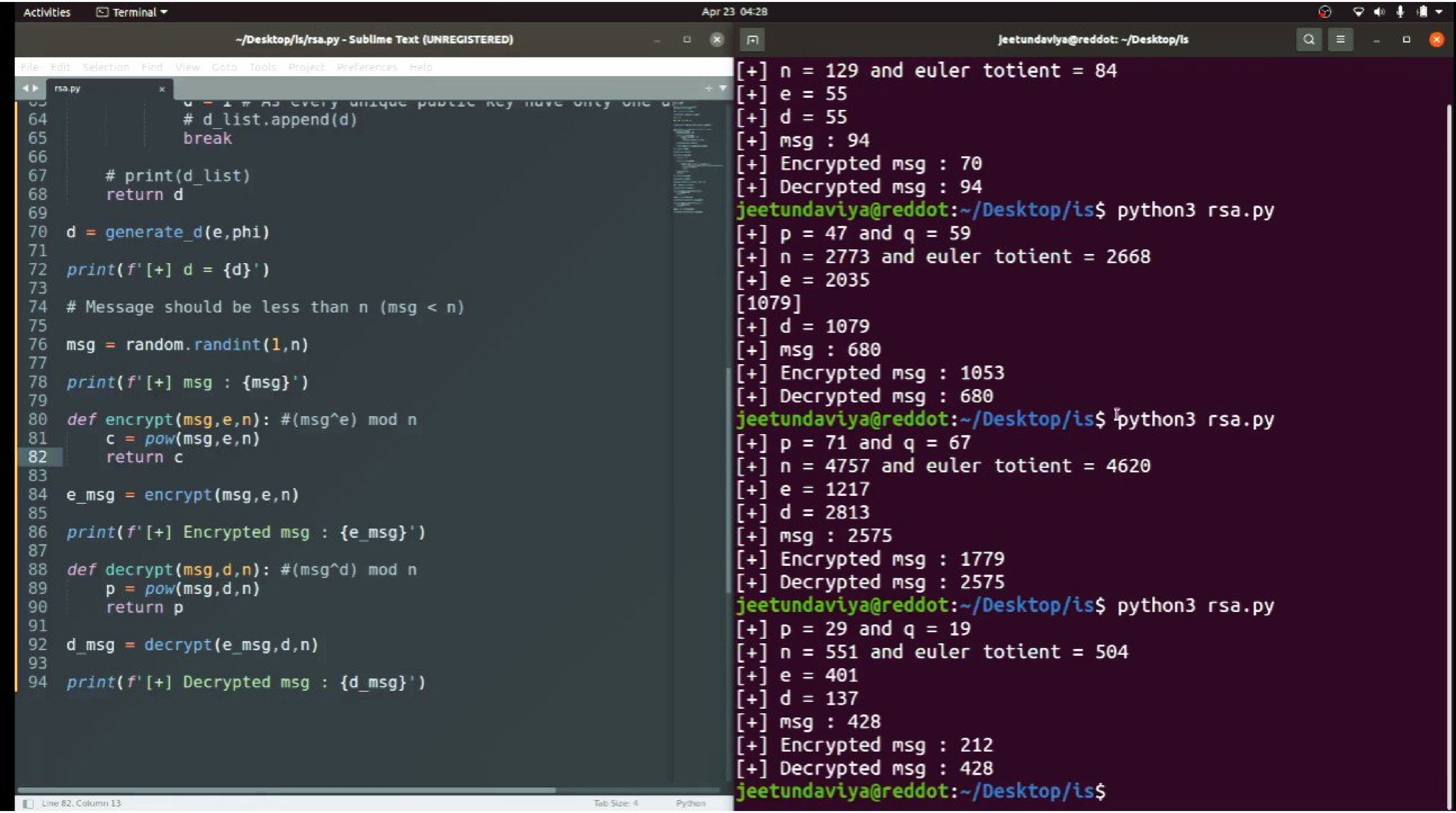
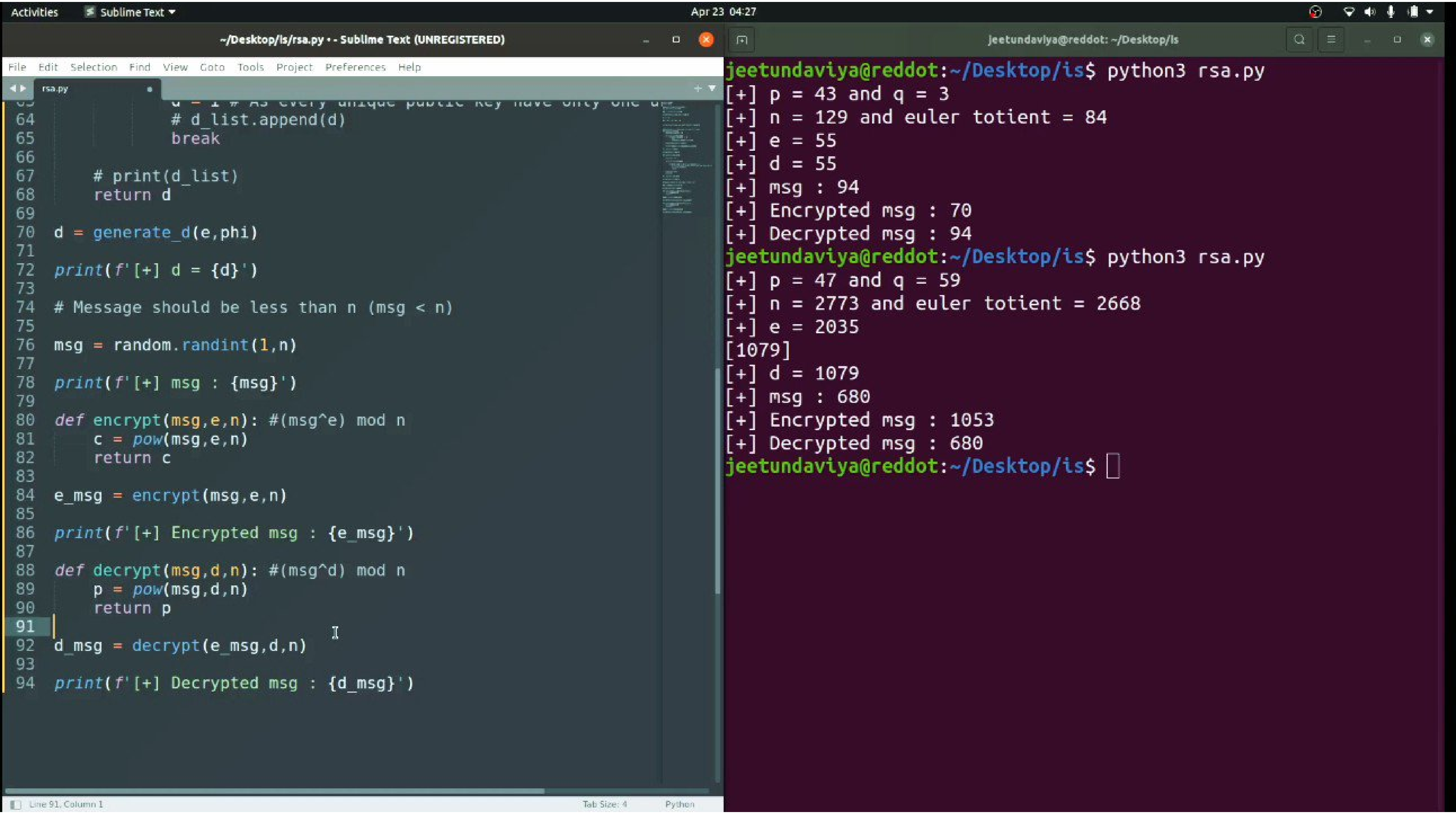

Activities
Terminal
Apr 23 04:28
~/Desktop/is/rsa.py - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
rsa.py
jeetundaviya@reddot: ~/Desktop/is
Line 82, Column 13
Tab Size: 4
Python

```python
            d = 1 # As every unique public key have only one d
            # d_list.append(d)
            break

    # print(d_list)
    return d

d = generate_d(e,phi)

print(f'[+] d = {d}')

# Message should be less than n (msg < n)

msg = random.randint(1,n)

print(f'[+] msg : {msg}')

def encrypt(msg,e,n): #(msg^e) mod n
    c = pow(msg,e,n)
    return c

e_msg = encrypt(msg,e,n)

print(f'[+] Encrypted msg : {e_msg}')

def decrypt(msg,d,n): #(msg^d) mod n
    p = pow(msg,d,n)
    return p

d_msg = decrypt(e_msg,d,n)

print(f'[+] Decrypted msg : {d_msg}')
```

```
[+] n = 129 and euler totient = 84
[+] e = 55
[+] d = 55
[+] msg : 94
[+] Encrypted msg : 70
[+] Decrypted msg : 94
jeetundaviya@reddot:~/Desktop/is$ python3 rsa.py
[+] p = 47 and q = 59
[+] n = 2773 and euler totient = 2668
[+] e = 2035
[1079]
[+] d = 1079
[+] msg : 680
[+] Encrypted msg : 1053
[+] Decrypted msg : 680
jeetundaviya@reddot:~/Desktop/is$ python3 rsa.py
[+] p = 71 and q = 67
[+] n = 4757 and euler totient = 4620
[+] e = 1217
[+] d = 2813
[+] msg : 2575
[+] Encrypted msg : 1779
[+] Decrypted msg : 2575
jeetundaviya@reddot:~/Desktop/is$ python3 rsa.py
[+] p = 29 and q = 19
[+] n = 551 and euler totient = 504
[+] e = 401
[+] d = 137
[+] msg : 428
[+] Encrypted msg : 212
[+] Decrypted msg : 428
jeetundaviya@reddot:~/Desktop/is$
```


Activities
Sublime Text
Apr 23 04:27
~/Desktop/is/rsa.py • - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
rsa.py
jeetundaviya@reddot: ~/Desktop/is
Line 91, Column 1
Tab Size: 4
Python

```python
            d = 1 # As every unique public key have only one d
            # d_list.append(d)
            break

    # print(d_list)
    return d

d = generate_d(e,phi)

print(f'[+] d = {d}')

# Message should be less than n (msg < n)

msg = random.randint(1,n)

print(f'[+] msg : {msg}')

def encrypt(msg,e,n): #(msg^e) mod n
    c = pow(msg,e,n)
    return c

e_msg = encrypt(msg,e,n)

print(f'[+] Encrypted msg : {e_msg}')

def decrypt(msg,d,n): #(msg^d) mod n
    p = pow(msg,d,n)
    return p

d_msg = decrypt(e_msg,d,n)

print(f'[+] Decrypted msg : {d_msg}')
```

```
jeetundaviya@reddot:~/Desktop/is$ python3 rsa.py
[+] p = 43 and q = 3
[+] n = 129 and euler totient = 84
[+] e = 55
[+] d = 55
[+] msg : 94
[+] Encrypted msg : 70
[+] Decrypted msg : 94
jeetundaviya@reddot:~/Desktop/is$ python3 rsa.py
[+] p = 47 and q = 59
[+] n = 2773 and euler totient = 2668
[+] e = 2035
[1079]
[+] d = 1079
[+] msg : 680
[+] Encrypted msg : 1053
[+] Decrypted msg : 680
jeetundaviya@reddot:~/Desktop/is$
```

```
import random
import math

#select 2 large prime numbers
def generate_p_and_q():

    #Calculating 1 to 100 prime numbers

    numbs = [i for i in range(2,101)]

    for n in range(2,101):
        for i in range(2,math.ceil(n/2)+1):
            if n % i == 0:
                numbs.remove(n)
                break
            else:
                continue

    #Selecting any 2 prime numbers randomly

    p = random.choice(numbs)
    numbs.remove(p)
    q = random.choice(numbs)

    return p, q

p,q =    generate_p_and_q()

print(f'[+] p = {p} and q = {q}')

n = p * q

phi = (p - 1) * (q - 1)


print(f'[+] n = {n} and euler totient = {phi}')


#Calculating e -> gcd(e,phi) = 1 and 1 < e <phi.
def generate_e(phi):
    possible_e_values = []

    for i in range(2,phi):
        if math.gcd(i,phi) == 1:
            e=i
            possible_e_values.append(e)

    # print(possible_e_values)

    return random.choice(possible_e_values)

e = generate_e(phi)

print(f'[+] e = {e}')

def generate_d(e,phi):
```

WPS Office

```
    # d_list = []

    for i in range(2,phi):

        if (i*e) % phi == 1: #    ed mod(phi) = 1
            d = i # As every unique public key have only one unique private key.
            # d_list.append(d)
            break

    # print(d_list)
    return d

d = generate_d(e,phi)

print(f'[+] d = {d}')

# Message should be less than n (msg < n)

msg = random.randint(1,n)

print(f'[+] msg : {msg}')

def encrypt(msg,e,n): #(msg^e) mod n
    c = pow(msg,e,n)
    return c

e_msg = encrypt(msg,e,n)

print(f'[+] Encrypted msg : {e_msg}')

def decrypt(msg,d,n): #(msg^d) mod n
    p = pow(msg,d,n)
    return p

d_msg = decrypt(e_msg,d,n)

print(f'[+] Decrypted msg : {d_msg}')
```

WPS Office