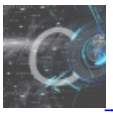
2021-07-05

原创

无名函数 于 2021-07-05 23:33:21 发布 86 收藏

分类专栏： Buu-crypto

本文链接：https://blog.csdn.net/m0_57291352/article/details/118499479



[AFCTF2018]你能看出这是什么加密么

题目

```
p=0x928fb6aa9d813b6c3270131818a7c54edb18e3806942b88670106c1821e0326364194a8c49392849432b37632f0abe3f3c52e909b939c91c50e41a7b8cd00c67d6743b4f

q=0xec301417ccdffa679a8dcc4027dd0d75baf9d441625ed8930472165717f4732884c33f25d4ee6a6c9ae6c44aedad039b0b72cf42cab7f80d32b74061

e=0x10001

c=0x70c9133e1647e95c3cb99bd998a9028b5bf492929725a9e8e6d2e277fa0f37205580b196e5f121a2e83bc80a8204c99f5036a07c8cf6f96c420369b4161d2654a7eccbdaf583204b645e137b3bd15c5ce865298416fd5831cba0d947113ed5be5426b708b89451934d11f9aed9085b48b729449e461ff0863552149b965e22b6
```

解题

非常明显的RSA加密

```
import gmpy2
from Crypto.Util.number import long_to_bytes

p=0x928fb6aa9d813b6c3270131818a7c54edb18e3806942b88670106c1821e0326364194a8c49392849432b37632f0abe3f3c52e909b939c91c50e41a7b8cd00c67d6743b4f
q=0xec301417ccdffa679a8dcc4027dd0d75baf9d441625ed8930472165717f4732884c33f25d4ee6a6c9ae6c44aedad039b0b72cf42cab7f80d32b74061
e=0x10001
c=0x70c9133e1647e95c3cb99bd998a9028b5bf492929725a9e8e6d2e277fa0f37205580b196e5f121a2e83bc80a8204c99f5036a07c8cf6f96c420369b4161d2654a7eccbdaf583204b645e137b3bd15c5ce865298416fd5831cba0d947113ed5be5426b708b89451934d11f9aed9085b48b729449e461ff0863552149b965e22b6

n = q*p
phi = (q-1) * (p-1)
d = gmpy2.invert(e,phi)
m = gmpy2.powmod(c,d,n)

print(long_to_bytes(m))
```

运行

```
b'\x02\xd3\xe4v\xea\x80r\x83\xda\x99\x88\xf5#\x08\xbbAT\x8b\xaf\xd2\xf4\xdc\x9f\xd3\xbf\xb7A\xc3\xcc\xc5`\xa1\x8
b\x86\x18y\xd0&\x88\x10\xef\xbe\x83\xcer\xceC\x17\xec[\xb7%\x08\xef\x16\x1f\xab\x0c\x96\xa3\xdc N^\x8e,\xa3\x11{
\x99U\xcd\x15o\xd7B\xf4L\x8f}&\xc5$\xca\xd5;\xf9\x02Y\xc1\xbbS\xfd4\x83M\x96\xa9\xbd;\x83/\xf7\x00afctf{R54_|5_$
0_$imp13}'
```

答案

```
flag{R54_|5_$0_$imp13}
```

[ACTF新生赛2020]crypto-rsa3

题目

output

```
17760650483649924697095903022687160888596932177821105108052463408451697333144164499389802957361229009585306926403653045925365287558626794687783105514754691022710056649665814838183468303736613455384801190325125272647404766127422313772768868953582353304677879313190214344440873561082116783871748885990224286368314573903785113823547710005409453611689847750526930736416823750714074908512897030709057495258304830359887371176539714284246123320209259266173955588681603806019124982999228259142295101669579104518417300289198838076344898341288308014072284472217752647113499281562901027823743794067192921160475815605303822100 49
```

rsa3

```
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)
```

解题

已知n、c、e

并且知道p、q相似，可以对n开平方

```
import gmpy2
import sympy
from Crypto.Util.number import long_to_bytes

n=17760650483649924697095903022687160888596932177821105108052463408451697333144164499389802957361229009585306926
40365304592536528755862679468778310551475469102271005664966581483818346830373661345538480119032512527264740476612
27422313772768868953582353304677879313190214344440873561082116783871748885990224286368 3
e = 65537
c=14573903785113823547710005409453611689847750526930736416823750714074908512897030709057495258304830359887371176
53971428424612332020925926617395558868160380601912498299922825914229510166957910451841730028919883807634489834128830801407228447221775264711349928156290102782374379406719292116047581560530382210049

n2=gmpy2.iroot(n,2)[0]
p=sympy.nextprime(n2)
q=n//p
phi=(p-1)*(q-1)
d=gmpy2.invert(e,phi)
m=pow(c,d,n)
print(long_to_bytes(m))
```

运行

```
b'actf{p_and_q_should_not_be_so_close_in_value}'
```

答案

flag{p_and_q_should_not_be_so_close_in_value}

鸡藕椒盐味

题目

公司食堂最新出了一种小吃，叫鸡藕椒盐味汉堡，售价八块钱，为了促销，上面有一个验证码，输入后可以再换取一个汉堡。但是问题是每个验证码几乎都有错误,而且打印的时候倒了一下。小明买到了一个汉堡，准备还原验证码，因为一个吃不饱啊~~验证码如下：1100 1010 0000 ,而且打印的时候倒了一下。把答案哈希一下就可以提交了~~。(答案为正确值(不包括数字之间的空格)的32位md5值的小写形式)

解密

验证码：1100 1010 0000
倒一下：000001010011
MD5加一下密，不对

漏了一条：每个验证码几乎都有错误。

尝试海明校验码校验

得到校验后的：0000 0001 0101 0011 1
倒一下：11100101010000000
哈希，错误

尝试奇偶校验码校验

得到校验后110110100000

MD5加密：
d14084c7ceca6359eaac6df3c234dd3b

忽然发现，鸡藕椒盐味是奇偶校验位的谐音□

答案

flag{d14084c7ceca6359eaac6df3c234dd3b}