Pandit Deendayal Energy University

School of Technology

Information Security Lab

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

PATEL VEDANT H.

19BCP138

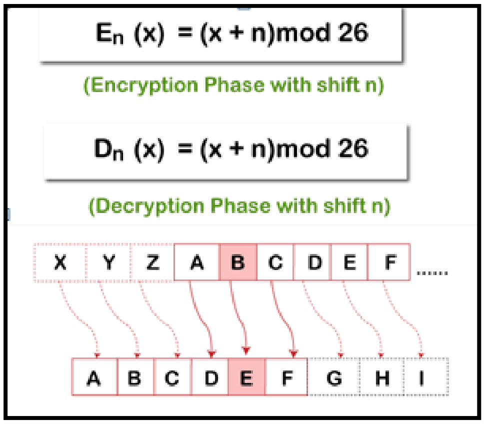
DIVISION – 2

Lab 2 Assignment

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

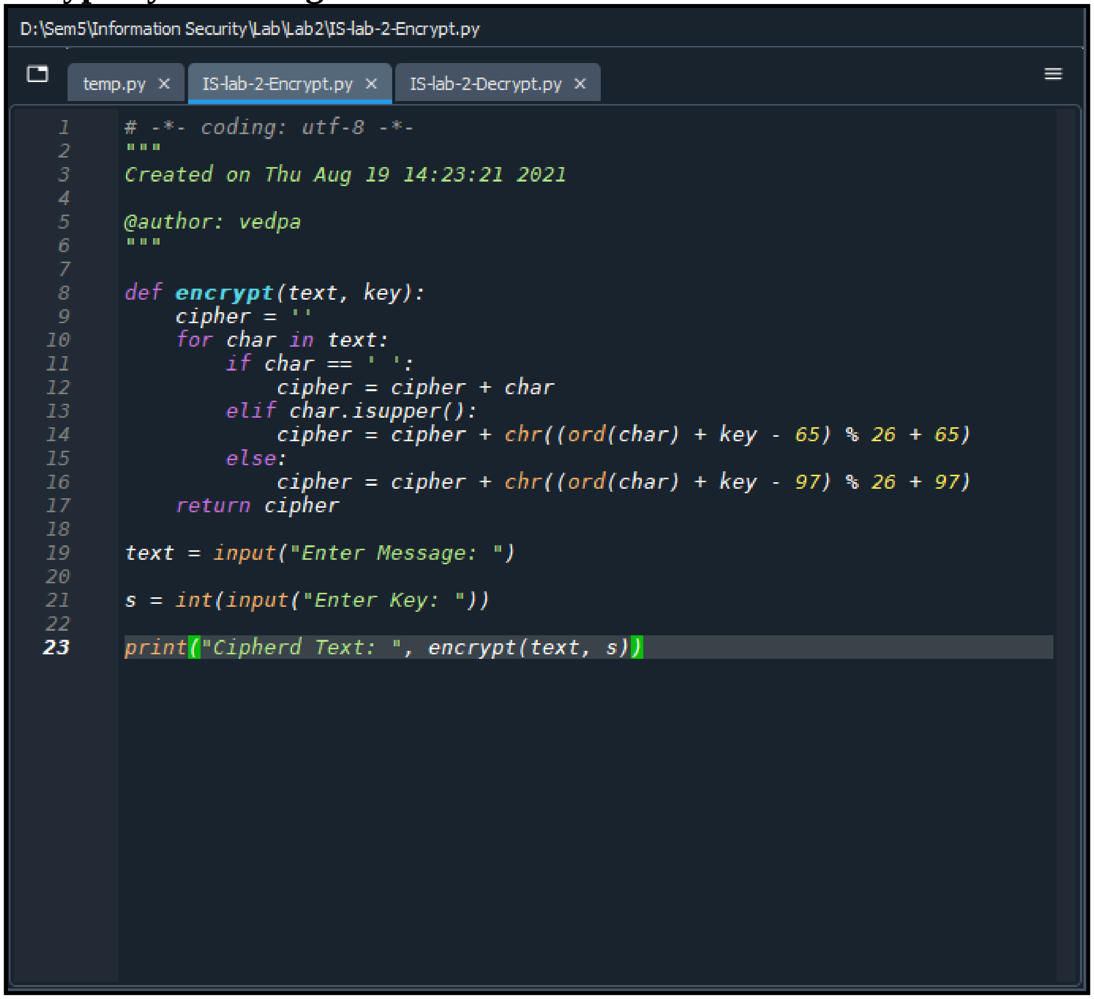
❖ Introduction:

In cryptography, Caesar cipher is one of the simplest and most widely known encryption techniques. The method is named after Julius Caesar, who used it in his private correspondence.
In this technique, each character is substituted by a letter certain fixed number position it's later or before the alphabet. For example, if you want to shift alphabets by key 3 then A → D, B → E, and similarly for other alphabets real value shifts by 3 positions. It is a simple type of substitute cipher.
There is an integer value required to define each latter of the text that has been moved down. This integer value is also known as the shift.


$E_n(x) = (x + n) \bmod 26$
(Encryption Phase with shift n)
$D_n(x) = (x + n) \bmod 26$
(Decryption Phase with shift n)
X
Y
Z
A
B
C
D
E
F
......
A
B
C
D
E
F
G
H
I

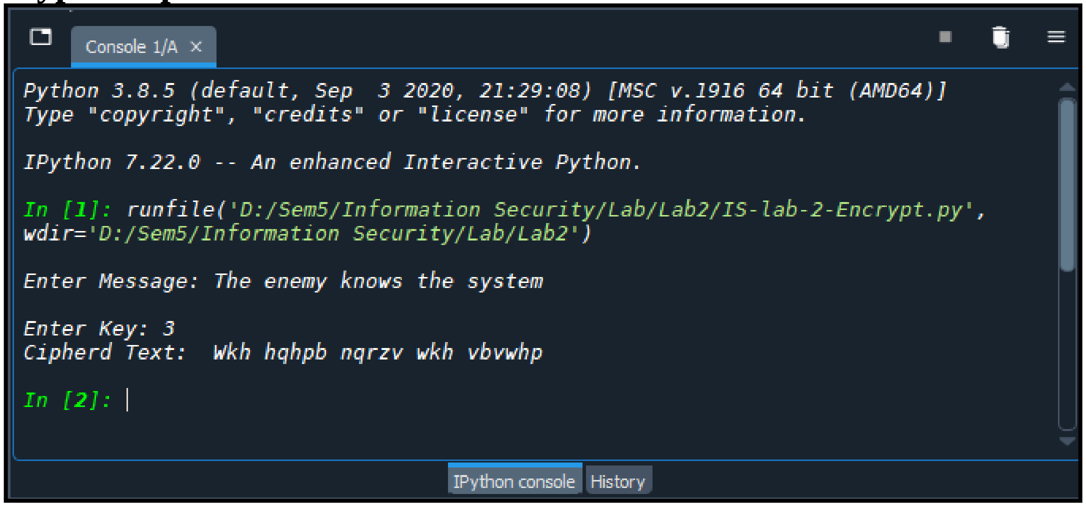
❖ Program:

➢ Encrypt Python Program:



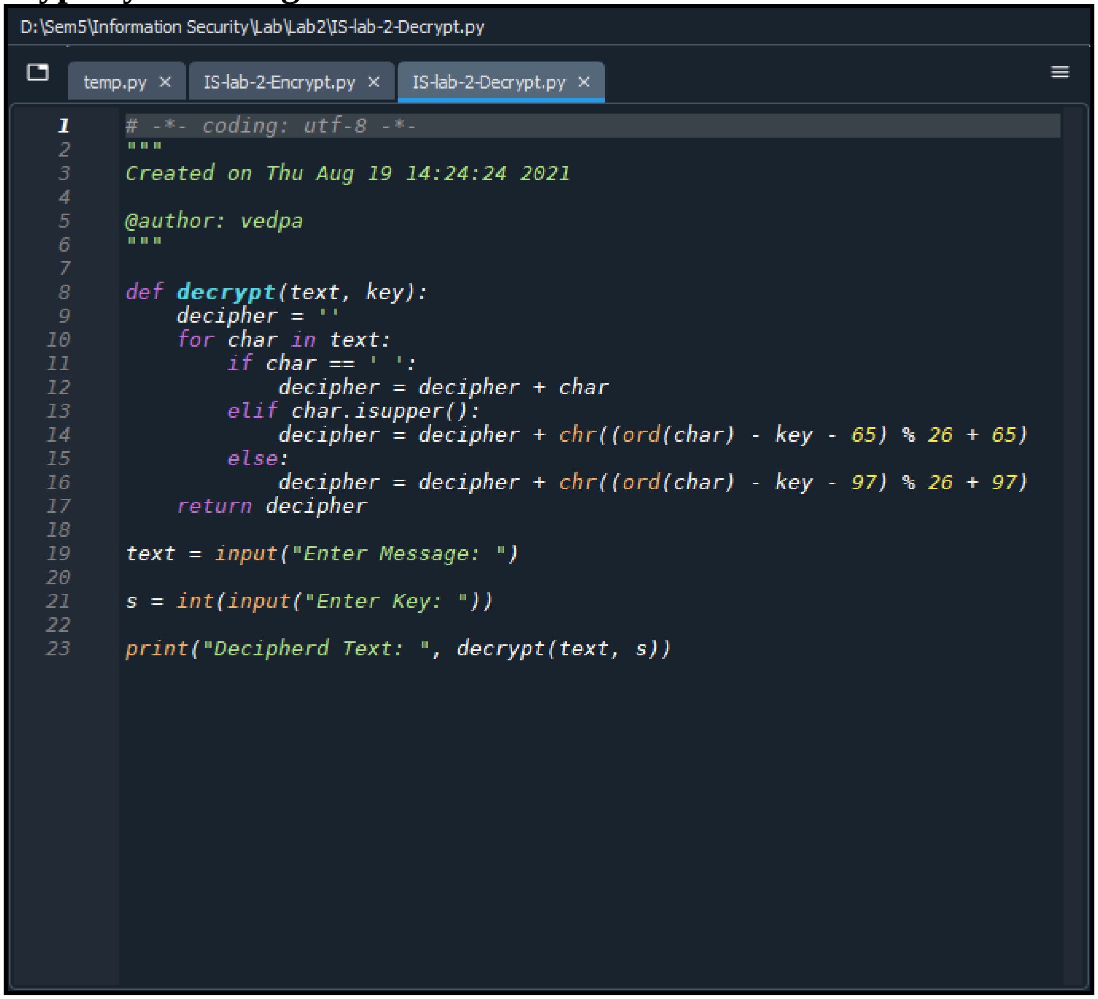
```python
# -*- coding: utf-8 -*-
"""
Created on Thu Aug 19 14:23:21 2021

@author: vedpa
"""

def encrypt(text, key):
    cipher = ''
    for char in text:
        if char == ' ':
            cipher = cipher + char
        elif char.isupper():
            cipher = cipher + chr((ord(char) + key - 65) % 26 + 65)
        else:
            cipher = cipher + chr((ord(char) + key - 97) % 26 + 97)
    return cipher

text = input("Enter Message: ")

s = int(input("Enter Key: "))

print("Cipherd Text: ", encrypt(text, s))
```

➢ Encrypt Output:



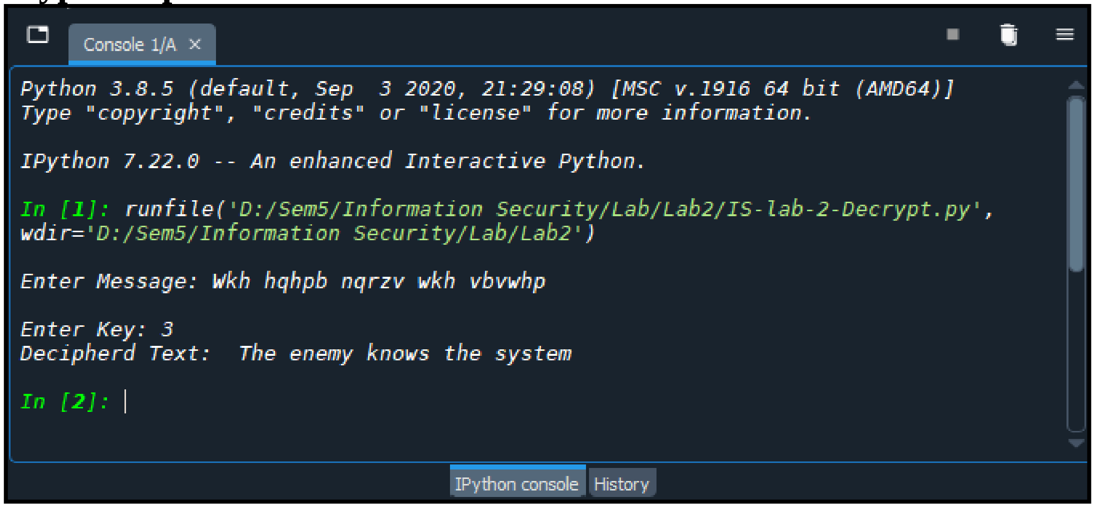
```
Python 3.8.5 (default, Sep  3 2020, 21:29:08) [MSC v.1916 64 bit (AMD64)]
Type "copyright", "credits" or "license" for more information.

IPython 7.22.0 -- An enhanced Interactive Python.

In [1]: runfile('D:/Sem5/Information Security/Lab/Lab2/IS-lab-2-Encrypt.py',
wdir='D:/Sem5/Information Security/Lab/Lab2')

Enter Message: The enemy knows the system

Enter Key: 3
Cipherd Text:  Wkh hqhpb nqrzv wkh vbvwhp

In [2]: |
```

- **Decrypt Python Program:**



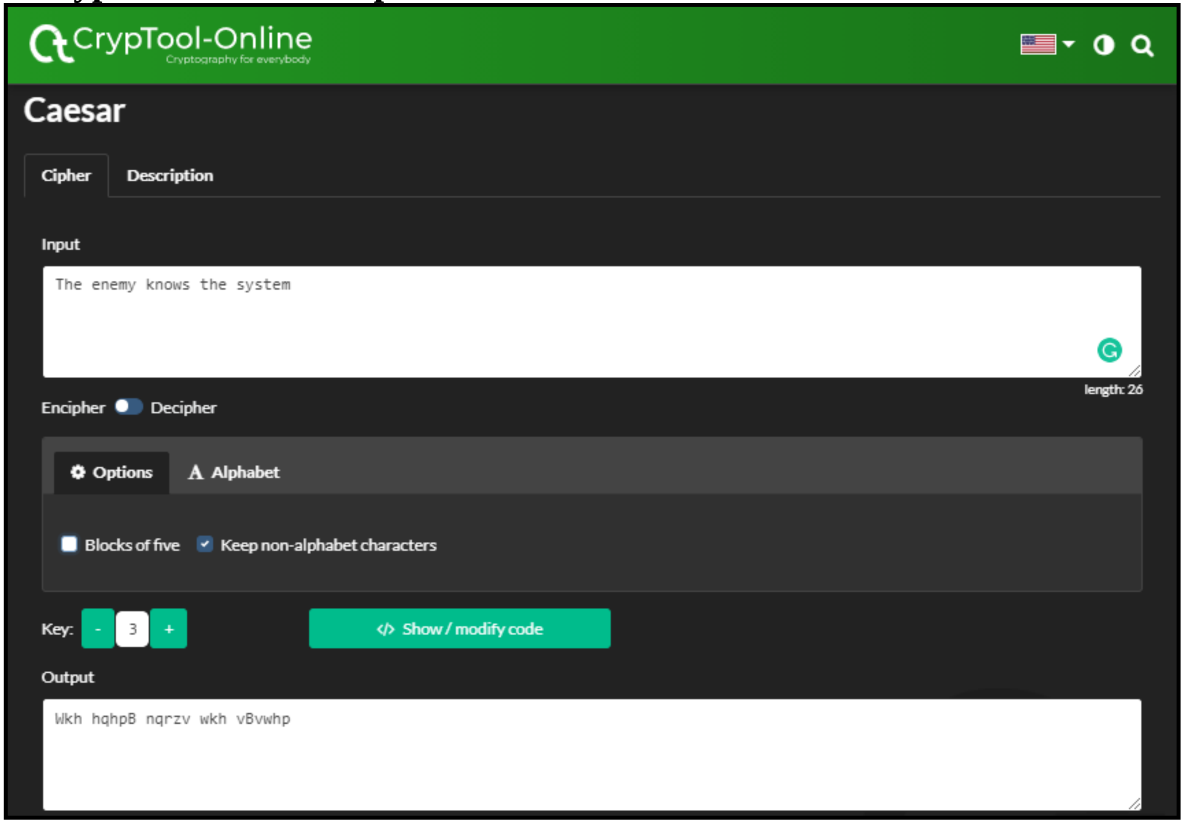
```python
# -*- coding: utf-8 -*-
"""
Created on Thu Aug 19 14:24:24 2021

@author: vedpa
"""

def decrypt(text, key):
    decipher = ''
    for char in text:
        if char == ' ':
            decipher = decipher + char
        elif char.isupper():
            decipher = decipher + chr((ord(char) - key - 65) % 26 + 65)
        else:
            decipher = decipher + chr((ord(char) - key - 97) % 26 + 97)
    return decipher

text = input("Enter Message: ")

s = int(input("Enter Key: "))

print("Decipherd Text: ", decrypt(text, s))
```

- **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/Lab2/IS-lab-2-Decrypt.py',
wdir='D:/Sem5/Information Security/Lab/Lab2')

Enter Message: Wkh hqhpb nqrzv wkh vbvwhp

Enter Key: 3
Decipherd Text:  The enemy knows the system

In [2]: 
```

➢ **CrypTool Online Output:**



Caesar

Input

```
The enemy knows the system
```

length: 26

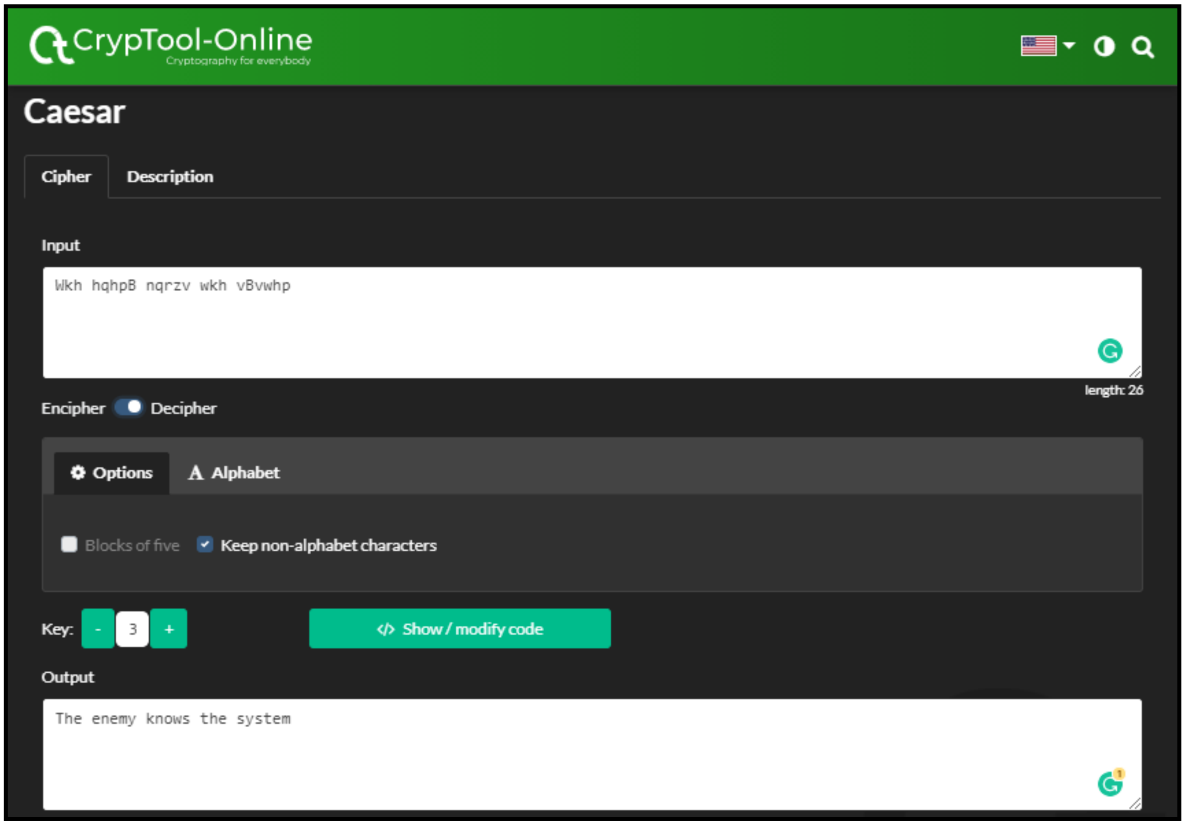
Encipher ● Decipher

□ Blocks of five ☑ Keep non-alphabet characters

Key: - 3 +

Output

```
Wkh hqhpB nqrzv wkh vBvwhp
```



Caesar

Input

```
Wkh hqhpB nqrzv wkh vBvwhp
```

length: 26

Encipher ● Decipher

□ Blocks of five ☑ Keep non-alphabet characters

Key: - 3 +

Output

```
The enemy knows the system
```

❖ Cryptanalysis:

Caesar cipher is simple to use and is not safest because an attacker knows (or guesses) that a Caesar cipher is in use, but does not know the shift value. As there are only 25 possible shifts available, they can each be tested in turn in a brute force attack. One way to do this is to write out a snippet of the cipher text in a table of all possible shifts or by using the advanced decoding methods available. And can easily decode the message.

❖ Applications:

- Caesar cipher can be found in the ROT13 cipher.
- Utilities for performing ROT13 can be found in the basic set of tools that ship with many Linux and UNIX operating systems.
- Hidden administrative and routing groups, it is difficult to move from one transport architecture to another without leaving some traces behind.
- Caesar ciphers can be found today in children's toys suchas secret decoder rings.

❖ Reference:

- **https://en.wikipedia.org/wiki/Caesar_cipher**
- **https://www.sciencedirect.com/topics/computer-science/caesar-cipher**
- **https://www.javatpoint.com/caesar-cipher-in-python**