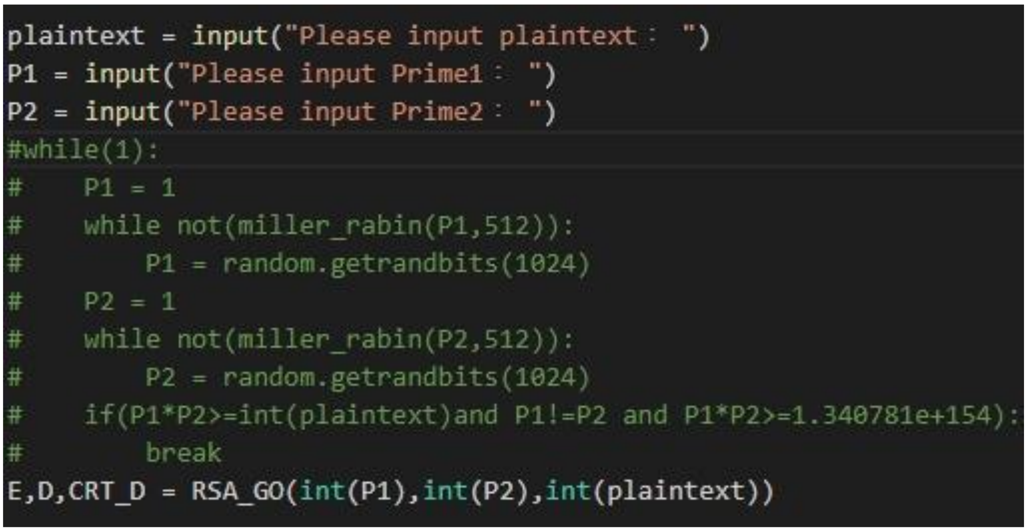
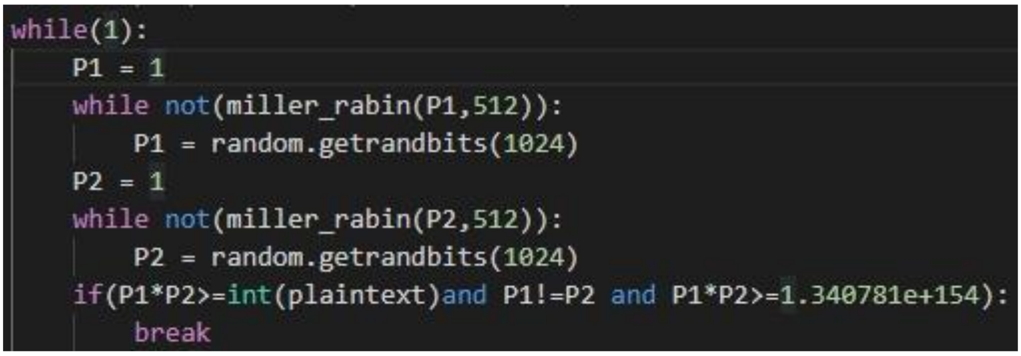
70分：



```
plaintext = input("Please input plaintext： ")
P1 = input("Please input Prime1： ")
P2 = input("Please input Prime2： ")
#while(1):
#    P1 = 1
#    while not(miller_rabin(P1,512)):
#        P1 = random.getrandbits(1024)
#    P2 = 1
#    while not(miller_rabin(P2,512)):
#        P2 = random.getrandbits(1024)
#    if(P1*P2>=int(plaintext)and P1!=P2 and P1*P2>=1.340781e+154):
#        break
E,D,CRT_D = RSA_GO(int(P1),int(P2),int(plaintext))
```

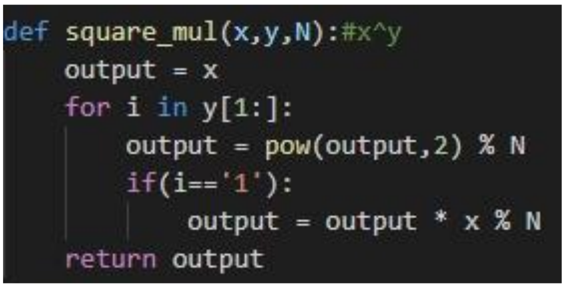
P1&P2：

產生兩個大質數，驗證次數為512次，並且兩質數相乘N要大於等於1024bit



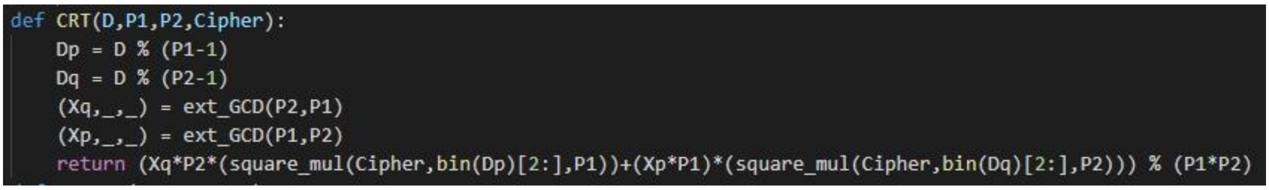
```
while(1):
    P1 = 1
    while not(miller_rabin(P1,512)):
        P1 = random.getrandbits(1024)
    P2 = 1
    while not(miller_rabin(P2,512)):
        P2 = random.getrandbits(1024)
    if(P1*P2>=int(plaintext)and P1!=P2 and P1*P2>=1.340781e+154):
        break
```

P3：



```
def square_mul(x,y,N):#x^y
    output = x
    for i in y[1:]:
        output = pow(output,2) % N
        if(i=='1'):
            output = output * x % N
    return output
```

P4：

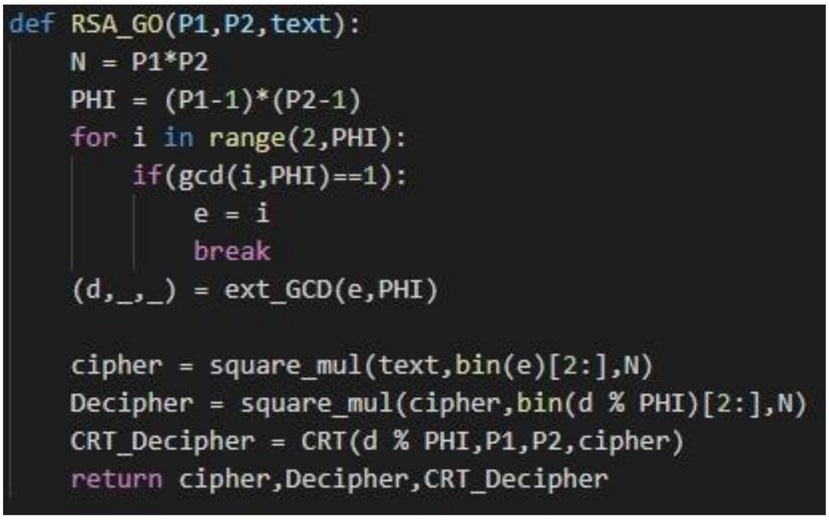


```
def CRT(D,P1,P2,Cipher):
    Dp = D % (P1-1)
    Dq = D % (P2-1)
    (Xq,_,_) = ext_GCD(P2,P1)
    (Xp,_,_) = ext_GCD(P1,P2)
    return (Xq*P2*(square_mul(Cipher,bin(Dp)[2:],P1))+(Xp*P1)*(square_mul(Cipher,bin(Dq)[2:],P2))) % (P1*P2)
```

整個RSA流程：

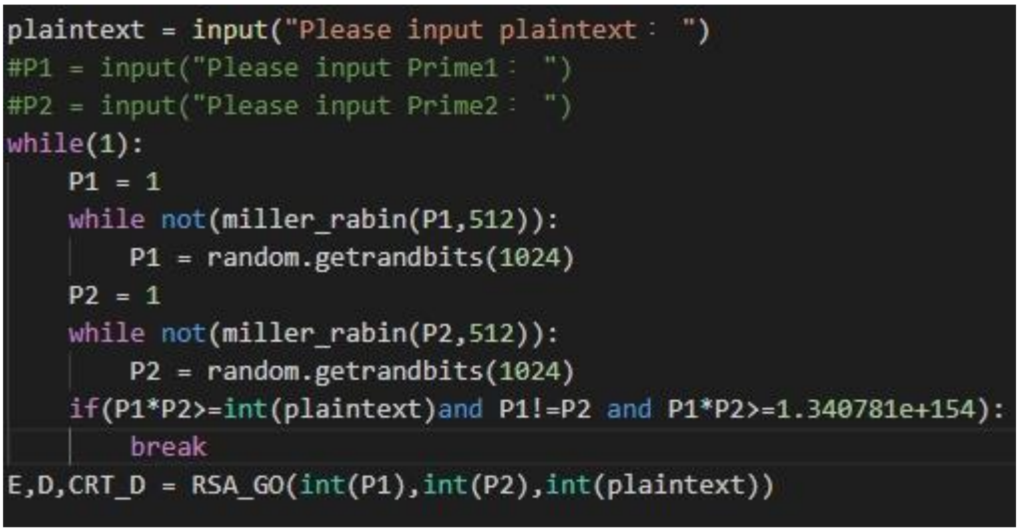
找到兩質數後，算N和PHI，再找出和PHI互質的數e，透過Extended Euclidean algorithm，得出e_inverse d，透過Square & multiply加速運算，分別

使用一般的和 Chinese Remainder Theorem 進行解密，得出結果

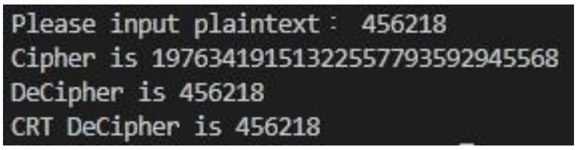


```python
def RSA_GO(P1,P2,text):
    N = P1*P2
    PHI = (P1-1)*(P2-1)
    for i in range(2,PHI):
        if(gcd(i,PHI)==1):
            e = i
            break
    (d,_,_) = ext_GCD(e,PHI)

    cipher = square_mul(text,bin(e)[2:],N)
    Decipher = square_mul(cipher,bin(d % PHI)[2:],N)
    CRT_Decipher = CRT(d % PHI,P1,P2,cipher)
    return cipher,Decipher,CRT_Decipher
```



```python
plaintext = input("Please input plaintext： ")
#P1 = input("Please input Prime1： ")
#P2 = input("Please input Prime2： ")
while(1):
    P1 = 1
    while not(miller_rabin(P1,512)):
        P1 = random.getrandbits(1024)
    P2 = 1
    while not(miller_rabin(P2,512)):
        P2 = random.getrandbits(1024)
    if(P1*P2>=int(plaintext)and P1!=P2 and P1*P2>=1.340781e+154):
        break
E,D,CRT_D = RSA_GO(int(P1),int(P2),int(plaintext))
```



```
Please input plaintext： 456218
Cipher is 19763419151322557793592945568
DeCipher is 456218
CRT DeCipher is 456218
```