Name: Shrikant Pawar
Roll No.: 57
Assignment No. 06

Title: Implement a client and a server on different computers using python. Perform the authentication ofsender between these two entities by using RSA digital signature cryptosystem

Client Code:

```
import random
import hashlib

def gcd(a,b):
    if b==0:
        return a
    else:
        return gcd(b,a%b)

def isPrime(n) :
    # Corner cases
    if (n <= 1) :
        return False
    if (n <= 3) :
        return True

    if (n % 2 == 0 or n % 3 == 0) :
        return False

    i = 5
    while(i * i <= n) :
        if (n % i == 0 or n % (i + 2) == 0) :
            return False
        i = i + 6

    return True

# Get a prime number
def generatePrime(num = 100):
    L1 = []
    for i in range(60, num + 1):
        if isPrime(i):
            L1.append(i)

    p = random.choice(L1)
    L1.pop(L1.index(p))
    q = random.choice(L1)
```

```
    t = (p-1)*(q-1)
    n = p*q

    for e in range(2,t):
        if gcd(e,t)== 1:
            break

    for i in range(1,10):
        x = 1 + i*t
        if x % e == 0:
            d = int(x/e)
            break

    return e,d,n

Alphabet_List = {'A': '01', 'B': '02', 'C': '03', 'D': '04', 'E': '05', 'F': '06', 'G': '07', 'H': '08', 'I': '09', 'J': '10',
                 'K': '11', 'L': '12', 'M': '13', 'N': '14', 'O': '15', 'P': '16', 'Q': '17', 'R': '18', 'S': '19', 'T': '20',
                 'U': '21', 'V': '22', 'W': '23', 'X': '24', 'Y': '25', 'Z': '26', ' ': '27', '1':'28', '2':'29', '3':'30',
                 '4':'31', '5':'32', '6':'33', '7':'34', '8':'35', '9':'36', '0':'37'}

key_list = list(Alphabet_List.keys())
val_list = list(Alphabet_List.values())


def convertText(msg,Ekey, N):
    li = list(msg)
    lii = [Alphabet_List[i] for i in li]
    if(len(lii)%2 != 0):
        lii.append('27')
    #print(lii)
    l1 = [int(lii[i]+lii[i+1]) for i in range(0,len(lii),2)]
    #print(l1)
    ctt = [str(pow(no,Ekey)%N).zfill(4) for no in l1]
    ct = ''.join(ctt)
    return ct

def decrypt(cipherText, Dkey, N):
    text = [str(pow(int(cipherText[i:i+4]),Dkey)%N).zfill(4) for i in range(0, len(cipherText), 4)]

    L1 = []
    for i in text:
        L1.append(i[0:2])
        L1.append(i[2:4])

    L2 = []
    for i in L1:
        L2.append(key_list[val_list.index(i)])
```

```
    msg = ''.join(L2)
    return msg
import socket,sys,threading

e,d,n = generatePrime()

msgFromClient = "Hello UDP Server!. My public Key is: "+str(e)+" "+str(n)
bytesToSend = str.encode(msgFromClient)
serverAddressPort = ("192.168.43.125", 20003)
bufferSize = 1024
def recv():
    while True:
        recieve= UDPClientSocket.recvfrom(bufferSize)
        msg = recieve[0].decode('utf-8')
        plainText = decrypt(msg, d, n)
        if not recieve[0]: sys.exit(0)
        print(plainText)

def Send(sA):
    while True:
        msg=input("Enter your reply  ").upper()
        L1 = list(msg.split())
        cipherText = convertText(L1[0], int(L1[1]), int(L1[2]))
        UDPClientSocket.sendto(cipherText.encode('utf-8'),sA)
        if msg=='BYE':
            sys.exit(0)

UDPClientSocket = socket.socket(family=socket.AF_INET, type=socket.SOCK_DGRAM)

UDPClientSocket.sendto(bytesToSend, serverAddressPort)

msgFromServer = UDPClientSocket.recvfrom(bufferSize)

msg = "Message from Server {}".format(msgFromServer[0].decode('utf-8'))
print(msg)

while(True):
    threading.Thread(target=recv).start()
    threading.Thread(target=Send(serverAddressPort)).start()
```

---------- OUTPUT ----------

```
Message from Server Hello UDP Client 3 7387
HELLOCLIENT
Enter your reply  HiiServer 3 7387
BYEBYE
Enter your reply  okBye 3 7387
```