攻防世界 Crypto easy_RSA

原创

==Microsoft== 于 2021-12-14 15:45:36 发布 802 收藏

分类专栏： Crypto 文章标签： 安全

地推任务网专注于地推业务，如果有地推、APP推广、公众号推广、小程序推广等业务可以去地推任务网免费发布任务。

本文链接：https://blog.csdn.net/MrTreebook/article/details/121928682

版权

Crypto 专栏收录该内容

17 篇文章 0 订阅

订阅专栏

攻防世界 Crypto easy_RSA

1.题目下载地址

点击下载

2.了解一下RSA机密方式

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=Me(mod n)；解密：M=Cd（mod n）

3. 看一下题目

在一次RSA密钥对生成中，假设p=473398607161，q=4511491，e=17

求解出d

本题没有密文，只要计算出私钥即可：

3.1.先计算欧拉函数

r(n) = 473398607160 * 4511490 = 2135733082216268400

3.2.欧拉函数+1再除以17即是私钥

(2135733082216268400+1)/17=125631357777427553

4.得到私钥

```
125631357777427553
```