# ASSIGNMENT-10

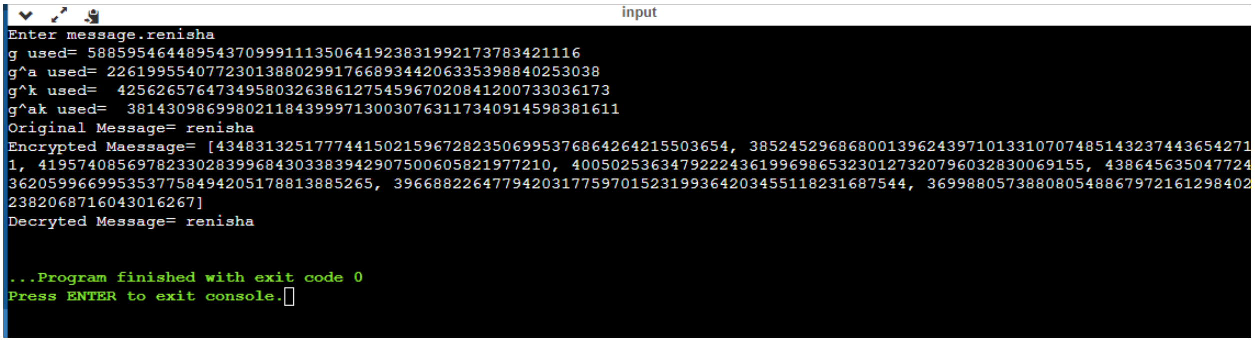
Aim: Elgamal Digital Signature Algorithm

## Code:

```
import random
from math import pow

a=random.randint(4,20)

#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])
   print("g^k used= ",p)
   print("g^ak used= ",s)
   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



msg=input("Enter message.")
q=random.randint(pow(10,20),pow(10,50))
```

```
g=random.randint(2,q)

key=gen_key(q)

h=power(g,key,q)

print("g used=",g)

print("g^a used=",h)

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=",d_msg)
```

## Output:



```
Enter message.renisha
g used= 58859546448954370999111350641923831992173783421116
g^a used= 22619955407723013880299176689344206335398840253038
g^k used=  42562657647349580326386127545967020841200733036173
g^ak used=  38143098699802118439997130030763117340914598381611
Original Message= renisha
Encrypted Maessage= [4348313251777441502159672823506995376864264215503654, 3852452968680013962439710133107074851432374436542711
1, 4195740856978233028399684303383942907500605821977210, 4005025363479222436199698653230127320796032830069155, 438645635047724
3620599669953537758494205178813885265, 3966882264779420317759701523199364203455118231687544, 369988057388080548867972161298402
2382068716043016267]
Decryted Message= renisha


...Program finished with exit code 0
Press ENTER to exit console.
```