

陇原战役 Crypto题目 WriteUP WP CTF竞赛

原创

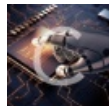
青少年网络安全 于 2022-03-27 05:40:48 发布 15 收藏

分类专栏: [CTF-WP](#) 文章标签: [网络安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/zxsctf/article/details/123767625>

版权



[CTF-WP 专栏收录该内容](#)

3 篇文章 0 订阅

订阅专栏

前几个星期发的陇原战役的Misc、Web WriteUP, 今天继续给大家分享Crypto的WP。

mostlycommon

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

def modulus(n,e1,e2,c1,c2):

    _,s,t = gcdext(e1, e2)
    m = (pow(c1,s,n) * pow(c2 , t , n)) % n
    print(long_to_bytes((iroot(m,2)[0])))

N=122031686138696619599914690767764286094562842112088225311503826014006886039069083192974599712685027825111
c1=39449016403735405892343507200740098477581039605979603484774347714381635211925585924812727991400278031892
c2=43941404835820273964142098782061043522125350280729366116311943171108689108114444447295511969090107129530
e1 = 65536
e2 = 270270
print(gcd(e1,e2))
modulus(N,e1,e2,c1,c2)
#SETCTF{now_you_master_common_mode_attack}
```

easytask

典型GGH公钥加密

```
from sage.modules.free_module_integer import IntegerLattice
e=[151991736758354,115130361237591,58905390613532,130965235357066,74614897867998,48099459442369,45894485782
W=[[-10150241248,-11679953514,-8802490385,-12260198788,-10290571893,-334269043,-11669932300,-2158827458,-70
[52255960212,48054224859,28230779201,43264260760,20836572799,8191198018,14000400181,4370731005,14251110],
[2274129180,-1678741826,-1009050115,1858488045,978763435,4717368685,-561197285,-1999440633,-6540190],
[45454841384,34351838833,19058600591,39744104894,21481706222,14785555279,13193105539,2306952916,7501297],
[-16804706629,-13041485360,-8292982763,-16801260566,-9211427035,-4808377155,-6530124040,-2572433293,-839373
[28223439540,19293284310,5217202426,27179839904,23182044384,10788207024,18495479452,4007452688,13046387],
[968256091,-1507028552,1677187853,8685590653,9696793863,2942265602,10534454095,2668834317,8694828],
[33556338459,26577210571,16558795385,28327066095,10684900266,9113388576,2446282316,-173705548,-577070],
[35404775180,32321129676,15071970630,24947264815,14402999486,5857384379,10620159241,2408185012,7841686]]
e = vector(e)
W = matrix(W)
e = vector(e)
W = matrix(W)
def babai(A, w):
    A = A.LLL()
    G = A.gram_schmidt()[0]
    t = w
    for i in reversed(range(A.nrows())):
        c = ((t * G[i]) / (G[i] * G[i])).round()
        t -= A[i] * c
    return w - t
V = babai(W,e)
m = V/W
print(m)

import hashlib
from Crypto.Util.number import *
from Crypto.Cipher import AES
c = int('1070260d8986d5e3c4b7e672a6f1ef2c185c7fff682f99cc4a8e49cfce168aa0',16)
m = [877, 619, 919, 977, 541, 941, 947, 1031, 821]
key = hashlib.sha256(str(m).encode()).digest()
cipher = AES.new(key, AES.MODE_ECB)
flag = cipher.decrypt(long_to_bytes(c))
print(flag)
```

Civet cat for Prince

```

from hashlib import sha256
from pwn import *
import string
from Crypto.Util.strxor import strxor

def proof_of_work(end, sha):
    for a in table:
        for b in table:
            for c in table:
                for d in table:
                    if sha256((a+b+c+d+end).encode()).hexdigest() == sha:
                        r.recvuntil(b'[+] Give Me XXXX :')
                        r.sendline((a+b+c+d).encode())
                        print(a+b+c+d)

table = string.ascii_letters + string.digits
r = remote(' ', )
r.recvuntil(b"[+] sha256(XXXX+)"
end = r.recv(8).decode()
r.recvuntil(b") == ")
sha = r.recvuntil(b'\n')[:-1].decode()
proof_of_work(end, sha)
r.recvuntil(b'2.Go away\n')
r.sendline(b'1')
r.recvuntil(b'\n')
r.sendline(b'a'*16)
r.recvuntil(b'Miao~ ')
iv = r.recvuntil(b'\n')[:-1]
print(iv)
r.recvuntil(b'3.say Goodbye\n')
r.sendline(b'1')
r.recvuntil(b"Permission:")
permission = r.recvuntil(b'\n')[:-1]
print(permission)
r.recvuntil(b'3.say Goodbye\n')
r.sendline(b'2')
r.recvuntil(b'Give me your permission:\n')
p1 = strxor(strxor(permission[:16], b'a_cat_permission'), b'Princepermission')
print(p1)
r.sendline(p1)
r.recvuntil(b'Miao~ \n')
r.sendline(iv)
r.recvuntil(b"The message is ")
m = r.recvuntil(b'\n')[:-1]
fiv = strxor(strxor(m, b'a'*16), iv)
r.recvuntil(b'3.say Goodbye\n')
r.sendline(b'3')
r.recvuntil(b"Give me your permission:\n")
r.sendline(p1+permission[16:])
r.recvuntil(b"What's the cat tell you?\n")
r.sendline(fiv)
r.interactive()

```