**题目名称：rsa**

**类型：Crypto**

**介绍：**

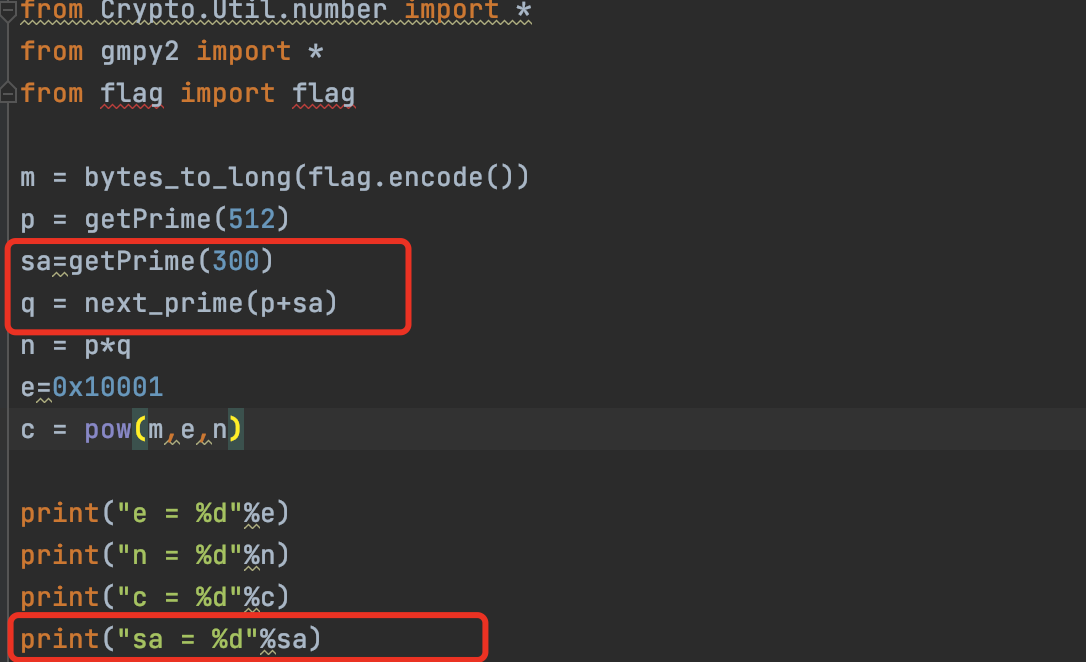
本题需要了解常规的rsa加密的参数以及加解密原理。

rsa的两个因子间存在一定的关系，分解出rsa公钥n的两个因子可以利用这个关系。其次就是常规的rsa求解了。

可以参考：<https://xz.aliyun.com/t/6459>

**解题步骤：**

**第一步：**分析加密脚本



这边非常规rsa加密部分在于这个因子q是取的p+sa的下一个质数。且sa给出。

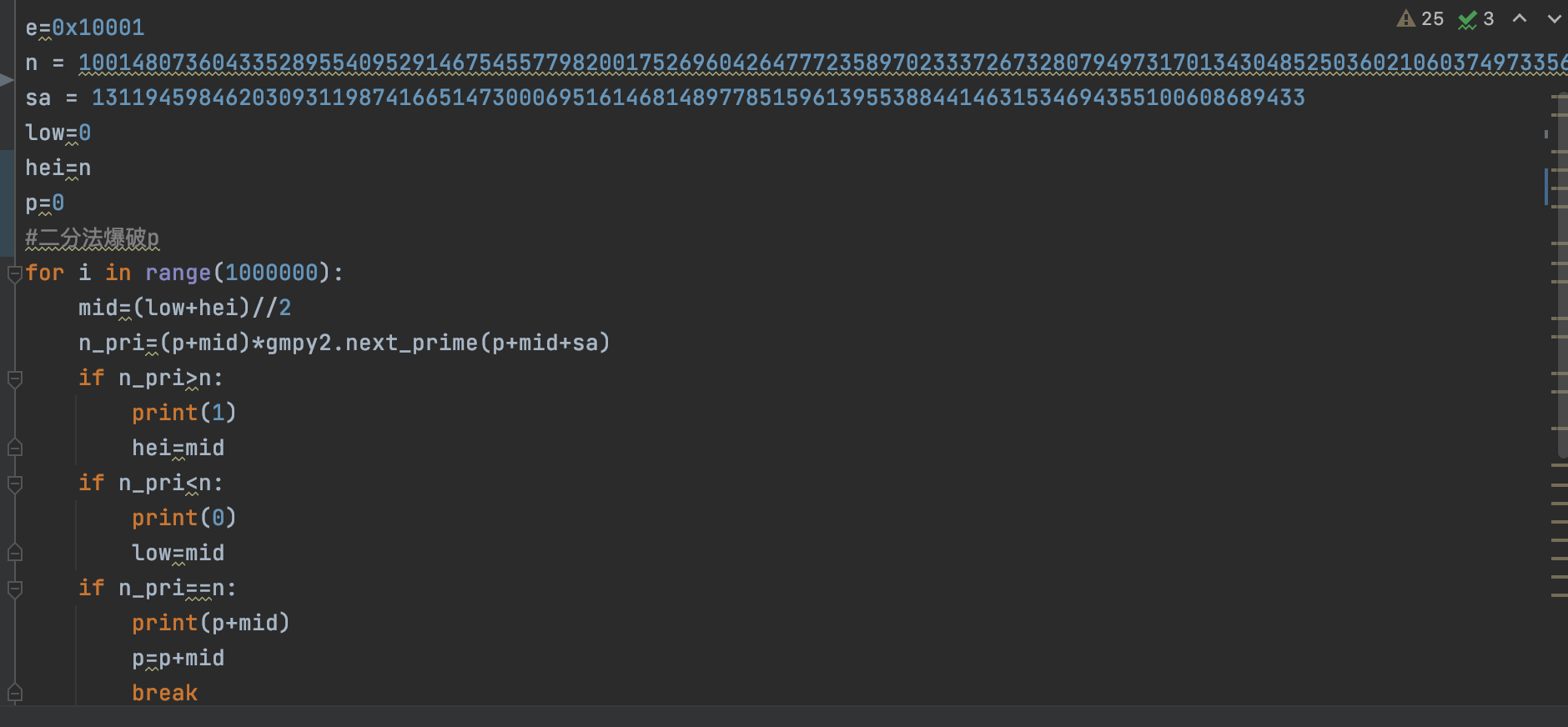
因为p\*q=n。又因为q = next\_prime(p+sa)

所以这边利用这两点可以分别求解出p和q。其次就是常规rsa求解了。

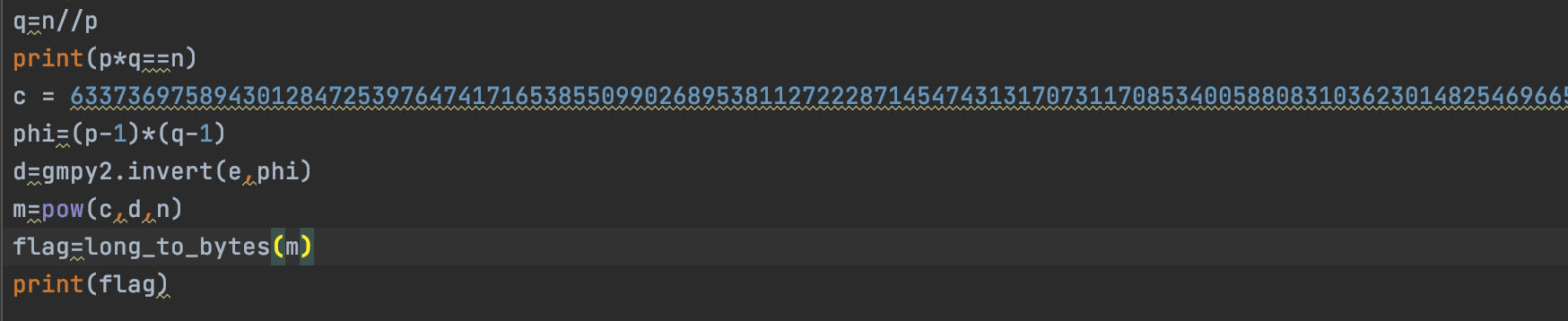
**第二步：**编写解密脚本

这边我用的是二分法直接爆破出p、q的，可能还有更好解法。

二分法爆破p



得到p、q求私钥d，计算明文flag



**简要总结：**分解公钥n的一种情景，因子之间存在一定的关系，可以利用这一点分解n。