**题目名称：抽卡第二弹**

**类型：Crypto**

**介绍：**

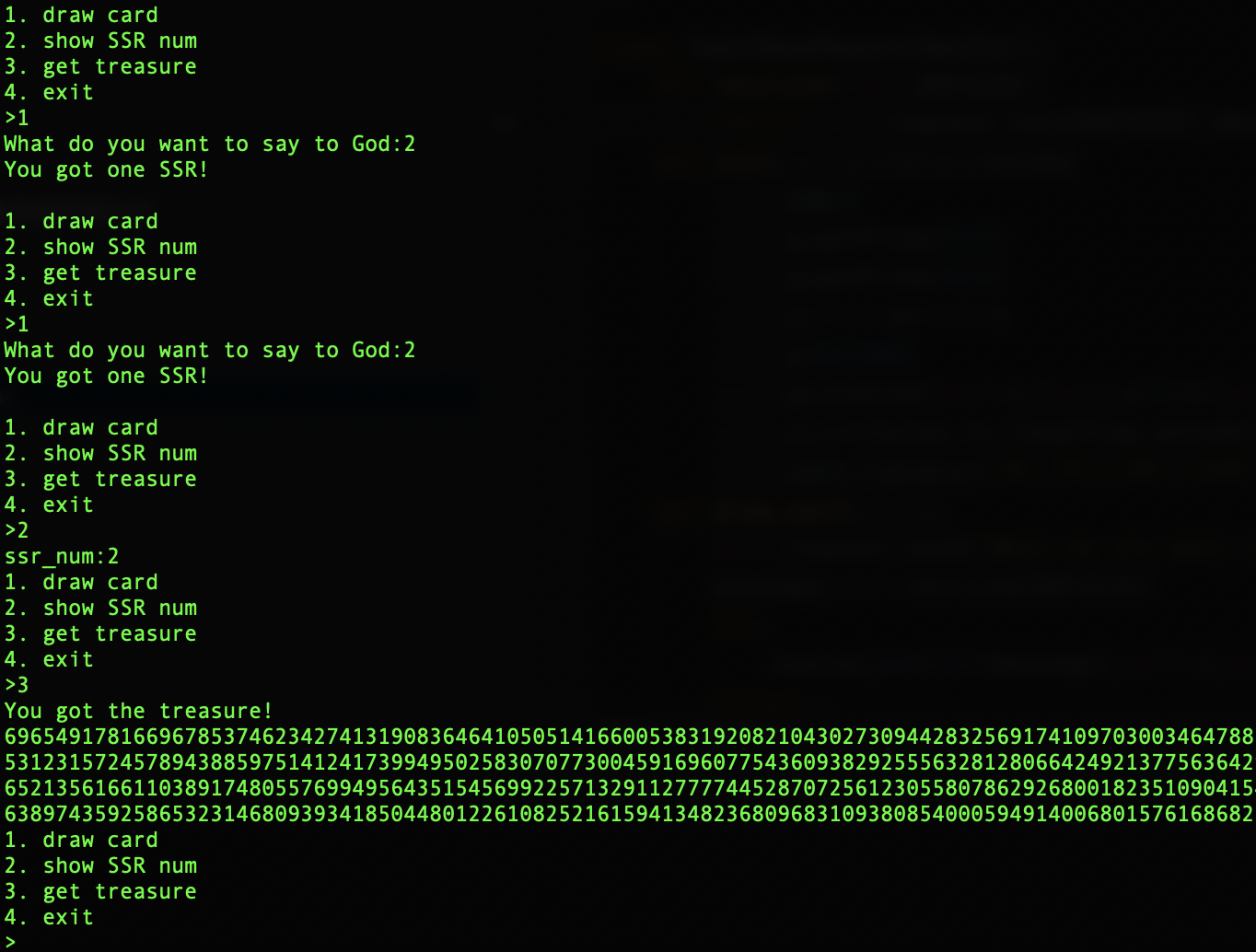
考查的知识点为RSA least significant bit oracle attack

原理参考：<https://www.jianshu.com/p/e569a2319e03>

场景：靶机部署的那个服务server会帮我们做RSA解密并把结果的最后1bit告诉你，这题相当于做一个rsa lsb oracle attack的拓展，拓展成2bit。

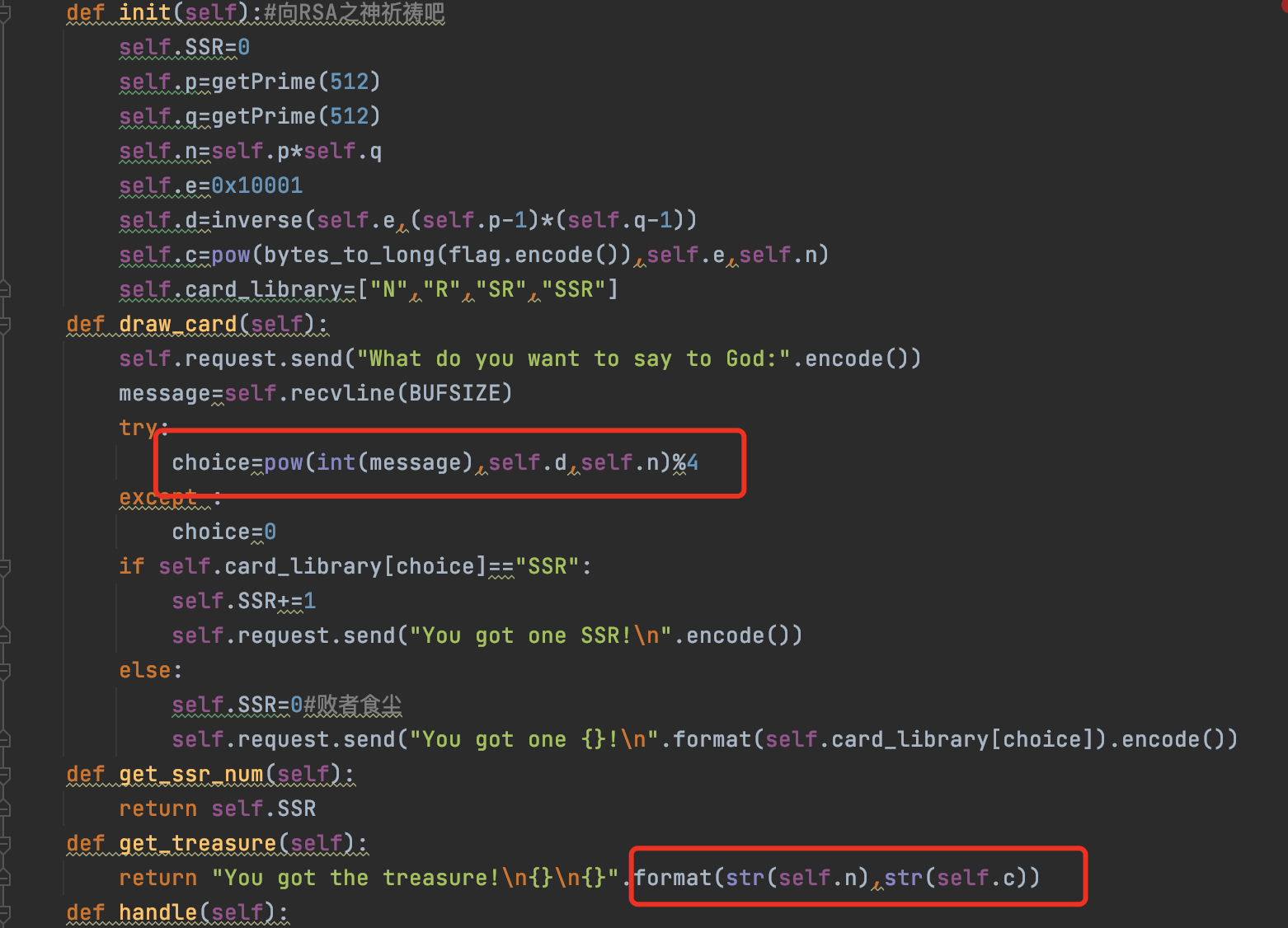
**解题步骤：**

**第一步：**功能&加密脚本分析



这一题功能看似在抽卡，实际上和抽卡无关，我只要找到能抽中SSR的数字，重复发就行了。但是我们无法通过收集SSR拿flag。

在get treasure这边可以获取到一些值。分析给出的附件python脚本。



我们在get treasure这边拿到的是rsa的公钥n，以及flag在rsa加密后的密文c。

而我们在抽卡那边输入的数会做rsa解密，返回给我们rsa解密结果的最后2bit的值。

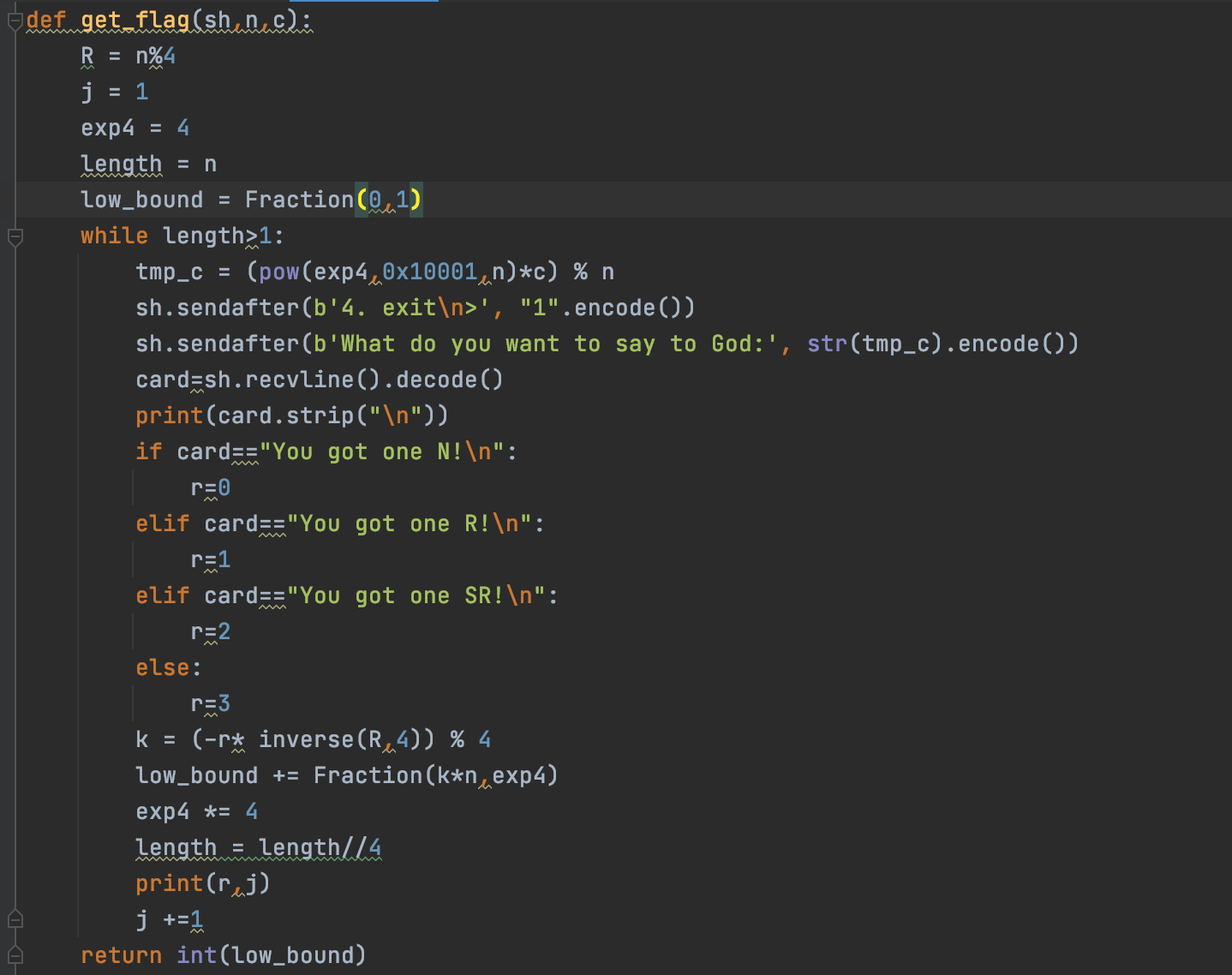
这边就存在一个标准的RSA least significant bit oracle attack的利用。原本返回的是最后1bit，这题返回最后2bit。

**第二步：**RSA least significant bit oracle attack 解题脚本编写

<https://www.jianshu.com/p/e569a2319e03>

这边给了原理和核心解密脚本

我们编写pwntools和靶机交互，修改下核心解密脚本的交互部分，即可求解flag。



**简要总结：**题目形式是多变的，找到本质即可，根据场景可以知道是RSA least significant bit oracle attack。