Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**«Отчёт по лабораторной работе 6»**

“ИЗУЧЕНИЕ УСТРОЙСТВА И ФУНКЦИОНАЛЬНЫХ ОСОБЕННОСТЕЙ

ШИФРОВАЛЬНОЙ МАШИНЫ «ЭНИГМА»”

**Выполнила:** студентка 3 курса

4 группы специальности ПОИТ

Сапегина Екатерина Игоревна,

Вариант 11

Минск 2023

***Цель:*** изучение и приобретение практических навыков разработки и использования приложений для реализации перестановочных шифров (работа рассчитана на 4 часа аудиторных занятий).

***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.

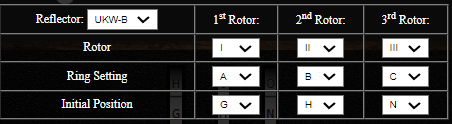
4. Получить практические навыки оценки криптостойкости подстановочных и перестановочных шифров на платформе «Энигма».

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

***Практическая часть:***

1. Произвести зашифрование сообщения (собственные имя, отчество, фамилия) при различных настройках машины-симулятора. Оценить частотные свойства символов в шифртекстах и сравнить этот параметр с частотными свойствами символов для исходного текста.

Шифрование теста: ***SapeginaEkaterinaIgorevna***



(менялось только ***Initial Position***)

1. Разработать приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя. Типы роторов (*L – M – R*) и отражателя *Re* следует выбрать из рис. 4.5 и 4.6 в соответствии со своим вариантом, представленным в таблице. Крайний правый столбец этой таблицы показывает, на какое число шагов (букв, *i*) перемещается соответствующий ротор при зашифровании одного (текущего) символа; число 0 означает перемещение соответствующего ротора на один шаг при условии, что расположенный правее ротор совершит один оборот.

***Код реализации:***

|  |
| --- |
| class Enigma  {  private const string alphabet = "ABCDEFGHIJKLMNOPQRSTUVWXYZ";      private string rotorVconf = "VZBRGITYUPSDNHLXAWMJQOFECK";  private string rotorBetaconf = "LEYJVCNIXWPBQMDRTAKZFGUHOS";  private string rotorGammaconf = "FSOKANUERHMBTIYCWLQPZXVGJD";  private const string reflectorBDUNNconf = "AEBNCKDQFUGYHWIJLOMPRXSZTV";  private int settingL = 0;  private int settingM = 0;  private int settingR = 0;    public Dictionary<char, char> useReflector { get; set; }  Dictionary<char,char> GetReflector(string nameReflector)  {  Dictionary<char, char> result = new Dictionary<char, char>();  for (int i = 0; i < nameReflector.Length; i += 2)  {  result.Add(nameReflector[i], nameReflector[i + 1]);  result.Add(nameReflector[i+1], nameReflector[i]);  }  return result;  }  Dictionary<int, char> GetDictionary(string param)  {  Dictionary<int, char> result = new Dictionary<int, char>();  for (int i = 0; i < param.Length; i++)  {  result.Add(i, param[i]);  }  return result;  }  public char Encript(char charForEncrypt)  {  char resultChar= ' ';  Dictionary<int, char> lRotor = GetDictionary(rotorBetaconf),  mRotor = GetDictionary(rotorGammaconf) ,  rRotor = GetDictionary(rotorVconf),  alphabetDictionary = GetDictionary(alphabet);  Dictionary<char, char> useReflector = GetReflector(reflectorBDUNNconf);  bool circleM = false;  int numberChar = alphabetDictionary.Where(v => v.Value == charForEncrypt).FirstOrDefault().Key;  forwardStepRotor(rRotor, alphabetDictionary, ref resultChar, ref numberChar);  Console.WriteLine($"Символ {charForEncrypt} после правого ротора {resultChar}");  forwardStepRotor(mRotor, alphabetDictionary, ref resultChar, ref numberChar);  Console.WriteLine($"Символ {charForEncrypt} после центрального ротора {resultChar}");  forwardStepRotor(lRotor, alphabetDictionary, ref resultChar, ref numberChar);  Console.WriteLine($"Символ {charForEncrypt} после левого ротора {resultChar}");  char t = useReflector.Where(k => k.Key == resultChar).FirstOrDefault().Value; ;  if (char.IsLetter(t))  {  resultChar = t;  numberChar = alphabetDictionary.Where(v => v.Value == resultChar).FirstOrDefault().Key;  }  Console.WriteLine($"Символ {charForEncrypt} после рефлектора {resultChar}");  backStepRotor(lRotor, alphabetDictionary, ref resultChar, ref numberChar);  Console.WriteLine($"Символ {charForEncrypt} после левого ротора {resultChar}");  backStepRotor(mRotor, alphabetDictionary, ref resultChar, ref numberChar);  Console.WriteLine($"Символ {charForEncrypt} после центрального ротора {resultChar}");  backStepRotor(rRotor, alphabetDictionary, ref resultChar, ref numberChar);  Console.WriteLine($"Символ {charForEncrypt} после правого ротора {resultChar}");    if (settingR % 26 != 0 || settingR == 0)  {  settingR += 2;  updateSettingRotor(ref rotorVconf, 2);  }  else if(settingR % 26 == 1)  {  settingR = 0;  settingR += 2;  updateSettingRotor(ref rotorVconf, 2);  }  if (settingM % 26 != 0 || settingM == 0)  {  settingM += 2;  updateSettingRotor(ref rotorGammaconf, 2);  }  else if (settingM % 26 == 1)  {  settingM = 0;  settingM += 2;  updateSettingRotor(ref rotorGammaconf, 2);  if(settingL % 26 == 0)  {  settingL += 1;  updateSettingRotor(ref rotorBetaconf, 1);  }  else if (settingL % 26 == 1)  {  settingL = 0;  settingL += 1;  updateSettingRotor(ref rotorBetaconf, 1);  }  }  return resultChar;  }  void updateSettingRotor(ref string rotor, int step)  {  string removeChar = "";  for (int i = 0; i < step; i++)  removeChar += rotor[i];  rotor = rotor.Remove(0, step);  rotor += removeChar;  }  void forwardStepRotor(Dictionary<int, char> rotor, Dictionary<int, char> alph, ref char character, ref int numberChar)  {  int num = numberChar;  character = rotor.Where(k => k.Key == num).FirstOrDefault().Value;  char s = character;  numberChar = alph.Where(v => v.Value == s).FirstOrDefault().Key;  }  void backStepRotor(Dictionary<int, char> rotor, Dictionary<int, char> alph, ref char character, ref int numberChar)  {  char s = character;  numberChar = rotor.Where(v => v.Value == s).FirstOrDefault().Key;  int num = numberChar;  character = alph.Where(k => k.Key == num).FirstOrDefault().Value;  }  } |

***Результат работы программы:***

|  |
| --- |
| Enter text:  SapeginaEkaterinaIgorevna  Encript  Symbol S after right rotor M  Symbol S after center rotor T  Symbol S after left rotor Z  Symbol S after reflector S  Symbol S after left rotor Z  Symbol S after center rotor U  Symbol S after right rotor I  Symbol A after right rotor B  Symbol A after center rotor K  Symbol A after left rotor P  Symbol A after reflector M  Symbol A after left rotor N  Symbol A after center rotor D  Symbol A after right rotor J  Symbol P after right rotor J  Symbol P after center rotor I  Symbol P after left rotor X  Symbol P after reflector R  Symbol P after left rotor P  Symbol P after center rotor P  Symbol P after right rotor F  Symbol E after right rotor S  Symbol E after center rotor J  Symbol E after left rotor W  Symbol E after reflector H  Symbol E after left rotor X  Symbol E after center rotor P  Symbol E after right rotor D  Symbol G after right rotor L  Symbol G after center rotor P  Symbol G after left rotor R  Symbol G after reflector X  Symbol G after left rotor I  Symbol G after center rotor F  Symbol G after right rotor O  Symbol I after right rotor M  Symbol I after center rotor V  Symbol I after left rotor G  Symbol I after reflector Y  Symbol I after left rotor C  Symbol I after center rotor F  Symbol I after right rotor M  Symbol N after right rotor K  Symbol N after center rotor V  Symbol N after left rotor G  Symbol N after reflector Y  Symbol N after left rotor C  Symbol N after center rotor D  Symbol N after right rotor Z  Symbol A after right rotor L  Symbol A after center rotor D  Symbol A after left rotor J  Symbol A after reflector I  Symbol A after left rotor H  Symbol A after center rotor V  Symbol A after right rotor M  Symbol E after right rotor Q  Symbol E after center rotor U  Symbol E after left rotor F  Symbol E after reflector U  Symbol E after left rotor W  Symbol E after center rotor A  Symbol E after right rotor A  Symbol K after right rotor B  Symbol K after center rotor P  Symbol K after left rotor R  Symbol K after reflector X  Symbol K after left rotor I  Symbol K after center rotor V  Symbol K after right rotor I  Symbol A after right rotor Q  Symbol A after center rotor M  Symbol A after left rotor Q  Symbol A after reflector D  Symbol A after left rotor O  Symbol A after center rotor I  Symbol A after right rotor L  Symbol T after right rotor X  Symbol T after center rotor P  Symbol T after left rotor R  Symbol T after reflector X  Symbol T after left rotor I  Symbol T after center rotor R  Symbol T after right rotor H  Symbol E after right rotor B  Symbol E after center rotor D  Symbol E after left rotor J  Symbol E after reflector I  Symbol E after left rotor H  Symbol E after center rotor L  Symbol E after right rotor Q  Symbol R after right rotor W  Symbol R after center rotor V  Symbol R after left rotor G  Symbol R after reflector Y  Symbol R after left rotor C  Symbol R after center rotor P  Symbol R after right rotor J  Symbol I after right rotor U  Symbol I after center rotor Z  Symbol I after left rotor S  Symbol I after reflector Z  Symbol I after left rotor T  Symbol I after center rotor M  Symbol I after right rotor S  Symbol N after right rotor H  Symbol N after center rotor E  Symbol N after left rotor V  Symbol N after reflector T  Symbol N after left rotor Q  Symbol N after center rotor S  Symbol N after right rotor K  Symbol A after right rotor V  Symbol A after center rotor X  Symbol A after left rotor H  Symbol A after reflector W  Symbol A after left rotor J  Symbol A after center rotor Y  Symbol A after right rotor H  Symbol I after right rotor U  Symbol I after center rotor Z  Symbol I after left rotor S  Symbol I after reflector Z  Symbol I after left rotor T  Symbol I after center rotor M  Symbol I after right rotor S  Symbol G after right rotor T  Symbol G after center rotor P  Symbol G after left rotor R  Symbol G after reflector X  Symbol G after left rotor I  Symbol G after center rotor N  Symbol G after right rotor M  Symbol O after right rotor L  Symbol O after center rotor B  Symbol O after left rotor E  Symbol O after reflector A  Symbol O after left rotor R  Symbol O after center rotor I  Symbol O after right rotor F  Symbol R after right rotor W  Symbol R after center rotor V  Symbol R after left rotor G  Symbol R after reflector Y  Symbol R after left rotor C  Symbol R after center rotor P  Symbol R after right rotor J  Symbol E after right rotor G  Symbol E after center rotor U  Symbol E after left rotor F  Symbol E after reflector U  Symbol E after left rotor W  Symbol E after center rotor Q  Symbol E after right rotor U  Symbol V after right rotor O  Symbol V after center rotor Y  Symbol V after left rotor O  Symbol V after reflector L  Symbol V after left rotor A  Symbol V after center rotor E  Symbol V after right rotor X  Symbol N after right rotor H  Symbol N after center rotor E  Symbol N after left rotor V  Symbol N after reflector T  Symbol N after left rotor Q  Symbol N after center rotor S  Symbol N after right rotor K  Symbol A after right rotor V  Symbol A after center rotor X  Symbol A after left rotor H  Symbol A after reflector W  Symbol A after left rotor J  Symbol A after center rotor Y  Symbol A after right rotor H  Encript result: IJFDOMZMAILHQJSKHSMFJUXKH  Decript  Symbol I after right rotor U  Symbol I after center rotor Z  Symbol I after left rotor S  Symbol I after reflector Z  Symbol I after left rotor T  Symbol I after center rotor M  Symbol I after right rotor S  Symbol J after right rotor D  Symbol J after center rotor N  Symbol J after left rotor M  Symbol J after reflector P  Symbol J after left rotor K  Symbol J after center rotor B  Symbol J after right rotor A  Symbol F after right rotor P  Symbol F after center rotor P  Symbol F after left rotor R  Symbol F after reflector X  Symbol F after left rotor I  Symbol F after center rotor J  Symbol F after right rotor P  Symbol D after right rotor P  Symbol D after center rotor X  Symbol D after left rotor H  Symbol D after reflector W  Symbol D after left rotor J  Symbol D after center rotor S  Symbol D after right rotor E  Symbol O after right rotor F  Symbol O after center rotor I  Symbol O after left rotor X  Symbol O after reflector R  Symbol O after left rotor P  Symbol O after center rotor L  Symbol O after right rotor G  Symbol M after right rotor F  Symbol M after center rotor C  Symbol M after left rotor Y  Symbol M after reflector G  Symbol M after left rotor V  Symbol M after center rotor M  Symbol M after right rotor I  Symbol Z after right rotor D  Symbol Z after center rotor C  Symbol Z after left rotor Y  Symbol Z after reflector G  Symbol Z after left rotor V  Symbol Z after center rotor K  Symbol Z after right rotor N  Symbol M after right rotor V  Symbol M after center rotor H  Symbol M after left rotor I  Symbol M after reflector J  Symbol M after left rotor D  Symbol M after center rotor L  Symbol M after right rotor A  Symbol A after right rotor A  Symbol A after center rotor W  Symbol A after left rotor U  Symbol A after reflector F  Symbol A after left rotor U  Symbol A after center rotor Q  Symbol A after right rotor E  Symbol I after right rotor V  Symbol I after center rotor I  Symbol I after left rotor X  Symbol I after reflector R  Symbol I after left rotor P  Symbol I after center rotor B  Symbol I after right rotor K  Symbol L after right rotor I  Symbol L after center rotor O  Symbol L after left rotor D  Symbol L after reflector Q  Symbol L after left rotor M  Symbol L after center rotor Q  Symbol L after right rotor A  Symbol H after right rotor R  Symbol H after center rotor I  Symbol H after left rotor X  Symbol H after reflector R  Symbol H after left rotor P  Symbol H after center rotor X  Symbol H after right rotor T  Symbol Q after right rotor L  Symbol Q after center rotor H  Symbol Q after left rotor I  Symbol Q after reflector J  Symbol Q after left rotor D  Symbol Q after center rotor B  Symbol Q after right rotor E  Symbol J after right rotor P  Symbol J after center rotor C  Symbol J after left rotor Y  Symbol J after reflector G  Symbol J after left rotor V  Symbol J after center rotor W  Symbol J after right rotor R  Symbol S after right rotor M  Symbol S after center rotor T  Symbol S after left rotor Z  Symbol S after reflector S  Symbol S after left rotor Z  Symbol S after center rotor U  Symbol S after right rotor I  Symbol K after right rotor S  Symbol K after center rotor Q  Symbol K after left rotor T  Symbol K after reflector V  Symbol K after left rotor E  Symbol K after center rotor H  Symbol K after right rotor N  Symbol H after right rotor Y  Symbol H after center rotor J  Symbol H after left rotor W  Symbol H after reflector H  Symbol H after left rotor X  Symbol H after center rotor V  Symbol H after right rotor A  Symbol S after right rotor M  Symbol S after center rotor T  Symbol S after left rotor Z  Symbol S after reflector S  Symbol S after left rotor Z  Symbol S after center rotor U  Symbol S after right rotor I  Symbol M after right rotor N  Symbol M after center rotor I  Symbol M after left rotor X  Symbol M after reflector R  Symbol M after left rotor P  Symbol M after center rotor T  Symbol M after right rotor G  Symbol F after right rotor I  Symbol F after center rotor R  Symbol F after left rotor A  Symbol F after reflector E  Symbol F after left rotor B  Symbol F after center rotor L  Symbol F after right rotor O  Symbol J after right rotor P  Symbol J after center rotor C  Symbol J after left rotor Y  Symbol J after reflector G  Symbol J after left rotor V  Symbol J after center rotor W  Symbol J after right rotor R  Symbol U after right rotor Q  Symbol U after center rotor W  Symbol U after left rotor U  Symbol U after reflector F  Symbol U after left rotor U  Symbol U after center rotor G  Symbol U after right rotor E  Symbol X after right rotor E  Symbol X after center rotor A  Symbol X after left rotor L  Symbol X after reflector O  Symbol X after left rotor Y  Symbol X after center rotor O  Symbol X after right rotor V  Symbol K after right rotor S  Symbol K after center rotor Q  Symbol K after left rotor T  Symbol K after reflector V  Symbol K after left rotor E  Symbol K after center rotor H  Symbol K after right rotor N  Symbol H after right rotor Y  Symbol H after center rotor J  Symbol H after left rotor W  Symbol H after reflector H  Symbol H after left rotor X  Symbol H after center rotor V  Symbol H after right rotor A  Decript result: SAPEGINAEKATERINAIGOREVNA |