**CSS PRACTICAL 2**

def euclid(m, n):

  if n == 0:

    return m

  else:

    r = m % n

    return euclid(n, r)

def exteuclid(a, b):

  r1 = a

  r2 = b

  s1 = int(1)

  s2 = int(0)

  t1 = int(0)

  t2 = int(1)

  while r2 > 0:

    q = r1//r2

    r = r1-q \* r2

    r1 = r2

    r2 = r

    s = s1-q \* s2

    s1 = s2

    s2 = s

    t = t1-q \* t2

    t1 = t2

    t2 = t

  if t1 < 0:

    t1 = t1 % a

  return (r1, t1)

p = int(input("Enter p value: "))

q = int(input("Enter q value: "))

n = p \* q

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

key = []

for i in range(2, Pn):

  gcd = euclid(Pn, i)

  if gcd == 1:

    key.append(i)

e =int(input("Enter e value (<{}): ".format(Pn)))

r, d = exteuclid(Pn, e)

if r == 1:

  d = int(d)

  print("decryption key is: ", d)

else:

  print("Multiplicative inverse for\ the given encryption key does not \ exist. Choose a different encryption key ")

# Enter the message to be sent

M = 19070

# Signature is created by Alice

S = (M\*\*d) % n

M1 = (S\*\*e) % n

if M == M1:

  print("As M = M1, Accept the message sent by Alice")

else:

  print("As M not equal to M1, Do not accept the message sent by Alice ")

