Assignment – 7

* Server:

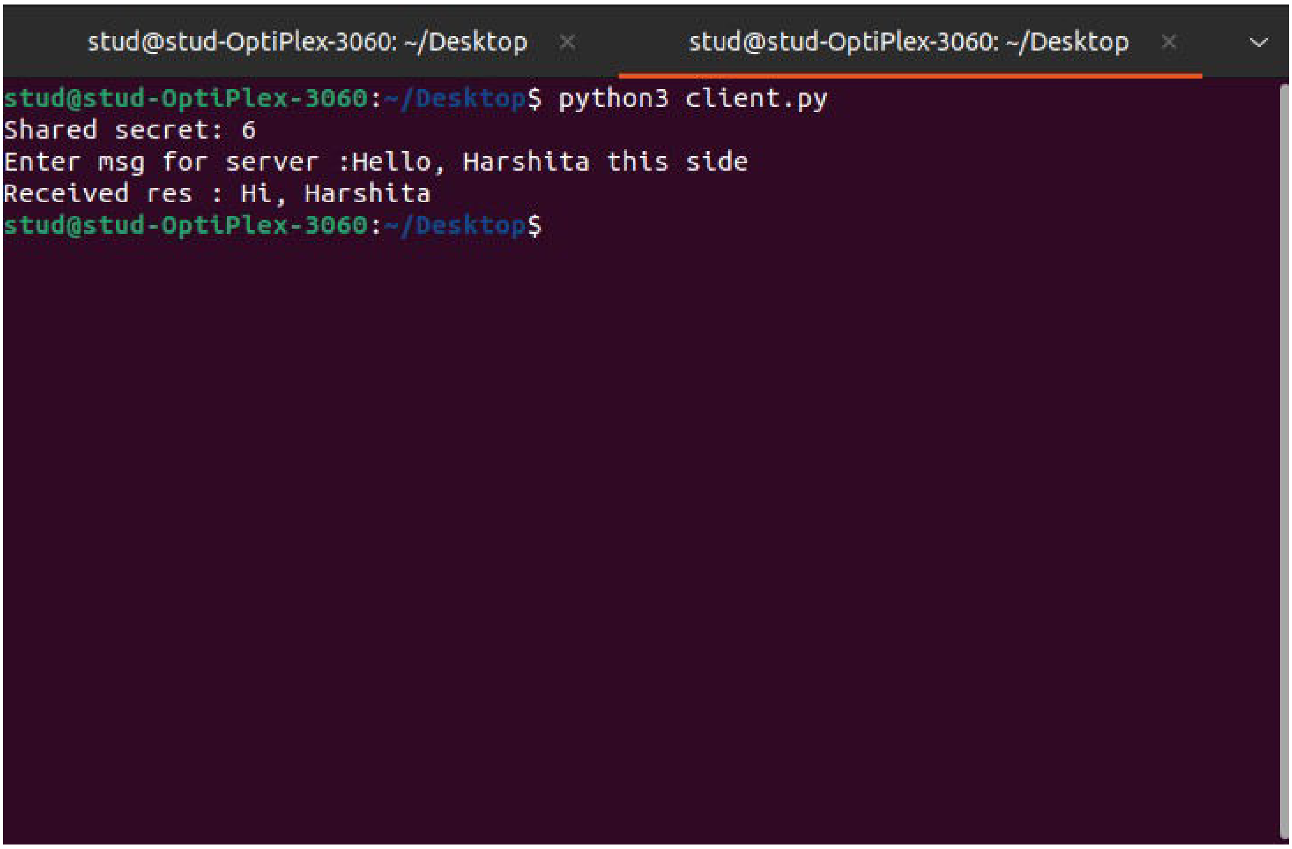
```
import socket
import random
from Crypto.Cipher import DES
from Crypto.Util.Padding import pad,unpad
prime=23
generator=5

private_key_s=random.randint(1,prime-1)
public_key_s=pow(generator,private_key_s,prime)
server_socket=socket.socket()
server_socket.bind(('localhost',8000))
server_socket.listen(1)
print("Server is listening...")

client_socket,address=server_socket.accept()
print("conneted to client:",address)

client_socket.send(str(public_key_s).encode())

public_key_c=int(client_socket.recv(1024).decode())
shared_secret=pow(public_key_c,private_key_s,prime)
print("Shared secret:",shared_secret)

key=str(shared_secret).zfill(8)[:8].encode()

cipher=DES.new(key,DES.MODE_ECB)

encrypted_msg=client_socket.recv(1024)
decrypted_msg=unpad(cipher.decrypt(encrypted_msg),DES.block_size)
print("Received msg :",decrypted_msg.decode())

response_msg=input("Enter response msg :")
encrypted_res=cipher.encrypt(pad(response_msg.encode(),DES.block_size))
client_socket.send(encrypted_res)

client_socket.close()
server_socket.close()
```

* Code:

```
import socket
import random
from Crypto.Cipher import DES
from Crypto.Util.Padding import pad,unpad
prime=23
generator=5
private_key_c=random.randint(1,prime-1)
```

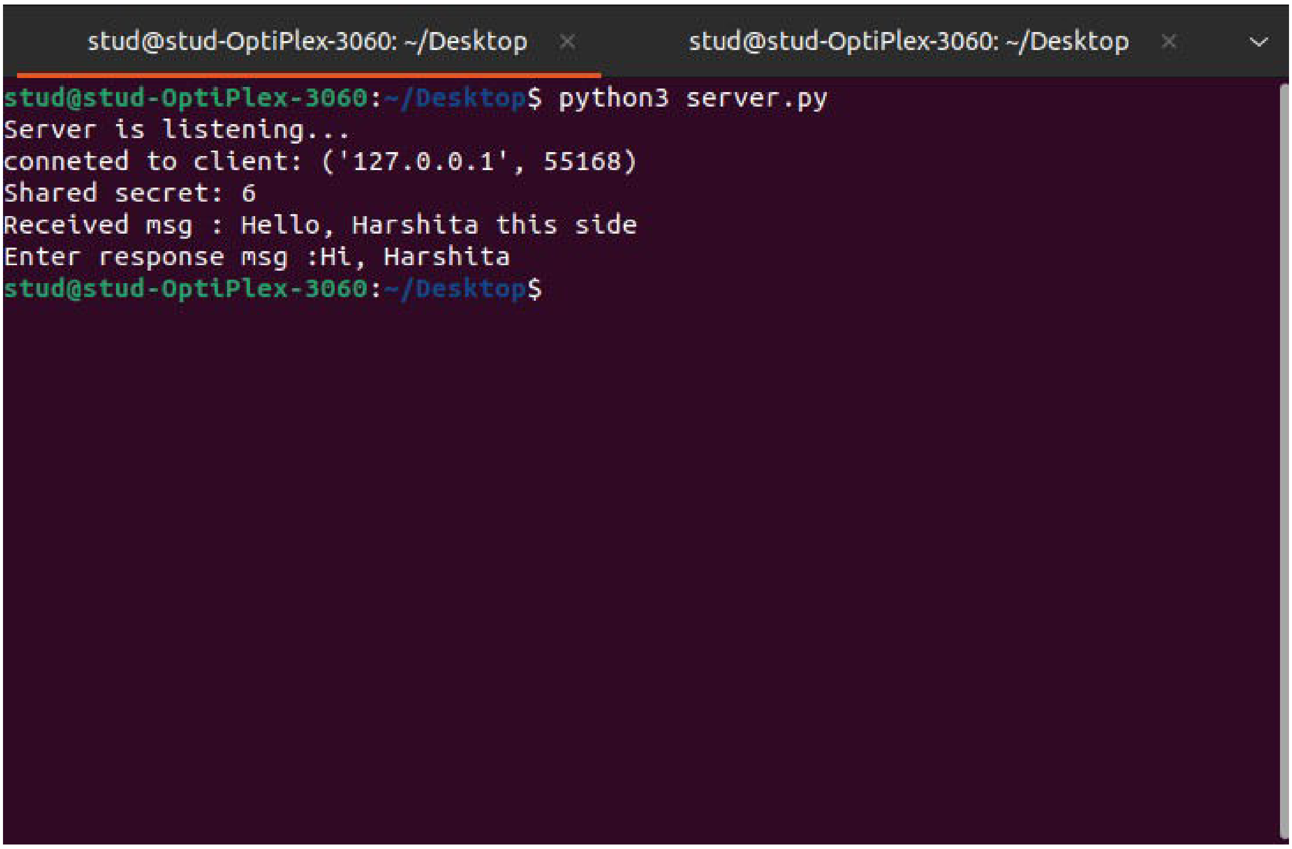
```
public_key_c=pow(generator,private_key_c,prime)
client_socket=socket.socket()
client_socket.connect(('localhost',8000))

client_socket.send(str(public_key_c).encode())

public_key_s=int(client_socket.recv(1024).decode())
shared_secret=pow(public_key_s,private_key_c,prime)
print("Shared secret:",shared_secret)

key=str(shared_secret).zfill(8)[:8].encode()

cipher=DES.new(key,DES.MODE_ECB)

msg=input("Enter msg for server :")
encrypted_msg=cipher.encrypt(pad(msg.encode(),DES.block_size))
client_socket.send(encrypted_msg)

encrypted_res=client_socket.recv(1024)
decrypted_res=unpad(cipher.decrypt(encrypted_res),DES.block_size)
print("Received res :",decrypted_res.decode())

client_socket.close()
```

* OUTPUT :



stud@stud-OptiPlex-3060: ~/Desktop
stud@stud-OptiPlex-3060: ~/Desktop

```
stud@stud-OptiPlex-3060:~/Desktop$ python3 client.py
Shared secret: 6
Enter msg for server :Hello, Harshita this side
Received res : Hi, Harshita
stud@stud-OptiPlex-3060:~/Desktop$
```



stud@stud-OptiPlex-3060: ~/Desktop
stud@stud-OptiPlex-3060: ~/Desktop

```
stud@stud-OptiPlex-3060:~/Desktop$ python3 server.py
Server is listening...
conneted to client: ('127.0.0.1', 55168)
Shared secret: 6
Received msg : Hello, Harshita this side
Enter response msg :Hi, Harshita
stud@stud-OptiPlex-3060:~/Desktop$
```