**题目名称：babyDsa**

**类型：Crypto**

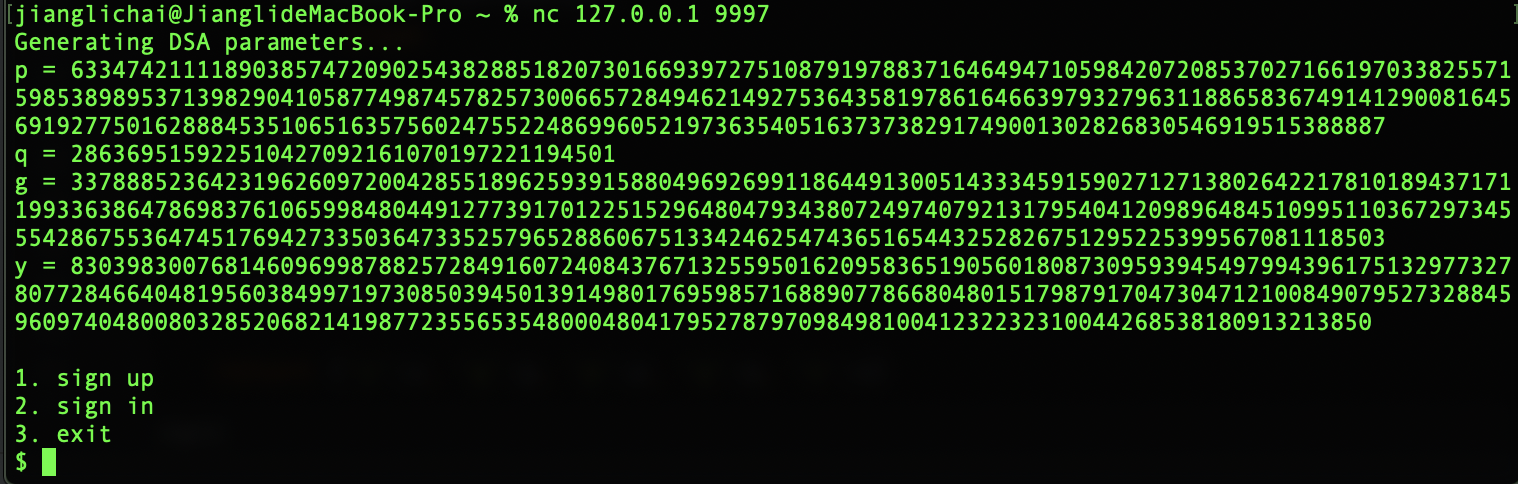
**介绍：**

dsa介绍：[https://wiki.x10sec.org/crypto/signature/dsa-zh](https://wiki.x10sec.org/crypto/signature/dsa-zh/#k)

本题泄露临时密钥k，可以通过求解私钥x来伪造dsa签名登陆。

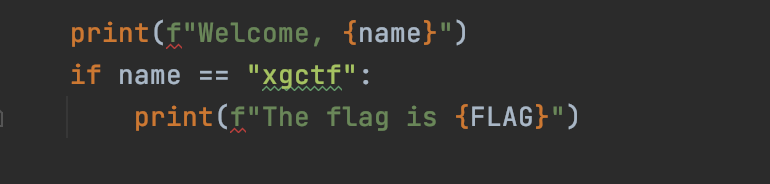
**解题步骤：**

**第一步：**功能&加密脚本分析



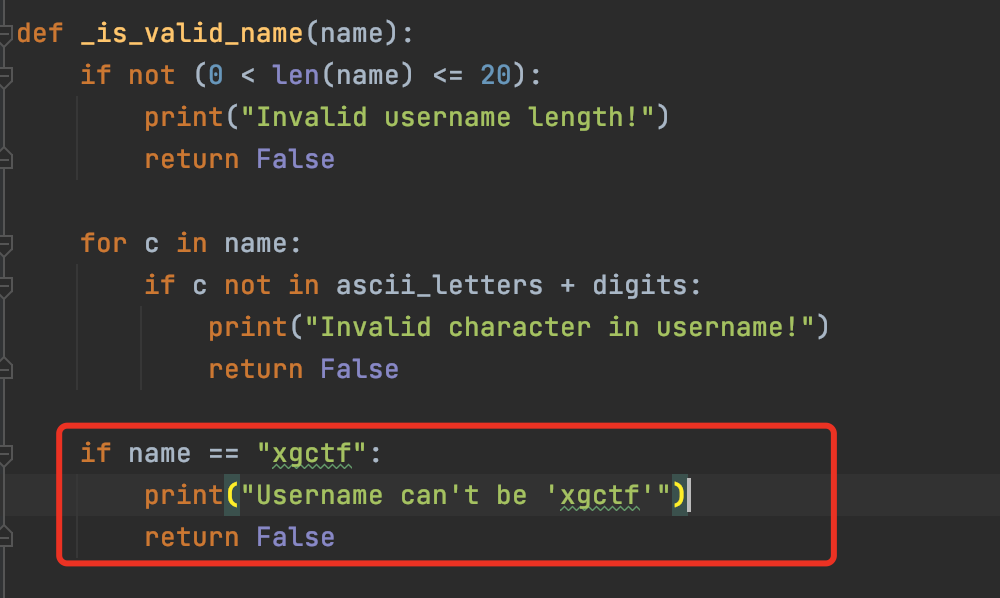
DSA公钥已给出

功能为注册和登陆



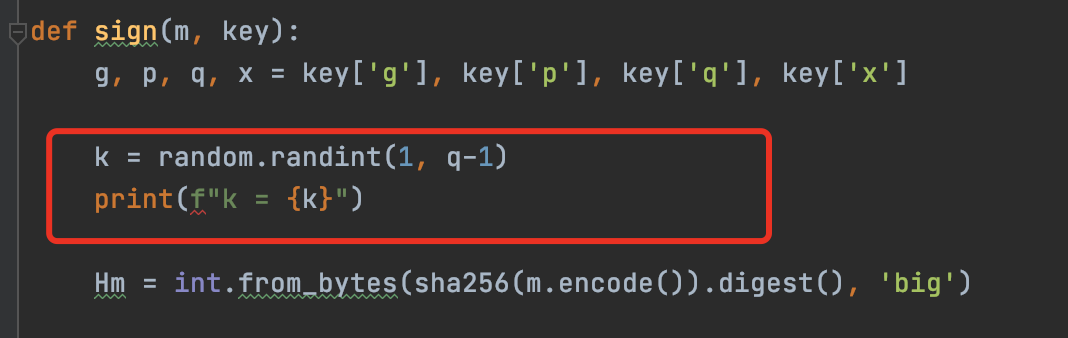
如果登陆用户为xgctf则可获得flag

但是发现在注册是会校验用户名，不可为xgctf

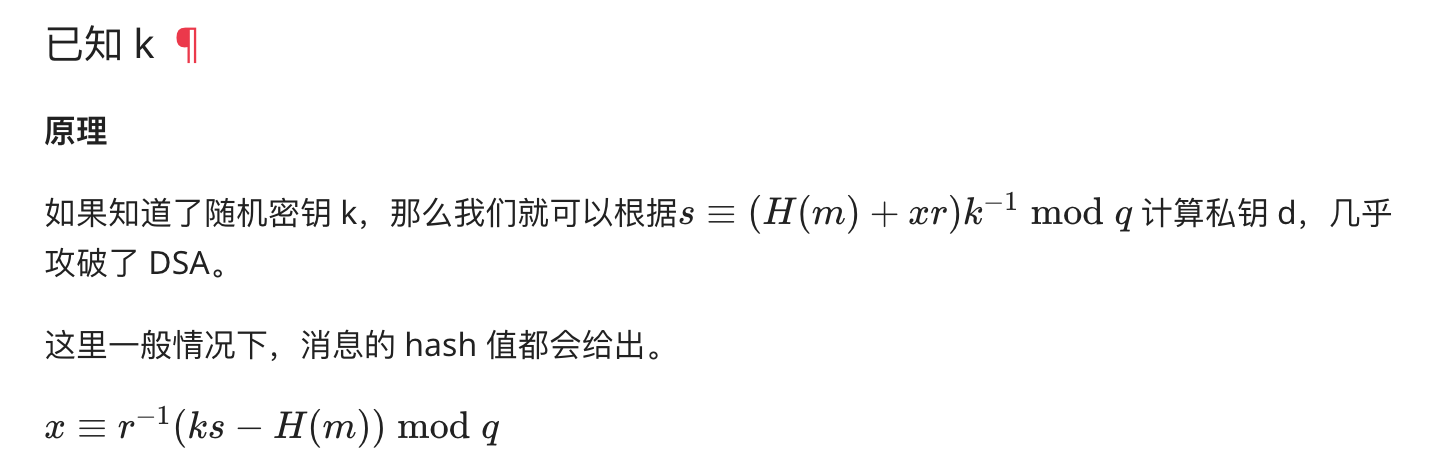


**第二步：**DSA签名伪造

我们要伪造DSA签名，还需要DSA的私钥x。这边如果泄露了临时私钥k的话是可以求解私钥x的。

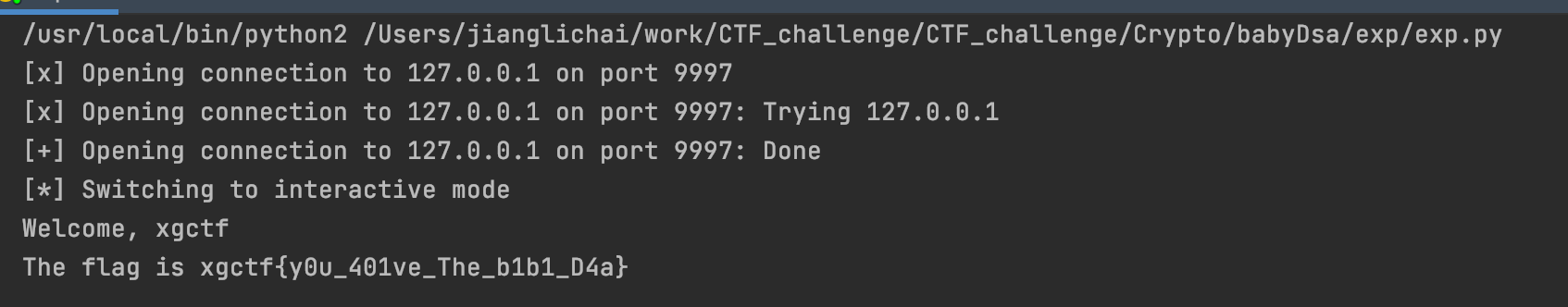


发现在注册处存在私钥k的泄露



所以直接伪造签名即可。





**简要总结：**了解DSA签名的基础知识，临时密钥k泄露导致的签名伪造。