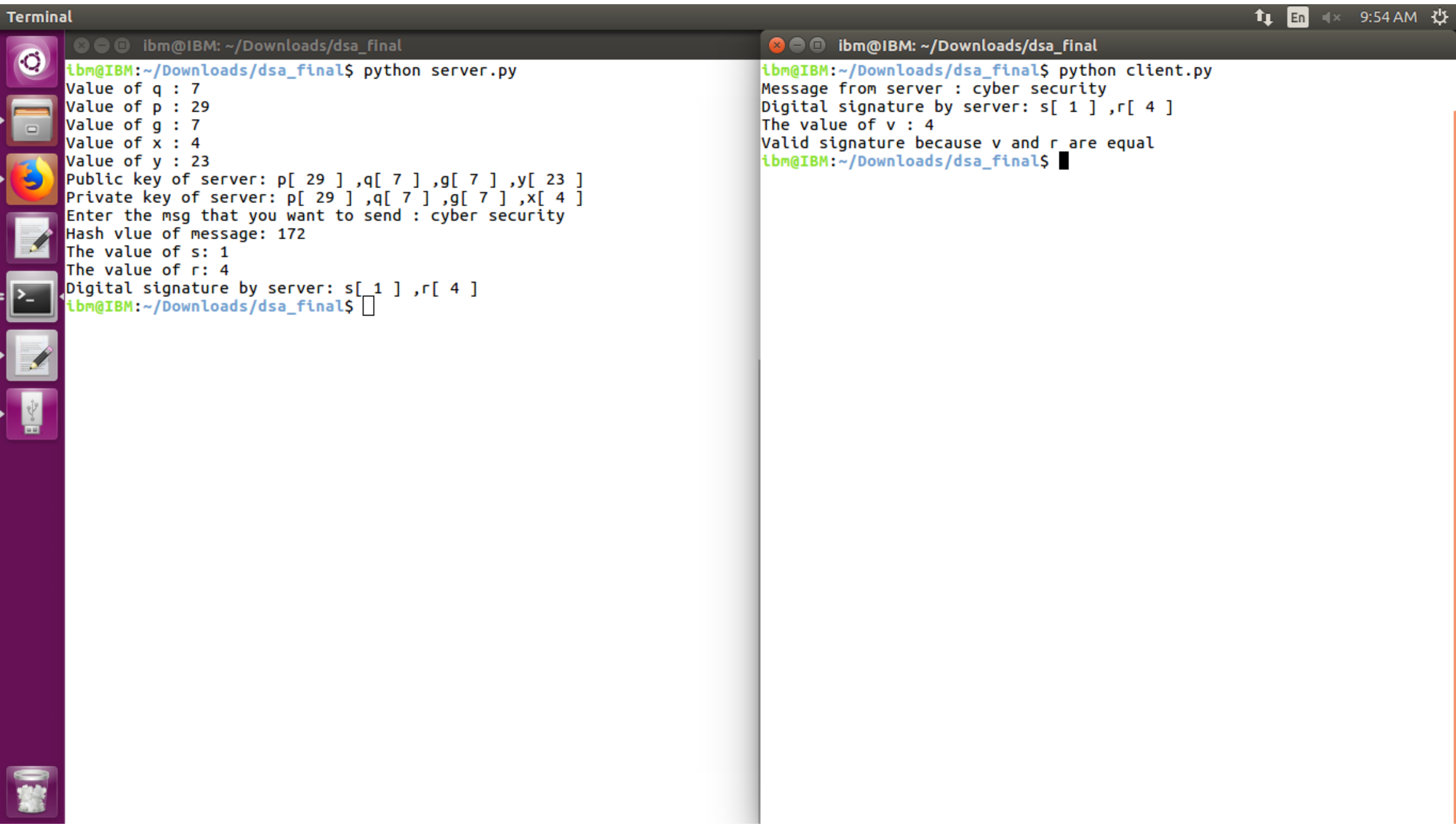
```
#Server

import socket
import hashlib
import sys
import random
import time as t
st = socket.socket()
port = int(raw_input("Enter the port number: "))
st.bind(("localhost",port))
st.listen(5)
c,addr = st.accept()
start = 2
stop = 10
def isprime(ran):
    if(ran > 2):
        for i in range(2,ran):
            if(ran%i==0):
                return 0
        return 1
while(1):
    q = random.randrange(start,stop)
    if(q>2):
        result = isprime(q)
    if(result == 0):
        continue
    else:
        break
print "Value of q :",q
temp = str(q)
c.send(temp)
t.sleep(.2)
p=0
while((p-1)%q!=0):
    while(1):
        p = random.randrange(2,31)
        result = isprime(p)
        if(result == 0):
            continue
        else:
            break

print "Value of p :",p
temp = str(p)
c.send(temp)
t.sleep(.2)
g=random.randrange(1,p)
h=random.randrange(1,p-1)
while(g**q%p!=1):
    g = h**((p-1)/q)%p
x = random.randrange(0,q)
y = g**x%p
```

```
print "Value of g :",g
temp = str(g)
c.send(temp)
t.sleep(.2)

print "Value of x :",x


print "Value of y :",y
temp = str(y)
c.send(temp)
t.sleep(.2)

print "Public key of server: p[",p,"] ,q[",q,"] ,g[",g,"] ,y[",y,"]"
print "Private key of server: p[",p,"] ,q[",q,"] ,g[",g,"] ,x[",x,"]"
msg = raw_input("Enter the msg that you want to send : ")
c.send(msg)
t.sleep(.2)

H = ord(hashlib.md5(msg).digest()[0])
print "Hash vlue of message:",H


s=0
while(s==0):
        k = random.randrange(1,q)
        r=(g**k%p)%q
        #print "the value of r :",r
        while(r==0):
                k = random.randrange(0,q)
                r=(g**k%p)%q
                #print "The value of r:",r
        i = random.randrange(1,40)
        while(k*i%q!=1):
                i = random.randrange(1,40)
                #print "the value of i:",i
        s = i*(H+r*x)%q
        #print "the value of s :",s
print "The value of s:",s
temp = str(s)
c.send(temp)
t.sleep(.2)

print "The value of r:",r
temp = str(r)
c.send(temp)
t.sleep(.2)

print "Digital signature by server: s[",s,"] ,r[",r,"]"
```

```
#client

import socket
import hashlib
import random
st = socket.socket()
port = int(raw_input("Enter the port number: "))
st.connect(("localhost",port))
q = st.recv(10)
q = int(q)
print "Value of q :",q

p = st.recv(10)
p = int(p)
print "Value of p :",p

g = st.recv(10)
g = int(g)
print "Value of g :",g

y = st.recv(10)
y = int(y)
print "Value of y :",y

print "Public key of server: p[",p,"] ,q[",q,"] ,g[",g,"] ,y[",y,"]"
msg = st.recv(1024)
print "Message from server :",msg

s = st.recv(10)
s = int(s)
print "The value of s :",s
r = st.recv(10)
r = int(r)
print "The value of r :",r
print "Digital signature by server: s[",s,"] ,r[",r,"]"

H = ord(hashlib.md5(msg).digest()[0])
w = random.randrange(1,100)
while((s*w)%q!=1):
	w = random.randrange(1,100)
u1 = H*w%q
u2 = r*w%q
v = (((g**u1)*(y**u2))%p)%q
print "The value of v :",v
if(v==r):
	print "Valid signature because v and r are equal"
else:
	print "Invalid signature"
```


Terminal
En
9:54 AM
ibm@IBM: ~/Downloads/dsa_final
ibm@IBM: ~/Downloads/dsa_final

```
ibm@IBM:~/Downloads/dsa_final$ python server.py
Value of q : 7
Value of p : 29
Value of g : 7
Value of x : 4
Value of y : 23
Public key of server: p[ 29 ] ,q[ 7 ] ,g[ 7 ] ,y[ 23 ]
Private key of server: p[ 29 ] ,q[ 7 ] ,g[ 7 ] ,x[ 4 ]
Enter the msg that you want to send : cyber security
Hash vlue of message: 172
The value of s: 1
The value of r: 4
Digital signature by server: s[ 1 ] ,r[ 4 ]
ibm@IBM:~/Downloads/dsa_final$
```

```
ibm@IBM:~/Downloads/dsa_final$ python client.py
Message from server : cyber security
Digital signature by server: s[ 1 ] ,r[ 4 ]
The value of v : 4
Valid signature because v and r are equal
ibm@IBM:~/Downloads/dsa_final$
```