暂时选用NIST P-256

因为算不出M-511的求解方法

**例3.1：**求椭圆曲线方程y2+a1xy+a3y=x3+a2x2+a4x+a6上，平常点A(x,y)的切线的斜率k。  
　　**解：**令F(x,y)= y2+a1xy+a3y-x3-a2x2-a4x-a6  
　　       求偏导数  
　 　      Fx(x,y)= a1y-3x2-2a2x-a4  
　　       Fy(x,y)= 2y+a1x +a3  
　　       则导数为：f'(x)=- Fx(x,y)/ Fy(x,y)=-( a1y-3x2-2a2x-a4)/(2y+a1x +a3)  
　　　　        　　　　 = (3x2+2a2x+a4-a1y) /(2y+a1x +a3)  
　　       所以k=(3x2+2a2x+a4-a1y) /(2y+a1x +a3)  ------------------------[3-3]

x4=k2+ka1+a2+x1+x2;

y4=k(x1-x4)-y1-a1x4-a3

115792089210356248762697446949407573529996955224135760342422259061068512044369

115792089210356248762697446949407573530086143415290314195533631308867097853951

y ^ 2 = x ^ 3 –3x

+41058363725152142129326129780047268409114441015993725554835256314039467401291   
modulo p = 2 ^ 256 - 2 ^ 224 + 2 ^ 192 + 2 ^ 96 - 1

TODO：

选用了M-511曲线，

y ^ 2 = x ^ 3 + 530438x ^ 2 + x   
modulo p = 2 ^ 511 - 187

其安全性证明来自

参考https://safecurves.cr.yp.to/

论文：Diego F. Aranha, Paulo S. L. M. Barreto, Geovandro C. C. F. Pereira, Jefferson Ricardini. "A note on high-security general-purpose elliptic curves." 2013

<https://eprint.iacr.org/2013/647>

基点

(48439561293906451759052585252797914202762949526041747995844080717082404635286,  
36134250956749795798585127919587881956611106672985015071877198253568414405109)

Secp256k1

55066263022277343669578718895168534326250603453777594175500187360389116729240,  
32670510020758816978083085130507043184471273380659243275938904335757337482424

大数开方参考

<https://blog.csdn.net/s1293678392/article/details/78934156>

对某明文m，需要经过编码将明文块m映射到有限域上的x坐标Pm。这个过程没有加密，任何人都可以编码或是解码。

已知G xG求x：不可能。也就是说明文m编码到的坐标的阶是绝对不可知的。

数字签名过程