**Introduction to fintech hw7**

系級: 資工碩一 姓名:胡嘉祐 學號: r07922162

1. Evaluate 4G.

( 103388573995635080359749164254216598308788835304023601477803095234286494993683 ,

78734948092074072410555668377823578303129767736939410369584297579653005861645 )

2. Evaluate 5G.

( 21505829891763648114329055987619236494102133314575206970830385799158076338148 , 17788380558553574189887744505607047724243097342766425233927699087598871091545 )

3. Evaluate Q = dG

d = 922162

( 2798153425552555926225095554771463950791038149621745973300740151376280545525 , 37390993050425453923041113037110202001157990738649604804893325562897915842592 )

4. With standard Double-and Add algorithm for scalar multiplications, how many doubles and additions respectively are required to evaluate dG?

d = 922162;

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Operation | value |  | Operation | value |
| First | Initial setting | 1 | 10 | Double and add | 1801 |
| 1 | Double and add | 3 | 11 | Double | 3602 |
| 2 | Double and add | 7 | 12 | Double | 7204 |
| 3 | Double | 14 | 13 | Double | 14408 |
| 4 | Double | 28 | 14 | Double and add | 28817 |
| 5 | Double | 56 | 15 | Double and add | 57635 |
| 6 | Double | 112 | 16 | Double | 115270 |
| 7 | Double and add | 225 | 17 | Double | 230540 |
| 8 | Double | 450 | 18 | Double and add | 461081 |
| 9 | Double | 900 | 19 | Double | 922162 |

double operation : 12 ,

double and add operation : 7

5. Note that it is effortless to find P from any P on a curve. If the addition of an inverse point is allowed, try your best to evaluate dG as fast as possible.

轉換成 : binary 形式 111000010100011001

(0的數量) 10- (1的數量) 8 = 2 < 3 直接計算

double operation : 12 ,

double and add operation : 7

6. Take a Bitcoin transaction as you wish. Sign the transaction with a random number k and your private key d.

k= 54489388430015745459267304896480809188106719484308647534451663508055451570103

sign = 109243827131280859280592421616830708848097681922800935277487900615287554784030

7. Verify the digital signature with your public key Q.

digital signature=

62489733749620412554425905433754300237570737479354872412535087295622577013958