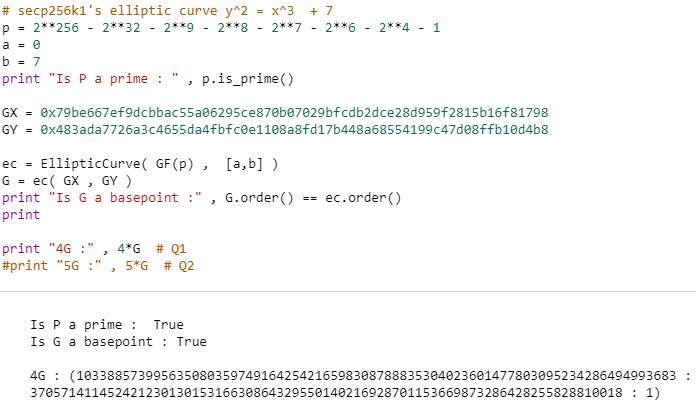
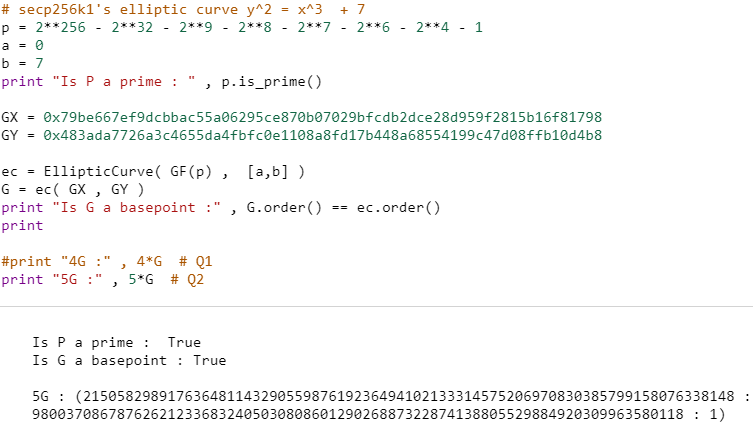
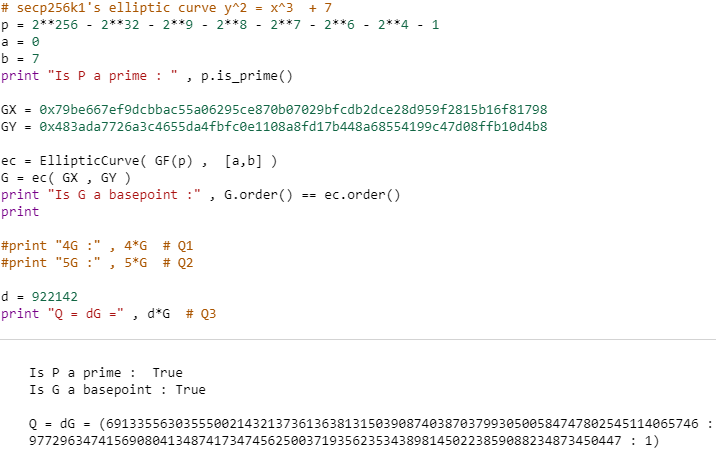
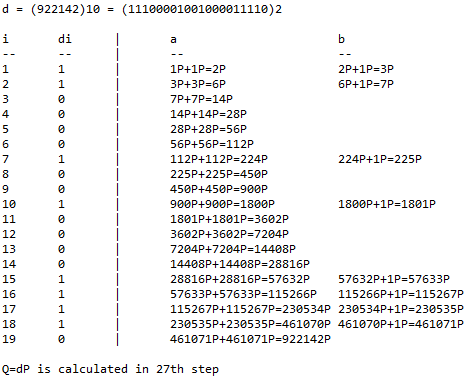
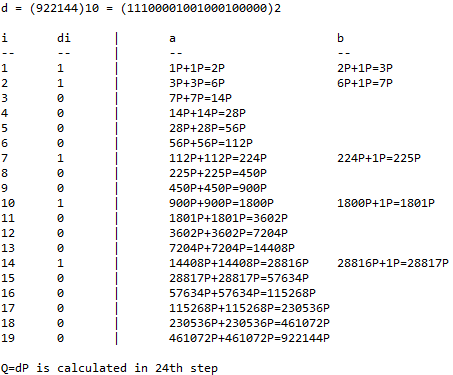
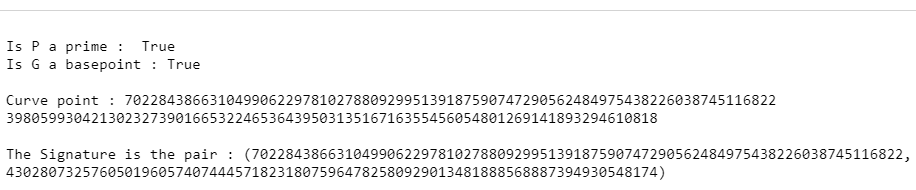
FinTech HW7  
歐政鷹 R07922142 資工所碩一

secp256k1's elliptic curve:

1. Evaluate 4G.  
   
2. Evaluate 5G.  
   
3. Evaluate Q = dG.  
   
4. Double-and Add algorithm.  
   
5. 從2進制角度來看，最後中執行了4次加法，若改寫成 可改成只利用一次加法及減法來運算，減少運算次數。  
   
6. Sign the transaction with a random number k and your private key d.  
     
   
7. Verify the digital signature with your public key Q.  
     
   