**Ex No:01 RSA**

**Date:**

AIM:

To execute RSA Algorithm Using python and encrypt and decrypt.

ALGORITHM:

1. Start.
2. Read the plaintext.
3. Generate public key and private key.
4. Then encrypt using public key.
5. And decrypt using private key.
6. Stop

PROGRAM:

import random

def gcd(a, b):

while b != 0:

a, b = b, a % b

return a

def multiplicative\_inverse(e, phi):

d = 0

x1, x2, y1, y2 = 0, 1, 1, 0

temp\_phi = phi

while e > 0:

temp1 = temp\_phi // e

temp2 = temp\_phi - temp1 \* e

temp\_phi = e

e = temp2

x = x2 - temp1 \* x1

y = y2 - temp1 \* y1

x2 = x1

x1 = x

y2 = y1

y1 = y

if temp\_phi == 1:

d = y2 + phi

return d

def generate\_keypair(p, q):

if not (is\_prime(p) and is\_prime(q)):

raise ValueError("Both numbers must be prime.")

elif p == q:

raise ValueError("p and q cannot be equal")

n = p \* q

phi = (p - 1) \* (q - 1)

e = random.randrange(1, phi)

g = gcd(e, phi)

while g != 1:

e = random.randrange(1, phi)

g = gcd(e, phi)

d = multiplicative\_inverse(e, phi)

return ((e, n), (d, n))

def encrypt(pk, plaintext):

key, n = pk

cipher = [pow(ord(char), key, n) for char in plaintext]

return cipher

def decrypt(pk, ciphertext):

key, n = pk

plain = [chr(pow(char, key, n)) for char in ciphertext]

return ''.join(plain)

def is\_prime(num):

if num == 2 or num == 3:

return True

if num < 2 or num % 2 == 0:

return False

for n in range(3, int(num\*\*0.5)+2, 2):

if num % n == 0:

return False

return True

# Example usage:

p = 61

q = 53

public\_key, private\_key = generate\_keypair(p, q)

print("Public Key:", public\_key)

print("Private Key:", private\_key)

message = "Hello, World!"

print("Original Message:", message)

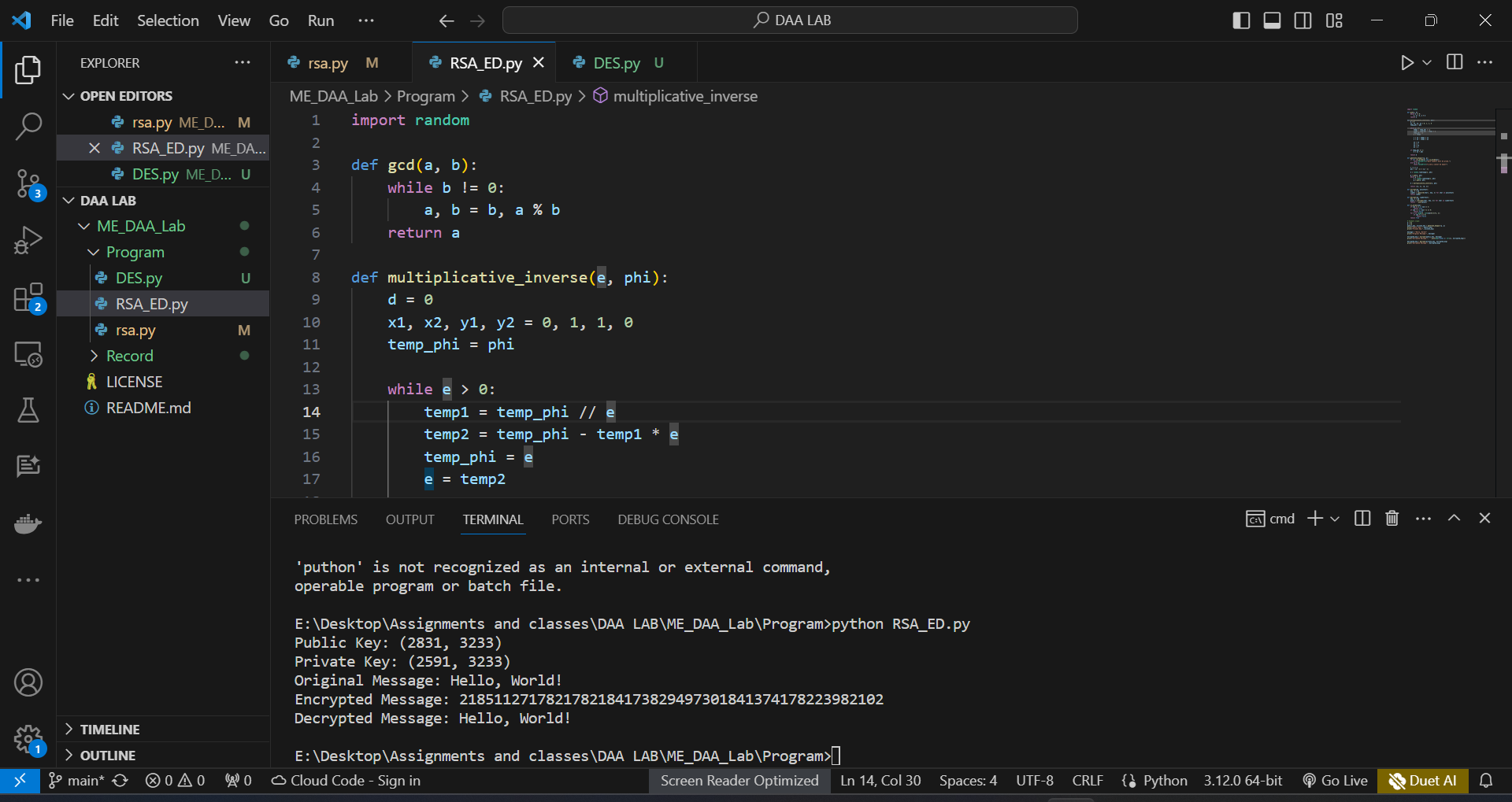
encrypted\_msg = encrypt(public\_key, message)

print("Encrypted Message:", ''.join(map(lambda x: str(x), encrypted\_msg)))

decrypted\_msg = decrypt(private\_key, encrypted\_msg)

print("Decrypted Message:", decrypted\_msg)

OUTPUT:



RESULT:

This RSA algorithm was executed successfully.

**Ex No:02 DES**

**Date:**

AIM:

ALGORITHM:

PROGRAM:

OUTPUT:

RESULT: