HGAME 2021 week4 writeup

Crypto

夺宝大冒险1

题目如下

```
import os

flag = "xxxx"

class Cxx1ff:
    c4ff1x = int.from_bytes(os.urandom(8),'big')
    c66f6 = int.from_bytes(os.urandom(8),'big')
    c4ff10 = int.from_bytes(os.urandom(8),'big')
    def __init__(self, seed):
        self.state = seed

    def next(self):
        self.state = (self.state * self.c4ff1x + self.c66f6) % self.c4ff10
        return self.state

class Cxx2ff:
    c4ff1x = int.from_bytes(os.urandom(8),'big')
    c66f6 = int.from_bytes(os.urandom(8),'big')
    c4ff10 = int.from_bytes(os.urandom(8),'big')
    def __init__(self, seed):
        self.state = seed
```

```
    def next(self):
        self.state = (self.state * self.c4ff1x + self.c66f6) % self.c4ff10
        return self.state

class Cxx3ff:
    c4ff1x = int.from_bytes(os.urandom(8),'big')
    c66f6 = int.from_bytes(os.urandom(8),'big')
    c4ff10 = int.from_bytes(os.urandom(8),'big')
    def __init__(self, seed):
        self.state = seed

    def next(self):
        self.state = (self.state * self.c4ff1x + self.c66f6) % self.c4ff10
        return self.state


def test1():
    gen = Cxx1ff(123)
    print((Cxx1ff.c4ff1x,Cxx1ff.c4ff10))
    print(gen.next())
    print(gen.next())
    t1 = input()
    try:
        if int(t1.strip())==Cxx1ff.c66f6:
            return 1
    except:
        pass
    return 0



def test2():
    gen = Cxx2ff(123)
    print((Cxx2ff.c4ff10))
    print(gen.next())
    print(gen.next())
    print(gen.next())
    t1 = input()
    t2 = input()
    try:
        if (int(t1.strip())==Cxx2ff.c4ff1x) and (int(t2.strip())==Cxx2ff.c66f6):
            return 1
    except:
        pass
    return 0

def test3():
    gen = Cxx3ff(123)
    print(gen.next())
    print(gen.next())
    print(gen.next())
    print(gen.next())
    print(gen.next())
    print(gen.next())
    print(gen.next())
    t1 = input()
    try:
```

```
        if int(t1.strip())==Cxx3ff.c4ff10:
            return 1
    except:
        pass
    return 0

if __name__ == "__main__":
    ans = 0
    ans += test1()
    ans += test2()
    ans += test3()
    if ans>=3:
        print("win")
        print(flag)
    else:
        print("fail")
```

一开始折腾了半天，啥也看不出来，问了一下学长，学长让我就`CTF Wiki`找同类型题，发现是`线性同余生成器`，然后找到一篇文章

[]: https://zeroyu.xyz/2018/11/02/Cracking-LCG/

用上面的方法写了代码发现算出的数并不一定是答案，其中实际的`modulus`可能是算出的倍数，而实际的`increment`和`multiplier`可能是算出的值加上`modulus`，有时给的数没有乘法逆元。同时符合答案的概率还挺小的，为了方便，使用`pwntool`

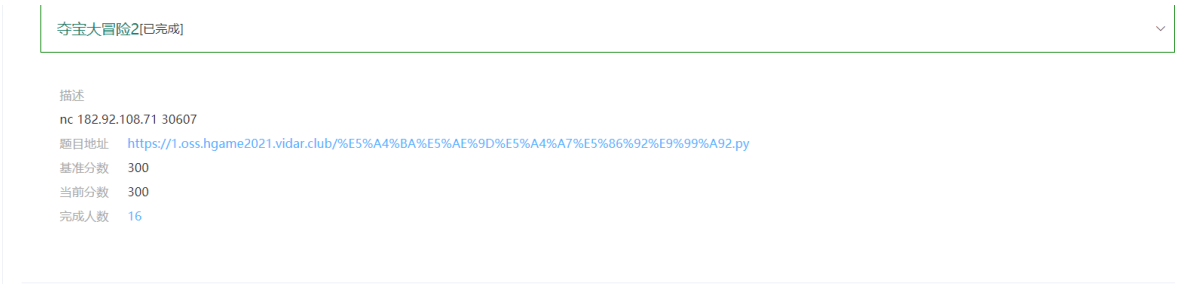
```
import gmpy2
from functools import reduce
from pwn import *

def crack_unknown_increment(multiplier,modulus,states):
    increment = (states[1] - states[0]*multiplier) % modulus + modulus
    return increment

def crack_unknown_multiplier(modulus ,states):
    multiplier = (states[2] - states[1]) * gmpy2.invert(states[1] - states[0],
modulus) % modulus
    return int(multiplier), int(crack_unknown_increment(
multiplier,modulus,states))

def crack_unknown_modulus(states):
    diffs = [s1 - s0 for s0, s1 in zip(states, states[1:])]
    zeroes = [t2*t0 - t1*t1 for t0, t1, t2 in zip(diffs, diffs[1:], diffs[2:])]
    modulus = abs(reduce(gmpy2.gcd, zeroes))
    return modulus

def main():
    a=int(io.recvuntil(",")[1:-1])
    b=int(io.recvline(keepends=True)[:-2])
    c=int(io.recvline(keepends=True))
    d = int(io.recvline(keepends=True))
    e=crack_unknown_increment(a,b,[c,d])
    io.sendline(str(e))
    f=crack_unknown_multiplier(int(io.recvline(keepends=True)),
[int(io.recvline(keepends=True)), int(io.recvline(keepends=True)),
int(io.recvline(keepends=True))])
```

```
    g=f[0]
    h=f[1]
    io.sendline(str(g))
    io.sendline(str(h))
    i=crack_unknown_modulus([int(io.recvline(keepends=True)),
int(io.recvline(keepends=True)), int(io.recvline(keepends=True)),
int(io.recvline(keepends=True)), int(io.recvline(keepends=True)),
int(io.recvline(keepends=True)), int(io.recvline(keepends=True))])
    io.sendline(str(i))
    flag=io.recvall()
    print(flag)

io = remote("182.92.108.71",30641)

main()
```

得flag

```
[x] Receiving all data: 0B
[x] Receiving all data: 56B
[+] Receiving all data: Done (56B)
[*] Closed connection to 182.92.108.71 port 30641
b'win\nhgame{Cracking^prng_Linear)Congruential&Generators}\n'

进程已结束,退出代码0
```

夺宝大冒险2



题目如下

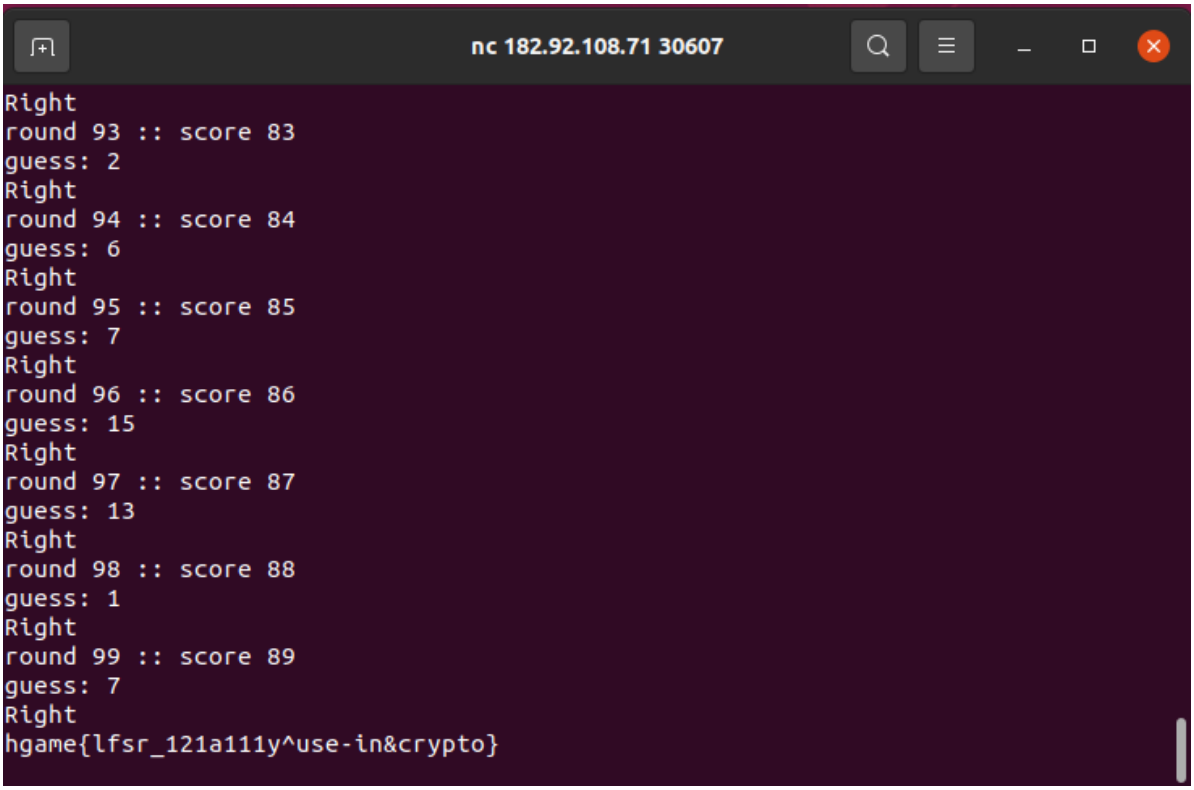
```
class LXFIQNN():
    def __init__(self, init, mask, length):
        self.init = init
        self.mask = mask
        self.lengthmask = 2**(length+1)-1

    def next(self):
        nextdata = (self.init << 1) & self.lengthmask
        i = self.init & self.mask & self.lengthmask
        output = 0
        while i != 0:
            output ^= (i & 1)
            i = i >> 1
        nextdata ^= output
        self.init = nextdata
```

```
        return output

    def random(self, nbit):
        output = 0
        for _ in range(nbit):
            output <<= 1
            output |= self.next()
        return output


from secret import init, FLAG
"""secret.py
import os
init = int.from_bytes(os.urandom(5), 'big')
FLAG = 'hgame{xxx}'
"""


prng = LXFIQNN(init, 0b1011001010001010000100001000111011110101, 40)

score = 0
for r in range(100):
    print(f"round {r} :: score {score}")
    try:
        guess = int(input("guess: "))
    except:
        break
    secret = prng.random(4)
    if secret == guess:
        print("Right")
        score += 1
    else:
        print(f"Wrong, the secret is {secret}")

if score >= 80:
    print(FLAG)
```

非预期

一开始一直想着怎么把`init`反解出来，后来发现其实不用，因为一次`self.next()`运算会将`init`第一位去除并在最后一位加上一个新位所以每10次猜数会产生一个新的`init`，而新的`init`的值可以已给出的`secret`推出，`secret`值的范围为`[0,15]`，将前10次得到的`secret`变成二进制再收尾相连即为第11次猜数的`init`，将新`init`带入原来的代码即可预测之后的`secret`

之后就可得flag（没想着写代码，直接全部手打，中间还打错了一个，虽然对结果没影响）



预期解

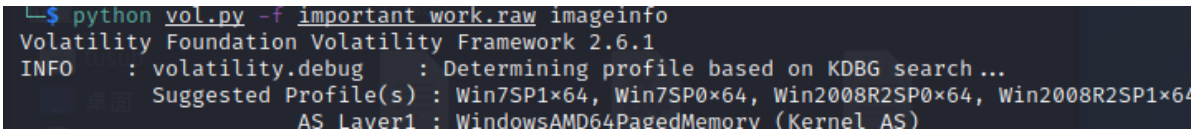
之后做了`夺宝大冒险1`才发现不是正解，这题的考点是`反馈移位寄存器`

学长一直催交`wp`，来不及写了😥，之后几天再试一试

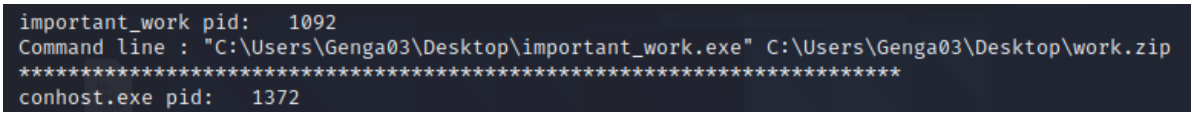
MISC

Akira之瞳-1

得`raw`文件，使用`volatility`，先用`python vol.py -f important_work.raw imageinfo`



`python vol.py -f important_work.raw --profile=Win7SP1x64 cmdline`，发现`work.zip`



找到`work.zip`并提取

```
└─$ python vol.py -f important_work.raw --profile=Win7SP1x64 filescan |grep "work.zip"
Volatility Foundation Volatility Framework 2.6.1
0x000000003ec703d0     18      2 R--rw- \Device\HarddiskVolume1\Users\Genga03\Desktop\work.zip
0x000000003ed673d0     18      2 R--rw- \Device\HarddiskVolume1\Users\Genga03\Desktop\work.zip
```

```
└─$ python vol.py -f important_work.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000003ec703d0 -D ./ -u
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x3ec703d0   None   \Device\HarddiskVolume1\Users\Genga03\Desktop\work.zip
SharedCacheMap 0x3ec703d0   None   \Device\HarddiskVolume1\Users\Genga03\Desktop\work.zip
```

压缩包属性提示密码来源

注释　　锘緫assword is sha256(login_password)

用命令`python vol.py -f important_work.raw windows.hashdump`（这里改用`volatility3`）

```
Administrator   500     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
Guest   501     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
Genga03 1001    aad3b435b51404eeaad3b435b51404ee        84b0d9c9f830238933e7131d60ac6436
```

解最后一个hash的密码

得到两张看上去相同的图


Blind.png


src.png

经学长提示得知是盲水印，用`BlindWaterMark`解后看图得flag

Akira之瞳-2

Akira之瞳-2[已完成]

描述

.....

"最后呢？"

"最后她还是没能幸免，人们在保险箱旁发现了她烧焦的尸体，打开保险箱人们发现了一个U盘，是她将回家画好的原稿带来时用的 ....."

题目地址　https://1.oss.hgame2021.vidar.club/secret_work_bd40aea1c133a4d6422925deccb139e9.7z

基准分数　400

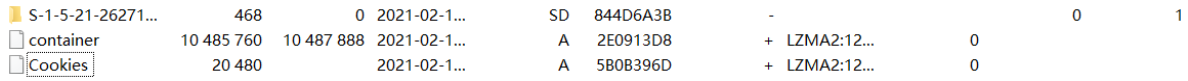
当前分数　400

完成人数　11

使用`python vol.py -f secret_work.raw --profile=Win7SP1x64 cmdline`，发现`dumpme.txt`并提取得以下内容

```
zip password is: 5trqES&P43#y&1TO
And you may need LastPass
```

拿到压缩包



S-1-5-21-26271...	468	0	2021-02-1...	SD	844D6A3B	-		0	1
container	10 485 760	10 487 888	2021-02-1...	A	2E0913D8	+ LZMA2:12...	0		
Cookies	20 480		2021-02-1...	A	5B0B396D	+ LZMA2:12...	0		

经学长提醒，搜到相关文章

[]: https://www.freebuf.com/articles/system/117553.html

使用插件和命令`python vol.py -f secret_work.raw --profile=Win7SP1x64 lastpass`获得内容

```
Found LastPass Entry for
live.com,bing.com,hotmail.com,live.com,microsoft.com,msn.com,windows.com,windows
azure.com,office.com,skype.com,azure.com
UserName: windows login & miscrosoft
Pasword: vIg*q3x6GFa5aFBA
```

之后学长让我去了解一下`mimikatz`并先解压缩包中的`Cookies`（`mimikatz`一开始直接被系统杀了，然后搞了台虚拟机就没事了）

直接提cookie会提示要`MasterKey`，用`dpapi::masterkey /in:"C:\Users\xxx\Desktop\secret\S-1-5-21-262715442-3761430816-2198621988-1001\57935170-beab-4565-ba79-2b09570b95a6" /password:"vIg*q3x6GFa5aFBA"`得`MasterKey`

```
[masterkey] with password: vIg*q3x6GFa5aFBA (normal user)
  key : 3cafd3d8e6a67edf67e6fa0ca0464a031949182b3e68d72ce9c08e22d7a720b5d2a768417291a28fb79c6def7d068f84955e774e87e37c6b
0b669e05fb7eb6f8
  sha1: 8fc9b889a47a7216d5b39c87f8192d84a9eb8c57
```

再提`Cookies`

```
Host     : localhost ( / )
Name     : VeraCrypt
Dates    : 2021/2/19 14:08:59 -> 2022/2/19 14:00:00
 * using CryptUnprotectData API
 * volatile cache: GUID:{57935170-beab-4565-ba79-2b09570b95a6};KeyHash:8fc9b889a47a7216d5b39c87f8192d84a9eb8c57;Key:avai
lable
 * masterkey     : 3cafd3d8e6a67edf67e6fa0ca0464a031949182b3e68d72ce9c08e22d7a720b5d2a768417291a28fb79c6def7d068f84955e7
74e87e37c6b0b669e05fb7eb6f8
Cookie: !bWjAqM2z!iSoJsV*&IRV@*AVI1VrtAb
```

再用`veracrypt`得名为`ADS.jpg`的图片，用`ntfs streams editor`得flag

```
[文本](自动识别编码类型:TMBCSEncoding)
hgame{Which_0nly_cryin9_3yes_c4n_de5cribe}
And you may be intertested in this bonus: https://eyes.hgame2021.cf
```

历时四周的`hgame`终于结束了，从中学到了很多，同时也感谢学长给予我的指导（特别是`Akira`学长，~~因为我只会做misc~~）。校内只排18名，感觉自己好菜啊。期待能通过线下赛进协会。