Name : Prasad Borkar

Class : TE(A)

Roll No.: COTA59

Assignment No.: 05

PROGRAM CODE :

```
from fractions import gcd

import math

# step 1

p = 3

q = 7

# step 2

n = p*q

print "n =", n

# step 3

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

# step 4

e = 2

while(e<phi):

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

break

else:

e += 1

print "e =", e

# step 5

k = 2

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

print "d =", d
```

```
print "Public key: (%d, %d)" % (e, n)

print "Private key: (%d, %d)" % (d, n)

# plain text

msg = 11

print "Original message:", msg

# encryption

C = pow(msg, e)

C = math.fmod(C, n)

print "Encrypted message:", C

# decryption

M = pow(C, d)

M = math.fmod(M, n)

print "Decrypted message:", M

n = 21

e = 5

d = 5
```

OUTPUT

```
Public key: (5, 21)

Private key: (5, 21)

Original message: 11

Encrypted message: 2.0

Decrypted message: 11.0
```