Project 9: verify the above pitfalls with proof-of-concept code

对sm2签名算法验证了

重用随机数K求解私钥d、

泄露随机数K求解私钥d、

不同的人使用相同的随机数K得到对方的私钥d、

不同的签名算法使用相同的k和d求得d

使用不验证消息m的签名验证算法进行签名的伪造，

ecdsa和schnoor同理(伪造中本聪与本例相似)

python代码直接运行即可

运行结果