Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
INS Practical 7

Aim : An organization wants to achieve encryption of data using Asymmetric key cryptography. The Public key will be available to all employee, and private key will be individual for each employee for communication. Your task is to find out Public key for organization and private key for 1 employee. Also provide how data will be encrypted using this public key & private key.

Code :

```
import random
import YSL_io as ysl

p = int(ysl.inputGRN("\n\tEnter the first large prime number : "))
q = int(ysl.inputGRN("\tEnter the second large prime number : "))
n = p * q
ysl.printMGNTA("\n\tThe value of n is : ", end="")
print(n)

phi_n = (p - 1) * (q - 1)
ysl.printMGNTA("\tThe value of phi(n) is:", end="")
print(phi_n)

lower = 0
upper = phi_n
primes = []
e_list = []

for e in range(lower, upper):
   if e > 1:
       for i in range(2, e):
           if (e % i) == 0:
               break
           else:
               primes.append(e)
```

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
INS Practical 7

```
def gcd(a, b):
   while b != 0:
       a, b = b, a % b
   return a


def coprime(a, b):
   return gcd(a, b) == 1


for i in primes:
   if coprime(i, phi_n) == True:
       e_list.append(i)

e = random.choice(e_list)
ysl.printBLU("\n\tSelected value of e : ", end="")
print(e)

d = pow(e, -1, phi_n)

ysl.printBLU("\tValue of d : ", end="")
print(d)

public_key = [e, n]
private_key = [d, n]
ysl.printRED("\tPublic key : ", end="")
print(public_key)
ysl.printRED("\tPrivate key : ", end="")
print(private_key)

stream_count = int(ysl.inputORNG("\n\tEnter the number of data streams :
```

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
INS Practical 7

```
"))
message = []
print()
for i in range(0, stream_count):
    temp = ysl.inputORNG(f"\tEnter data stream {i+1} : ")
    message.append(temp)

cipher = []
decrypted_text = []

for i in message:
    temp_i = int(i)
    temp_cipher = pow(temp_i, e, n)
    cipher.append(temp_cipher)

ysl.printRED("\n\tEncrypted Cipher text :", end="")
print(cipher)

for i in cipher:
    temp_i = int(i)
    temp_decrypt = pow(temp_i, d, n)
    decrypted_text.append(temp_decrypt)

ysl.printRED("\n\tDecrypted Plain text :", end="")
print(decrypted_text)
```

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
INS Practical 7

Output :