлектор B. Для зашифрования и расшифрования использовался код представленный в листинге 1.

|  |
| --- |
| public string Crypt(string text, int posL, int posM, int posR)  {  var rotorR = new Rotor(rotor3, posR);  var rotorM = new Rotor(rotor2, posM);  var rotorL = new Rotor(rotor1, posL);  var result = new StringBuilder(text.Length);  foreach (var ch in text)  {  Console.WriteLine(ch);  char symbol = rotorR[alph.IndexOf(ch)];  WriteText(symbol);  symbol = rotorM[alph.IndexOf(symbol)];  WriteText(symbol);  symbol = rotorL[alph.IndexOf(symbol)];  WriteText(symbol);  symbol = reflectorB.First(x => x.Contains(symbol)).First(x => !x.Equals(symbol));  WriteText(symbol);  symbol = rotorL[alph.IndexOf(symbol)];  WriteText(symbol);  symbol = rotorM[alph.IndexOf(symbol)];  WriteText(symbol);  symbol = rotorR[alph.IndexOf(symbol)];  WriteText(symbol);  Console.WriteLine();  result.Append(symbol);  }  return result.ToString();  }  public string Decrypt(string text, int posL, int posM, int posR)  {  var rotorR = new Rotor(rotor3, posR);  var rotorM = new Rotor(rotor2, posM);  var rotorL = new Rotor(rotor1, posL);  StringBuilder result = new StringBuilder(text.Length);  foreach (var ch in text)  {  Console.WriteLine(ch);  char symbol = alph[rotorR.IndexOf(ch)];  WriteText(symbol);  symbol = alph[rotorM.IndexOf(symbol)];  WriteText(symbol);  symbol = alph[rotorL.IndexOf(symbol)];  WriteText(symbol);  symbol = reflectorB.First(x => x.Contains(symbol)).First(x => !x.Equals(symbol));  WriteText(symbol);  symbol = alph[rotorL.IndexOf(symbol)];  WriteText(symbol);  symbol = alph[rotorM.IndexOf(symbol)];  WriteText(symbol);  symbol = alph[rotorR.IndexOf(symbol)];  WriteText(symbol);  Console.WriteLine();  result.Append(symbol);  }  return result.ToString();  } |

Листинг 1 – Реализация симулятора шифровальной машины

Результат работы для шифрования и дешифрования фамилии приведен на рисунке 1, 2.

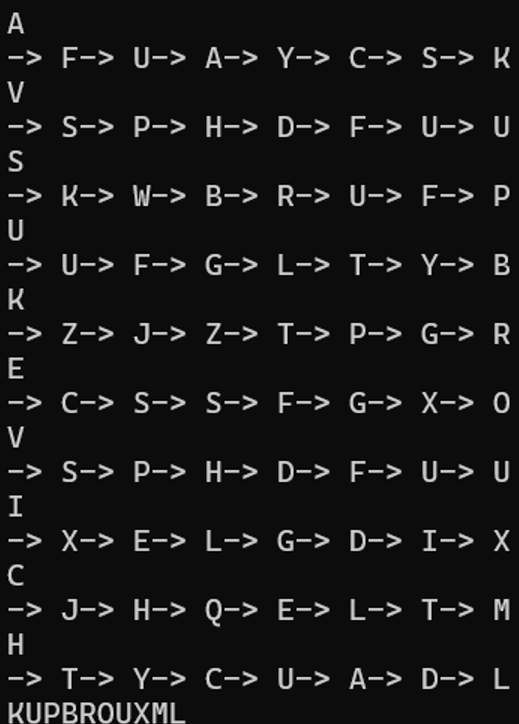


Рисунок 1 – Результат зашифрования

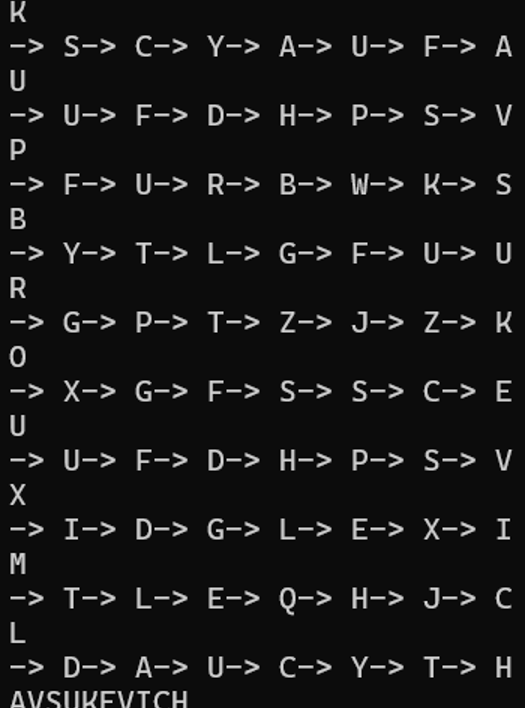


Рисунок 3 – Результат расшифрования

Гистограмма частоты появления символов в исходном и зашифрованном тексте представлена на рисунке 3, 4.

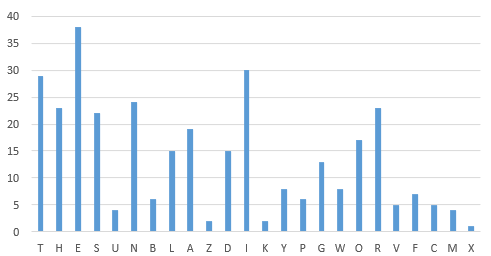


Рисунок 4 – Гистограмма исходного текста

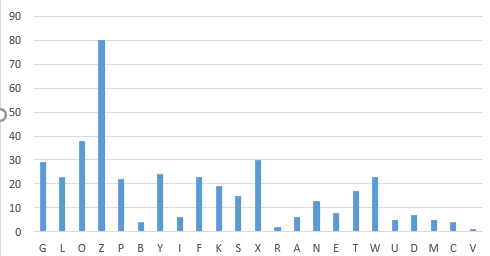


Рисунок 5 – Гистограмма зашифрованного текста

**Вывод:** В ходе выполнения лабораторной работы мы углубились в принципы работы шифровальной машины «Энигма» – одного из самых известных шифровальных устройств времён Второй мировой войны. Мы изучили, как шифровальная машина «Энигма» использовала электромеханические роторы для шифрования текстовых сообщений, а также какие компоненты входили в её состав, такие как роторы, рефлектор и алфавит. Для лучшего понимания принципов работы «Энигмы» мы разработали программу, имитирующую работу данной машины. В результате мы создали класс EnigmaMachine, который содержит методы для шифрования и дешифрования текстовых сообщений, а также класс Rotor, отвечающий за работу с роторами.

Машина Энигма с типом отражателя B и роторами 1, 2, 3 имеет криптостойкость, определяемую количеством возможных настроек ее компонентов. В данном случае, для выбора 2 роторов из 3 доступных существует 6 комбинаций. Каждый ротор имеет 26 положений, что дает 17576 различных комбинаций для установки роторов. Каждое кольцо на роторе влияет на шаг перемещения расположенного левее ротора. Так как слева от третьего ротора нет другого ротора, влияние кольца ограничено только на средний и правый роторы, что дает 676 комбинаций кольцевых настроек. Следовательно, общее количество возможных комбинаций настроек для данной машины Энигма составляет: 6×17576×676=71288256. Таким образом, у данной машины Энигма имеется более 71 миллиона возможных настроек, что придает ей высокую степень криптостойкости.