Program

• Write a Program to do Encryption and Decryption using Vigenere Cipher. 2. Do the Cryptanalysis of Vigenere Cipher (Use sufficiently large Cipher Text). Use Index of Coincidence to verify the guessed Key Length. Use Mutual Index of Coincidence to guess the Key.

• Code:

```
import java.util.Arrays;
public class VigenereCipher
  public String generateNewKey(String plainText, String key)
     char[] newKey = new char[plainText.length()];
     for(int i = 0, j = 0; i < plainText.length(); i += 1, j += 1)
       if(j == key.length())
         i = 0;
       newKey[i] = key.charAt(j);
     return String.valueOf(newKey);
   }
  public String encryption(String plainText, String newKey)
     char[] cipherText = new char[plainText.length()];
     for(int i = 0; i < plainText.length(); i++)
       cipherText[i] = (char)(((int)plainText.charAt(i) +
(int)newKey.charAt(i)) % 26) + 'A');
     return String.valueOf(cipherText);
   }
```

```
public String decryption(String cipherText,String newKey)
         {
               char[] plainText = new char[cipherText.length()];
               for(int i = 0; i < cipherText.length(); i++)
                        plainText[i] = (char)((((int)cipherText.charAt(i) -
(int)newKey.charAt(i) + 26) % 26) + 'A');
               return String.valueOf(plainText);
         }
        public void cryptanalysis()
               double
english_freq[] = \{8.167, 1.492, 2.782, 4.253, 12.702, 2.228, 2.015, 6.094, 6.996, 0.123, 12.702, 2.228, 2.015, 6.094, 6.996, 0.123, 12.702, 2.228, 2.015, 6.094, 6.996, 0.123, 12.702, 2.228, 2.015, 6.094, 6.996, 0.123, 12.702, 2.228, 2.015, 6.094, 6.996, 0.123, 12.702, 2.228, 2.015, 6.094, 6.996, 0.123, 12.702, 2.228, 2.015, 6.094, 6.996, 0.123, 12.702, 2.228, 2.015, 6.094, 6.996, 0.123, 12.702, 2.228, 2.015, 6.094, 6.996, 0.123, 12.702, 2.228, 2.015, 6.094, 6.996, 0.123, 12.702, 2.228, 2.015, 6.094, 6.996, 0.123, 12.702, 2.228, 2.015, 6.094, 6.996, 0.123, 12.702, 2.228, 2.015, 6.094, 6.996, 0.123, 12.702, 2.228, 2.015, 6.094, 6.996, 0.123, 12.702, 2.228, 2.015, 6.094, 6.996, 0.123, 12.702, 2.228, 2.015, 6.094, 6.996, 0.123, 12.702, 2.228, 2.015, 6.094, 6.996, 0.123, 12.702, 2.228, 2.015, 6.094, 6.996, 0.123, 12.702, 2.228, 2.015, 0.123, 12.702, 2.228, 2.015, 0.123, 12.702, 2.228, 2.015, 0.123, 12.702, 2.228, 2.015, 0.123, 12.702, 2.228, 2.015, 0.123, 12.702, 2.228, 2.015, 0.123, 12.702, 2.228, 2.015, 0.123, 12.702, 2.228, 2.015, 0.123, 12.702, 2.228, 2.015, 0.123, 12.702, 2.228, 2.015, 0.123, 12.702, 2.228, 2.015, 0.123, 12.702, 2.228, 2.015, 0.123, 12.702, 2.228, 2.015, 0.123, 12.702, 2.228, 2.015, 0.123, 12.702, 2.228, 2.015, 0.123, 12.702, 2.228, 2.015, 0.123, 12.702, 2.228, 2.015, 0.123, 12.702, 2.228, 2.015, 0.123, 12.702, 2.228, 2.015, 0.123, 12.702, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 2.228, 
153,0.772,4.025,2.406,6.749,7.507,1.929,0.095,5.987,6.327,9.056,2.758,0.9
78,2.360,0.150,1.974,0.074};
               double[] p = new double[26];
               for(int i = 0; i < 26; i++)
                       p[i] = english_freq[i] / 100;
                }
               //char
Y1[]={'C','T','L','S','S','Y','N','Z','I','R','I','Y','M','O','R','T','T','I','N','E','O','E','T
'};
                  //char
Y1[]={'R','A','Y','T','T','O','A','I','N','M','O','S','S','R','T','U','H','D','A','C','F','S',
'E'};
               // char
Y1[]={'Y','N','S','H','U','F','L','N','F','A','N','T','I','D','O','D','E','D','S','T','T','Y','
M'
                  char
Y1[]={'P','A','I','E','D','A','Y','G','O','T','S','E','N','E','S','Y','H','E','P','S','H','S','
S'};
               int[] freq = new int[26];
```

```
Arrays.fill(freq, 0);
    double[] q = new double[26];
    for(int i = 0; i < Y1.length; i++)
       freq[Y1[i] - 65] = freq[Y1[i] - 65] + 1;
    }
    for(int i = 0; i < 26; i++)
      q[i] = (double)(freq[i]) / Y1.length;
    }
    int a = 65;
    for(int k = 0; k < 26; k++)
       double sum = 0.0;
       for(int i = 0; i < 26; i++)
         sum = sum + (p[i] * q[(i + k) % 26]);
       System.out.println("Sum = "+sum+" and k = "+k+"["+(char)a+"]");
       a += 1;
    }
  public static void main(String[] args)
    VigenereCipher vc = new VigenereCipher();
    String plainText =
"CRYPTANALYSISTHESTUDYOFANALYZINGINFORMATIONSYST
EMSINORDERTOSTUDYTHEHIDDENASPECTSOFTHESYSTEMS";
    String key = "LION";
    System.out.println("Your plain texts are: "+plainText);
    String newKey = vc.generateNewKey(plainText, key);
```

```
System.out.println("New generated key is: "+newKey);

String cipherText = vc.encryption(plainText, newKey);

System.out.println("Encrypted string is: "+cipherText);

System.out.println("Decrypted string is: "+vc.decryption(cipherText, newKey));

System.out.println("Performing Cryptanalysis...");

vc.cryptanalysis();

}
```

• **Output 1:**

```
::\Jeet\D2D\Sem 6\NIS\Labs\Lab 3>java VigenereCipher
our plain texts are: CRYPTANALYSISTHESTUDYOFANALYZINGINFORMATIONSYSTEMSINORDERTOSTUDYTHEHIDDENASPECTSOFTHESYSTEMS/
Encrypted sting is: NZMCEIBNWGGVDBVRDBIQJWTNYIZLKQBTTVTBCUOGTWBFJAHRXAWAZZRRCBCFECRLEPSUTLRRYIGCPKHFZNHUPAMFEMAF
Decrypted string is: CRYPTANALYSISTHESTUDYOFANALYZINGINFORMATIONSYSTEMSINORDERTOSTUDYTHEHIDDENASPECTSOFTHESYSTEMS
Performing Cryptanalysis..
Sum = 0.06477869565217392 and k = 0[A]
Sum = 0.03962304347826087 and k = 1[B]
Sum = 0.028882173913043478 and k = 2[C]
form = 0.02176217391304348 and form = 3[D]
5um = 0.04959826086956522 and k = 4[E]
Sum = 0.0455095652173913 and k = 5[F]
Sum = 0.04636739130434782 and k = 6[G]
Sum = 0.03235695652173914 and k =
Sum = 0.03545521739130434 and k
                                                  Cryptanalysis for Group 1
Sum = 0.030203478260869568 and k = 9[J]
Sum = 0.04334086956521739 and k = 10[K]
6um = 0.04934130434782608 and k = 11[L]
Sum = 0.03523521739130434 and k
   = 0.03764304347826087 and k
um = 0.03607304347826087 and k = 14[0]
Sum = 0.047972608695652175 and k = 15[P]
Sum = 0.03638782608695652 and k = 16[Q]
Sum = 0.04081304347826087 and k = 17[R]
Sum = 0.024753478260869568 and k = 18[S]
Sum = 0.03481739130434782 and k = 19[T]
Sum = 0.04312130434782609 and k =
5um = 0.04244304347826087 and k = 
   = 0.029117391304347828 and k =
   = 0.030769130434782608 and k =
   = 0.035964347826086956 and k
   = 0.03795999999999994 and k
```

• Output 2:

```
:\Jeet\D2D\Sem 6\NIS\Labs\Lab 3>java VigenereCipher
our plain texts are: CRYPTANALYSISTHESTUDYOFANALYZINGINFORMATIONSYSTEMSINORDERTOSTUDYTHEHIDDENASPECTSOF<u>THESYSTEMS</u>
Encrypted sting is:
                   NZMCEIBNWGGVDBVRDBIQJWTNYIZLKQBTTVTBCUOGTWBFJAHRXAWAZZRRCBCFECRLEPSUTLRRYIGCPKHFZNHUPAMFEMAF
Decrypted string is: CRYPTANALYSISTHESTUDYOFANALYZINGINFORMATIONSYSTEMSINORDERTOSTUDYTHEHIDDENASPECTSOFTHESYSTEMS
Performing Cryptanalysis..
Sum = 0.06477869565217392 and k = 0[A]
Sum = 0.03962304347826087 and k = 1[B]
Sum = 0.028882173913043478 and k = 2[C]
Sum = 0.02176217391304348 and k = 3[D]
Sum = 0.04959826086956522 and k = 4[E]
Sum = 0.0455095652173913 and k = 5[F]
Sum = 0.04636739130434782 and k = 6[G]
Sum = 0.03235695652173914 and k
                                             Cryptanalysis for Group 1
5um = 0.03545521739130434 and k
Sum = 0.030203478260869568 and k = 9[J]
Sum = 0.04334086956521739 and k = 10[K]
Sum = 0.04934130434782608 and k
                              11[L]
Sum = 0.03523521739130434 and k = 12[M]
Sum = 0.03764304347826087 and k
                            = 13[N]
Sum = 0.03607304347826087 and k = 14[0]
Sum = 0.047972608695652175 and k = 15[P]
Sum = 0.03638782608695652 and k = 16[Q]
Sum = 0.04081304347826087 and k = 17[R]
sum = 0.024753478260869568 and k = 18[S]
  = 0.03481739130434782 and k = 19[T]
Sum = 0.04312130434782609 and k =
                              20[U]
Sum = 0.04244304347826087 and k = 21[V]
Sum = 0.029117391304347828 and k = 22[W]
Sum = 0.030769130434782608 and k = 23[X]
Sum = 0.035964347826086956 and k = 24[Y]
```

• Output 3:

```
:\Jeet\D2D\Sem 6\NIS\Labs\Lab 3>java VigenereCipher
our plain texts are: CRYPTANALYSISTHESTUDYOFANALYZINGINFORMATIONSYSTEMSINORDERTOSTUDYTHEHIDDENASPECTSOFTHESYSTEMS
Encrypted sting is: NZMCEIBNWGGVDBVRDBIQJWTNYIZLKQBTTVTBCUOGTWBFJAHRXAWAZZRRCBCFECRLEPSUTLRRYIGCPKHFZNHUPAMFEMAF
Decrypted string is: CRYPTANALYSISTHESTUDYOFANALYZINGINFORMATIONSYSTEMSINORDERTOSTUDYTHEHIDDENASPECTSOFTHESYSTEMS
Performing Cryptanalysis..
Sum = 0.05734217391304347 and k = 0[A]
Sum = 0.045765652173913034 and k = 1[B]
Sum = 0.02895 and k = 2[C]
Sum = 0.031396956521739135 and k = 3[D]
Sum = 0.031052608695652174 and k = 4[E]
Sum = 0.05028391304347826 and k = 5[F]
Sum = 0.03667173913043477 and k = 6[G]
                                                  Cryptanalysis of Grop 3
Sum = 0.03954478260869565 and k = 0.03954478260869565
Sum = 0.03473086956521739 and k = 9[\bar{J}]
Sum = 0.04090130434782609 and k
Sum = 0.04655521739130434 and k
Sum = 0.04472347826086956 and k = 12[M]
6um = 0.03569434782608695 and k
                               = 13[N]
Sum = 0.03401565217391304 and k = 14[0]
Sum = 0.04421739130434782 and k
                               = 15[P]
Sum = 0.04151173913043477 and k
Sum = 0.03215347826086956 and k
Sum = 0.03553434782608695 and k
Sum = 0.03561521739130434 and k
Sum = 0.04588391304347825 and k
                                 20[U]
Sum = 0.03608217391304348 and k = 21[V]
Sum = 0.03640739130434782 and k = 22[W]
Sum = 0.027416956521739137 and k = 23[X]
Sum = 0.03125043478260869 and k = 24[Y]
Sum = 0.04961826086956521 and k = 25[Z]
```

• Output4:

```
::\Jeet\D2D\Sem 6\NIS\Labs\Lab 3>java VigenereCipher
our plain texts are: CRYPTANALYSISTHESTUDYOFANALYZINGINFORMATIONSYSTEMSINORDERTOSTUDYTHEHIDDENASPECTSOFTHESYSTEMS/
Encrypted sting is: NZMCEIBNWGGVDBVRDBIQJWTNYIZLKQBTTVTBCUOGTWBFJAHRXAWAZZRRCBCFECRLEPSUTLRRYIGCPKHFZNHUPAMFEMAF
Decrypted string is: CRYPTANALYSISTHESTUDYOFANALYZINGINFORMATIONSYSTEMSINORDERTOSTUDYTHEHIDDENASPECTSOFTHESYSTEMS
Performing Cryptanalysis..
Sum = 0.06754217391304349 and k = 0[A]
Sum = 0.04044565217391304 and k = 1[B]
Sum = 0.02906608695652174 and k = 2[C]
Sum = 0.02940217391304348 and k = 3[D]
Sum = 0.050176956521739126 and k = 4[E]
Sum = 0.036344347826086955 and k = 5[f]
Sum = 0.03144521739130435 and k = 6[G]
Sum = 0.04155565217391304 and k = 7[H]
Sum = 0.025159565217391305 and k = 8[I]
                                                Cryptanalysis of Grop 4
Sum = 0.020509130434782613 and k = 9[J]
Sum = 0.04194347826086957 and k = 10[K]
Sum = 0.05898260869565217 and k = 11[L]
Sum = 0.03788869565217391 and k = 12[M
Sum = 0.038921304347826084 and k = 13[N]
Sum = 0.04905434782608694 and k = 14[0]
Sum = 0.04505434782608695 and k = 15[P]
Sum = 0.039627826086956516 and k = 16[0]
Sum = 0.029000869565217385 and k = 17[R]
Sum = 0.03873739130434783 and k = 18[S]
Sum = 0.03226130434782609 and k = 19[T]
Sum = 0.034695652173913044 and k = 20[U]
Sum = 0.02599086956521739 and k = 21[V]
Sum = 0.051586956521739134 and k = 22[W]
Sum = 0.03025608695652174 and k = 23[X]
Sum = 0.03001130434782609 and k = 24[Y]
```