МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

Специальность Информационные системы и технологии

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №4 НА ТЕМУ:**

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

Выполнил студент 3 курса 4 группы

Раченок И.А.

2023 г.

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации перестановочных шифров.

**Задачи:**

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочно-перестановочных шифров.

2. Изучить структуру, принципы функционирования, реализацию процедур зашифрования сообщений в машинах семейства «Энигма».

3. Изучить и приобрести практические навыки выполнения криптопреобразований информации на платформе «Энигма», реализованной в виде симуляторов.

4. Получить практические навыки оценки криптостойкости подстановочных и перестановочных шифров на платформе «Энигма».

5. Результаты выполнения лабораторной работы оформить в виде отчета о проведенных исследованиях, методике выполнения практической части задания и оценке криптостойкости шифров.

**Теоретические сведения**

Машина «Энигма» – это электромеханическое устройство. Как и другие роторные машины, «Энигма» состоит из комбинации механических и электрических подсистем.

Механическая часть включает в себя клавиатуру, набор вращающихся дисков – роторов, которые расположены вдоль вала и прилегают к нему, и ступенчатого механизма, двигающего один или несколько роторов при каждом нажатии на клавишу. Электрическая часть, в свою очередь, состоит из электрической схемы, соединяющей между собой клавиатуру, коммутационную панель, лампочки и роторы (для соединения роторов использовались скользящие контакты).

На рис. 1 показана фотография одной из моделей «Энигмы» с указанием месторасположения основных модулей машины. Как видно на этом рисунке, «Энигма» состоит из 5 основных блоков:

* панели механических клавиш 1 (дают сигнал поворота роторных дисков);
* трех (или более) роторных дисков 2, каждый имеет контакты по сторонам, по 26 на каждую, которые коммутируют в случайном порядке; по окружности нанесены буквы латинского алфавита либо числа;
* рефлектора 3 (имеет контакты с крайним слева ротором);
* коммутационной панели 4 (служит для того, чтобы дополнительно менять местами электрические соединения (контакты) двух букв);
* панели в виде электрических лампочек 5; индикационная панель с лампочками служит индикатором выходной буквы в процессе шифрования.

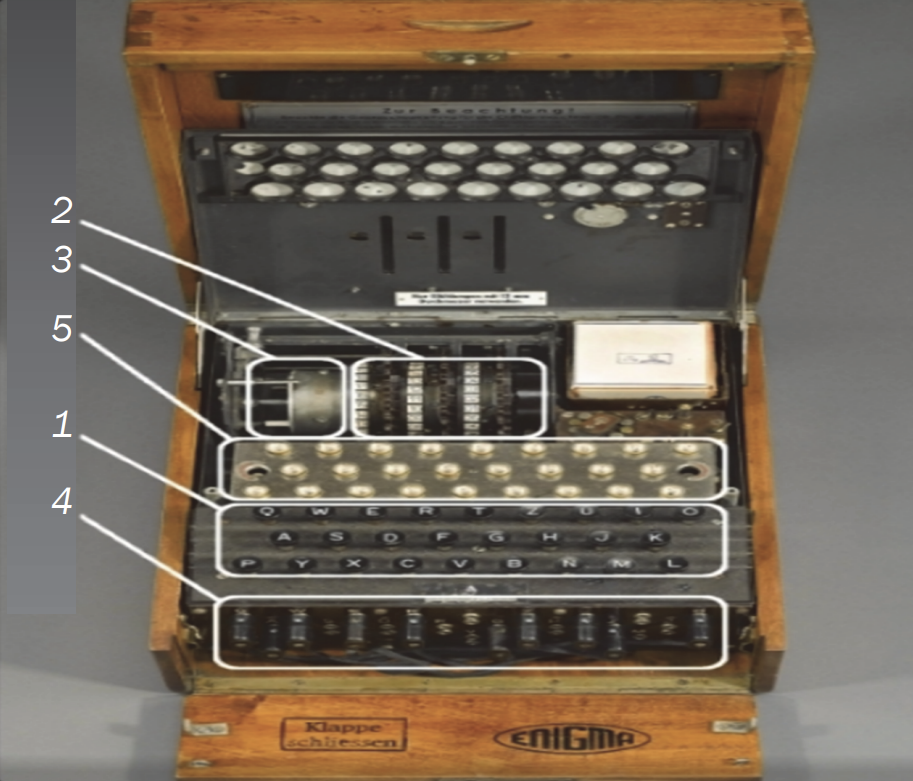


Рис.1 – Трехроторная модель «Энигмы»

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/расшифрование сообщений основано на выполнении ряда замен (подстановок) одного символа другим. Идея А. Шербиуса состояла в том, чтобы добиться этих подстановок электрическими связями.

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 (или расшифрованного сообщения). На рис. 2 показаны упрощенная конструкция ротора (а) и рефлектора (б). Замыкание цепи происходило за счет рефлектора. На рис. 3 схематично показано, как некоторая буква (например, «а») будет зашифрована другой буквой (например, «g»), а следующая за ней буква сообщения (также «а») – уже буквой «с».

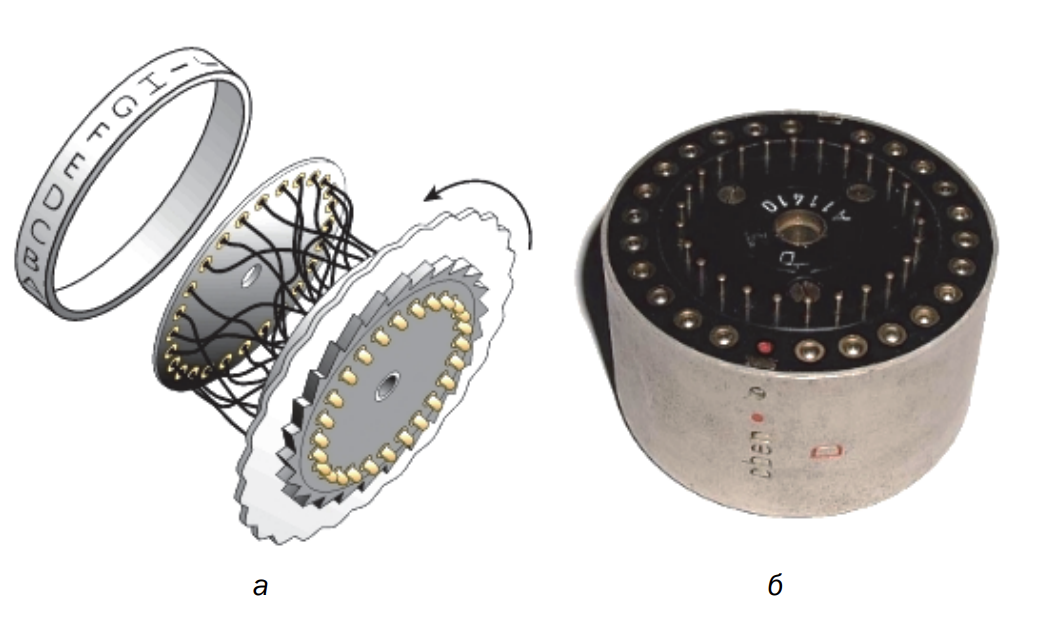


Рис.2 – Упрощенная конструкция ротора (а) и рефлектора (б) «Энигмы»

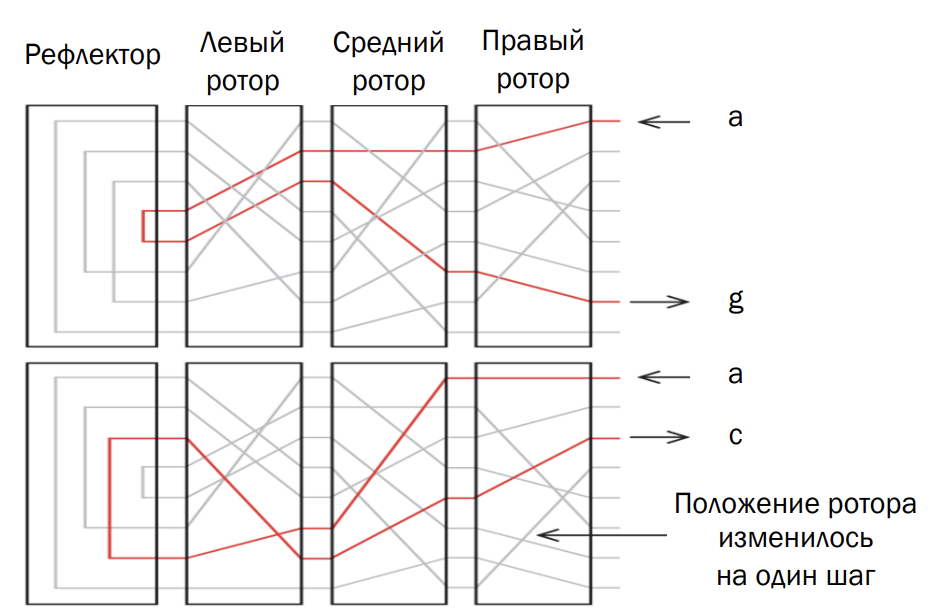


Рис.3 – Пояснение к принципу шифрования путем формирования электрической цепи

На рис. 3 электрическая цепь не представлена в виде замкнутой, поскольку не показаны части коммутационной панели и электрическая лампочка. Замкнутые электрические цепи хорошо иллюстрирует рис. 4.

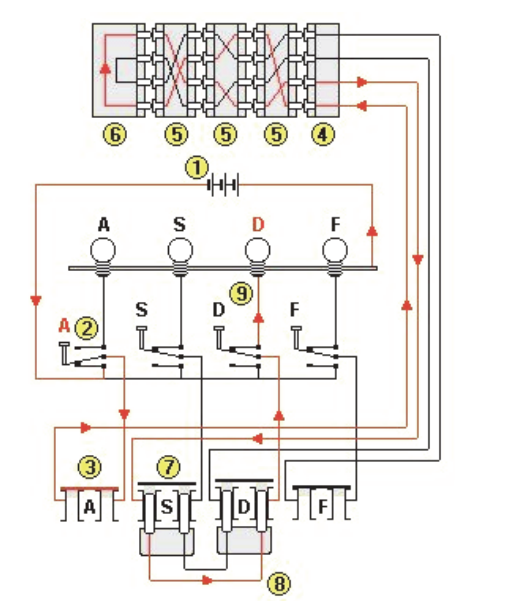


Рис.4 – Пояснение к принципу формирования зашифрованного символа с помощью замкнутой электрической цепи

Замкнутую цепь составляют: батарея 1 (это могут быть и иные источники питания), нажатая двунаправленная буквенная клавиша 2, разъем коммутационной панели 3 (как видим, в одном случае – буква «а» – коммутационного перехода на другую букву нет), входной разъем (входное колесо) роторного модуля 4, роторный модуль 5 (состоит из трех роторов, как в версии «Энигмы» для Вермахта, Wehrmacht Enigma М3, или четырех – в версии «Энигмы» для военно-морского флота, Kriegsmarine Enigma M4), рефлектор 6. Последний возвращает ток (цепь) по другому пути через те же узлы, «зажигая» на ламповой панели букву «D», к другому полюсу батареи. Обратим внимание, что обратная часть цепи уже проходит с учетом выполненной коммутации (7 и 8).

**Алгоритм зашифрования и расшифровки сообщения с помощью «Энигмы»**

Зашифрование:

1) Установка начальной позиции роторов согласно текущей кодовой таблицу (коду дня), например WZA

2) Выбрать случайный ключ сообщения, например SXT

3) Зашифровать ключ сообщения SXT. Например, получилось UHL

4) Оператор ставит ключ сообщения SXT как начальную позицию роторов и зашифровал собственно сообщение

5) Отправляет стартовую позицию WZA и зашифрованный ключ UHL вместе с сообщением

Расшифрование:

1) Роторы ставим в соответствии с первой треграммой WZA

2) Расшифровываем вторую треграмму UHL –> извлекаем исходный ключ SXT

3) Используем исходный ключ как стартовую позицию для расшифрования текста

«Энигма» строится на основе подстановочных шифров, подобных шифру Цезаря, в котором, как известно, ключ сообщения, который должен знать получатель, – это просто смещение между двумя алфавитами. Принято считать, что в основе шифра «Энигмы» лежит динамический шифр Цезаря.

Рассмотрим пример шифрования символа на конкретном примере с настройками роторов и рефлектора, данными в лабораторной работе.

1. На клавиатуре вводим букву K, она попадает в правый ротор(V), на выходе из него кодируется в букву S
2. Буква S попадает на средний ротор(III), на выходе из него кодируется в букву G
3. Буква G попадает на левый ротор(II), на выходе из него кодируется в букву R
4. Буква R попадает на рефлектор где меняется на букву K
5. Буква К попадает снова на левый ротор(II), на выходе из него кодируется в букву L
6. Буква L попадает на средний ротор(III), на выходе из него кодируется в букву V
7. Буква V попадает на правый ротор(V), на выходе из него кодируется в букву O



Рис. 5 – Кодирование буквы в приложении

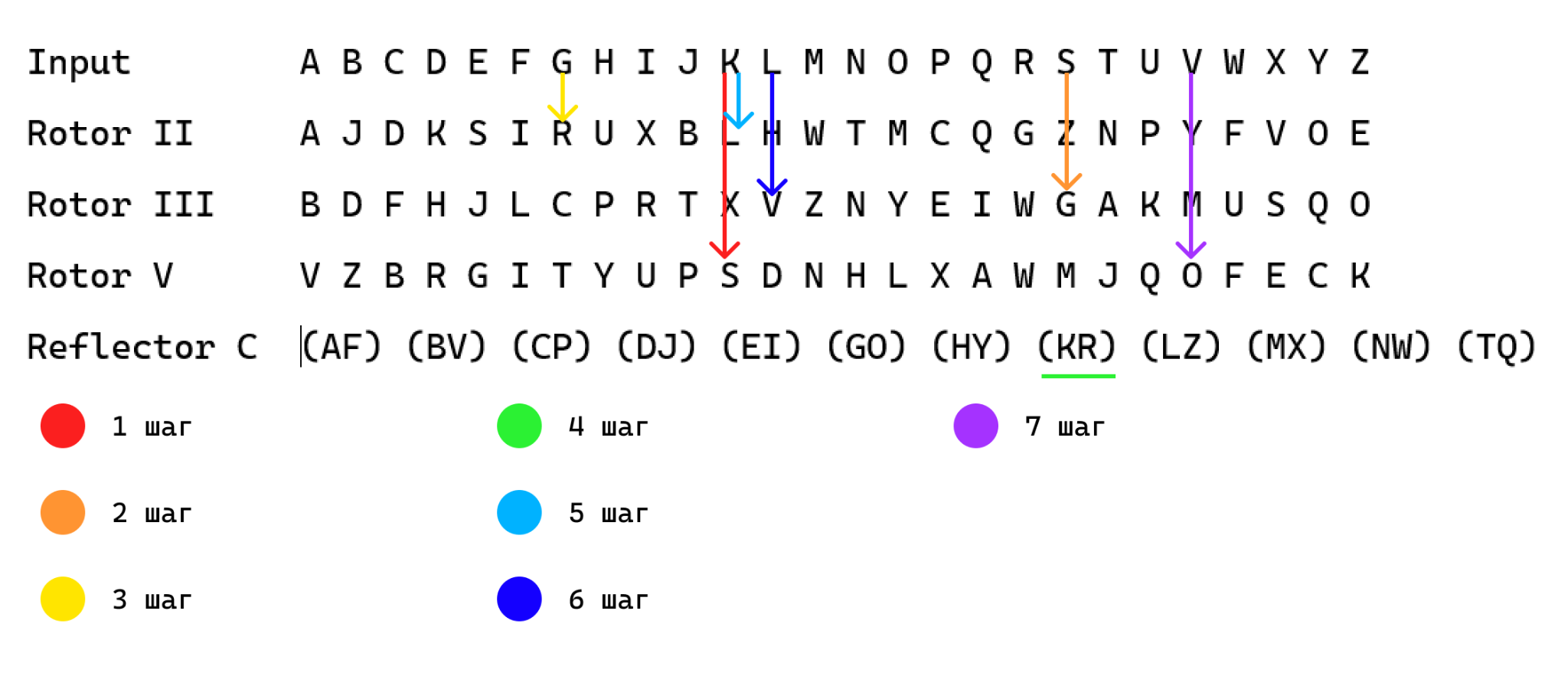


Рис. 6 – Шаги шифрования

**Практическая часть**

1. Ознакомится с эмулятором шифровальной машины «Энигмы». Опробовать различные конфигурации роторов. Сделать частотный анализ зашифрованных сообщений.

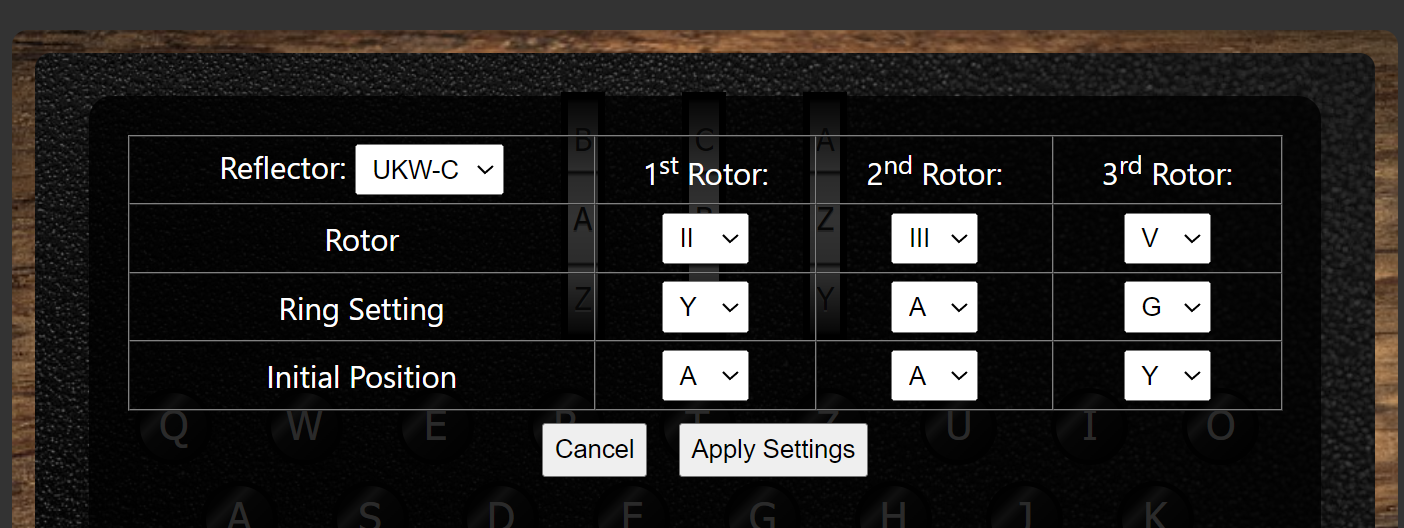


Рис. 7 – Начальная настройка машины (I)

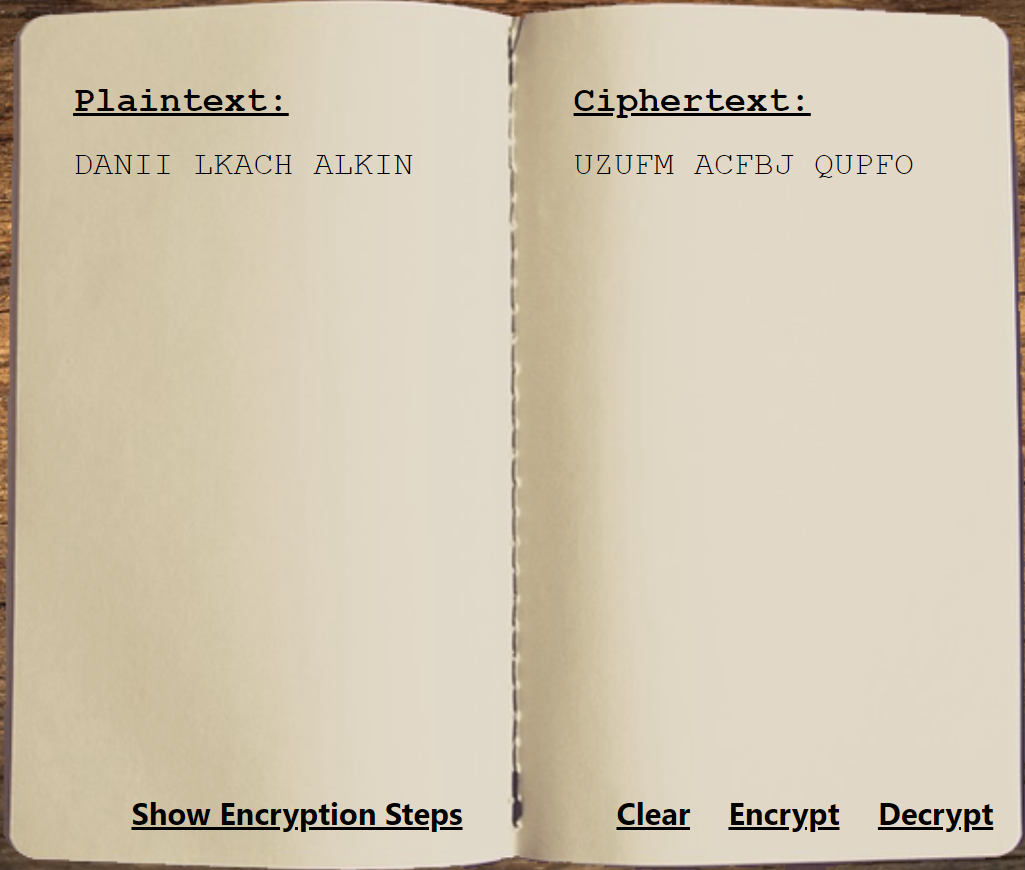


Рис. 8 – Результат шифрования (I)

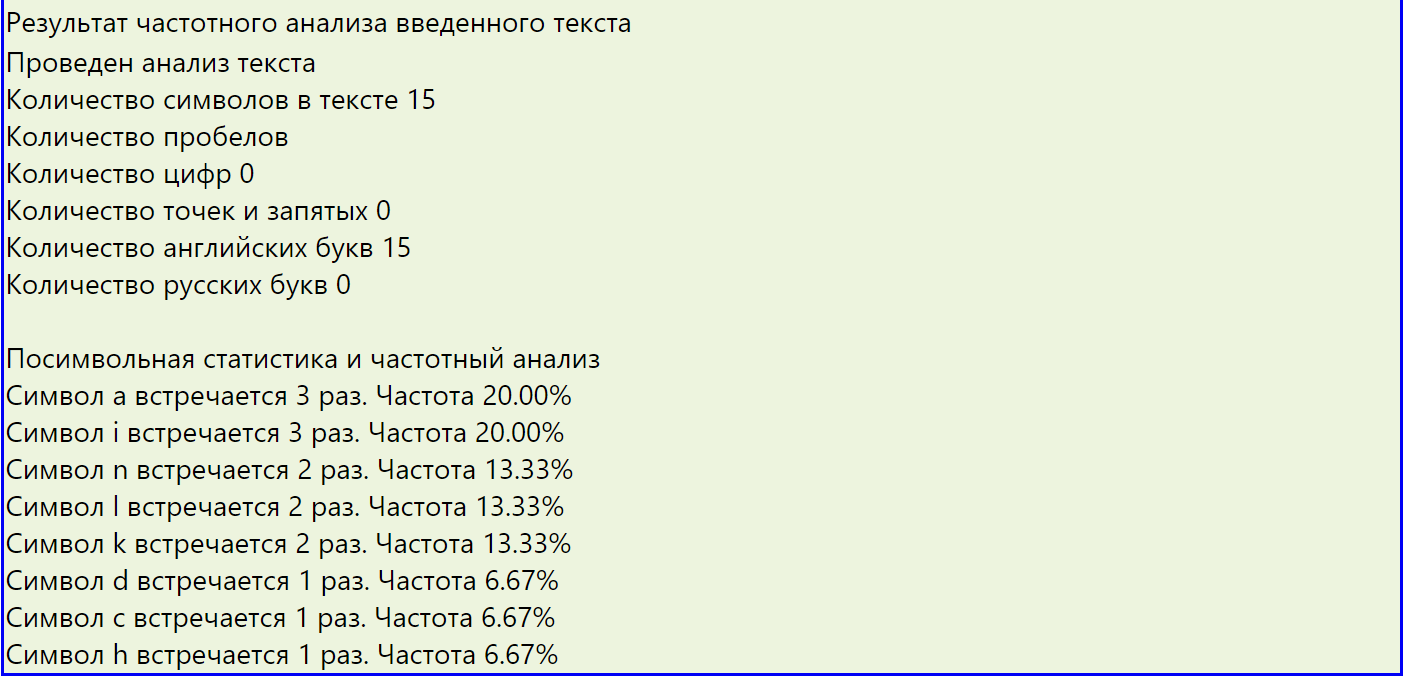


Рис. 9 – Частотный анализ исходного сообщения

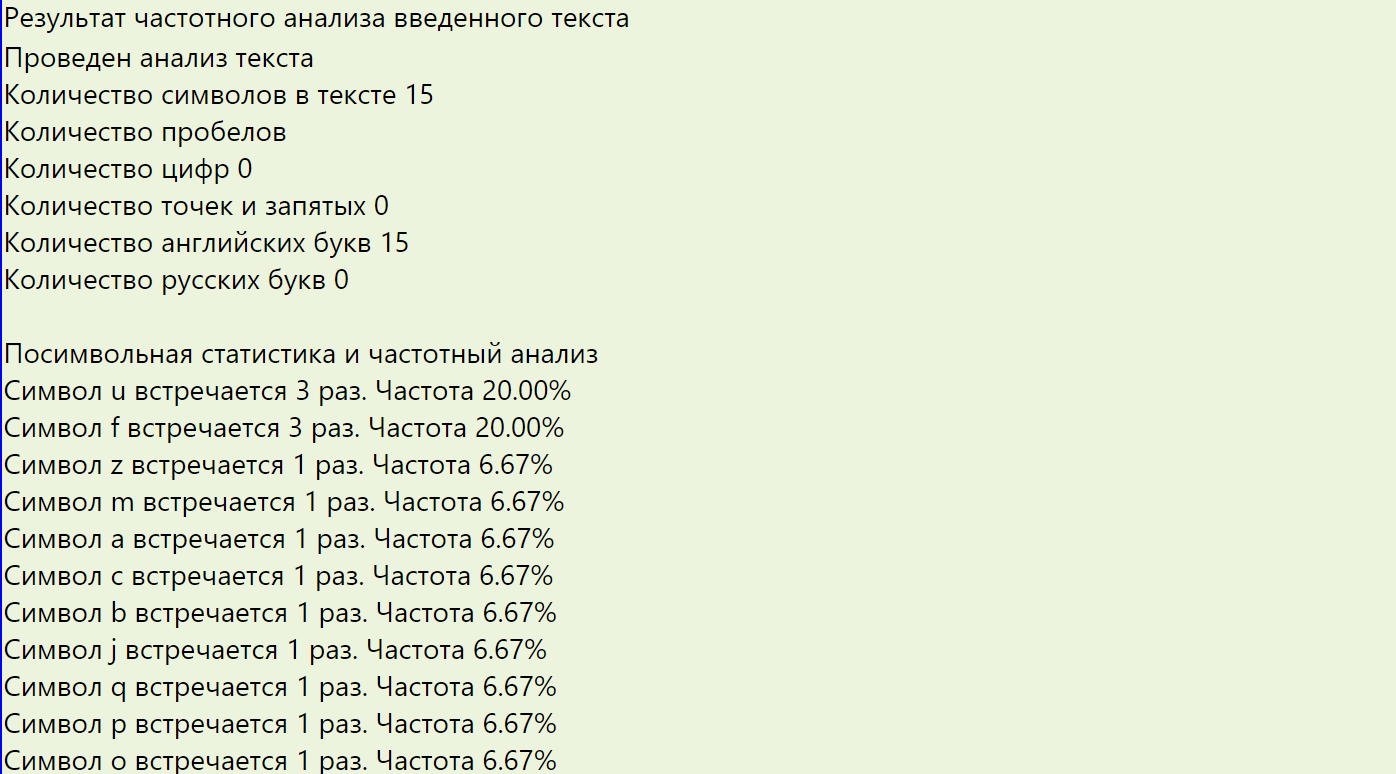


Рис. 10 – Частотный анализ зашифрованного сообщения (I)

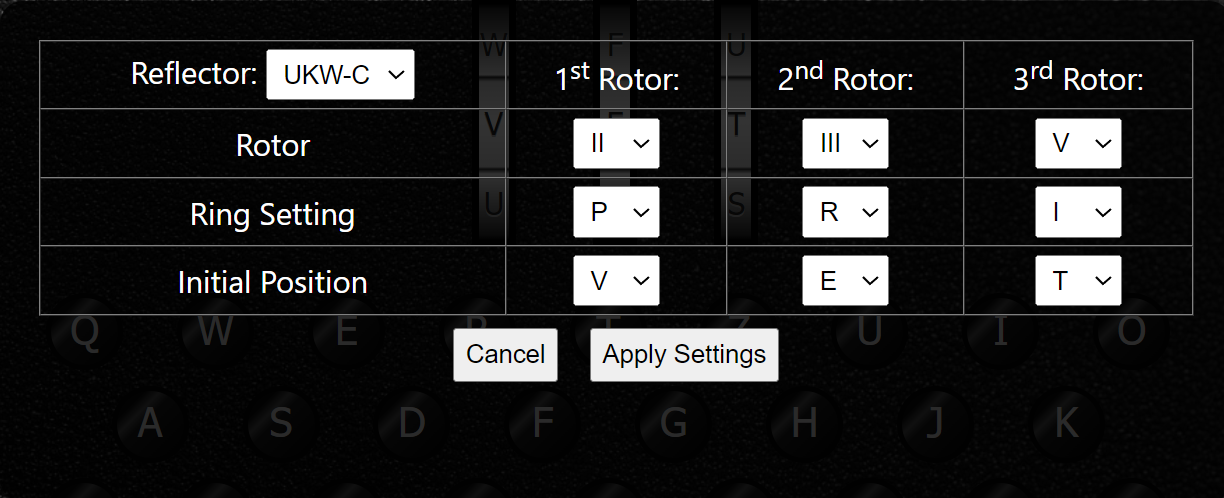


Рис. 11 – Начальная настройка машины (II)



Рис. 12 – Результат шифрования (II)

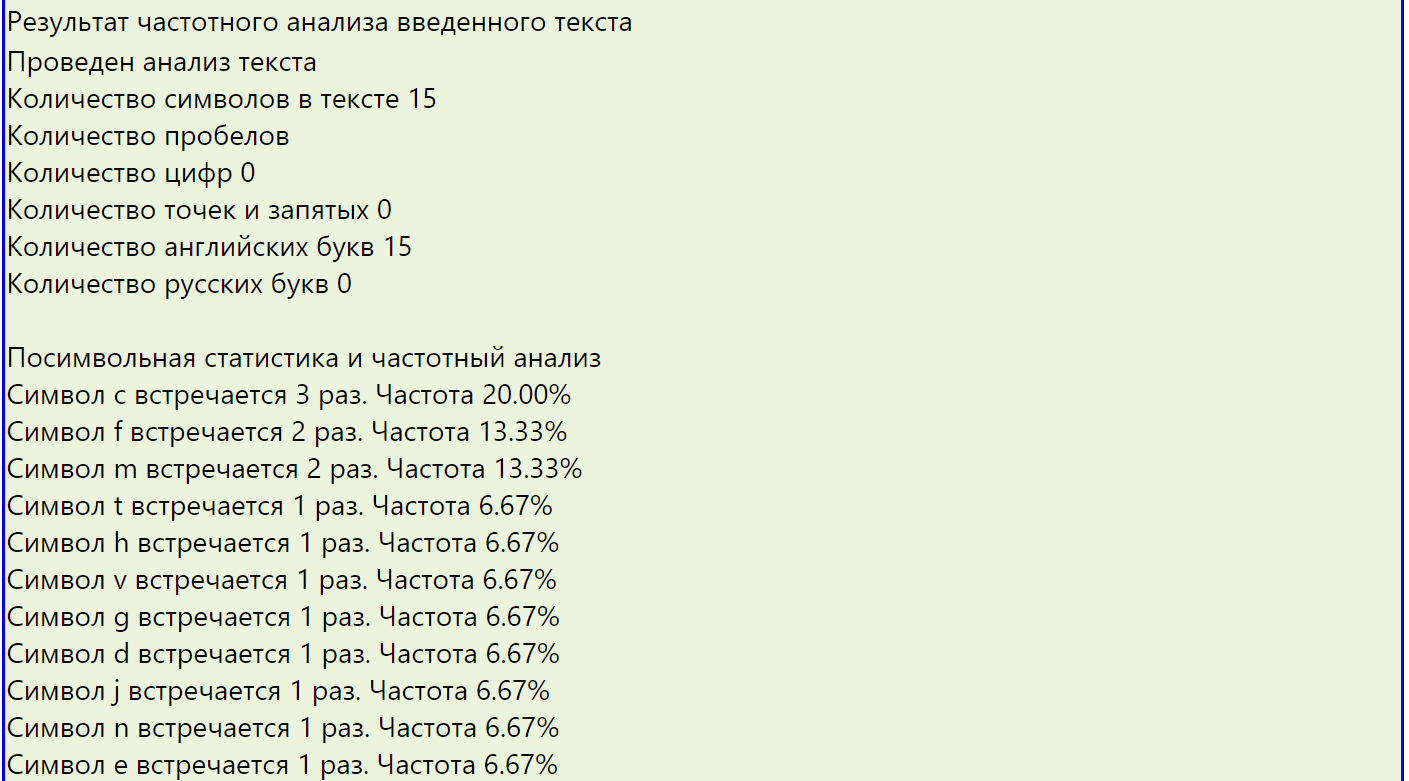


Рис. 13 – Частотный анализ зашифрованного сообщения (II)

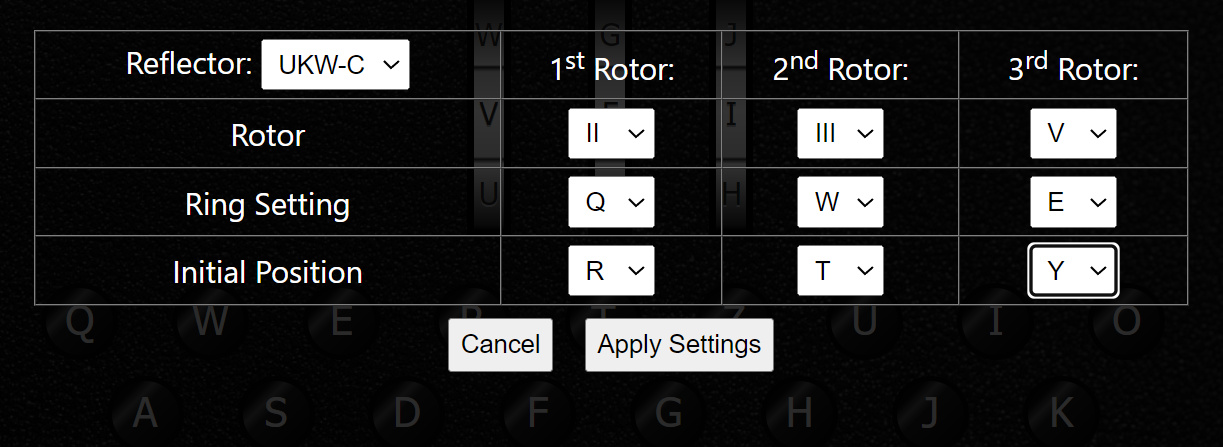


Рис. 14 – Начальная настройка сообщения (III)

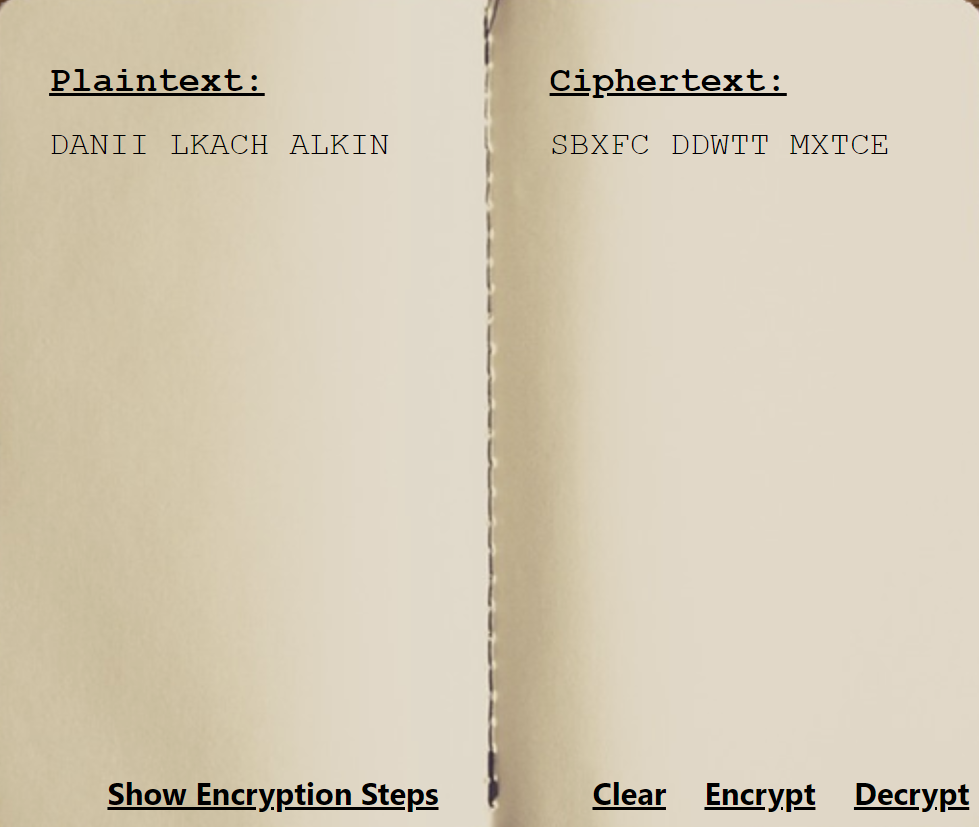


Рис. 15 – Зашифрованное сообщение (III)



Рис. 16 – Частотный анализ зашифрованного сообщения (III)

1. Разработать приложение-симулятор машины «Энигма» в соответствии со своим вариантом

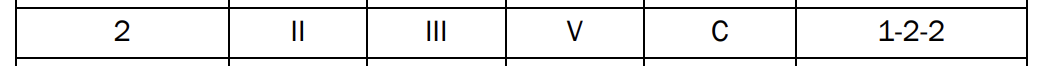


Рис. 17 – Исходные данные для варианта 2

Ниже представлен код программы:

|  |
| --- |
| namespace lab4  {  public class Enigma //Класс машины с конфигурацией роторов и рефлектора  {  private static readonly string \_alphabet = "ABCDEFGHIJKLMNOPQRSTUVWXYZ";  private static readonly string \_rotor2 = "AJDKSIRUXBLHWTMCQGZNPYFVOE";  private static readonly string \_rotor3 = "BDFHJLCPRTXVZNYEIWGAKMUSQO";  private static readonly string \_rotor5 = "VZBRGITYUPSDNHLXAWMJQOFECK";  private static readonly string[] \_reflectorС = { "AF", "BV", "CP", "DJ", "EI", "GO", "HY", "KR", "LZ", "MX", "NW", "TQ", "SU" };  public string Crypt(string text, int posL, int posM, int posR) //метод для шифровки  {  var rotorL = new Rotor(\_rotor2, posL);  var rotorR = new Rotor(\_rotor5, posR);  var rotorM = new Rotor(\_rotor3, posM);  StringBuilder result = new StringBuilder(text.Length);  foreach (var ch in text)  {  Console.Write(ch);  char symbol = rotorR[\_alphabet.IndexOf(ch)];  Output.Print(symbol);  symbol = rotorM[\_alphabet.IndexOf(symbol)];  Output.Print(symbol);  symbol = rotorL[\_alphabet.IndexOf(symbol)];  Output.Print(symbol);  symbol = \_reflectorС.First(x => x.Contains(symbol)).First(x => !x.Equals(symbol));  Output.Print(symbol);  symbol = rotorL[\_alphabet.IndexOf(symbol)];  Output.Print(symbol);  symbol = rotorM[\_alphabet.IndexOf(symbol)];  Output.Print(symbol);  symbol = rotorR[\_alphabet.IndexOf(symbol)];  Output.Print(symbol);  Console.WriteLine();  result.Append(symbol);  rotorR.MoveRotor(posR);  rotorM.MoveRotor(posM);  rotorL.MoveRotor(posL);  }  return result.ToString();  }  public string Decrypt(string text, int posL, int posM, int posR) //метод для дешифровки  {  var rotorR = new Rotor(\_rotor5, posR);  var rotorM = new Rotor(\_rotor3, posM);  var rotorL = new Rotor(\_rotor2, posL);  StringBuilder result = new StringBuilder(text.Length);  foreach (var ch in text)  {  Console.Write(ch);  char symbol = \_alphabet[rotorR.IndexOf(ch)];  Output.Print(symbol);  symbol = \_alphabet[rotorM.IndexOf(symbol)];  Output.Print(symbol);  symbol = \_alphabet[rotorL.IndexOf(symbol)];  Output.Print(symbol);  symbol = \_reflectorС.First(x => x.Contains(symbol)).First(x => !x.Equals(symbol));  Output.Print(symbol);  symbol = \_alphabet[rotorL.IndexOf(symbol)];  Output.Print(symbol);  symbol = \_alphabet[rotorM.IndexOf(symbol)];  Output.Print(symbol);  symbol = \_alphabet[rotorR.IndexOf(symbol)];  Output.Print(symbol);  Console.WriteLine();  result.Append(symbol);  rotorR.MoveRotor(posR);  rotorM.MoveRotor(posM);  rotorL.MoveRotor(posL);  }  return result.ToString();  }  }  public class Rotor //Класс ротора  {  private readonly char[] \_rotorChar;  private int \_currentIndex;  public Rotor(string rotorString, int startIndex)  {  \_rotorChar = rotorString.ToCharArray();  \_currentIndex = startIndex >= rotorString.Length ? 0 : startIndex;  }  public char this[int index]  {  get  {  return \_rotorChar[(index + \_currentIndex) % \_rotorChar.Length];  }  }  public int IndexOf(char symbol)  {  int index = \_rotorChar.ToList().IndexOf(symbol);  int rightOffset = \_rotorChar.Length - \_currentIndex;  int offsetRotorIndex = (index + rightOffset) % \_rotorChar.Length;  return offsetRotorIndex;  }  // Возвращает «true», если ротор совершил полный оборот  public bool MoveRotor(int offset)  {  \_currentIndex = \_currentIndex + offset;  if (\_currentIndex >= \_rotorChar.Length)  {  \_currentIndex = \_currentIndex % \_rotorChar.Length;  return true;  }  return false;  }  public char CurrentRotor()  {  return \_rotorChar[\_currentIndex];  }  public void Reset()  {  \_currentIndex = 0;  }  }  public class Program //инициализация машины  {  static void Main(string[] args)  {  Enigma enigma = new Enigma();  string encoded = enigma.Crypt("KACHALKIN", 1, 2, 2);  Console.WriteLine(encoded);  Console.WriteLine(enigma.Decrypt(encoded, 1, 2, 2));  Console.ReadKey();  }  }  } |

Листинг 1 – Код программы-симулятора «Энигмы»

Ниже представлены скриншоты результатов выполнения программы-симулятора.

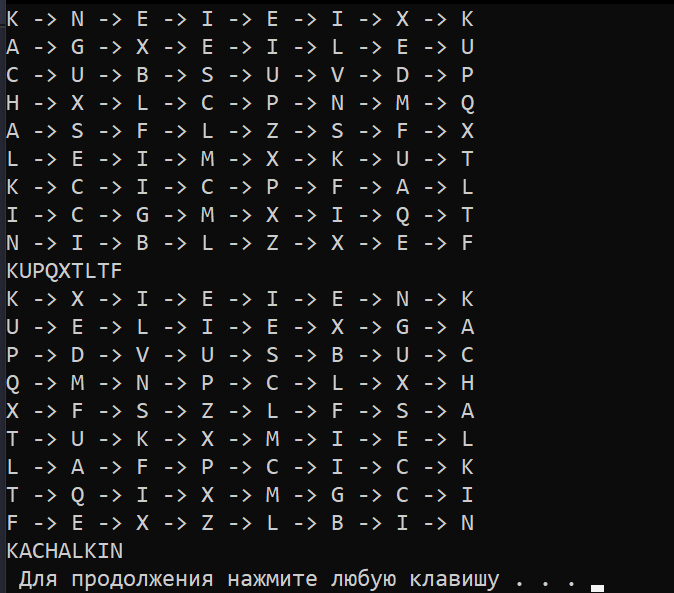


Рис. 18 – Результат выполнения программы

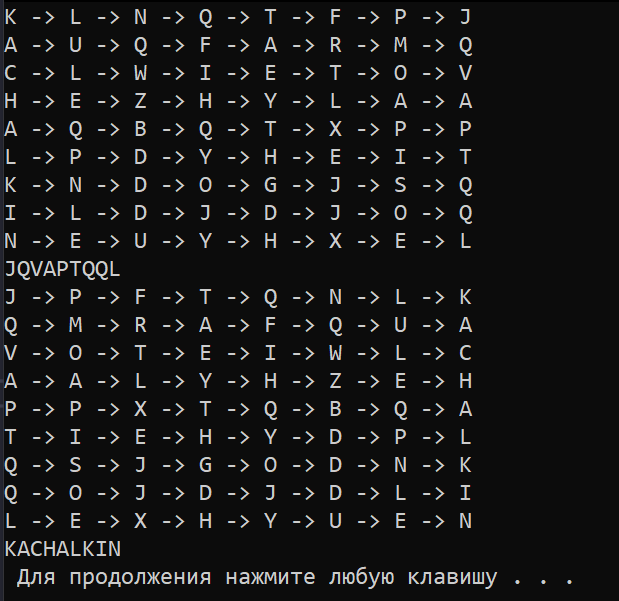


Рис. 19 – Результат выполнения программы с другой настройкой роторов

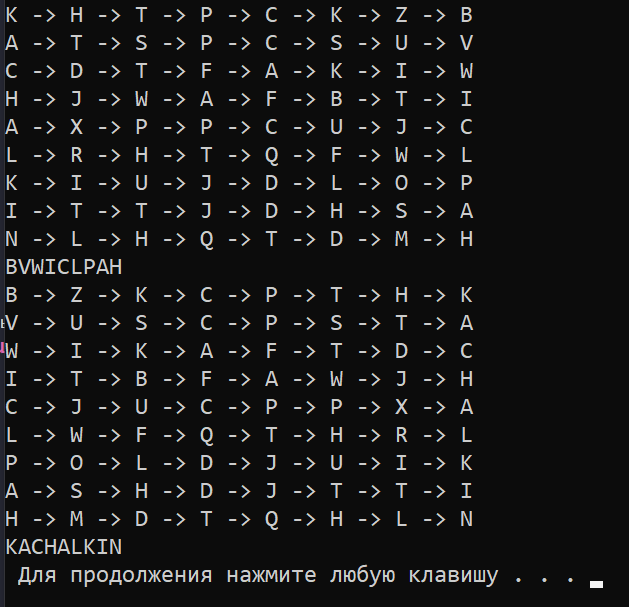


Рис. 20 – Результат выполнения программы с другой настройкой роторов



Рис. 21 – Результат выполнения программы с другой настройкой роторов

**Вывод:** в ходе лабораторной работы было изучено устройство и функциональные особенности шифровальной машины «Энигма». А также были приобретены практические навыки оценки криптостойкости подстановочных и перестановочных шифров на платформе «Энигма».

**Контрольные вопросы**

**1. Дать пояснение к структуре шифровальных машин «Энигма».**

– 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/расшифрование сообщений основано на выполнении ряда замен (подстановок) одного символа другим.

– при нажатии на клавишу, контур замыкается, включается одна из набора лампочек, показывающая искомую букву шифртекста

**2. На основе каких шифров строится машина «Энигма»?**

«Энигма» строится на основе подстановочных шифров, подобных шифру Цезаря, в котором, как известно, ключ сообщения, который должен знать получатель, – это просто смещение между двумя алфавитами. Принято считать, что в основе шифра «Энигмы» лежит динамический шифр Цезаря.

**3. Дать пояснение к принципам зашифрования сообщений.**

Более сложная система использует случайный ряд символов для нижнего алфавита. Принцип, положенный в основу этой «случайности», имеет много общего с перестановочными шифрами.

Принцип подстановки, основанный на взаимной перестановке во втором (нижнем) алфавите в 13 парах символов, расположенных случайным образом.

**4. Дать характеристику криптостойкости шифровальной машины Энигма.**

Преобразование «Энигмы» для каждой буквы может быть определено математически как результат подстановок.

оценить криптостойкость шифра, нужно учитывать все возможные настройки машины. Для этого необходимо рассмотреть следующие свойства «Энигмы»:

• выбор и порядок роторов;

• разводку (коммутацию) роторов;

• настройку колец на каждом из роторов;

• начальное положение роторов в начале сообщения;

• отражатель;

• настройки коммутационной панели.

Немецкие криптологии полагали, что один ротор может быть подключен 4\*10^26 различными способами. Сочетание трех роторов и отражателя позволяет получить астрономические цифры возможных вариантов подстановок. Для союзников, которые знали конструкции роторов, число различных вариантов существенно уменьшалось.

Проблема криптоанализа шифров «Энигмы» была экстраординарной (с учетом электромеханических конструкций устройств для криптоанализа, применяемых в то время). Исчерпывающий поиск всех возможных 1,07 · 10^23 настроек был невозможен в 1940-х гг., а его сопоставимый 77-битный ключ огромен даже для современных электронных систем. Чтобы дать представление о размере этого числа, представим, что у нас есть 1,07 · 10^23 листов бумаги толщиной около 1 мм. Из этих листов можно сложить примерно 70 000 000 стопок бумаги, каждая из которых простирается от Земли до Солнца. Кроме того, 1,07 · 10^23 дюйма равно 288 500 световых лет.

**5. Дать характеристику криптостойкости машины-симулятора на основе разработанного приложения.**

Модель Энигмы имеет 3 различных ротора, пронумерованных римскими цифрами.

При шифровании роторы можно располагать в любой последовательности, что для трех роторов дает 6 разных комбинаций.

Помимо этого, каждый ротор может быть установлен в одной из 26 возможных стартовых позиций. Т.е. начальное положение роторов имеет всего 6\*26^3=105456 комбинаций.

Количество всех возможных соединений на коммутационной панели вычисляется по формуле n! /((n-2m)! m! 2^m), где n — количество букв алфавита, m — количество соединенных пар.

Для 26 букв английского алфавита и 10 пар это составляет 150738274937250=2^47 различных комбинаций.

Таким образом базовая версия Энигмы с тремя роторами имеет солидное даже по современным меркам пространство ключей:

150738274937250\*105456=15,896,255,521,782,636,000≈2^64.

Частоты символов в исходном тексте и зашифрованном сообщении сильно отличаются: некоторые символы вообще не появляются в шифре, а некоторые хоть и встречаются с такой же частотой, на находятся в совершенно других местах. Таким образом, криптостойкость разработанного симулятора такая же, как и у оригинальной машины.

**6. Пояснить основные принципы расшифрования сообщений «Энигмы».**

Процедура расшифрования шифртекстов предусматривала настройку отражателя, роторов и коммутационной панели машины в соответствии с таблицами (книгами) и использованными при зашифровании паролями.