

PRACTICAL 8

AIM: Implement Caesar Cipher Encryption-Decryption in Python.

Definition:

The Caesar Cipher is a simple and well-known encryption technique where each letter in the plaintext is shifted a certain number of places down or up the alphabet. It is a type of substitution cipher.

For example, with a shift of 3:

- A becomes D,
- B becomes E,
- Z becomes C, and so on.

Steps to Implement Caesar Cipher in Python:

1. Define a function for encryption:

- Accept a string (plaintext) and a shift key.
- Loop through each character.
- Shift letters forward by the key (maintaining case).
- Keep non-alphabet characters unchanged.

2. Define a function for decryption:

- Similar to encryption, but shift letters backward by the key.

3. Handle both uppercase and lowercase letters

4. Test the functions:

- Try encrypting and then decrypting to verify results.

The screenshot shows a Microsoft Visual Studio Code (VS Code) interface. The main area displays a Python script named 'Caesar_Cipher.py' with syntax highlighting. The code implements a Caesar cipher for both uppercase and lowercase letters. Below the code, the terminal window shows the execution of the script and its output. The status bar at the bottom indicates the file has 14 lines, 43 columns, uses UTF-8 encoding, is a Python file, and was last saved at 3:13:2.

```
1 def encrypt(text, key):
2     return ''.join(
3         chr((ord(char) - 65 + key) % 26 + 65) if char.isupper() else
4         chr((ord(char) - 97 + key) % 26 + 97) if char.islower() else
5         chr for char in text
6     )
7
8 text = input("Enter The Message : ")
9 key = int(input("Enter The Shift Value : "))
10 encrypted = encrypt(text, key)
11 print(encrypted)
12
13 decrypted_text = encrypt(encrypted, -key)
14 print("Decrypted Text : ", decrypted_text)
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

```
PS C:\Users\sonip> & C:/Users/sonip/AppData/Local/Programs/Python/Python313/python.exe c:/Users/sonip/OneDrive/Desktop/Caesar_Cipher.py
Enter The Message : ab
Enter The Shift Value : 1
bc
Decrypted Text :  ab
PS C:\Users\sonip> []
```

Ln 14 Col 43 Spaces: 4 CRLF {} Python 3:13:2

Code:

```
def encrypt(text, key):
    return "join(
        chr((ord(char) - 65 + key) % 26 + 65) if char.isupper() else
        chr((ord(char) - 97 + key) % 26 + 97) if char.islower() else
        chr for char in text
    )
```

```
text = input("Enter The Message : ")
key = int(input("Enter The Shift Value : "))
encrypted = encrypt(text, key)
print(encrypted)

decrypted_text = encrypt(encrypted, -key)
print("Decrypted Text : ", decrypted_text)
```

Output:

```
Enter The Message : ab
Enter The Shift Value : 1
bc
Decrypted Text : ab
```

Conclusion:-

The Caesar Cipher is an introductory concept in cryptography, demonstrating how a simple shift can encode and decode a message. Though it is not secure for modern use, it's a great way to understand how encryption and decryption work. Implementing it in Python is straightforward using basic string manipulation and character encoding.