Exp No: 4 **Roll.No:** 210701314
Date:

RSA Algorithm

Aim:

To implement RSA algorithm with key generation, encryption and decryption for the user input message.

Algorithm:

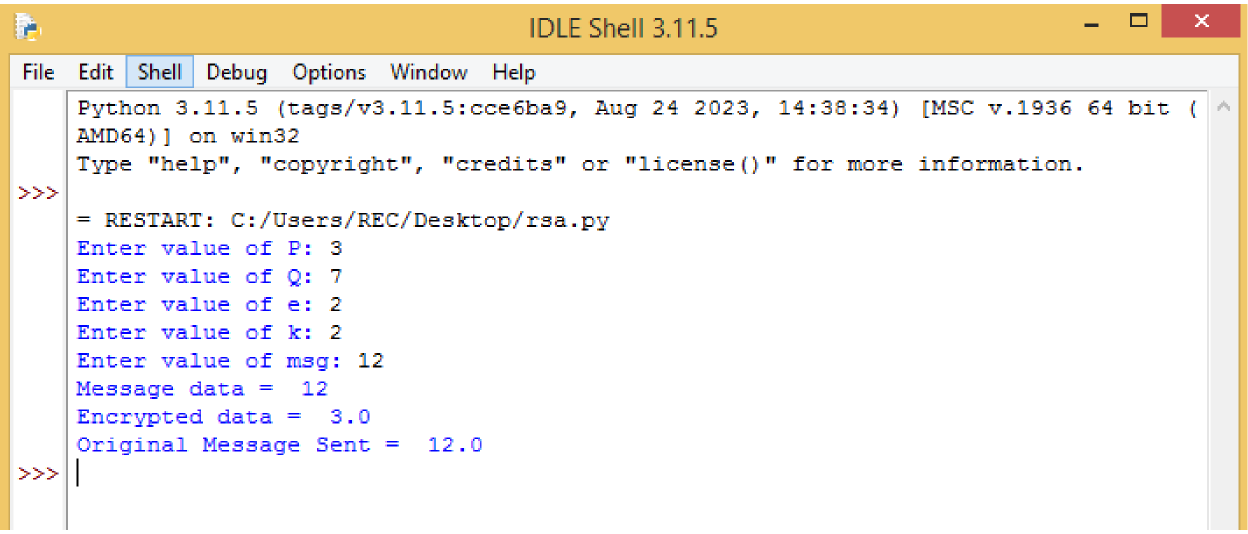
Step 1: Get two prime numbers P and Q from the user
Step 2: Initiate generate_keypair() function to create public key and private key
Step 3: Public key will be selected based on satisfying of conditions
Step 4: Private key will be found based on D=E-1mod ((P-1)*(Q-1))
Step 5: Get the message from the user to be encrypted
Step 6: Encrypted the message using public key
Step 7: Decrypt the message using private key

Program:

```
import math


def gcd(a, h):
    temp = 0
    while(1):
        temp = a % h
        if (temp == 0):
            return h
        a = h
        h = temp


P = int(input("Enter value of P: "))
Q = int(input("Enter value of Q: "))
n = P*Q
e = int(input("Enter value of e: "))
phi = (P-1)*(Q-1)
```

```
while (e < phi):


    if(gcd(e, phi) == 1):
        break
    else:
        e = e+1



k = int(input("Enter value of k: "))
d = (1 + (k*phi))/e


msg = int(input("Enter value of msg: "))

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:



```
Python 3.11.5 (tags/v3.11.5:cce6ba9, Aug 24 2023, 14:38:34) [MSC v.1936 64 bit (
AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: C:/Users/REC/Desktop/rsa.py
Enter value of P: 3
Enter value of Q: 7
Enter value of e: 2
Enter value of k: 2
Enter value of msg: 12
Message data =  12
Encrypted data =  3.0
Original Message Sent =  12.0
>>>
```

Result:

Thus the RSA Algorithm implemented successfully to process the user input message.