

# Pandit Deendayal Energy University

## School of Technology

### Information Security Lab

#### B.Tech-Computer Science & Engineering (Sem-V)

PATEL VEDANT H.

19BCP138

DIVISION – 2

#### Lab 5 Assignment

❖ **Aim:** Study and Implement program for Vigenere Cipher.

❖ **Introduction:**

The Vigenère cipher is a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword (employs poly-alphabetic substitution). To encrypt, a table of alphabets can be used, termed a *Vigenère table*. It has the alphabet 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.

	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

Vigenère table

For example, suppose that the plaintext to be encrypted is ATTACKATDAWN. The person sending the message chooses a keyword and repeats it until it matches the length of the plaintext, for example, the keyword "LEMON". For successive letters of the message, successive letters of the key string will be taken and each message letter enciphered by using its corresponding key row. For example, the first letter of the plaintext, A, is paired with L, the first letter of the key. Similarly, for the second letter of the plaintext, the second letter of the key is used. The rest of the plaintext is enciphered in a similar fashion:

Plaintext: **ATTACKATDAWN**

Key: **LEMONLEMONLE**

Cipher-text: **LXFOPVEFRNHR**

Decryption is performed by going to the row in the table corresponding to the key, finding the position of the cipher text letter in that row and then using the column's label as the plaintext. For example, in row L (from LEMON), the cipher text L appears in column A, which is the first plaintext letter. Next, in row E (from LEMON), the cipher text X is located in column T. Thus T is the second plaintext letter.

## ❖ Program:

### ➤ Encrypt and Decrypt Python Program:

```
D:\Sem5\Information Security\Lab\Lab5\IS-lab-5-Encrypt-Decrypt.py
temp.py x IS-lab-5-Encrypt-Decrypt.py x
1  # -*- coding: utf-8 -*-
2  """
3  Created on Thu Sep  9 10:30:07 2021
4
5  @author: vedpa
6  """
7
8  def generateKey(string, key):
9      key = list(key)
10     if len(string) == len(key):
11         return(key)
12     else:
13         for i in range(len(string) - len(key)):
14             key.append(key[i % len(key)])
15     return("".join(key))
16
17 def encrypt(string, key):
18     encrypt_text = []
19     for i in range(len(string)):
20         x = (ord(string[i]) + ord(key[i])) % 26
21         x += ord('A')
22         encrypt_text.append(chr(x))
23     return("".join(encrypt_text))
24
25 def decrypt(encrypt_text, key):
26     decrypt_text = []
27     for i in range(len(encrypt_text)):
28         x = (ord(encrypt_text[i]) - ord(key[i]) + 26) % 26
29         x += ord('A')
30         decrypt_text.append(chr(x))
31     return("".join(decrypt_text))
32
33 # Driver code
34 if __name__ == "__main__":
35     string = input("Enter the text: ")
36     keyword = input("Enter a key: ")
37     key = generateKey(string, keyword)
38     encrypt_text = encrypt(string, key)
39     choice = int(input("Choose 1 to Encrypt and 2 to Decrypt(Vigenere Cipher)"))
40     if choice == 1:
41         print("\nEncrypted text is:", encrypt_text)
42     elif choice == 2:
43         print("\nDecrypted Message is:", decrypt(string, key))
44     else:
45         print("Please Enter A Valid Number")
46
```

## ➤ Encrypt and Decrypt Output:

```
Python 3.8.5 (default, Sep 3 2020, 21:29:08) [MSC v.1916 64 bit (AMD64)]
Type "copyright", "credits" or "license" for more information.

IPython 7.22.0 -- An enhanced Interactive Python.

In [1]: runfile('D:/Sem5/Information Security/Lab/Lab5/IS-lab-5-Encrypt-
Decrypt.py', wdir='D:/Sem5/Information Security/Lab/Lab5')

Enter the text: LAUGHTER

Enter a key: FUN

Choose 1 to Encrypt and 2 to Decrypt(Vigenere Cipher):1

Encrypted text is: QUHLBGJL

In [2]: |
```

```
Python 3.8.5 (default, Sep 3 2020, 21:29:08) [MSC v.1916 64 bit (AMD64)]
Type "copyright", "credits" or "license" for more information.

IPython 7.22.0 -- An enhanced Interactive Python.

In [1]: runfile('D:/Sem5/Information Security/Lab/Lab5/IS-lab-5-Encrypt-
Decrypt.py', wdir='D:/Sem5/Information Security/Lab/Lab5')

Enter the text: QUHLBGJL

Enter a key: FUN


Choose 1 to Encrypt and 2 to Decrypt(Vigenere Cipher):2

Decrypted Message is: LAUGHTER

In [2]: |
```

## ➤ CrypTool Online Encrypt and Decrypt Output:

- **Encryption:**

**WIZARD**

MESSAGE INPUT

Here, you can input the message and the key to use.

Encrypt or Decrypt:  

Encrypt

Message to encrypt/decrypt:  

WELCOME TO INDIA

Key:  

BIRD

Start

Encryption/Decryption

Classic Encryption/Decryption

Vigenère

Back

Next


Abort

Message to encrypt/decrypt:  
WELCOME TO INDIA

Vigenère Output:  
XMCFPUV WP QEGJI

16 characters, 1 line

- **Decryption:**

 **WIZARD** MESSAGE INPUT

Here, you can input the message and the key to use.

Encrypt or Decrypt:  
Decrypt

Message to encrypt/decrypt:  
XMCFPUV WP QEGJI

Key:  
BIRD

Start Encryption/Decryption Classic Encryption/Decryption Vigenère

Back Next Abort

Message to encrypt/decrypt:  
XMCFPUV WP QEGJI

Vigenère Output:  
WELCOME TO INDIA

16 characters, 1 line

❖ **Cryptanalysis:**

The Kasiski Test uses the occasional aligning of groups of letters with the keyword to determine the length of the keyword. This will produce repeated groups of letters in the cipher text. By counting the number of letters between the beginnings of these repeated groups of letters and finding a number which is the multiple of those distances, we can estimate the length of the keyword.

Key:	ABCDABCDABCDABCDABCDABCDABCD
Plaintext:	CRYPTOISSHORTFORCRYPTOGRAPHY
Ciphertext:	CSASTPKVSIQUTGQUCSASTPIUAQJB

The distance between the repetitions of CSASTP is 16. If it is assumed that the repeated segments represent the same plaintext segments that imply that the key is 16, 8, 4, 2, or 1 characters long. Since key lengths 2 and 1 are unrealistically short, one needs to try only lengths 16, 8 or 4. Longer messages make the test more accurate because they usually contain more repeated cipher text segments.

### ❖ **Applications:**

- Vigenere Cipher was first used to encrypt messages and was known as the “unbreakable cipher”.
- Now in today’s time, Vigenere Cipher is used in combination with other ciphers to provide secure transmission of online messages.
- Many applications use Vigenere Cipher to encrypt messages with the help of One Time Password to generate a unique key.
- Vigenere Cipher can be modified and used in digital image security. The image can be encrypted to be safely sent, and decrypted to its original shape in accordance with the original image using Vigenere Cipher.

### ❖ **Reference:**

- [https://en.wikipedia.org/wiki/Vigen%C3%A8re\\_cipher](https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher)
- <https://www.geeksforgeeks.org/vigenere-cipher/>
- <https://www.codespeedy.com/vigenere-cipher-using-python/>
- <https://www.tutorialspoint.com/program-to-encrypt-a-string-using-vigenere-cipher-in-python>