МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Отчет по лабораторной работе №4

Изучение устройства и функциональных особенностей

шифровальной машины «Энигма»

Выполнил студент: Плюто Э. В.

ФИТ 3 курса, 5 группа

Проверил: Савельева М. Г.

Минск 2024

**Практическое задание:**

**1)** Разработать приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя. Типы роторов: *L* – *Beta*, *M* – VIII, *R* – I, отражателя – *B Dunn*. Сдвиги: 3, 1, 3.

Реализация шага ротора представлена ниже.

|  |
| --- |
| static string Step(string message, string alphabet, string rotor, int shift)  {  StringBuilder sb = new StringBuilder(message);  for (int i = 0; i < message.Length; i++) {  if (alphabet.IndexOf(message[i]) + (i \* shift) >= alphabet.Length)  {  sb[i] = rotor[(alphabet.IndexOf(message[i]) + (i \* shift)) % (alphabet.Length - 1)];  }  else  sb[i] = rotor[alphabet.IndexOf(message[i]) + (i \* shift)];  }  return sb.ToString();  } |

Листинг 1 – Реализация шага ротора

Реализация выполнения шифрования представлена на листинге 2.

|  |
| --- |
| string firstStep = Step(FIO, alphabet, rotorRI, 3);  string secondStep = Step(firstStep, alphabet, rotorMVIII, 1);  string thirdStep = Step(secondStep, alphabet, rotorLBeta, 3);  string reflector = Reflector(thirdStep, alphabet, reflectorBDunn);  string firstBStep = Step(reflector, rotorLBeta, alphabet, 3);  string secondBStep = Step(firstBStep, rotorMVIII, alphabet, 1);  string thirdBStep = Step(secondBStep, rotorRI, alphabet, 3); |

Листинг 2 – Реализация шифрования

Рефлектор реализован аналогичным способ, но без учёта сдвигов.

Результат выполнения программы представлен на рисунке 1.



Рисунок 1 – Результат выполнения шифрования

Гистограмма исходного сообщения представлена ниже.

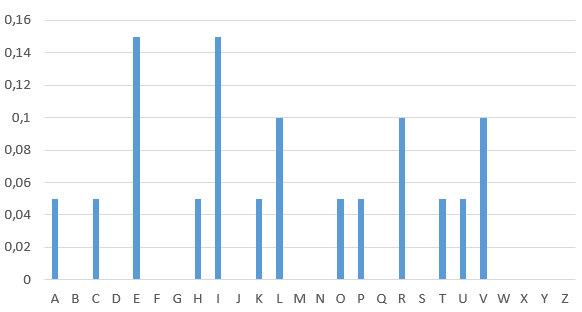


Рисунок 2 – Частота появления символов исходного текста

Гистограмма зашифрованного сообщения представлена на рисунке 3.

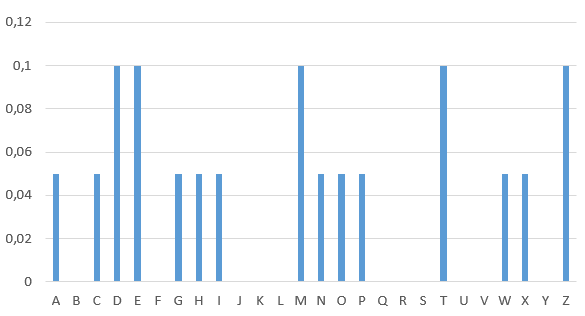


Рисунок 3 – Частота появления символов зашифрованного текста

Оценка криптостойкости шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя: чтобы выбрать 3 ротора из возможных 5, существует 60 комбинаций (5 · 4 · 3). Каждый ротор (его внутренняя проводка) может быть установлен в любом из 26 положений. Следовательно, с 3 роторами имеется 17 576 различных положений ротора (26 · 26 · 26). Кольцо на каждом роторе содержит маркировку ротора (что здесь неважно) 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).

**Вывод:**

Были приобретены практические навыки разработки и использования приложений для реализации перестановочных шифров. Был реализован алгоритм шифрования машины «Энигма», построены гистограммы появления частот символов исходного и зашифрованного текстов, оценена криптостойкость заданной шифровальной машины.