**NAME: ANUSHKA BHARDE**

**PRN: 121A9005**

**BATCH: B1**

**SUBJECT: CSS**

**EXPERIMENT NO. 1**

**AIM:** Implementation of caesar cipher.

**Theory:**

The Caesar cipher is a simple encryption technique that was used by Julius Caesar to send secret messages to his allies. It works by shifting the letters in the plaintext message by a certain number of positions, known as the “shift” or “key”. It is based on substitution cipher. Each character is shifted by a specific number of characters, which is the key.

**Algorithm:**

* Initialize a variable shift to the value of k.
* Iterate through each character c in the message −
* If c is a letter (uppercase or lowercase), shift it by shift positions in the alphabet.
* The formula of Caesar cipher encryption is **En(x) = (x + n) mod 26.**
* The Formula for Caesar cipher decryption is **Dn(x) = (x – n) mod 26**.
* To shift an uppercase letter, subtract 'A' from the letter, add the shift value, and take the modulus 26. Then add 'A' back to get the shifted letter.
* To shift a lowercase letter, subtract 'a' from the letter, add the shift value, and take the modulus 26. Then add 'a' back to get the shifted letter.
* b. Append the shifted letter to the encoded message.
* Return the encoded message.

**Code:**

def encryption\_ceasarcipher(message, key):

alphabet = 'abcdefghijklmnopqrstuvwxyz'

text=""

message= message.lower()

for i in message:

if i in alphabet:

index = alphabet.find(i)

index = (index + key) % 26

if index < 0:

index = index + 26

text = text + alphabet[index]

return text

def decryption\_ceasarcipher(message, key):

alphabet = 'abcdefghijklmnopqrstuvwxyz'

text=""

message= message.lower()

for i in message:

if i in alphabet:

index = alphabet.find(i)

index = (index - key) % 26

if index < 0:

index = index + 26

text = text + alphabet[index]

return text

msg=input("Enter message:")

shift= int(input("Enter shift:"))

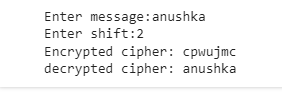
ceasarcipher\_text\_encryp = encryption\_ceasarcipher(msg, shift)

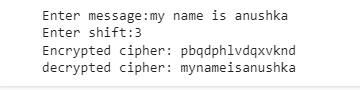
print("Encrypted cipher:",ceasarcipher\_text\_encryp )

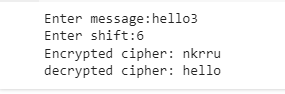
ceasarcipher\_text\_decryp = decryption\_ceasarcipher(ceasarcipher\_text\_encryp , shift)

print("decrypted cipher:",ceasarcipher\_text\_decryp)

**Output:**

****

****

****