安全-rsarsa（BUUCTF）

原创

小狐狸FM 于 2021-08-09 17:57:47 发布 337 收藏 2

分类专栏： 安全 # CTF夺旗 文章标签： python rsa

本文链接：https://blog.csdn.net/smallfox233/article/details/119543540

安全 同时被 2 个专栏收录

91 篇文章 9 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

> 如果安装 `gmpy2` 的时候报错，可以看下方的文章

Python-解决下载gmpy2的报错问题

安全-RSA算法基础

一、题目

题目链接


```
Math is cool! Use the RSA algorithm to decode the secret message, c, p, q, and e are parameters for the RSA algo
rithm.


p =  964842302901051567659055174001042653494573763923573980064398935203985250729849139956103500916342705037010757073363335091169128029777716020062528166537848 3
q =  118748438379802970320924058486536568527609101545433809076500401907042833589092085782510630477324439922306479038875100655479473135432993032619860534865694 07
e =  65537
c =  832082989951746041747735902982036393605400248712561268928896613457424033149298619391004926666056473166465764865262174570063768422808697285817267464015837058999417682141387422596893348407356335530538876418476511737762518202930872128856701803674068074067659236389731613758173927377478327627516901044238690190 34

Use RSA to find the secret message
```

二、WriteUp

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

> 目前已知的量是 `p、q、e、c` 求 `m`
> 使用 `gmpy2` 来求解 `d`

```
================== RESTART: C:\Users\86138\Desktop\代码\test.py ================
==
p:96484230290105156765905517400104265349457376392357398006439893520398525072984913995610350091634270503701075707336333509116912802977771602006252816653784830
q:11874843837980297032092405848653656852760910154543380907650040190704283358909208578251063047732443992230647903887510065547947313543299303261986053486569407
e:65537
c:83208298995174604174773590298203639360540024871256126892889661345742403314929861939100492666605647316646576486526217457006376842280869728581726746401583705899941768214138742259689334840735633553053887641847651173776251820293087212885670180367406807406765923638973161375817392737747832762751690104423869019034
m: 55774466335544665777688799880
>>>
```



```python
# coding=utf-8
# 作者：小狐狸FM
import gmpy2
p = int(input("p:"))
q = int(input("q:"))
e = int(input("e:"))
c = int(input("c:"))
n = p*q
fn = (p-1) * (q-1) #欧拉函数
d = int(gmpy2.invert(e,fn))
m = pow(c,d,n)
print("m:",m)
```