安全-veryRSA（i春秋）

原创

小狐狸FM 于 2020-09-01 20:35:26 发布 146 收藏

分类专栏： 安全 # CTF夺旗 文章标签： python gmpy2 ctf i春秋

安全 同时被 2 个专栏收录

91 篇文章 8 订阅

订阅专栏

CTF夺旗

38 篇文章 0 订阅

订阅专栏

文章目录

前言

> 该题需要使用到一个第三方库 `gmpy2`，你可以根据下面的教程来进行安装 `gmpy2`

相关介绍

Python-解决下载gmpy2的报错问题

CTF笔记-RSA算法基础

一、题目

已知RSA公钥生成参数：

p = 348758394758943758923795872389234625477 7 q = 876786784356893476598347658437657838 9

e = 65537

求d =

请提交PCTF{d}

二、WriteUp

> 已知量是 `p、q和e`，我们可以根据 `p、q` 先计算出 `n`，然后通过 `n和e` 计算出 `d` 的值。
> 下面是有关RSA的公式

n = p*q

φ(n) = (p-1)*(q-1)

c = (m^e) mod n

d = 1 mod φ(n) / e

m = (c^d) mod n

我们可以利用 `gmpy2` 库中的函数 `gmpy2.invert()` 来计算 `d` 的值，代码如下：

```
import gmpy2

p = 348758394758943758923795872389234625477 7

q = 876786784356893476598347658437657838 9

e = 65537

n = p*q

d = int(gmpy2.invert(e , (p-1) * (q-1)))

print(d)
```