网鼎杯第四场 shenyue2 writeup

原创

tanomy 于 2018-08-30 22:44:43 发布 703 收藏

文章标签： 网鼎杯 writeup 第四场 shenyue2 密码学

1. shenyue2题目分析

这是一道RSA相关的密码学题目，给出了RSA相关的公钥

$$k = (p - r)d\ k$$

其实这是一道2018 CodeGate CTF 的原题，直接按照 CTF-WIKI中介绍的解法就可以求出来。而我写这篇文章的目的是向大家介绍另外一种方法，一种适用范围更广的方法，帮助大家在以后的CTF比赛中求解更难的题。

2. RSA中的数学推导

先把所有RSA相关的已知公式列举出来：

3.结束语

由于时间和精力有限，我只是简单地将解题思路介绍了一下，如果关于公式的推导有疑问可以直接留言提出来，有需要解题源码的同学也可以留下自己的邮箱账号。