虎符-ctf crypto writeup

原创

逃课的小学生 于 2020-04-23 14:58:38 发布 1029 收藏
分类专栏： ctf crypto

本文链接：https://blog.csdn.net/zhang14916/article/details/105639269

1.GM

由于题目中描述了这时一个GM密码系统，所以我们在网上查到FM密码系统破解方式https://blog.csdn.net/qq_26816591/article/details/82957481

首先根据n,phin建立一元二次方程求解n的因子p，q，再带入到解密公式中求解

```
import gmpy2

phi=9433451661749413225919414595243321311762902037908850954799703396083863718641136503053215995576558003171
n=943345166174941322591941459524332131176290203790885095479970339608386371864113650305321599557655800317124
cc=密文
a=1
b=phi-n-1
c=n
delat=gmpy2.iroot(pow(b,2)-4*a*c,2)
assert delat[1]
p=(delat[0]-b)/(2*a)
print p
assert n%p==0
q=n//p
print c%p
m=""
for i in cc:
 if gmpy2.jacobi(i,p)==1 and gmpy2.jacobi(i,q)==1:
  m=m+"0"
 elif gmpy2.jacobi(i,p)==-1 and gmpy2.jacobi(i,q)==-1:
  m=m+"1"
 else:
  m=m+"k"
print m
```

2.pell

我们发现这时一个Pell's Equation问题，我们在网上找到求解方案https://brilliant.org/wiki/quadratic-diophantine-equations-pells-equation/

Suppose $x_1^2 - ny_1^2 = 1$. Applying Brahmagupta's identity repeatedly gives an infinite sequence of solutions $(x_1, y_1), (x_2, y_2), (x_3, y_3), \ldots$ to the equation $x^2 - ny^2 = 1$, where

$$x_k = x_{k-1}x_1 + ny_{k-1}y_1$$
$$y_k = x_{k-1}y_1 + y_{k-1}x_1.$$

These solutions are said to be *generated by* (x_1, y_1).

Note that if $x_1 + y_1\sqrt{n} = \alpha$, then $x_2 + y_2\sqrt{n} = \alpha^2$, $x_3 + y_3\sqrt{n} = \alpha^3$, and so on. The solutions (x_k, y_k) correspond to $\alpha^k = x_k + y_k\sqrt{n}$.

于是我们只需要将第一个爆破出来，然后按照公式就可以找到后面的149组$x^2 - ny^2 = 1$的解

```
from pwn import *
import hashlib
import math
import gmpy2

def proof(a,b):
 ss="abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789"
 print b
 for i in ss:
  for j in ss:
   for k in ss:
    for o in ss:
     jie=i+j+k+o+a
     ll=hashlib.sha256(jie).hexdigest()
     if ll==b:
      return jie
io=remote("39.97.210.182",61235)
io.recvuntil("+")
tian=io.recvuntil(")")[:-1]
io.recvuntil("== ")
sh256=io.recvuntil("\n")[:-1]
print tian.encode("hex")
print sh256.encode("hex")
io.recvuntil(":")
haha=proof(tian,sh256)
print haha
io.sendline(haha[:4])
io.recvuntil("Where a = ")
a=io.recvuntil(",")[:-1]
io.recvuntil("b = ")[:-1]
b=io.recvuntil("\n")
aint=int(a)
bint=int(b)
print aint,bint
if bint==2:
 print "bintwrong"
 io.interactive()
if gmpy2.iroot(aint,2)[1]:
 print "aintwrong"
 io.interactive()
xjie=[]
yjie=[]
for i in xrange(2,1000000):
 xx=gmpy2.iroot(1+aint*pow(i,2),2)
 if xx[1]:
  xjie.append(xx[0])
  yjie.append(i)
  break
```

```
print xjie[0],yjie[0]
io.sendline(str(xjie[0]))
io.sendline(str(yjie[0]))
for i in xrange(1,150):
 sleep(1)
 print i
 xk=xjie[-1]*xjie[0]+aint*yjie[-1]*yjie[0]
 yk=xjie[-1]*yjie[0]+yjie[-1]*xjie[0]
 io.sendline(str(xk))
 io.sendline(str(yk))
 xjie.append(xk)
 yjie.append(yk)
io.interactive()
```