Academic Year 2022-23

SAP ID:60003200076

SHRI VILEPARLE KELAVANI MANDAL'S
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING
(Autonomous College Affiliated to the University of Mumbai)
NAAC ACCREDITED with "A" GRADE (CGPA : 3.18)

DEPARTMENT OF INFORMATION TECHNOLOGY

COURSE CODE: DJ19ITL501 **DATE: 22/10/22**

COURSE NAME: Cryptography and Network Security Lab **Class: A3**

LAB EXPERIMENT NO. 3

AIM: Design and Implementation of diffie hellman key exchange

DESCRIPTION OF EXPERIMENT:

The Diffie-Hellman algorithm is being used to establish a shared secret that can be used for secret communications while exchanging data over a public network using the elliptic curve to generate points and get the secret key using the parameters.

Security of diffie hellman lies in the fact that while its relatively easy to calculate exponent modulas for a prime it is very difficult to calculate discrete logs of large prime number.

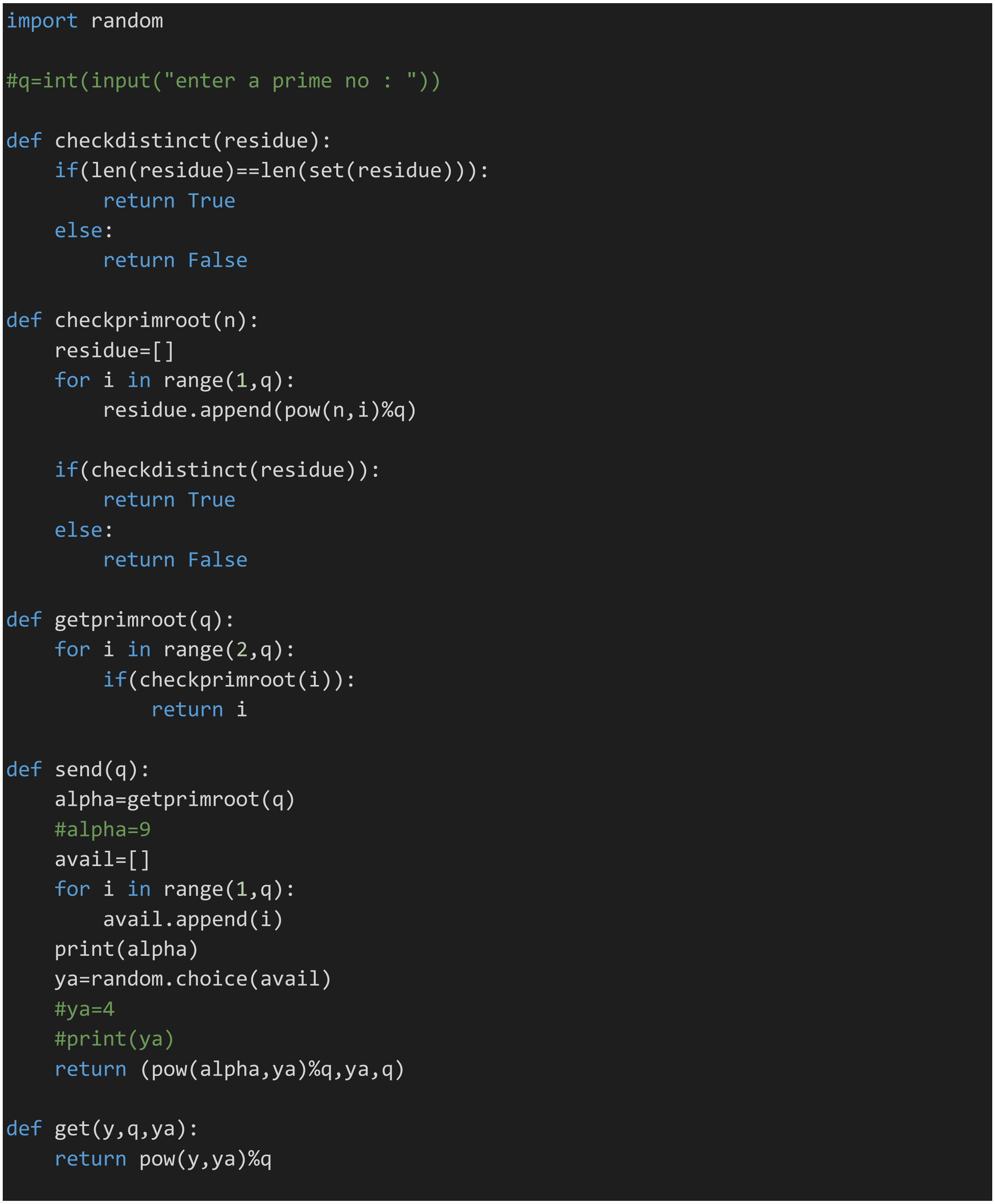
ALGORITHM:

1) Public Keys available = q(prime), alpha(primitive root of q) on both sides
2) Private Key Selected by person a= a
   Private Key Selected by person b= b
3) Key generated at a : xa= alpha^a mod q
   Key generated at b: xb= alpha^b mod q
4) Key exchange between a and b , a receives xb, b receives xa
5) Generated Secret Key of b by a: k1 = xb^a mod q
   Generated Secret Key of a by b: k2 = xa^b mod q
6) Algebraically, it can be shown that k1=k2

TECHNOLOGY STACK : Python

DESIGN AND IMPLEMENTATION CODE:

1) Diffie hellman:



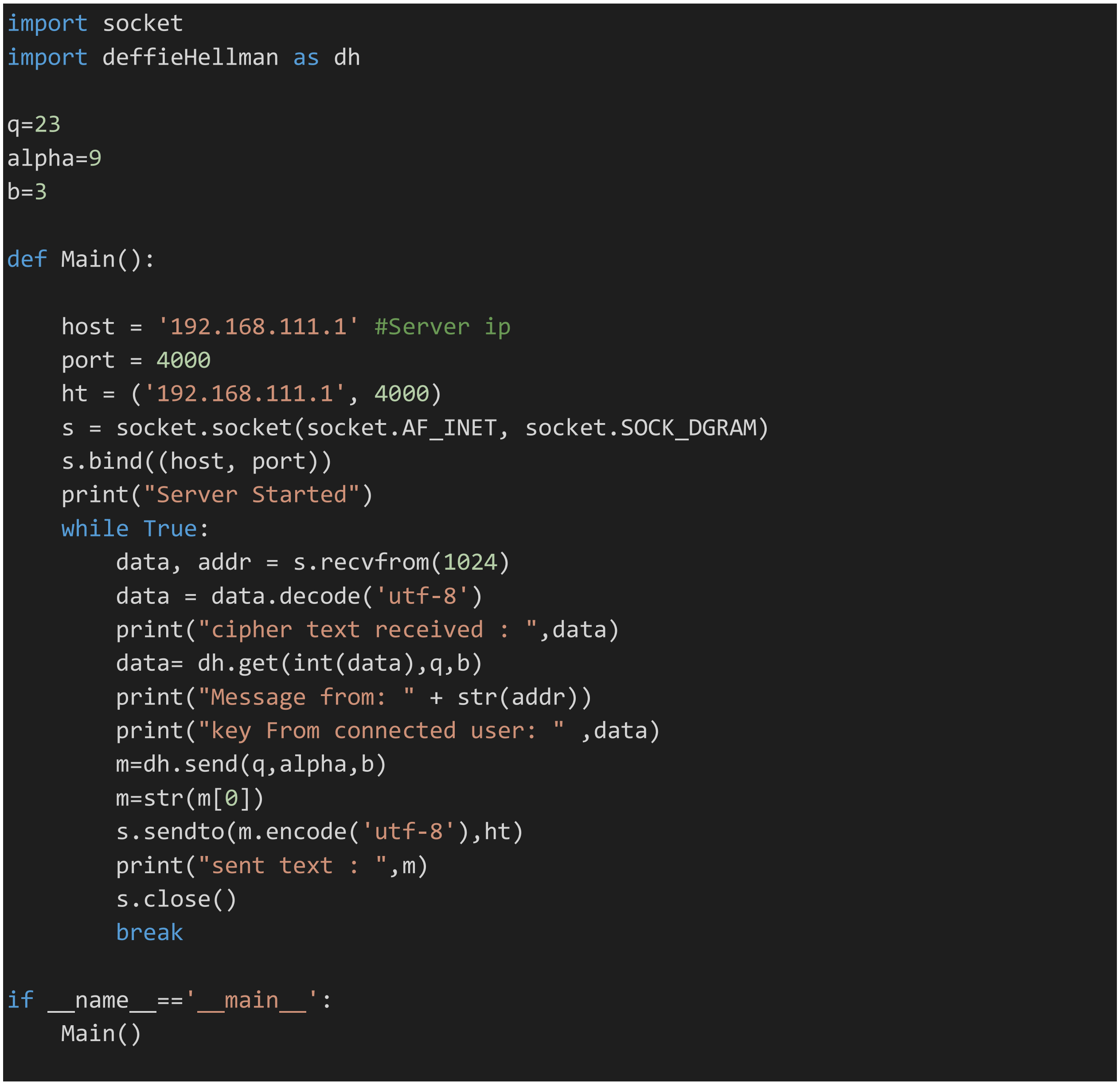
```
import random

#q=int(input("enter a prime no : "))

def checkdistinct(residue):
    if(len(residue)==len(set(residue))):
        return True
    else:
        return False

def checkprimroot(n):
    residue=[]
    for i in range(1,q):
        residue.append(pow(n,i)%q)

    if(checkdistinct(residue)):
        return True
    else:
        return False

def getprimroot(q):
    for i in range(2,q):
        if(checkprimroot(i)):
            return i

def send(q):
    alpha=getprimroot(q)
    #alpha=9
    avail=[]
    for i in range(1,q):
        avail.append(i)
    print(alpha)
    ya=random.choice(avail)
    #ya=4
    #print(ya)
    return (pow(alpha,ya)%q,ya,q)

def get(y,q,ya):
    return pow(y,ya)%q
```

```
#y=send(23)
#print(send(23))#(6, 4, 23)   (16, 3, 23)
#print(get(16,23,4))
```

2) Client:

```
import socket
import deffieHellman as dh

q=23
alpha=9
a=4

def Main():

    host='192.168.111.1' #client ip
    port = 4005

    server = ('192.168.111.1', 4000)

    s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
    s.bind((host,port))
    m=dh.send(q,alpha,a)
    m=str(m[0])
    s.sendto(m.encode('utf-8'), server)
    print("sent text : ",m)
    data= 16
    print("key From connected user: " ,dh.get(data,q,a))
    '''
    while True:
        data, addr = s.recvfrom(1024)
        data = data.decode('utf-8')
        print("cipher text received : ",data)
        data= dh.get(int(data),q,a)
        print("Message from: " + str(addr))
        print("key From connected user: " ,data)
        s.close()
        '''



if __name__=='__main__':
    Main()
```

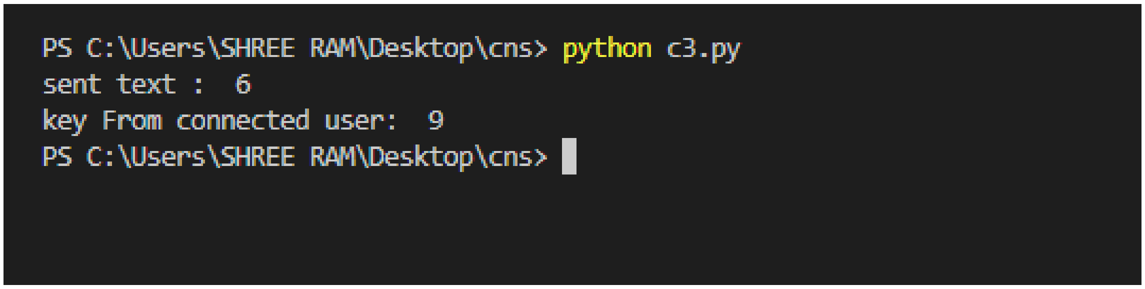
3) Server:



```
import socket
import deffieHellman as dh

q=23
alpha=9
b=3

def Main():

    host = '192.168.111.1' #Server ip
    port = 4000
    ht = ('192.168.111.1', 4000)
    s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
    s.bind((host, port))
    print("Server Started")
    while True:
        data, addr = s.recvfrom(1024)
        data = data.decode('utf-8')
        print("cipher text received : ",data)
        data= dh.get(int(data),q,b)
        print("Message from: " + str(addr))
        print("key From connected user: " ,data)
        m=dh.send(q,alpha,b)
        m=str(m[0])
        s.sendto(m.encode('utf-8'),ht)
        print("sent text : ",m)
        s.close()
        break

if __name__=='__main__':
    Main()
```

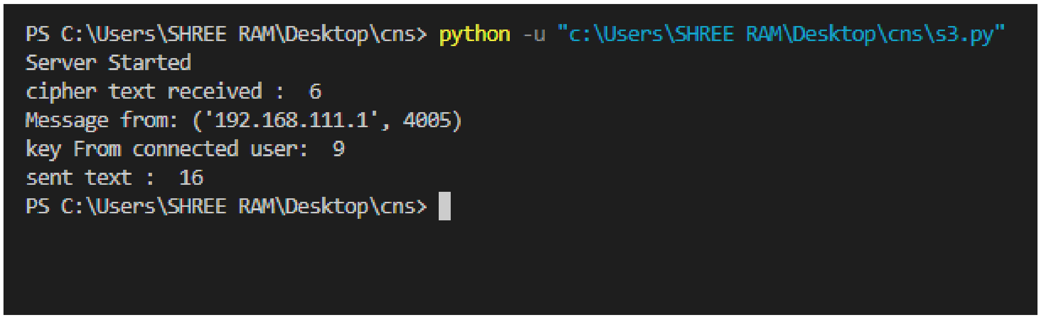
OUTPUT:

Client:



```
PS C:\Users\SHREE RAM\Desktop\cns> python c3.py
sent text :  6
key From connected user:  9
PS C:\Users\SHREE RAM\Desktop\cns> 
```

Server:



```
PS C:\Users\SHREE RAM\Desktop\cns> python -u "c:\Users\SHREE RAM\Desktop\cns\s3.py"
Server Started
cipher text received :  6
Message from: ('192.168.111.1', 4005)
key From connected user:  9
sent text :  16
PS C:\Users\SHREE RAM\Desktop\cns> 
```

CONCLUSION:

Thus, we have studied and implemented diffie hellman key exchange algorithm.