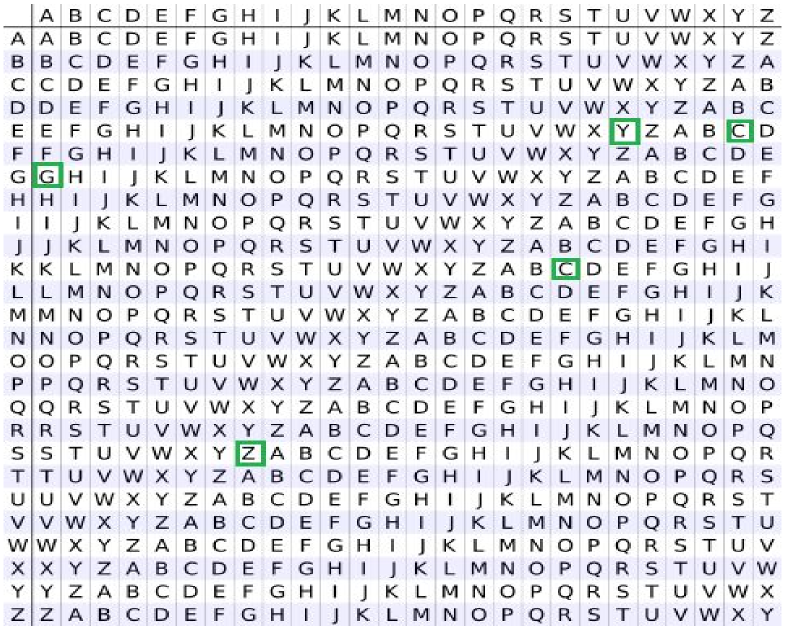
Experiment 4

Aim: Write a program to implement Polyalphabetic Cipher encryption-decryption.

Theory: In a polyalphabetic cipher, multiple cipher alphabets are used. To facilitate encryption, all the alphabets are usually written out in a large table, traditionally called a tableau. Usually the tableau is 26 × 26, so that 26 full ciphertext alphabets are available. The method of filling the tableau, and of choosing which alphabet to use next, defines the particular polyalphabetic cipher. All such ciphers are easier to break than were believed since the substitution alphabets are repeated for sufficiently large plaintexts. One of the most popular was that of Vigenere cipher.



	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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Source Code:

```
import java.util.*;
import java.util.Scanner;
public class polyalpha
{
static String generateKey(String str, String key)
{
   int x = str.length();
   for (int i = 0; ; i++)
   {
      if (x == i)
```

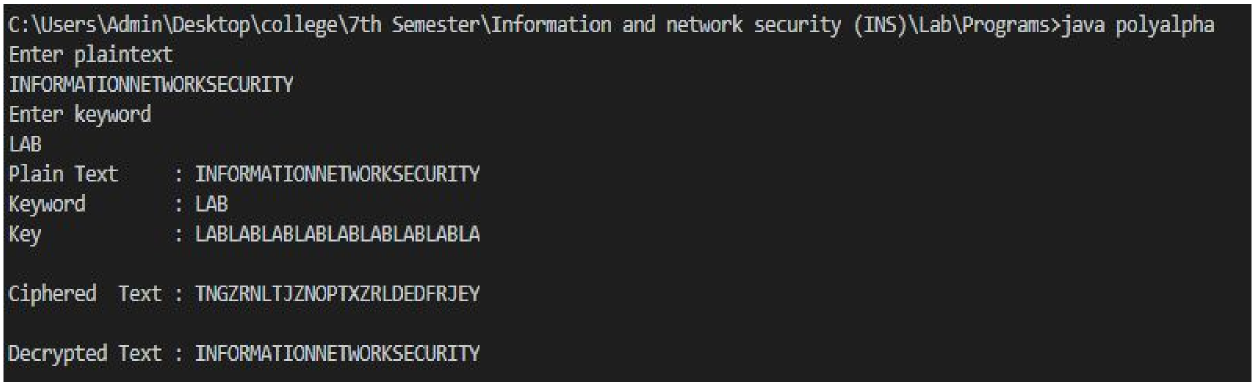
```
            i = 0;
        if (key.length() == str.length())
            break;
        key+=(key.charAt(i));
    }
    return key;
}

static String cipherText(String str, String key)
{
    String cipher_text="";
    for (int i = 0; i < str.length(); i++)
    {
        int x = (str.charAt(i) + key.charAt(i)) %26;
        x += 'A';
        cipher_text+=(char)(x);
    }
    return cipher_text;
}

static String originalText(String cipher_text, String key)
{
    String orig_text="";
    for (int i = 0 ; i < cipher_text.length() && i < key.length(); i++)
    {
        int x = (cipher_text.charAt(i) - key.charAt(i) + 26) %26;
        x += 'A';
        orig_text+=(char)(x);
    }
    return orig_text;
}

public static void main(String[] args)
    {
    final Scanner sc = new Scanner(System.in);
    System.out.println("Enter plaintext");
    final String str = sc.nextLine();
    System.out.println("Enter keyword");
    final String keyword = sc.nextLine();
    String key = generateKey(str, keyword);
    String cipher_text = cipherText(str, key);
    System.out.println("Ciphertext : " + cipher_text + "\n");
    System.out.println("Decrypted Text : " + originalText(cipher_text, key));
    sc.close();
    }
}
```

Output:



```
C:\Users\Admin\Desktop\college\7th Semester\Information and network security (INS)\Lab\Programs>java polyalpha
Enter plaintext
INFORMATIONNETWORKSECURITY
Enter keyword
LAB
Plain Text     : INFORMATIONNETWORKSECURITY
Keyword        : LAB
Key            : LABLABLABLABLABLABLABLABLA

Ciphered  Text : TNGZRNLTJZNOPTXZRLDEDFRJEY

Decrypted Text : INFORMATIONNETWORKSECURITY
```

Learning Outcomes:

The advantage of Polyalphabetic ciphers is that they make frequency analysis more difficult. For instance if P occurred most in a ciphertext whose plaintext is in English, one could suspect that P corresponded to E, because E is the most frequently used letter in English. Using the Polyalphabetic cipher, E can be enciphered as any of several letters in the alphabet in the cipher, thus defeating simple frequency analysis