R07922106 曾俊為 Fintech Homework 2

**1. 4G**

(103388573995635080359749164254216598308788835304023601477803095234286494993683 : 37057141145242123013015316630864329550140216928701153669873286428255828810018 : 1)

**2. 5G**

(21505829891763648114329055987619236494102133314575206970830385799158076338148 : 98003708678762621233683240503080860129026887322874138805529884920309963580118 : 1)

**3. Q = 2106G**

(91063512616269295105126874043630389817347371097093778755952242141067937507215 : 17164231569873168822386559926976266793122514524372287693171331474023035444063 : 1)

**4. Double-and-add algorithm**

d=2106  
將2106轉成二進位表示成100000111010  
所以2106G=2(2(2(2(2(2(2(2(2(2(2G))))))+1)+1)+1))+1)  
總共需要11個doubles和4個additions。

**5. Evaluate 2106G as fast as possible**

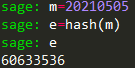
距離2106最近的2的power為2的11次方也就是2048，如果要用減法的方式又要減少計算量勢必要從2的12次方也就是4096扣回來，但是4096-1990用double-and-add algorithm顯然不會比原本的11 + 4 = 15次計算量還少，因為4096就需要12個doubles，1990不可能在3個計算內完成，所以保持第四題的計算方式上還是比較快。

**6. ECDSA Signing**

照講義P31步驟 ，以下用secp256k1來當橢圓曲線。  
(1) calculate e=hash(m)，這裡的hash function為自訂3\*m+2021。



(2) let z be the 6 leftmost bits of e，這裡假設message m為20210505。

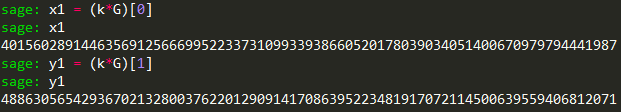




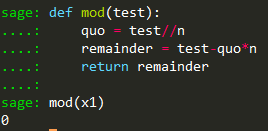
(3) select a random integer k from [1,n-1]



(4) calculate the curve point (x1,y1) = k\*G



(5) calculate r =x1 mod n, go back to step3 if r = 0



這裡我經過多次嘗試，結果都為0，所以接下來的步驟無法繼續進行。

(6) calculate s = k^(-1)(z+r\*2106) mod n, go back to step3 if s = 0

(7) signature = (r,s)

**7. ECDSA Verification**

照講義P32步驟

1. verify r and s are integers in [1,n-1]，由於簽章未完成且r = 0，這步驟也無法繼續進行。
2. calculate e =hash(m)
3. let z be the 6 leftmost bits of e
4. calculate w = s^(-1) mod n
5. calculate u1 = zw mod n and u2 = rw mod n
6. calculate the curve point(x1,y1) = u1\*G+u2\*Q
7. the signature is valid if r=x1 (mod n)

**8. Quadratic polynomial**

P(1) = 10, P(2) = 100, P(3) = 2106

By Lagrange Interpolation,

P(x) = 10\*(x-2)(x-3)/(1-2)(1-3)+100\*(x-1)(x-3)/(2-1)(2-3)+2106\*(x-1)(x-2)/(3-1)(3-2)

可得P(x) = 958x^2-2784x+1836。