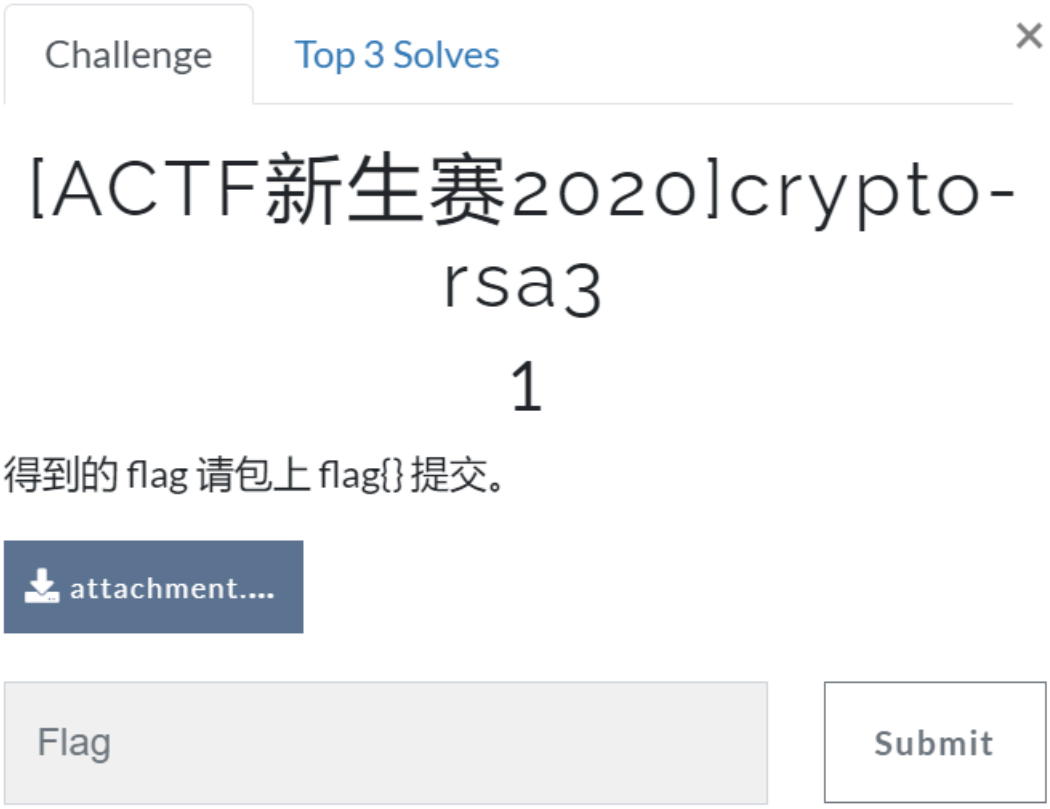
2021-05-10

原创

阿趣 于 2021-05-10 22:05:53 发布 19 收藏

BUUCTF [ACTF新生赛2020]crypto-rsa3

这题应该是非常对应标题吧，这么久了，我还是个新生/_\



打开附件：

.. (上级目录)			文件夹	
PaxHeader			文件夹	
._output.txt	1 KB	1 KB	文本文档	2020-03-05 18:03
._rsa3.py	1 KB	1 KB	Python File	2020-03-05 18:03
output.txt	1 KB	1.0 KB	文本文档	2020-03-05 18:03
rsa3.py	1 KB	1 KB	Python File	2020-03-05 18:03

感觉也就第二个程序有用

打开：

```
from flag import FLAG
from Cryptodome.Util.number import *
import gmpy2
import random

e=65537
p = getPrime(512)
q = int(gmpy2.next_prime(p))
n = p*q
m = bytes_to_long(FLAG)
c = pow(m,e,n)
print(n)
print(c)
```

这里的n,c应为：

*output.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
17760650483649924697095903022687160888596932177821105108052463408451697333144164499389802957361229009585306926403653045925365287558626794687783105514754691022710056649665814838183468303736613455384801190325125272647404766127422313772768868953582353304677879313190214344440873561082116783871748885990224286368314573903785113823547710005409453611689847750526930736416823750714074908512897030709057495258304830359887371176539714284246123320209259266173955588681603806019124982999228259142295101669579104518417300289198838076344898341288308014072284472217752647113499281562901027823743794067192921160475815605303822100 49
```


看完题目也基本可以确定思路，找到p,q的值；

用在线分解n试还真出来了

Search	Sequences	Report results	Factor tables	Status	Downloads	Login

Additional information (Internal ID 1100000002518323590)	
Digits (Base 10)	155
Number	133269090503574476435265858368339693780781470577230547014328421929887176493857314300950556223035495772334957937155800048016342685057252555650215198171792 93

Search	Sequences	Report results	Factor tables	Status	Downloads	Login

Additional information (Internal ID 1100000002518323589)	
Digits (Base 10)	155
Number	133269090503574476435265858368339693780781470577230547014328421929887176493857314300950556223035495772334957937155800048016342685057252555650215198171792 31

factordb.com - 6 queries to generate this page (0.01 seconds) (limits) (Imprint) (Privacy Policy)

得到p,q的值，就好办了

代码：

```
import gmpy2
from Crypto.Util.number import *
p = 133269090503574476435265858368339693780781470577230547014328421929887176493857314300950556223035495772334957
937155800048016342685057252555650215198171792 31

q = 133269090503574476435265858368339693780781470577230547014328421929887176493857314300950556223035495772334957
937155800048016342685057252555650215198171792 93

n = 177606504836499246970959030226871608885969321778211051080524634084516973331441644993898029573612290095853069
264036530459253652875586267946877831055147546910227100566496658148381834683037366134553848011903251252726474047 6
612742231377276886895358235330467787931319021434444087356108211678387174888599022428636 83

c = 145739037851138235477100054094536116898477505269307364168237507140749085128970307090574952583048303598873711
765397142842461233202092592661739555886816038060191249829992282591422951016695791045184173002891988380763448983 4
128830801407228447221775264711349928156290102782374379406719292116047581560530382210049

phi = (p-1)*(q-1)

e=65537

d = gmpy2.invert(e,phi)

m = gmpy2.powmod(c,d,n)
print(long_to_bytes(m))
```

Python 2.7.6 Shell

File Edit Shell Debug Options Windows Help

```
Python 2.7.6 (default, Nov 10 2013, 19:24:24) [MSC v.1500 6
32
Type "copyright", "credits" or "license()" for more informa
>>> ========== RESTART ==========
>>>
actf{p_and_q_should_not_be_so_close_in_value}
>>>
```