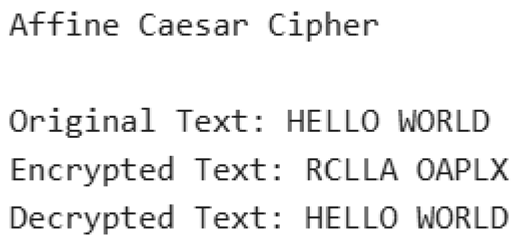
23) Write a python program for Caesar cipher, known as the affine Caesar cipher, has the following form: For each plaintext letter p, substitute the ciphertext letter C: C = E([a, b], p) = (ap + b) mod 26 A basic requirement of any encryption algorithm is that it be one-to-one. That is, if p q, then E(k, p) E(k, q).Otherwise, decryption is impossible, because more than one plaintext character maps into the same ciphertext character. The affine Caesar cipher is not one-to-one for all values of a. For example, for a = 2 and b = 3, then E([a, b], 0) = E([a, b], 13) = 3.

<u>PROGRAM:-</u>

```
from math import gcd
def mod_inverse(a, m):
    for x in range(1, m):
        if (a * x) % m == 1:
            return x
    return None  # No mod inverse if gcd(a, m) ≠ 1
def affine_encrypt(text, a, b):
    if gcd(a, 26) != 1:
        raise ValueError(f"a = {a} is invalid. It must be coprime with 26.")
    result = ""
    for char in text.upper():
        if char.isalpha():
            p = ord(char) - ord('A')
            c = (a * p + b) % 26
            result += chr(c + ord('A'))
        else:
            result += char
    return result
def affine_decrypt(cipher, a, b):
    a_inv = mod_inverse(a, 26)
    if a_inv is None:
        raise ValueError(f"Modular inverse for a = {a} does not exist. Choose a coprime with 26.")
    result = ""
    for char in cipher.upper():
        if char.isalpha():
            c = ord(char) - ord('A')
            p = (a_inv * (c - b)) % 26
            result += chr(p + ord('A'))
        else:
            result += char
    return result
if __name__ == "__main__":
    a = 5  # Must be coprime with 26
    b = 8
    plaintext = "HELLO WORLD"
    print("Affine Caesar Cipher\n")
    print("Original Text:", plaintext)
    encrypted = affine_encrypt(plaintext, a, b)
    print("Encrypted Text:", encrypted)
    decrypted = affine_decrypt(encrypted, a, b)
    print("Decrypted Text:", decrypted)
```

OUTPUT:-



```
Affine Caesar Cipher

Original Text: HELLO WORLD
Encrypted Text: RCLLA OAPLX
Decrypted Text: HELLO WORLD
```