Experiment 04

Aim: Write a program in Java or Python to perform Cryptanalysis or decoding Vigenere Cipher.

Roll No.	70
Name	Mayuri Shridatta Yerande
Class	D15-B
Subject	Internet Security Lab
LO Mapped	LO1: To apply the knowledge of symmetric cryptography to implement classical ciphers.

Aim: Write a program in Java or Python to perform Cryptanalysis or decoding of Vigenere cipher.

Theory:

Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the *Vigenère square or Vigenère table*.

- The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.
- At different points in the encryption process, the cipher uses a different alphabet from one of the rows.
- The alphabet used at each point depends on a repeating keyword.

Code:-

```
public class assign4
{
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;
```

```
}
static String LowerToUpper(String s)
{
StringBuffer str =new StringBuffer(s);
for(int i = 0; i < s.length(); i++)
{
if(Character.isLowerCase(s.charAt(i)))
{
str.setCharAt(i, Character.toUpperCase(s.charAt(i))); }
}
s = str.toString();
return s ;
}
public static void main(String[] args)
{
String Str = "Mayuri";
String Keyword = "vesit";
String str = LowerToUpper(Str);
String keyword = LowerToUpper(Keyword);
String key = generateKey(str, keyword);
String cipher_text = cipherText(str, key);
System.out.println("Ciphertext : " + cipher_text + "\n");
System.out.println("Original/Decrypted Text : " +
originalText(cipher_text, key));
}
}
```

Output :-

```
[Running] cd "c:\Users\mayuri\Downloads\" && javac assign4.java && java assign4
Ciphertext : HEQCKD

Original/Decrypted Text : MAYURI
```

Conclusion :- We learned about Vigenere cipher and programmed a java code to implement it.