Kartik Padave

A022

70362019039

Experiment 1

Aim

To implement Caesar Cipher.

Theory

In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code, or Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence. The encryption step performed by a Caesar cipher is often incorporated as part of more complex schemes, such as the Vigenère cipher, and still has modern application in the ROT13 system. As with all single-alphabet substitution ciphers, the Caesar cipher is easily broken and in modern practice offers essentially no communications security.

Code

```
text = input("Enter plain text: ").upper()
shift = int(input("Enter shift value: "))
encrypt_text = ""

for i in range(len(text)):
    char = text[i]
    encrypt_text += chr((ord(char) + shift-65) % 26 + 65)

print(f"Plain Text: {text}")
print(f"Shift value: {shift}")
print(f"Encrypted Text: {encrypt_text}")
```

Output

```
E:\Programs\College-Labs\CRYPTO-Lab>python Caesar-cipher.py
Enter plain text: My name is kartik
Enter shift value: 3
Plain Text: MY NAME IS KARTIK
Shift value: 3
Encrypted Text: PBWQDPHWLVWNDUWLN
```

Conclusion

Hence, we were able to perform Caesar Cipher.