SEMESTER LAB EXAMINATION

REG NUM: 312217104133

NAME: SAADHANA LAKSHMI NARASIMHAN

CLASS: 4TH YEAR CSE-C

SUBJECT CODE: IT8761

SUBJECT NAME: SECURITY LABORATORY

DATE: 18/12/2020

SESSION: AFTERNOON

DATE: 18/II/2020

SESSION: AN.

REG: 312217104133

NAME: SAADHANA LAKSHMI NARASIMHAN

CLASS: 4th YEAR CSE-C

SUBJECT CODE: IT8761

SUBJECT NAME: SECURITY LABORATORY

AIM: To develop a java program to implement vigenere matrix and decryption.

ALGORITHM:

1) Display Matrix

```
(1.1) For i from 0 to 25 do 1.2
(1.2)     print all letters from 'A' to 'Z' rotated left by row
          number i.
(1.3) Display 26 × 26 matrix of characters.
```

$$\begin{array}{c|cccccccccccccccccccccccccc}
0 & A & B & C & D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\
1 & B & C & D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z & A \\
2 & & & & & & & & & & & & & & & & & & & & & & & & & & \\
3 & & & & & & & \vdots & & & & & & & & \vdots & & & & & & & & & & & \\
\vdots & & & & & & & \vdots & & & & & & & & \vdots & & & & & & & & & & & \\
25 & Z & A & B & C & D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y
\end{array}$$

2) DECRYPTION OF VIGENERE

(2.1) Accept cipher text, verify if it has only letters.

(2.2) Accept key, verify if it has only letters.

(2.3) Repeat key until length of cipher text.

(2.4) Do steps 2.5-2.7 until length of cipher text.

(2.5) Row index is key character

(2.6) Find cipher text character in this row.

(2.7) Append column index to result.

(2.8) Return cipher text.

METHODS USED:

① Constructor to generate matrix. (26 × 26).

→ This each row has letters from A to Z.

→ Each successive rows is left shifted by 1 character.

② Int keyVerify

- returns 1 if key has only letters

0 otherwise.

③ int cipherVerify:

- returns 1 if cipher has only characters and spaces

- 0 otherwise.

(4) String decrypt.

- for each character of cipher text, find corresponding plaintext character from matrix.
- return result.

CODE

```
import java.util.*;
class VigenereEval{
  char key[][];
  public VigenereEval()
  {
    key=new char[26][26];
    for(int i=0;i<26;i++)
    {
      for(int j=0;j<26;j++)
      {
        key[i][j]=(char)((i+j)%26+'A');

      }
    }
    System.out.println("MATRIX FOR VIGENERE");
    for(int i=0;i<26;i++)
    {
      for(int j=0;j<26;j++)
        System.out.print(key[i][j]+" ");
        System.out.println();
    }
  }

  int keyVerify(String k)
  {
      for(int i=0;i<k.length();i++)
        if(!Character.isLetter(k.charAt(i)))
        {
            System.out.println("Invalid characters in key");
            return 0;
        }
      return 1;
  }

  int cipherVerify(String cipher)
  {
      for(int i=0;i<cipher.length();i++)
```

```
if(!Character.isLetter(cipher.charAt(i))&&cipher.charAt(i)!=
' ')
        {
            System.out.println("Invalid characters in cipher
text");
            return 0;
        }
      return 1;
  }

  String decrypt(String cipher,String k)
  {

    StringBuilder res=new StringBuilder();
    k=k.toUpperCase();
    cipher=cipher.toUpperCase();
    String temp=k;
      while(k.length()<cipher.length())
          k=k+temp;
        k=k.substring(0,cipher.length());

         for(int  j=0;j<cipher.length();j++)
        {
          if(cipher.charAt(j)==' ')
            res.append(' ');
          else
if(cipher.charAt(j)>='A'&&cipher.charAt(j)<='Z')
          {  for(int i=0;i<26;i++)
              {
                if(key[k.charAt(j)-
'A'][i]==cipher.charAt(j))
                {
                  res.append((char)(i+'A'));
                  break;
                }
              }
          }
  }
  return res.toString();
}
}
public class Main{
  public static void main(String args[])
  {
    VigenereEval eval=new VigenereEval();
    Scanner stdin=new Scanner(System.in);
    String key,cipher;
    System.out.println("\nEnter key consisting only of
letters: ");
    key=stdin.nextLine();
    while(eval.keyVerify(key)==0)
    {
      System.out.println("\nEnter key consisting only of
letters: ");
      key=stdin.nextLine();
    }
    System.out.println("Enter cipher text consisting only of
letters or space: ");
    cipher=stdin.nextLine();
    while(eval.cipherVerify(cipher)==0)
    {
      System.out.println("\nEnter cipher consisting only of
letters or space: ");
      cipher=stdin.nextLine();
    }
    String res=eval.decrypt(cipher,key);
    if(res!=null)
    {
      System.out.println("DECRYPTED MESSAGE:  "+res);
      if(res.contains(" "))
      {
        System.out.println("DECRYPTED MESSAGE WITHOUT
SPACES:  "+res.replace(" ",""));
      }
    }
  }
```

```
}
```

OUTPUT

```
java -classpath .:/run_dir/junit-4.12.jar:target/dependency/* Main

MATRIX FOR VIGENERE

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

B C D E F G H I J K L M N O P Q R S T U V W X Y Z A

C D E F G H I J K L M N O P Q R S T U V W X Y Z A B

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

E F G H I J K L M N O P Q R S T U V W X Y Z A B C D

F G H I J K L M N O P Q R S T U V W X Y Z A B C D E

G H I J K L M N O P Q R S T U V W X Y Z A B C D E F

H I J K L M N O P Q R S T U V W X Y Z A B C D E F G

I J K L M N O P Q R S T U V W X Y Z A B C D E F G H

J K L M N O P Q R S T U V W X Y Z A B C D E F G H I

K L M N O P Q R S T U V W X Y Z A B C D E F G H I J

L M N O P Q R S T U V W X Y Z A B C D E F G H I J K

M N O P Q R S T U V W X Y Z A B C D E F G H I J K L

N O P Q R S T U V W X Y Z A B C D E F G H I J K L M

O P Q R S T U V W X Y Z A B C D E F G H I J K L M N

P Q R S T U V W X Y Z A B C D E F G H I J K L M N O

Q R S T U V W X Y Z A B C D E F G H I J K L M N O P

R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
```

```
S T U V W X Y Z A B C D E F G H I J K L M N O P Q R

T U V W X Y Z A B C D E F G H I J K L M N O P Q R S

U V W X Y Z A B C D E F G H I J K L M N O P Q R S T

V W X Y Z A B C D E F G H I J K L M N O P Q R S T U

W X Y Z A B C D E F G H I J K L M N O P Q R S T U V

X Y Z A B C D E F G H I J K L M N O P Q R S T U V W

Y Z A B C D E F G H I J K L M N O P Q R S T U V W X

Z A B C D E F G H I J K L M N O P Q R S T U V W X Y


Enter key consisting only of letters:

KEY

Enter cipher text consisting only of letters or space:

DIVDXM

DECRYPTED MESSAGE: TEXTTO
```

RESULT AND INFERENCE:

RESULT: vigenere matrix was displayed and decryption was performed.

INFERENCE:

1. Vigenere is a polyalphabetic stream cipher.
2. Decryption is performed by subtracting key value from cipher character.
3. Vigenere can be used only if text length is limited.
4. Same key has to be repeated throughout length of cipher text.
5. Formula for encryption: $C[i] = (P[i] + K[i]) \% 26$
6. Formula for decryption: $P[i] = (C[i] - K[i]) \% 26$.
7. This can be done using matrix look up.

SAMPLE I/O.

```
Key Matrix :   A B C . . . . .
               .
               .
               .
               .
               .
               Z A B C . . .

Enter Key   : KEY
Enter cipher: DIVDXM
PLAIN TEXT: TEXTTO.
```