HW4 RSA

我這次做的是 70 分的作業

環境就 jupyter notebook 然後 python3

小數字的 RSA 加解密

```
        else:
            index = index + 1

p = int(input("p = "))
q = int(input("q = "))
plain_text = int(input("Plain_text = "))
n = p * q
phi_n = (p - 1) * (q - 1)
e = find_e(phi_n)
d = mod( e, phi_n )
cipher_text = pow( plain_text, e, n )
decrypted = pow( cipher_text, d, n)

print("Plain text: " + str(plain_text))
print("Encrypted text: " + str(cipher_text))
print("Decrypted text: " + str(decrypted))
```

```
p = 3
q = 11
Plain_text = 4
Plain text: 4
Encrypted text: 31
Decrypted text: 4
```

輸入 p,q,跟明文 透過蒙哥馬利演算法算出加解密的結果

心得的話，大概就是 python 真的是一種很強大的高階語言