【CTF】攻防世界——easy_RSA（Crypto）

原创

eGlhb2hlaQ== 于 2019-05-04 03:00:51 发布 11824 收藏 13

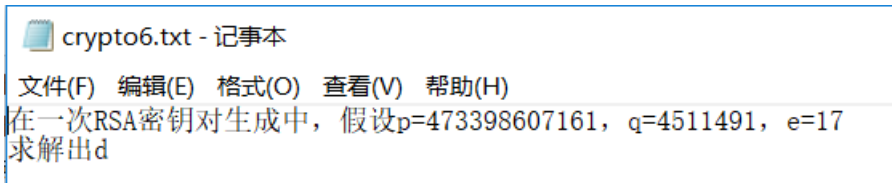
分类专栏： CTF 文章标签： CTF CRYPTO RSA

本文链接：https://blog.csdn.net/asd413850393/article/details/89810137

eGl的CTF之路——easy_RSA（Crypto）

早就有动手写博客的想法了，素材也攒了不少，然而万事开头难。最近看到同学在这里发过的博客，终于决定动笔记录一下自己的成长之路了。

第一篇博客记录一道最基本的rsa私钥计算题：

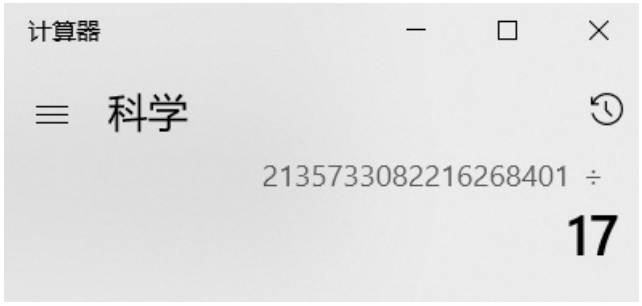


RSA的计算过程是：

- 任选两个大质数p和q，p!=q，计算N=pq
- 计算N的欧拉函数r(n)=(p-1)(q-1)
- 任选一个e满足 **1<e<r(n)** ,且e与r(n)互质
- 找到d，使e*d/r(n)=x……1（x是多少不重要，重要的是余数为1）
- 至此（n，e）为公钥，（n，d）为私钥
- 加密：$C=M^e(\mod n)$；解密：$M=C^d$（mod n）

本题没有密文，只要计算出私钥即可：
用windows自带的科学计算器：
1.先计算欧拉函数

2.欧拉函数+1再除以17即是私钥



3.将私钥套上flag格式提交即可（格式在Morse题目描述那里有说明）

> 我是分割线

好了，这就是我的第一篇博客，之后会把我做的有价值的ctf题目或者某次比赛后的wp也记录在这里。也许还会发一些我学到的技术，希望自己能坚持下去，在安全的道路上闯出名堂!

{you_can_call_me_**eGl**_for_mynames_eGlhb2hlaQ==}
?这个不是flag，是我随便写的字符串。flag是上面计算出的私钥。在某群里看见有人拿这个提交，然后说平台有问题，笑死2333