一: SM2

简介：SM2是国家密码管理局于2010年12月17日发布的椭圆曲线公钥密码算法 ，SM2为非对称加密，基于ECC。

SM2性能更优更安全：密码复杂度高、处理速度快、机器性能消耗更小

①加密算法以及流程:

输入：需要发送的消息为比特串M，klen为M的比特长度。

1.用随机数发生器产生随机数k∈[1,n-1],k的值为1到n-1

2.计算椭圆曲线点C1=[k]G=(x1,y1)，将C1的数据类 型转换为比特串

3.计算椭圆曲线点S=[h]PB，若S是无穷远点，则报错并退出

4.计算椭圆曲线点[k]PB=(x2,y2)，按本文本第1部分4.2.5和4.2.4给出的细节，将坐标x2、y2 的 数据类型转换为比特串

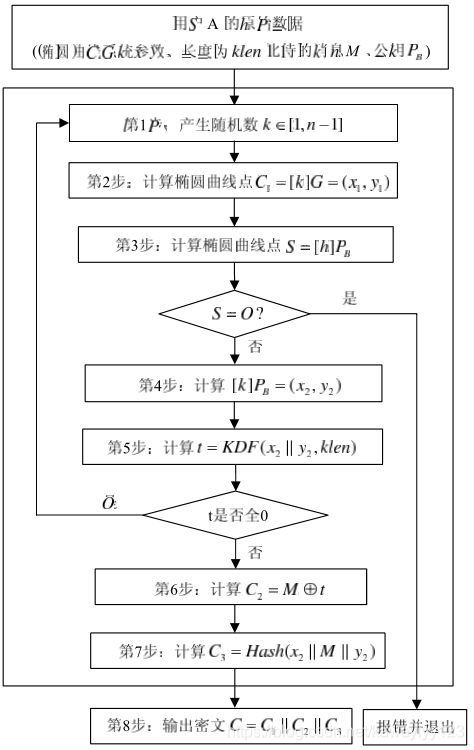
5.计算t=KDF(x2 ∥y2, klen)，若t为全0比特串，则返回A1

6.计算C2 = M ⊕t

7.计算C3 = Hash(x2 ∥ M ∥ y2)

8.输出密文C = C1 ∥ C2 ∥ C3

加密算法流程：



②：解密算法以及流程1.从C中取出比特串C1，按本文本第1部分4.2.3和4.2.9给出的细节，将C1的数据类型转换为椭 圆曲线上的点，验证C1是否满足椭圆曲线方程，若不满足则报错并退出

2.计算椭圆曲线点S=[h]C1，若S是无穷远点，则报错并退出

3.计算[dB]C1=(x2,y2)，按本文本第1部分4.2.5和4.2.4给出的细节，将坐标x2、y2的数据类型转 换为比特串

4.计算t=KDF(x2 ∥y2, klen)，若t为全0比特串，则报错并退出

5.从C中取出比特串C2，计算M′ = C2 ⊕t

6.计算u = Hash(x2 ∥ M′ ∥ y2)，从C中取出比特串C3，若u ̸= C3，则报错并退出

7.输出明文M′

③：SM2椭圆曲线公钥密码算法推荐曲线参数

椭圆曲线方程：y2 = x3 + ax + b。

曲线参数：

p=FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFF

a=FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFC

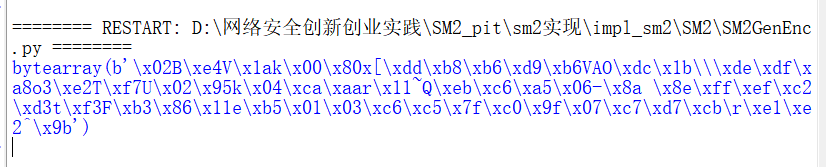
b=28E9FA9E 9D9F5E34 4D5A9E4B CF6509A7 F39789F5 15AB8F92 DDBCBD41 4D940E93

n=FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF 7203DF6B 21C6052B 53BBF409 39D54123

Gx=32C4AE2C 1F198119 5F990446 6A39C994 8FE30BBF F2660BE1 715A4589 334C74C7

Gy=BC3736A2 F4F6779C 59BDCEE3 6B692153 D0A9877C C62A4740 02DF32E5 2139F0A0

加密运行结果



代码参考

[Ujimatsu-Chiya/SM2-SM3-SM4-encryption-system-implementation: 国密SM2、SM3与SM4的Python实现。 (github.com)](https://github.com/Ujimatsu-Chiya/SM2-SM3-SM4-encryption-system-implementation)