Fintech hw6

R08944052 斯曉宇

Private key d = 944052

1. 4G = (103388573995635080359749164254216598308788835304023601477803095234286494993683 , 37057141145242123013015316630864329550140216928701153669873286428255828810018)

2. 5G = (21505829891763648114329055987619236494102133314575206970830385799158076338148 , 98003708678762621233683240503080860129026887322874138805529884920309963580118)

3. Q = dG = 944052G

(69911091709759721880789243265636197136441885614673903871710885378333602519135, 37845052702926721736303725680106054418295406492842005363183630332713819274285)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| step | binary | operation | value |  | step | binary | operation | value |
| 0 | 1 | Initialization | G |  | 10 | 1 | Double and add | 1843G |
| 1 | 1 | Double and add | 3G |  | 11 | 1 | Double and add | 3687G |
| 2 | 1 | Double and add | 7G |  | 12 | 1 | Double and add | 7375G |
| 3 | 0 | Double | 14G |  | 13 | 0 | Double | 14750G |
| 4 | 0 | Double | 28G |  | 14 | 1 | Double and add | 29501G |
| 5 | 1 | Double and add | 57G |  | 15 | 1 | Double and add | 59003G |
| 6 | 1 | Double and add | 115G |  | 16 | 0 | Double | 118006G |
| 7 | 0 | Double | 230G |  | 17 | 1 | Double and add | 236013G |
| 8 | 0 | Double | 460G |  | 18 | 0 | Double | 472026G |
| 9 | 1 | Double and add | 921G |  | 19 | 0 | Double | 944052G |

4. Q = dG = 944052G = (11100110011110110100)2G

Doubles = 19

Adds = 11

5. 從第二位開始左至右觀察二進制位

d = 944052 = (11100110011110110100)2

Init 1

Add 1+1 = 10，double 10\*10 =100 ，double 100\*10 =1000

Add inverse 1000-1 = 111，double 111\*10=1110

依此類推得到下面的演算法

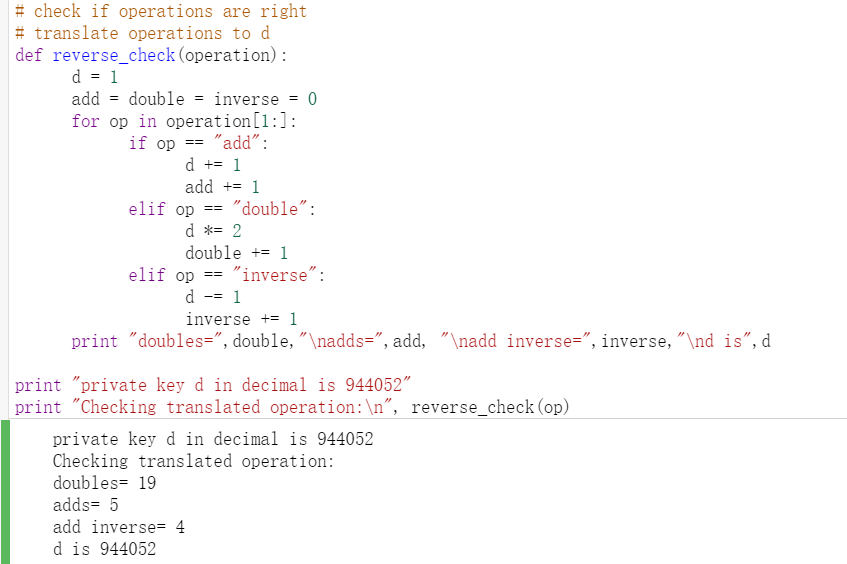
1）如果出現連續n個1後面跟著一個0，where n≥2。遇到1的部分則可以先做add，然後double n次，再add an inverse point。

2）如果只有一個1後面跟著一個0，遇到1的部分則做double and add。

3）遇到0，直接做double。

轉換成程式碼（sage）如下：





New Doubles = 19

New Adds = 5

Add inverse = 4

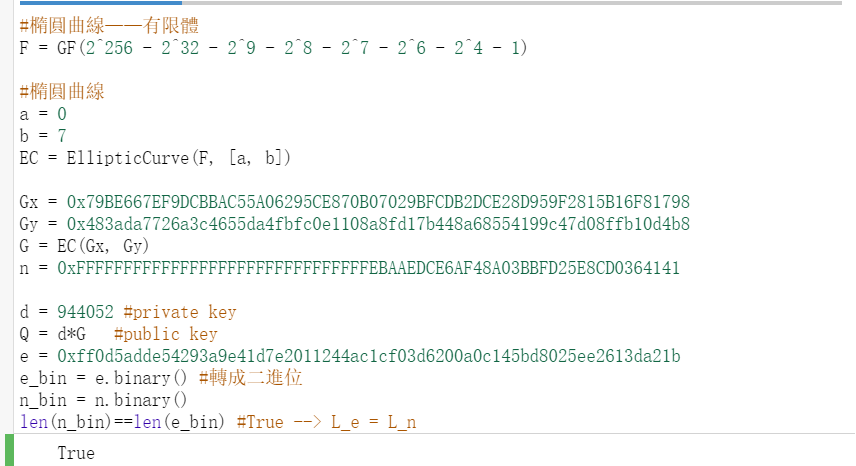
6.

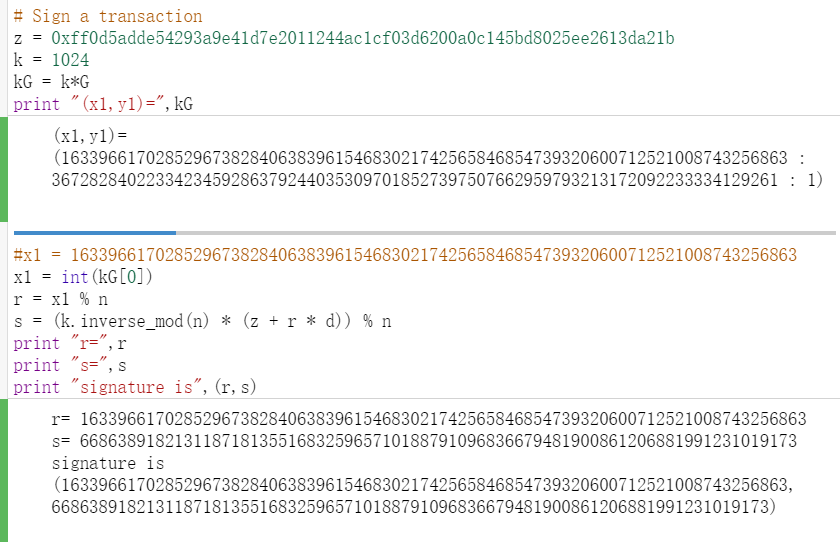
d = 944052 #private key

# Sign a transaction

z=ff0d5adde54293a9e41d7e2011244ac1cf03d6200a0c145bd8025ee2613da21b

k = 1024





7. Verification

