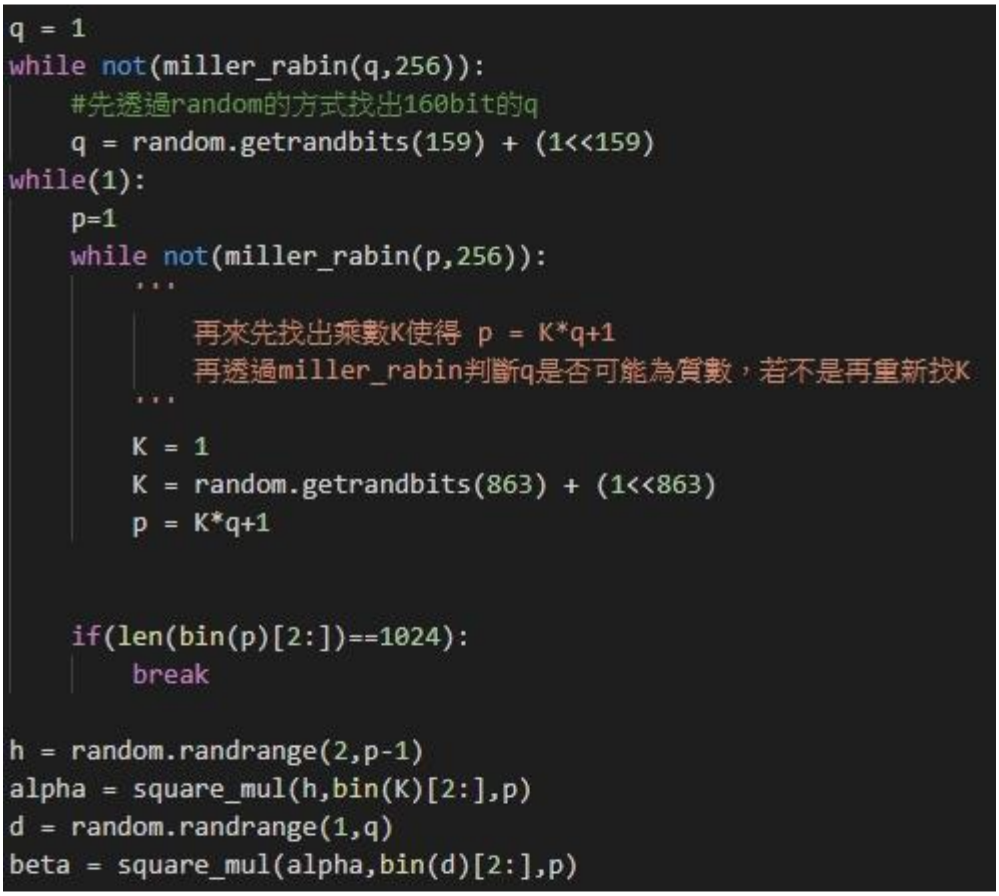
組員：

B10415039　曾柏誠

B10415040　杜佳謙

python3

key(杜佳謙)：

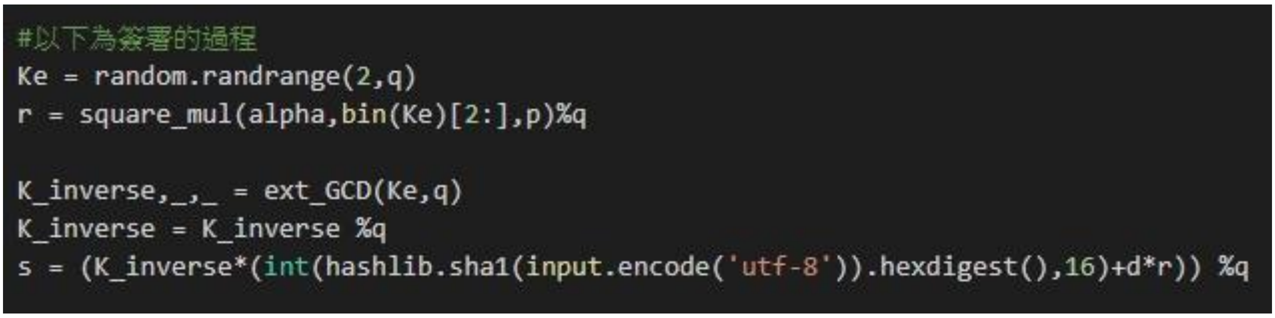


```
q = 1
while not(miller_rabin(q,256)):
    #先透過random的方式找出160bit的q
    q = random.getrandbits(159) + (1<<159)
while(1):
    p=1
    while not(miller_rabin(p,256)):
        '''
            再來先找出乘數K使得 p = K*q+1
            再透過miller_rabin判斷q是否可能為質數，若不是再重新找K
        '''
        K = 1
        K = random.getrandbits(863) + (1<<863)
        p = K*q+1


    if(len(bin(p)[2:])==1024):
        break

h = random.randrange(2,p-1)
alpha = square_mul(h,bin(K)[2:],p)
d = random.randrange(1,q)
beta = square_mul(alpha,bin(d)[2:],p)
```

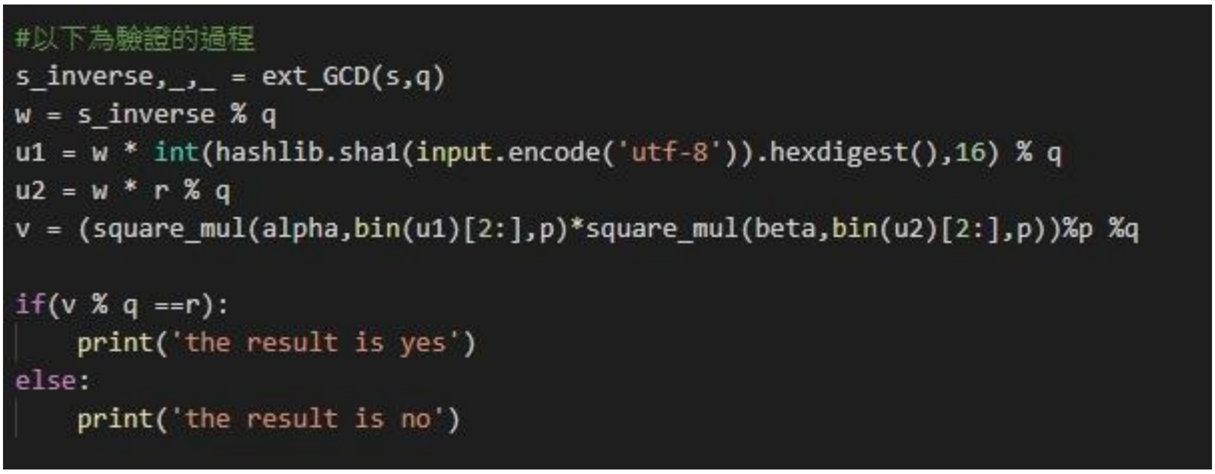
簽署(杜佳謙)：



```
#以下為簽署的過程
Ke = random.randrange(2,q)
r = square_mul(alpha,bin(Ke)[2:],p)%q

K_inverse,_,_ = ext_GCD(Ke,q)
K_inverse = K_inverse %q
s = (K_inverse*(int(hashlib.sha1(input.encode('utf-8')).hexdigest(),16)+d*r)) %q
```

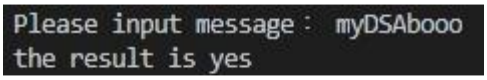
驗證(曾柏誠)：



```
#以下為驗證的過程
s_inverse,_,_ = ext_GCD(s,q)
w = s_inverse % q
u1 = w * int(hashlib.sha1(input.encode('utf-8')).hexdigest(),16) % q
u2 = w * r % q
v = (square_mul(alpha,bin(u1)[2:],p)*square_mul(beta,bin(u2)[2:],p))%p %q

if(v % q ==r):
    print('the result is yes')
else:
    print('the result is no')
```

執行結果：



```
Please input message： myDSAbooo
the result is yes
```