**Applied Cryptography and Network Security**

**(CSI3002)**

**LAB ASSESSMENT – 5**

**Name : RITHIV.R**

**Reg No : 19MIC0113**

**Slot : L27+L28**

1. **ELGAMAL DIGITAL SIGNATURE**

**Code:**

print('RITHIV.R-19MIC0113')

def inverse(n):

i=1

while((k\*i)%(p-1) != 1):

i=i+1

return i

m=5

p=11

g=2

d=8

#message Hashing

e = (g\*\*d)%p

#after hashing

m= 12

#Value of Should be be gcd(k,p-1) = 1

k = 9

y1 = (g\*\*k)%p

print("y1: "+ str(y1))

inv\_k = inverse(k)

print("inv\_k: "+ str(inv\_k))

if inv\_k\*(m - d\*y1) > 0:

y2 =(inv\_k\*(m - d\*y1)) % (p-1)

else:

y2 = (p-1) - ((-1\*(inv\_k\*(m - d\*y1)))%(p-1))

print("y2: "+ str(y2))

value1 = (g\*\*m) % p

value2 = ((e\*\*y1) \* (y1\*\*y2))% p

print("value1: "+str(value1))

print("value2: "+ str(value2))

#Verification

if(value1==value2):

print("The message is not corrupted")

else:

print("The message is corrupted")

**Output:**

