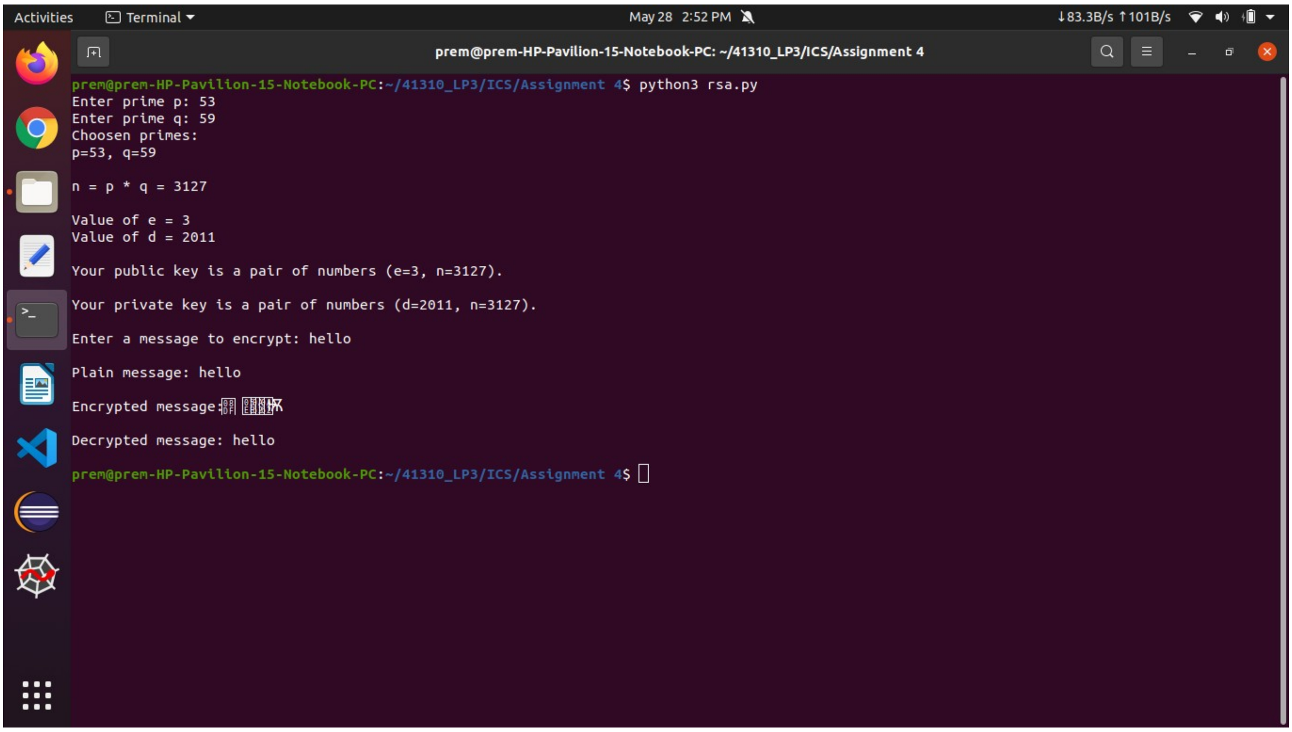
Name : Prem Vinod Bansod
Roll no : 41310
Assignment No : 04 (ICS)

Code:

```
def gcd(a, b):
    while b != 0:
        c = a % b
        a = b
        b = c
    return a

def isPrime(num):
        if num > 1:
                for i in range(2, num//2):
                        if (num % i) == 0:
                                return False
                        else:
                                return True
        else:
                return False

def cal_d(e, phi):
    d = 0
    k = 1
    while True:
        temp = 1 + k * phi
        if temp % e == 0 and temp / e != e:
            d = temp/e
            break
        k += 1
    return d

def encrypt_block(m):
    c = m ** e % n
    return c


def decrypt_block(c):
    m = c ** d % n
    return m


def encrypt_string(s):
    return ".join([chr(encrypt_block(ord(x))) for x in list(s)])


def decrypt_string(s):
    return ".join([chr(decrypt_block(ord(x))) for x in list(s)])

if __name__ == "__main__":
```

```
p = int(input('Enter prime p: '))
q = int(input('Enter prime q: '))

if( isPrime(p) == False or isPrime(q) == False):
    print('Both numbers are not prime')
    exit()

print("Choosen primes:\np=" + str(p) + ", q=" + str(q) + "\n")

n = p * q
print("n = p * q = " + str(n) + "\n")

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

e = int(2)
while (e < phi):
    if gcd(e,phi) == 1:
        break
    else:
        e += 1

print("Value of e = "+str(e))

d = int(cal_d(e,phi))
print("Value of d = "+str(d))


print("\nYour public key is a pair of numbers (e=" + str(e) + ", n=" + str(n) + ").\n")
print("Your private key is a pair of numbers (d=" + str(d) + ", n=" + str(n) + ").\n")

s = input("Enter a message to encrypt: ")
print("\nPlain message: " + s + "\n")
enc = encrypt_string(s)
print("Encrypted message: ", enc, "\n")
dec = decrypt_string(enc)
print("Decrypted message: " + dec + "\n")
```

Output:



Activities
Terminal
May 28 2:52 PM
↓83.3B/s ↑101B/s
prem@prem-HP-Pavilion-15-Notebook-PC: ~/41310_LP3/ICS/Assignment 4

```
prem@prem-HP-Pavilion-15-Notebook-PC:~/41310_LP3/ICS/Assignment 4$ python3 rsa.py
Enter prime p: 53
Enter prime q: 59
Choosen primes:
p=53, q=59

n = p * q = 3127

Value of e = 3
Value of d = 2011

Your public key is a pair of numbers (e=3, n=3127).

Your private key is a pair of numbers (d=2011, n=3127).

Enter a message to encrypt: hello

Plain message: hello

Encrypted message:ࣟ ׮੢੢Ѭ

Decrypted message: hello

prem@prem-HP-Pavilion-15-Notebook-PC:~/41310_LP3/ICS/Assignment 4$ 
```