CSA5122-CRYPTOGRAPHY FOR NETWORK AND SECURITY

LAB PROGRAMS EXECUTION

11.RSA ALGORITHM

import math

# step 1

p = 3

q = 7

# step 2

n = p\*q

print("n =", n)

# step 3

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

# step 4

e = 2

while(e<phi):

if (math.gcd(e, phi) == 1):

break

else:

e += 1

print("e =", e)

# step 5

k = 2

d = ((k\*phi)+1)/e

print("d =", d)

print(f'Public key: {e, n}')

print(f'Private key: {d, n}')

# plain text

msg = 11

print(f'Original message:{msg}')

# encryption

C = pow(msg, e)

C = math.fmod(C, n)

print(f'Encrypted message: {C}')

# decryption

M = pow(C, d)

M = math.fmod(M, n)

print(f'Decrypted message: {M}')

