**forge a signature to pretend that you are Satoshi**

在ECDSA未检查签名邮件时，伪造签名假装自己是Satoshi

**一、ECDSA**

**1、概念**

椭圆曲线y^2 = (x^3 + a \* x + b) mod p

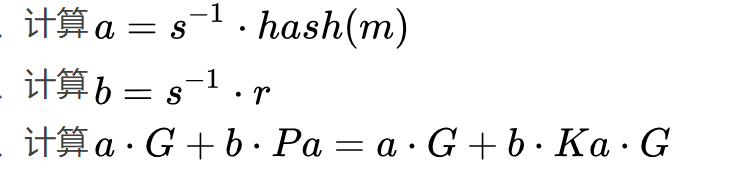
R=k\*P的性质，已知R与P的值，无法推出k的值, 而知道k值于P值是很容易计算R值(log(n))。这是ECDSA签名算法的理论基础。给验证人一个 R和P，那只有签名人才能提供K，则K可以作为一个签名指纹。

私钥生成：在椭圆曲线上任选一个点，点G，然后随机生成一个大整数，就是私钥Ka

公钥生成：公钥Pa就是Ka个G在曲线上相加得到，因此Pa = Ka\* G

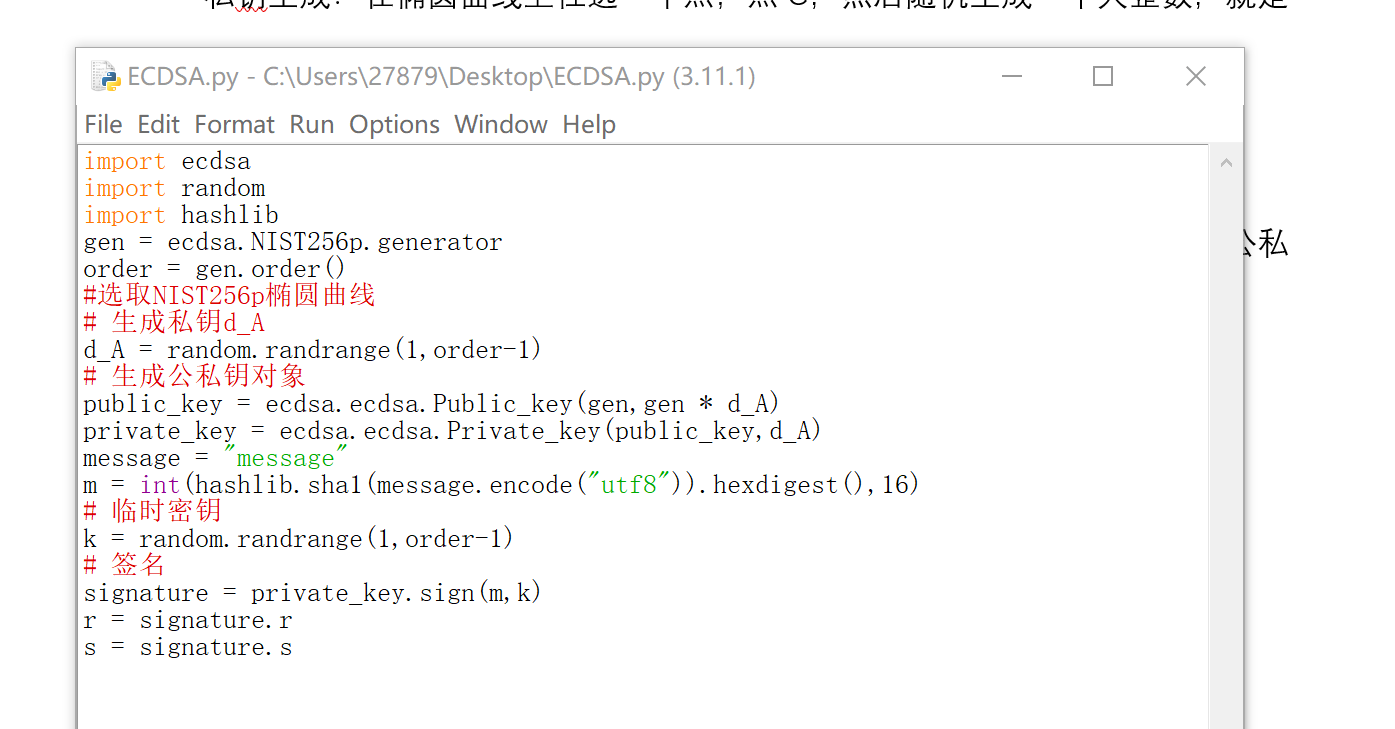
签名过程：假设公私钥为Ka和Pa，需要验证的消息为m，随机生成新的公私钥对，K和P，r就是P的x坐标值，记作 r=Xp，计算，得到（r，s）为签名结果

认证签名：计算P的x坐标，若和r相同，则认证成功，反之不然



**2、算法实现**

如图：在pycharm中安装ecdsa与hashlib两个库，选取NIST256p椭圆曲线



**二、伪造攻击**

**三、验证攻击结果**

**四、参考资料**

【1】ECDSA算法原理https://www.jianshu.com/p/05a134852a4a

【2】ECDSA算法实现https://blog.csdn.net/m0\_57291352/article/details/123486909