EXPERIMENT 5

Shashwat Shah
TYBtech Comps B
C22
60004220126

AIM: Study and Implement RSA Algorithm.

CODE:

```
import math
def enc(plain,e,n):
    return (plain**e)%n
def dec(cipher,d,n):
    return (cipher**d)%n
def get_public_key(phi):
    e = 2
    while e < phi:
        if math.gcd(e,phi) == 1:
            break
        else:
            e += 1
    return e
def get_private_key(e,phi):
    d = 2
    while d < phi:
        if (d*e)%phi == 1:
            break
        else:
            d += 1
    return d
if __name__=='__main__':
    p,q = input('Enter two prime numbers: ').split()
    plain = int(input('Enter the plain text: '))
    p,q = int(p),int(q)
    n = p*q
    phi = (p-1)*(q-1)
    e = get_public_key(phi)
    d = get_private_key(e,phi)
    print('Public key(e,n): ',e,n)
    print('Private key(d,n): ',d,n)
    cipher = enc(plain,e,n)
    print('Cipher text: ',cipher)
    print('Plain text: ',dec(cipher,d,n))
```

OUTPUT:

```
uments/BTech/Docs/6th Sem/IS/Code/Exp5/RSA.py"
Enter two prime numbers: 1291 607
Enter the plain text: 909
Public key(e,n):  7 783637
Private key(d,n):  670063 783637
Cipher text:  359730
Plain text:  909
```