**题目名称：抽卡吗少年**

**类型：Crypto**

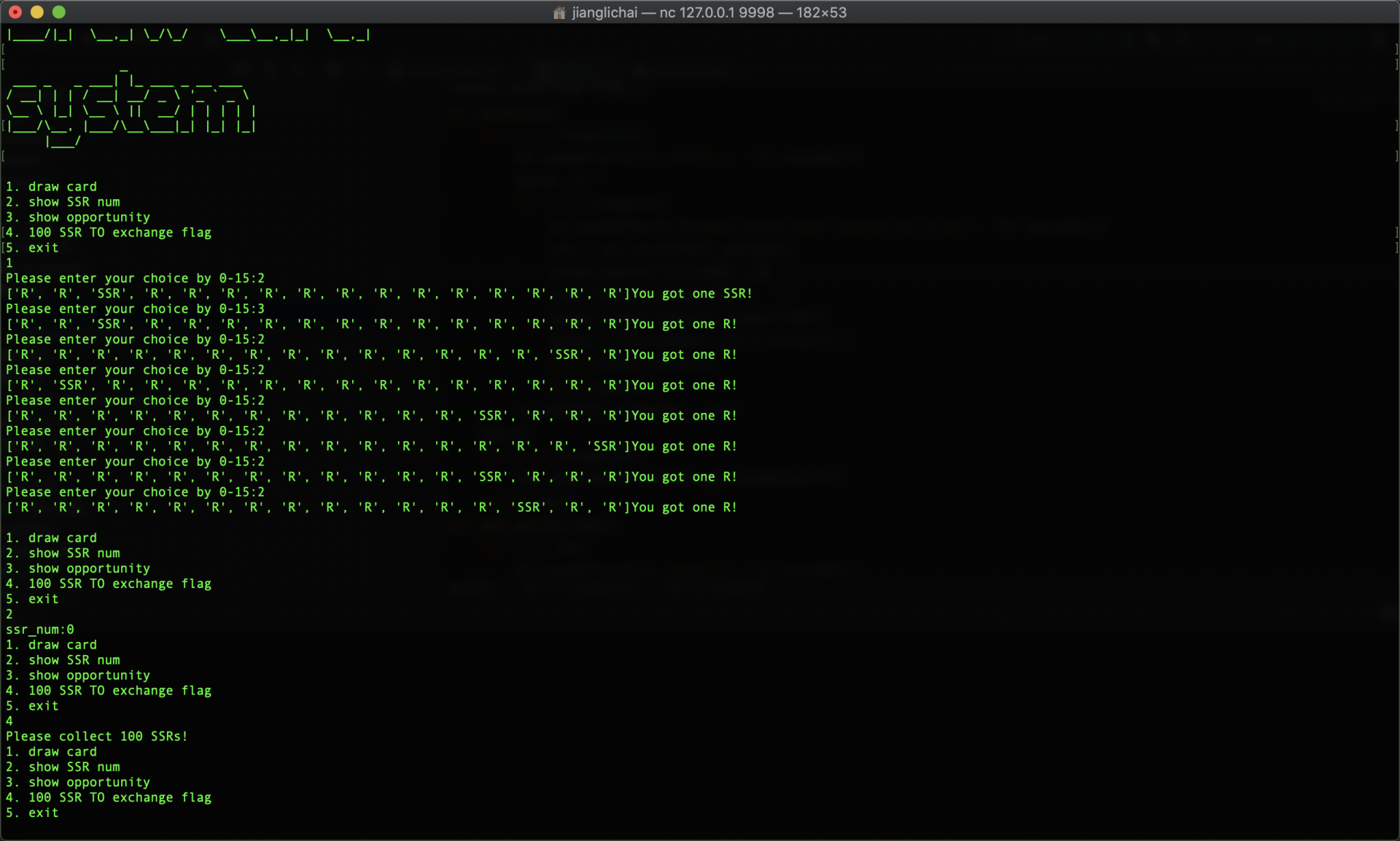
**介绍：**

python的random随机数预测

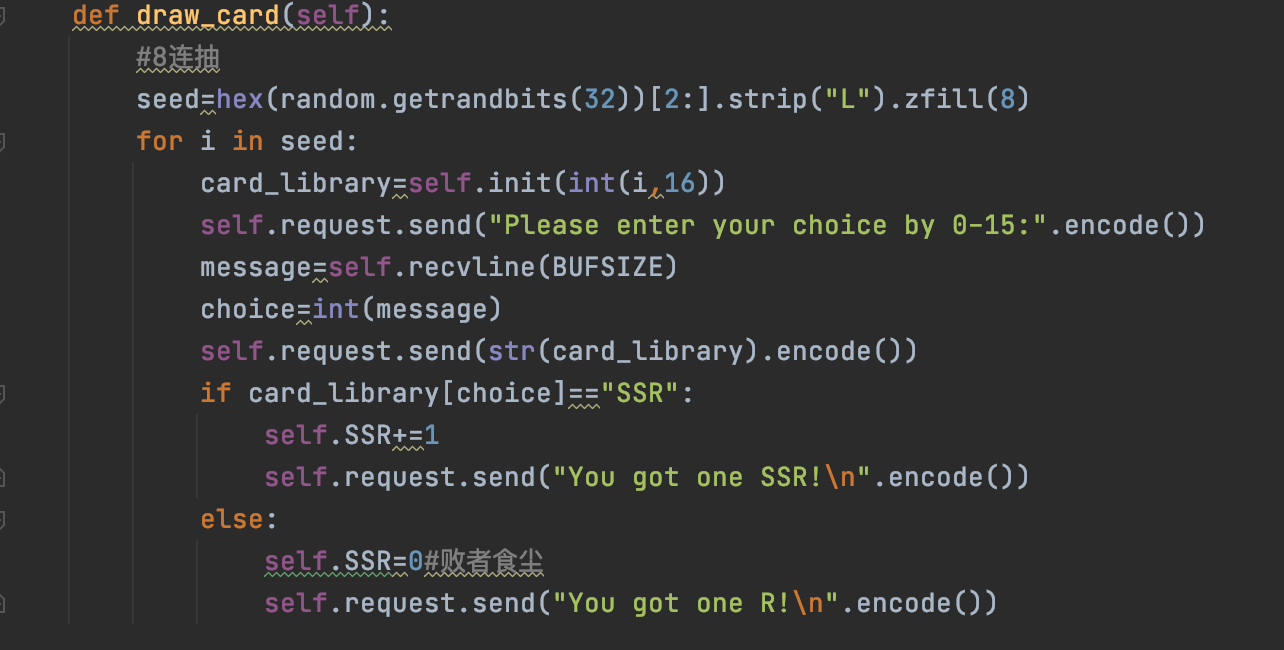
<https://github.com/tna0y/python-random-module-cracker>

**解题步骤：**

**第一步：**功能&加密脚本分析



主要就是抽卡，连续抽100张SSR，可以拿到flag

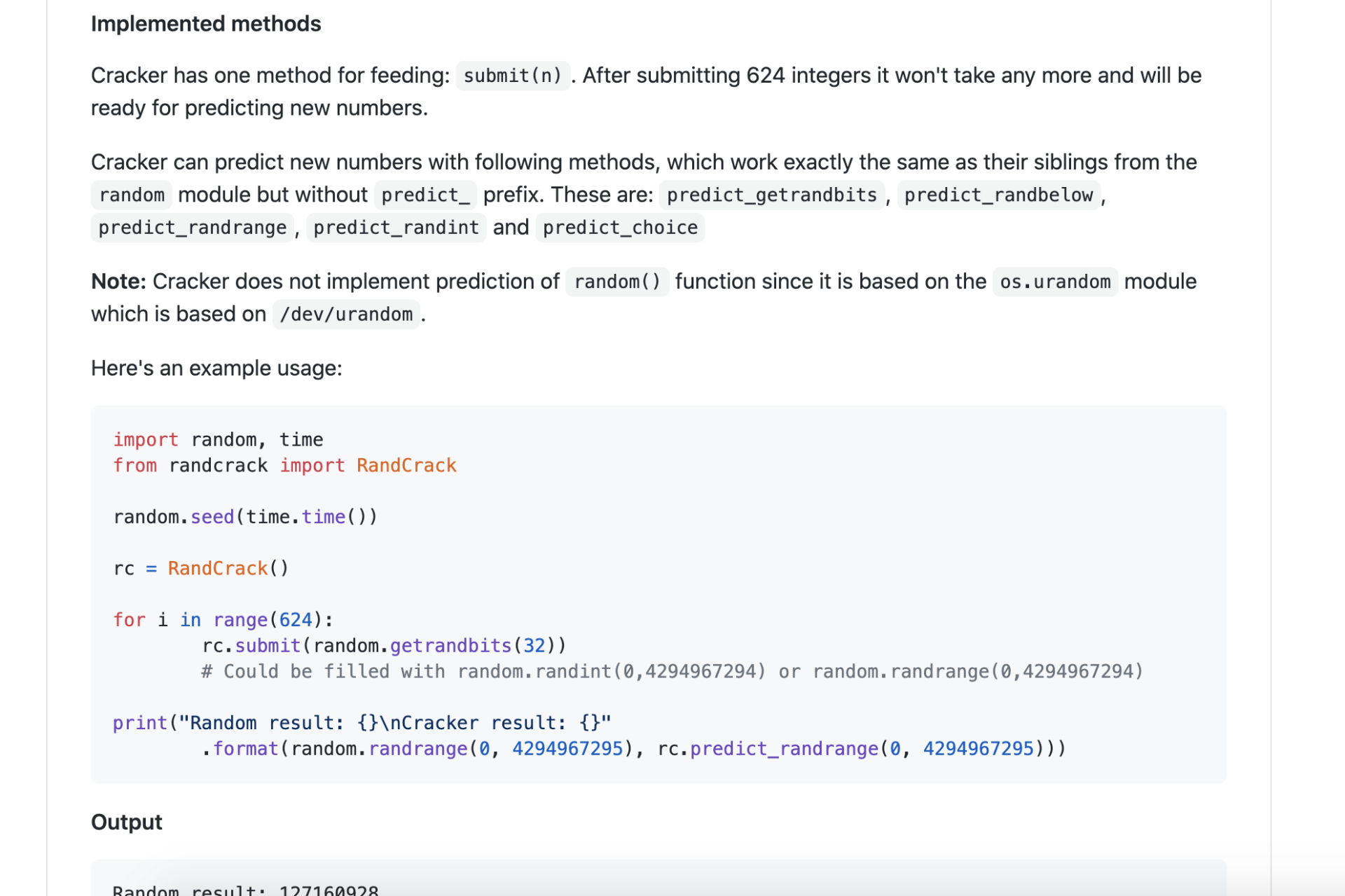


这边抽卡实现是用的python的random库，获取32bit的随机数，然后分8次抽的。

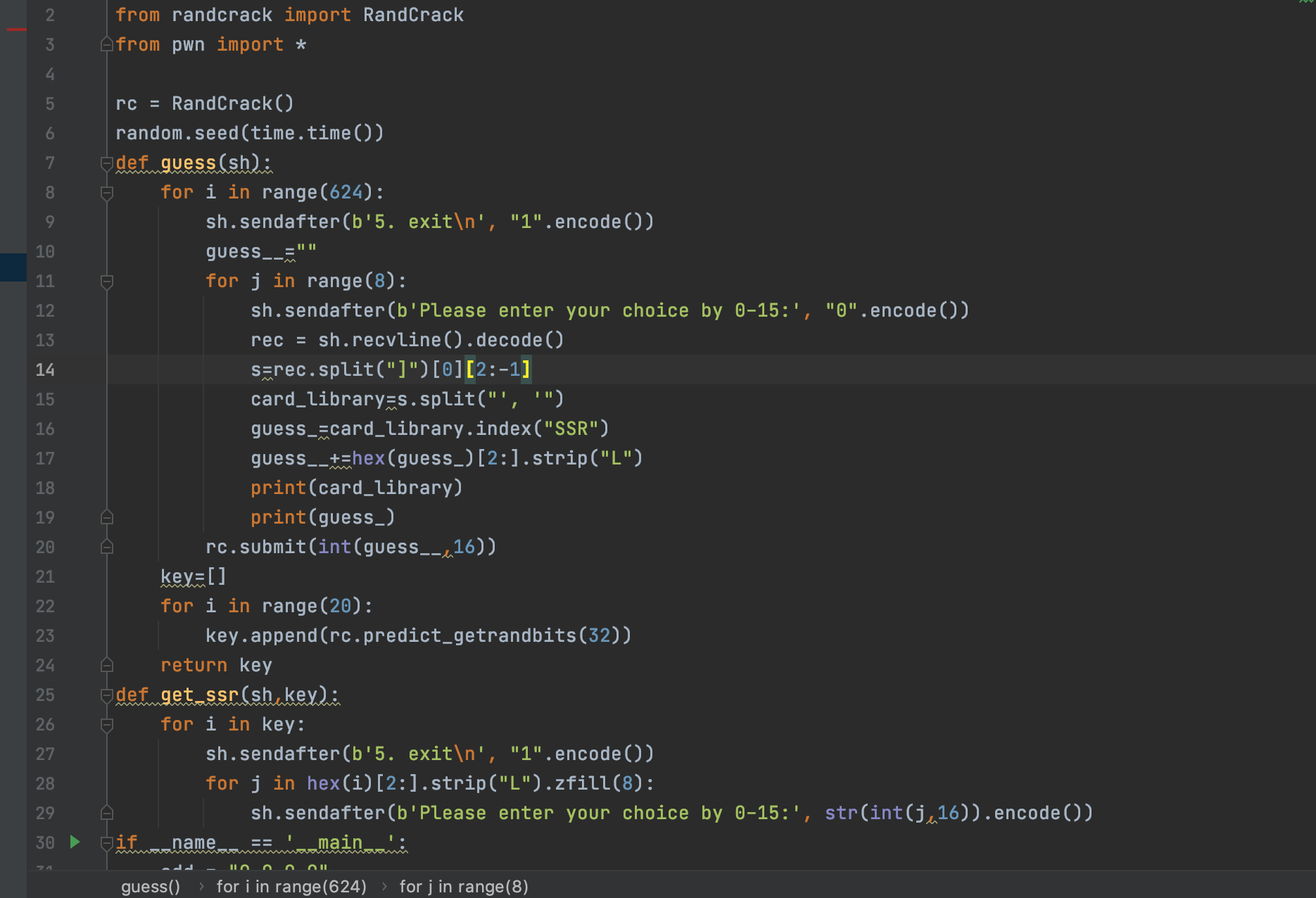
**第二步：**python random随机数预测

<https://github.com/tna0y/python-random-module-cracker>

32bit的随机数是可以预测的。



需要先给出624个python random生成的32bit随机数，然后可以预测接下来产生的随机数。



我们利用这一点先获取前624\*8次的抽卡结果，然后预测接下来生成的卡池连续抽100张SSR即可。

**简要总结：**随机数预测是CTF中经常出现，本题可以直接从github上找到crack脚本，无需分析随机数生成规则。