[ACTF新生赛2020]crypto-rsa0

原创

雨后初雾& 于 2022-04-24 00:11:06 发布 81 收藏
分类专栏： 密码学CTF 文章标签： Crypt CTF

首先涉及MISC一个伪加密

伪加密原理：zip伪加密是在文件头的加密标志位做修改，进而再打开文件时识被别为加密压缩

包。 一般来说，文件各个区域开头就是50 4B，然后后面两个字节是版本，再后面两个就是判断

是否有加密的关键了

方法：
遇到504B0304，把其的第3、4个byte改成0000
遇到504B0102，把其的第5、6个byte改成0000即可破解伪加密。

直接解压

```
from Cryptodome.Util.number import *
import random

FLAG=#hidden, please solve it
flag=int.from_bytes(FLAG,byteorder = 'big')


p=getPrime(512)
q=getPrime(512)

print(p)
print(q)
N=p*q
e=65537
enc = pow(flag,e,N)
print (enc)
```

output在另一个

```
90185880664342063772402771624767392713862401730886765262953151639909683470229228412991282745
75470056738777382578357297600377652133400366963507663242291436131799321451221306857785040624
50996206925961019415256003394743594106061473865032792073035954925875056079762626648452348856
```

经典RSA加密，直接解

```
from Crypto.Util.number import inverse,long_to_bytes
import random
p=90185880664342063772402771624767392713862401730886765262953151639909683470229228412991282745514829264909
q=75470056738777382578357297600377652133400366963507663242291436131799321451221306857785040624101370436359
c=50996206925961019415256003394743594106061473865032792073035954925875056079762626648452348856255575840166
n=p*q
e=65537
phi=(p-1)*(q-1)
d=inverse(e,phi)
m=pow(c,d,n)
print(m)
#m=142333444721306535632717992082388745526585033179517
#m=616374667b6e30775f7930755f7365655f5253417d (16进制)
#actf{n0w_y0u_see_RSA}
```