writeup: 实验吧 CTF模拟试题 解密关-RSARSA

原创

sinat_33769106 于 2018-04-19 00:32:07 发布 2684 收藏
文章标签： CTF RSA加密

两种解法:

- java

要加载security包的一系列子包，用到一大串base64加解密函数，太麻烦

- python

首先要安装python gmpy2模块,windows下安装一直没成功，在kali linux下安装的。

【在gmpy2模块下，有很多针对大数的高精度计算的函数，可以一步计算欧拉函数、求1 modphi。】

脚本如下：

```
importgmpy2


p =
96484230290105156765905517400104265349457376392357398006439893520398525072984913995610350
q
= 11874843837980297032092405848653656852760910154543380907650040190704283358909208578251(
e =  65537
c
= 83208298995174604174773590298203639360540024871256126892889661345742403314929861939100
phi = (p- 1) * (q - 1)
d =long(gmpy2.invert(e, phi))
n = p *q
printpow(c, d, n)
```

最终结果是：

flag{557744663355446657776887988}}