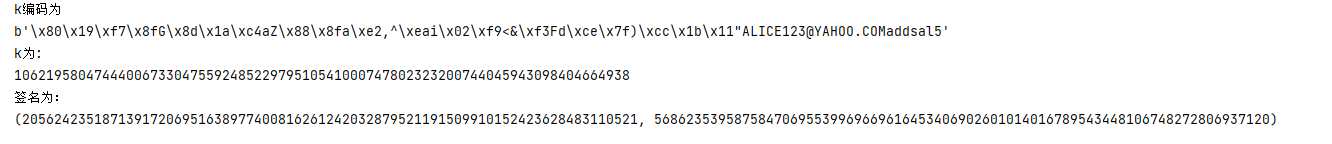
Sm2的PGP方案

按照规定，k随机。故对其进行补字和哈希。

所以我们规定k=（d||ID||"addsalt"）其中d为私钥，ID为ID，再接一个混淆的字符串，用sm3算法进行hash处理，最后得到一个随机的数。这就导致k相同的概率很小很小，不会由于k相同而产生安全问题

结合sm2算法完成该实验

最后运行程序可得结果：



最后可得耗时：

