SM2 Project: Implement the above ECMH scheme

李晨漪

可直接运行python文件

思路：

ECMH实现SM2椭圆曲线公钥加密算法

主要函数：

(1)ext\_gcd(a,b)。扩展欧几里得算法，即 a mod b的逆元，返回的第一个值为结果。

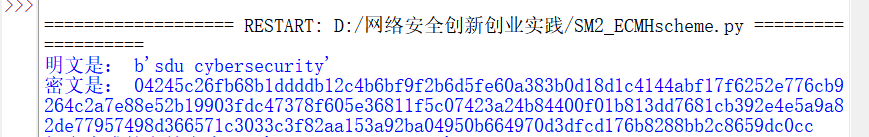
(2) sameAdd(xl,y1)。计算椭圆曲线上2\*(x1,y1)。

(3)NsameA dd(x1,y1,x\_G,y\_G)。返回(x3,y3)=(x1,y1)+(x\_G,y\_G)。

(4)multiply(x1,y1,k,x\_G,y\_G)。调用函数(2)(3)，使用类似快速模指数算法，计算(x1,y1)=k(x\_G,y\_G)。

1. Point\_bit(x1,y1)。选用未压缩格式，将(x1,y1)化为比特串。
2. SHA256(str)。利用hashlib.sha256()将str加密。
3. KDF(x,klen)。调用SHA256函数进行密钥扩展。
4. xor(bit\_M,t)。进行逐比特异或。
5. bit\_Point(hexC1)。将16进制字符串转为点坐标。(10）Point\_Cl\_in(Point\_C1)。判断这个点是否在方程上。

运行截图



参考文献

https://blog.csdn.net/joker\_clown/article/details/101114356?spm=1001.2014.3001.5506