Q.No.13 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: import random

e = 31

n = 3599

def phi(n):

result = n

p = 2

while p \* p <= n:

if n % p == 0:

while n % p == 0:

n //= p

result -= result // p

p += 1

if n > 1:

result -= result // n

return result

phi\_n = phi(n)

def mod\_inv(a, m):

m0 = m

y = 0

x = 1

if m == 1:

return 0

while a > 1:

q = a // m

t = m

m = a % m

a = t

t = y

y = x - q \* y

x = t

if x < 0:

x += m0

return x

d = mod\_inv(e, phi\_n)

print("Public key: (e = {}, n = {})".format(e, n))

print("Private key: (d = {})".format(d))

Output:

Public key: (e = 31, n = 3599)

Private key: (d = 3031)