

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("Chooosen 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:

A screenshot of a Linux terminal window titled "Terminal". The window shows the execution of a Python script named "rsa.py". The user enters prime numbers p=53 and q=59, which are chosen primes. The script calculates n = p \* q = 3127, e = 3, and d = 2011. It then displays the public key (e=3, n=3127) and the private key (d=2011, n=3127). A message "hello" is entered for encryption, resulting in the encrypted message "H8P8". Decryption of "H8P8" yields the original message "hello". The terminal prompt is "prem@prem-HP-Pavilion-15-Notebook-PC: ~/41310\_LP3/ICS/Assignment 4\$". The system status bar at the top indicates the date as May 28, 2:52 PM, and network speeds of 83.3B/s download and 101B/s upload. The left sidebar shows various application icons like Firefox, Chrome, Files, and Settings.