**EXTERNAL PRACTICAL**

**AIM**: Implement the Elgamal algorithm for encryption and decryption of the messages which contains alphabets as well as digits

**PROGRAMMING LANGUAGE**

Python

**PROGRAM CODE**

import random

from math import pow

a=random.randint(2,10)

#To fing gcd of two numbers

def gcd(a,b):

if a<b:

return gcd(b,a)

elif a%b==0:

return b

else:

return gcd(b,a%b)

#For key generation i.e. large random number

def gen\_key(q):

key= random.randint(pow(10,20),q)

while gcd(q,key)!=1:

key=random.randint(pow(10,20),q)

return key

def power(a,b,c):

x=1

y=a

while b>0:

if b%2==0:

x=(x\*y)%c;

y=(y\*y)%c

b=int(b/2)

return x%c

#For asymetric encryption

def encryption(msg,q,h,g):

ct=[]

k=gen\_key(q)

s=power(h,k,q)

p=power(g,k,q)

for i in range(0,len(msg)):

ct.append(msg[i])

for i in range(0,len(ct)):

ct[i]=s\*ord(ct[i])

return ct,p

#For decryption

def decryption(ct,p,key,q):

pt=[]

h=power(p,key,q)

for i in range(0,len(ct)):

pt.append(chr(int(ct[i]/h)))

return pt

print("ID : 18DCS007\nNAME : RUDRA BARAD")

msg=input("Enter message for Encryption : ")

q=random.randint(pow(10,20),pow(10,50))

g=random.randint(2,q)

key=gen\_key(q)

h=power(g,key,q)

ct,p=encryption(msg,q,h,g)

print("Original Message = ",msg)

print("Encrypted Maessage = ",ct)

pt=decryption(ct,p,key,q)

d\_msg=''.join(pt)

print("Decryted Message after Decryption = ",d\_msg)

**OUTPUT**

