Cryptography & Network Security

PRN - 2019BTECS00026

Name - Niraja Vasudev Kulkarni

Batch - B1

Assignment - 11

Title: Diffie-Hellman Key Exchange

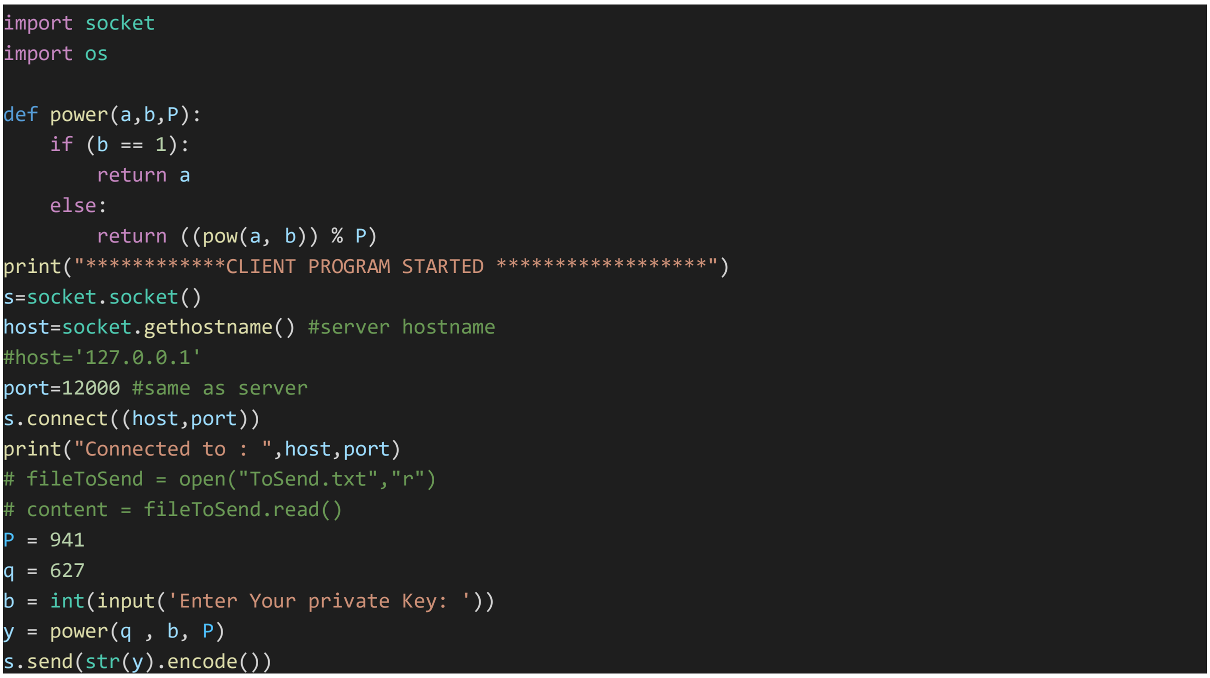
Aim: To Demonstrate Diffie-Hellman Key Exchange

Theory:

Diffie–Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as conceived by Ralph Merkle and named after Whitfield Diffie and Martin Hellman.

Code:

Client -



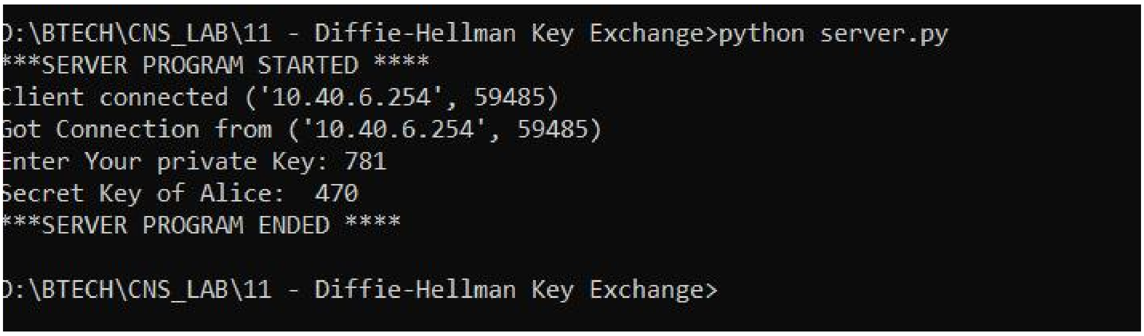
```
import socket
import os

def power(a,b,P):
    if (b == 1):
        return a
    else:
        return ((pow(a, b)) % P)
print("************CLIENT PROGRAM STARTED *****************")
s=socket.socket()
host=socket.gethostname() #server hostname
#host='127.0.0.1'
port=12000 #same as server
s.connect((host,port))
print("Connected to : ",host,port)
# fileToSend = open("ToSend.txt","r")
# content = fileToSend.read()
P = 941
q = 627
b = int(input('Enter Your private Key: '))
y = power(q , b, P)
s.send(str(y).encode())
```

```
x = int(s.recv(100).decode())
kb = power(x, b, P);
print('Secret Key of Bob: ' ,kb)
print("************CLIENT PROGRAM ENDED ******************")
```

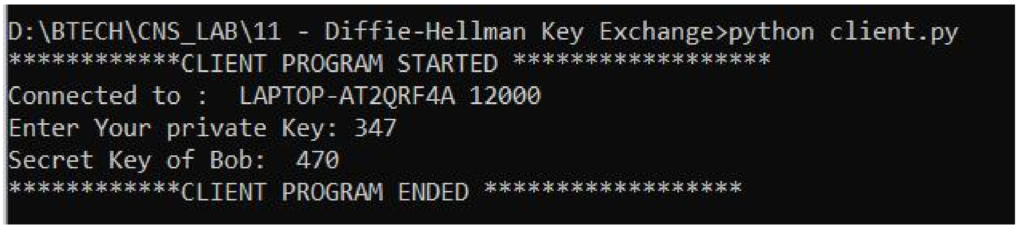
Server -

```
import socket
import os
import sys

def power(a,b,P):
    if (b == 1):
        return a
    else:
        return ((pow(a, b)) % P)
print("***SERVER PROGRAM STARTED ****")
s=socket.socket()
host=socket.gethostname()
#host='127.0.0.1'
port=12000 #ports after 6000 are free
s.bind((host,port))
s.listen(10)
P = 941
q = 627
while True:
    c,addr=s.accept()
    print ("Client connected",addr)
    print ('Got Connection from' ,addr)
    a = int(input('Enter Your private Key: '))
    x = power(q , a, P)
    y=int(c.recv(100).decode())
    if not y:
        break
    c.send(str(x).encode())
    ka = power(y, a, P); #Secret key for Alice
    print('Secret Key of Alice: ', ka)
    break
print("***SERVER PROGRAM ENDED ****")
```

Output:



```
D:\BTECH\CNS_LAB\11 - Diffie-Hellman Key Exchange>python server.py
***SERVER PROGRAM STARTED ****
Client connected ('10.40.6.254', 59485)
Got Connection from ('10.40.6.254', 59485)
Enter Your private Key: 781
Secret Key of Alice:  470
***SERVER PROGRAM ENDED ****

D:\BTECH\CNS_LAB\11 - Diffie-Hellman Key Exchange>
```



```
D:\BTECH\CNS_LAB\11 - Diffie-Hellman Key Exchange>python client.py
************CLIENT PROGRAM STARTED ******************
Connected to :  LAPTOP-AT2QRF4A 12000
Enter Your private Key: 347
Secret Key of Bob:  470
************CLIENT PROGRAM ENDED ******************
```

Conclusion:

The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric-key cipher.