HW02-FinTech BlockChain

1.

4G = 1146601765987638938066882755650177400131162291140234889017661421504861504036448

2.

5G = 1433252207484548672583603444562721750163952863925293611272076776881076880045560

3.

Q = 609418838622430095582548184628069288169712757741034843512887045529833889395372112

4.

2126 = 100001001110

🡪doubles 11 time, additions 5 times

5.

2126 = 2048 + 64 + 16 – 2 = 2^11 + 2^6 + 2^4 - 2^1

🡪doubles 11 times, addition s 4 times

6.

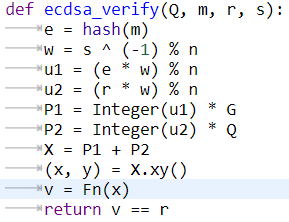
d = 2126

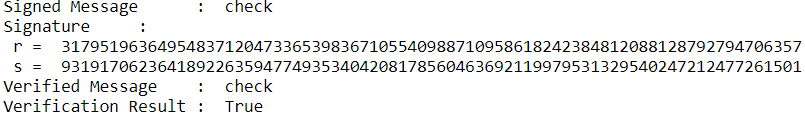
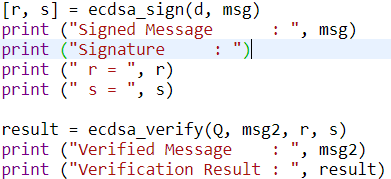
Signature :

r = 46982215225654375603918090048681837627027723004128585947282394951671886053713

s = 113073258239035569103389947389864743025040185669688871587697341106627041779713

7.





8.

Z10007 = {0, 1, 2, … , 10006}

p(x) = (10x + 80(x-1) + 968(x-1)(x-2))%10007

=(10x + 80x – 80 + 968x^2 -2904x+1936)%10007

=(968x^2 -2814x + 1856)%10007