Experiment 04

Write a program in Java or Python to perform Cryptanalysis or decoding of Vigenere Cipher

Roll No.	14
Name	Ishika Sanjay Devare
Class	D15-A
Subject	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

Introduction:

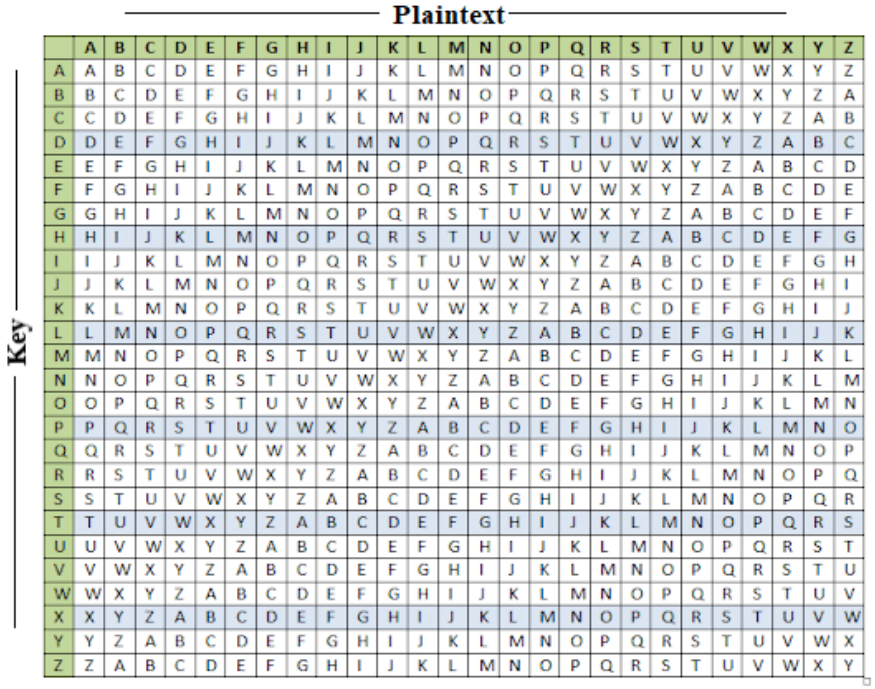
What is a Cipher?

In cryptography, a cipher (or cypher) is an algorithm for performing encryption or decryption—a series of well-defined steps that can be followed as a procedure.

What is Vigenere Cipher?

Method 1

When the vigenere table is given, the encryption and decryption are done using the vigenere table (26 * 26 matrix) in this method.



	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

Example: The plaintext is "JAVATPOINT", and the key is "BEST".

To generate a new key, the given key is repeated in a circular manner, as long as the length of the plain text does not equal the new key.

J	A	V	A	T	P	O	I	N	T
B	E	S	T	B	E	S	T	B	E

Encryption

The first letter of the plaintext is combined with the first letter of the key. The column of plain text "J" and row of key "B" intersect the alphabet of "K" in the vigenere table, so the first letter of ciphertext is "K".

Similarly, the second letter of the plaintext is combined with the second letter of the key. The column of plain text "A" and row of key "E" intersect the alphabet of "E" in the vigenere table, so the second letter of ciphertext is "E".

This process continues continuously until the plaintext is finished.

Ciphertext = KENTUTGBOX

Decryption

Decryption is done by the row of keys in the vigenere table. First, select the row of the key letter, find the ciphertext letter's position in that row, and then select the column label of the corresponding ciphertext as the plaintext.

K	E	N	T	U	T	G	B	O	X
B	E	S	T	B	E	S	T	B	E

For example, in the row of the key is "B" and the ciphertext is "K" and this ciphertext letter appears in the column "J", that means the first plaintext letter is "J".

Next, in the row of the key is "E" and the ciphertext is "E" and this ciphertext letter appears in the column "A", that means the second plaintext letter is "A".

This process continues continuously until the ciphertext is finished.

Plaintext = JAVATPOINT

Method 2

When the vigenere table is not given, the encryption and decryption are done by Vigenere algebraically formula in this method (convert the letters (A-Z) into the numbers (0-25)).

Formula of encryption is-

$$E_i = (P_i + K_i) \bmod 26$$

Formula of decryption is-

$D_i = (E_i - K_i) \bmod 26$

If any case (D_i) value becomes negative (-ve), in this case, we will add 26 in the negative value.

Where,

E denotes the encryption.

D denotes the decryption.

P denotes the plaintext.

K denotes the key.

Algorithm:

Step 1 : Read the plaintext from the user.

Step 2 : Read the key from the user.

Step 3 : The key will be repeated as many times as the length of the plaintext.

Step 4 : The plaintext is converted into cipher text using the values of plaintext and key .

Step 5 : The first letter of the plaintext is paired with the first letter of the key. Similarly, for the second letter of the plaintext, the second letter of the key is used and The rest of the plaintext is enciphered in a similar fashion.

Step 6 : The values of ciphertext are converted into the corresponding alphabets.

Step 6 : Display the obtained Cipher text.

Step 7 : Decryption is performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in this row, and then using the column's label as the plaintext.

Step 8 : Again display the plaintext which we obtain .

Code:

```
import java.util.Scanner;

public class VigenereCipher {
public static void main(String[] args) {
```

```
System.out.println("Vigenere Cipher\n");
Scanner in = new Scanner(System.in);

// Allow the user to choose if they want to encrypt or decrypt a message
System.out.println("Press 1 to encrypt a message\nPress 2 to decrypt a message");
int input = in.nextInt();

if (input == 1) {
System.out.print("Enter the key in UPPER Case: \n");
String key = in.next();
System.out.print("Enter the message that would like to be encrypted by Vigenere cipher:
\n");
String EMessage = in.next();
String encryptMessage = encrypt(EMessage, key);
System.out.println("The encrypted message is: \n" + encryptMessage);
}
else if (input == 2) {
System.out.print("Enter the key in UPPER Case: \n");
String key = in.next();
System.out.print("Enter the message that would like to be decrypted by Vigenere cipher:
\n");
String DMessage = in.next();
String decryptMessage = decrypt(DMessage, key);
System.out.println("The decrypted message is: \n" + decryptMessage);
}
else {
System.out.println("Wrong Input!");
}
in.close();
}

// Encryption
// Encryption Logic: Using ASCII Dec Representation:
// Example:
// ASCII: "H" is 72 && "S" is 83
// ((72-65) + (83-65)) % 26 + 65 >> Encrypted "Z"
public static String encrypt(String Message, String Key) {
String EMessage = "";
Message = Message.toUpperCase();
for (int i = 0, j = 0; i < Message.length(); i++) {
```

```
char letter = Message.charAt(i);
EMessage += (char)(((letter - 65) + (Key.charAt(j)-65)) % 26 + 65);
j = ++j % Key.length();
}
return EMessage;
}

// Decryption
// Decryption Logic: Using ASCII Dec Representation:
// Example:
// ASCII: "Z" is 90 && "S" is 83
// (90-83+26) % 26 + 65 >> Encrypted "Z"
public static String decrypt(String Message, String Key) {
String DMessage = "";
Message = Message.toUpperCase();
for (int i = 0, j = 0; i < Message.length(); i++) {
char letter = Message.charAt(i);
DMessage += (char)((letter - Key.charAt(j) + 26) % 26 + 65);
j = ++j % Key.length();
}
return DMessage;
}
}
```

Results:

```
java -cp /tmp/GZJoRCwviy VigenereCipher
Vigenere Cipher

Press 1 to encrypt a message
Press 2 to decrypt a message
1
Enter the key in UPPER Case:
BESTBEST
Enter the message that would like to be encrypted by Vigenere cipher:
HIGARVIT
The encrypted message is:
IMYTSZAM
```

```
java -cp /tmp/Y8ZQlxnRuH VigenereCipher
Vigenere Cipher
Press 1 to encrypt a message
Press 2 to decrypt a message
2
Enter the key in UPPER Case:
BESTBEST
Enter the message that would like to be decrypted by Vigenere cipher:
IMYTSZAM
The decrypted message is:
HIGARVIT
```

Conclusion: Hence, we successfully wrote a program in Java to perform Cryptanalysis or decoding of Vigenere Cipher.