**Ex. No.:2A**

**Date: 24/02/2024**

**RSA ALGORITHM**

**Aim:**

To write a Python program to implement RSA Algorithm.

**Algorithm:**

1. Select 2 prime numbers preferably p and q.
2. Calculate n=p\*q.
3. Calculate phi(n) = (p-1)(q-1)
4. Choose a value of e such that 1<e<phi(n) and gcd(phi(n),e)-1.
5. Calculate d such that d=(e^-1)mod phi(n).

**Program:**

**#DSA Algorithm**

n = p\*q

e = int(input("Enter the value:"))

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

while(e < phi):

#e must be coprime to phi and smaller that phi

if(gcd(e, phi) == 1):

break

else:

e = e+1

k = 2

d = (1 + (k\*phi))/e

msg = float(input('Enter message:'))

print('Message data =', msg)

c = pow(msg, e)

c = math.fmod(c, n)

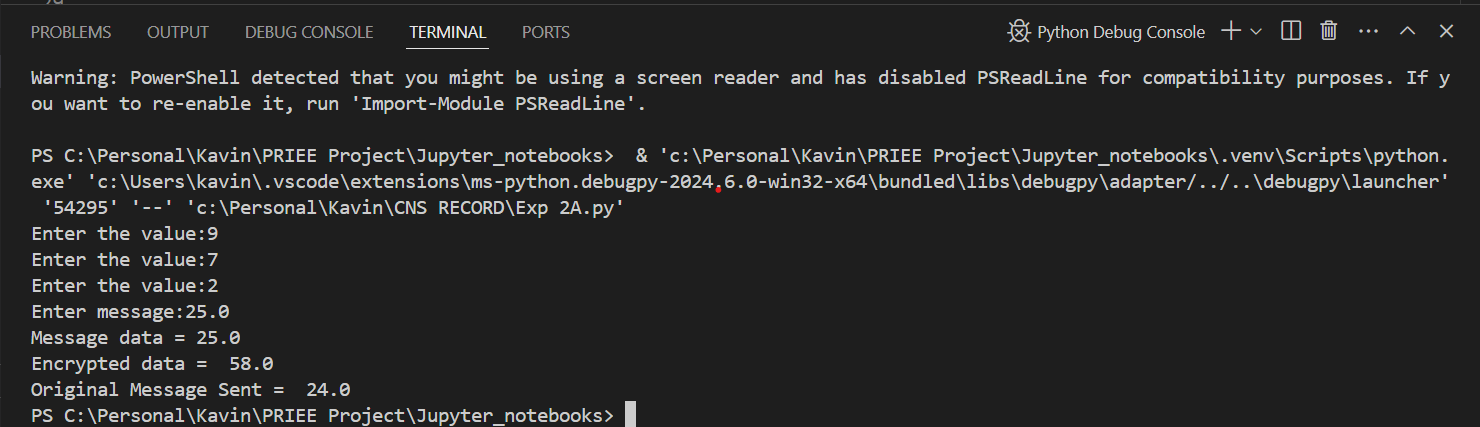
print('Encrypted data = ', c)

m = pow(c, d)

m = math.fmod(m, n)

print('Original Message Sent = ', m)

**Output:**



**Result:**

Hence, DSA Algorithm has been implemented successfully.