DAY 3

12.Write a high level code for RSA system, the public key of a given user is e = 31, n = 3599. What is the private key of this user?

PROGRAM:

e = 31

n = 3599

def generate\_private\_key(e, n):

p = 61

q = 59

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

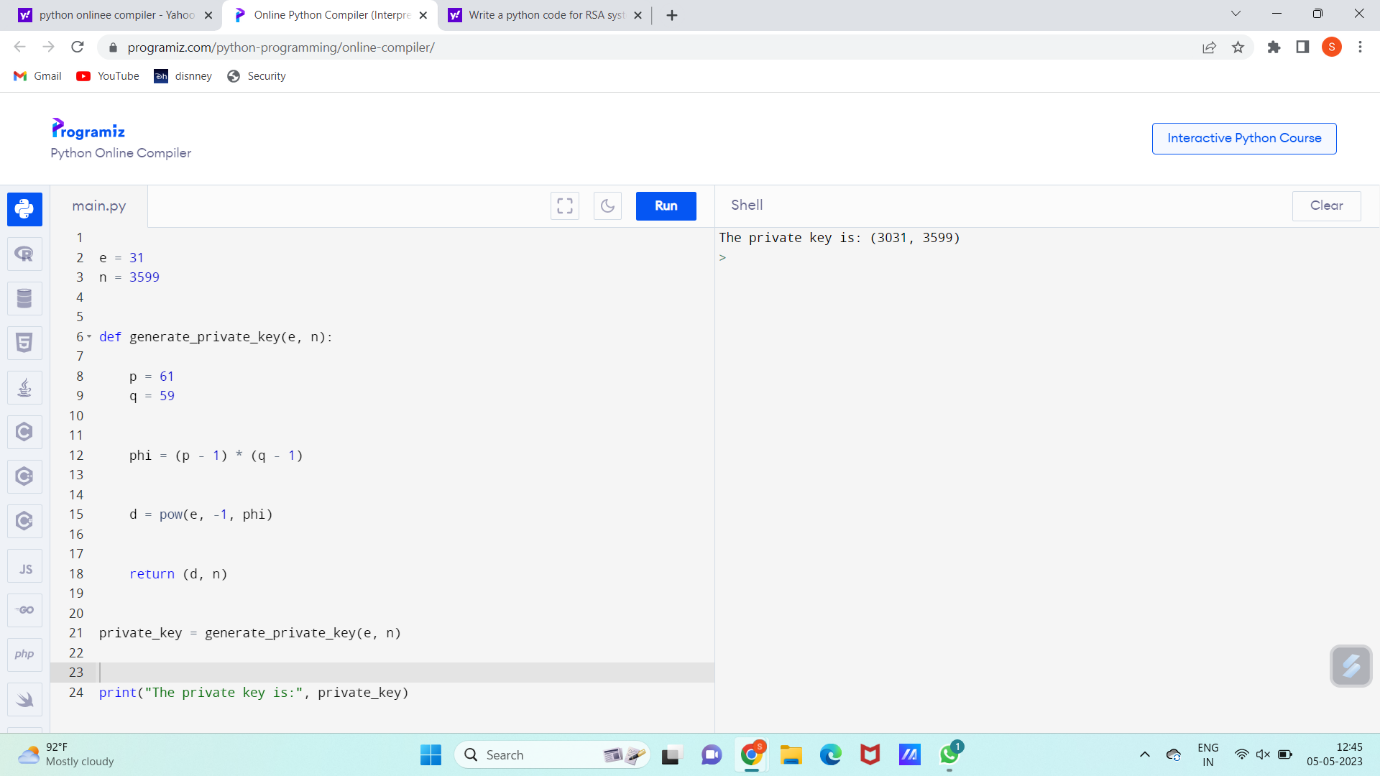
d = pow(e, -1, phi)

return (d, n)

private\_key = generate\_private\_key(e, n)

print("The private key is:", private\_key)

output:



13. Write a high-level code for set of blocks encoded with the RSA algorithm and we don’t have the private key. Assume n = pq, e is the public key. Suppose also someone tells us they know one of the plaintext blocks has a common factor with n. Does this help us in any way?

Program:

e = 31

encoded\_blocks = [1221, 1335, 1765, 1963, 2345]

def check\_common\_factor(block):

if n % block == 0:

return True, n // block

else:

return False, None

for block in encoded\_blocks:

has\_common\_factor, factor = check\_common\_factor(block)

if has\_common\_factor:

print("Block {} has a common factor with n: {}".format(block, factor))

break

else:

print("No plaintext block has a common factor with n.")

output:

