|  |  |
| --- | --- |
| Name: | Prerna Sunil Jadhav |
| Sap Id: | 60004220127 |
| Class: | T. Y. B. Tech (Computer Engineering) |
| Course: | Information Security Laboratory |
| Course Code: | DJ19CEL603 |
| Experiment No.: | 05 |

**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:**

