# 实验吧 rsarsa crypto Writeup

原创

FrancisQiu 于 2019-02-25 11:12:01 发布 341 收藏 1

分类专栏： CTFwriteup CTF crypto 密码学 实验吧



本文链接：https://blog.csdn.net/qq_40737798/article/details/87913505



## 题目

> Math is cool! Use the RSA algorithm to decode the secret message, c, p, q, and e are parameters for the RSA algorithm.
> 解题链接： http://ctf5.shiyanbar.com/crypto/rsarsa/rsa.txt

## 思路

打开链接获取得到rsa.txt内容：

```
p =  96484230290105156765905517400104265349457376392357398006439893520398525072984913995610350091634270503701075
70733633350911691280297777160200625281665378483
q =  11874843837980297032092405848653656852760910154543380907650040190704283358909208578251063047732443992230647
90388751006554794731354329930326198605348656940 7
e =  65537
c =  83208298995174604174773590298203639360540024871256126892889661345742403314929861939100492666605647316646576
48652621745700637684228086972858172674640158370589994176821413874225968933484073563355305388764184765117377625 18
20293087212885670180367406807406765923638973161375817392737747832762751690104423869019034

Use RSA to find the secret message
```

显然这是个很中规中矩的rsa习题，p、q、e、c都挺大的，但是针对rsa大数处理我们可以使用gmpy2这个库。

以下是计算脚本：

```
p =  96484230290105156765905517400104265349457376392357398006439893520398525072984913995610350091634270503701075
707336333509116912802977771602006252816653784 83
q =  11874843837980297032092405848653656852760910154543380907650040190704283358909208578251063047732443992230647
903887510065547947313543299303261986053486569407
e =  65537
c =  83208298995174604174773590298203639360540024871256126892889661345742403314929861939100492666605647316646576
486526217457006376842280869728581726746401583705899941768214138742259689334840735633553053887641847651173776251 8
202930872128856701803674068074067659236389731613758173927377478327627516901044238690190 34
from gmpy2 import *
d=invert(e,(q-1)*(p-1))
n=mul(p,q)
a=powmod(c,d,n)
print(a)
```

> gmpy2 documention:https://gmpy2.readthedocs.io/en/latest/