**Name : Aarya Tiwari**

**Batch : B2:**

**Roll No. : 16010421119**

**Course: INS Lab**

**Experiment No. : 4**

**Code:**

import math

import sympy

*# step 1*

*# p = 127*

*# q = 131*

p = int(input("Enter the value of p: "))

q = int(input("Enter the value of q: "))

if not sympy.isprime(p) or not sympy.isprime(q):

    print("p and q must be prime numbers.")

    exit()

print("p =", p)

print("q =", q)

*# step 2*

n = p\*q

print("n =", n)

*# step 3*

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

*# step 4*

e = 2

while (e < phi):

    if (math.gcd(e, phi) == 1):

        break

    else:

        e += 1

print("e =", e)

*# step 5*

k = 2

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

print("d =", d)

print(f'Public key: {e, n}')

print(f'Private key: {d, n}')

*# plain text*

msg = 11

print(f'Original message:{msg}')

*# encryption*

C = pow(msg, e)

C = math.fmod(C, n)

print(f'Encrypted message: {C}')

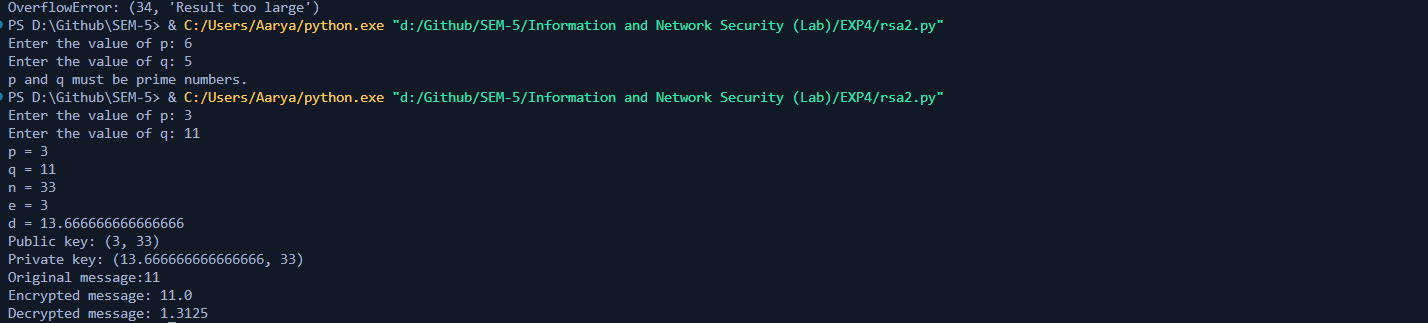
*# decryption*

M = pow(C, d)

M = math.fmod(M, n)

print(f'Decrypted message: {M}')

**Output:**

****