

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

```
pytest in test.py  verify_pitfalls (1)
D:\anaconda\python.exe D:/创新实践课/项目9/verify_pitfalls.py
M: sdu_cst
ID_A: 282888141016
M_: pku_cst
ID_B: 282888141046
signatureA: (29993393634508672875803595534929895586251060975511580598411799483368543681687, 544905522213884993202825715835336404738979776443381893685935382022189499347042)

-----code to verify the sig -----
验证通过!

-----leaking k to cal d-----
leaking k to cal d : succeed!

-----reusing k to cal d-----
reusing k to cal d : succeed!

-----two users reusing k to cal d of the other-----
Alice get the secret key of Bob!
Bob get the secret key of Alice!

-----two algorithms reusing k and d to cal d-----
two algorithms reusing k and d to cal d: succeed!

-----forge signature with verifying without m-----
伪造签名: (r,s,e)
(19676138975237615456203852889185894552973481515339388118419276654468528613914, 302257774954054911832171658086416927378628126357094806327386426108253568817574, 39312455888406757)
验证通过!

进程已结束，退出代码 0
```