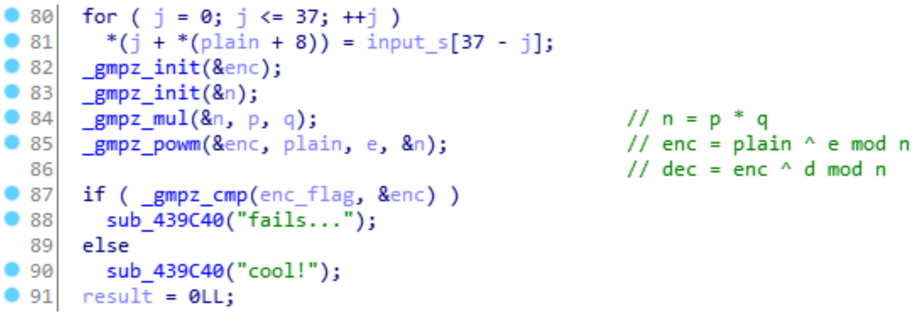
Week2_Rev 公式Writeup

0x00 wtfitis

ida打开，代码很丑。先看下字符串，有提到gmp的字样，说明静态库。
描述也在暗示，没符号那就去做符号。
先搞到gmp的静态链接库文件(.a)，再利用工具FLAIR即可作出.sig符号文件。(网上教程一堆
成功载入符号文件后:



```
for ( j = 0; j <= 37; ++j )
  *(j + *(plain + 8)) = input_s[37 - j];
_gmpz_init(&enc);
_gmpz_init(&n);
_gmpz_mul(&n, p, q);                        // n = p * q
_gmpz_powm(&enc, plain, e, &n);             // enc = plain ^ e mod n
                                            // dec = enc ^ d mod n
if ( _gmpz_cmp(enc_flag, &enc) )
  sub_439C40("fails...");
else
  sub_439C40("cool!");
result = 0LL;
```

到这里应该就没任何难度了，已知p,q,e，用ex_gcd求出d

```
p = 0xD0E7CDA746B95CC87A9950A39D517741673BB5
q = 0x9703D6BF1C83E5283B493280E3023189C1FCEB
e = 0x10001
n = 0x7B3BDC42CDCE6AEFC66B1188FFC7E36DDB1C6DD5CB564CF51BE91EEA11
phi_n = 0x7B3BDC42CDCE6AEFC66B1188FFC7E36DDB1C6C6DDFB1E691DEA72E
enc = 0x448EEEBA1CF31BA2E9E22A9E6F37AB2C70A2E19485E819A8CB5D897E


def ExtendedEuclidean(a,b):
    r0 = a;
    r1 = b;
    x0 = 1;
    x1 = 0;
    y0 = 0;
    y1 = 1;
    z = [r0,x0,y0];
    while r1>0:
        r = r0%r1;
        q = (r0-r)/r1;
        x = x0-q*x1;
        y = y0-q*y1;
        z = [r1,x1,y1];
        x0 = x1;
        y0 = y1;
        x1 = x;
        y1 = y;
        r0 = r1;
        r1 = r;
    print("\ngcd(", a, ",", b, ") =", r0, "\nWeight s: ", x0, "\

a = e
b = phi_n
ExtendedEuclidean(a,b);
# a * s + b * t = gcd(a,b)

d = hex(160899983500320508286855970148380530736037066678692385 11
print d
```

得到plain

```
6867616D657B336173795F7273615F486176655F555F666967757265645F3174
hgame{3asy_rsa_Have_U_figured_1t_0ut?}
```

0x01 miaomiaowu

py2exe。用unpy2exe也好，工具很多。我这边使用rePy2exe
提取出py文件

```
#!/usr/bin/env python
# visit http://tool.lu/pyc/ for more information
import md5
import random
import string

def o0o0(o0oo0):
    o0oo0 = int(o0oo0)
    for i in range(95, o0oo0 / 2 + 1):
        if o0oo0 % i == 0:
            print hex(i)return o0o0(o0oo0 / i),

    print o0oo0



def o_0(o00o):
    m = md5.new()
    m.update(o00o)
    return m.hexdigest()
```

```
def l11_l(l1o0):
    oo_0 = list(string.oo_0) + list(string.digits) + [
        '+',
        '/']
    for i in l1o0:
        if i != '=':
            continue
            oo_o = []['{:0>6}'.format(str(bin(oo_0.index(i))).re
            ll111l = ''
            o0_o0 = l1o0.count('=')
            for x in [
                0,
                8,
                16]:
                continue
                o1_o1 = [][oo_o0[x:x + 8]]
                for x in o1_o1:
                    if x:
                        continue
                        o1_o1 = [][int(x, 2)]
                        continue
                        ''.join += []([ chr(x) for x in o1_o1 ])
                        oo_o = oo_o[4:]
                    return ll111l

if __name__ == '__main__':
    print "Welcome to hammer's miaomiaowu"
    while True:
        print 'Give me your choice:'
        print '1) fuck hammer'
        print '2) hit hammer'
        print '3) save hammer'
        l1l = raw_input()
        if l1l == '1':
            lll = raw_input('plz input your public key:')
            if lll == '1543788':
                print 'Here is your key:'
                o0o0(lll)

        if l1l == '2':
            print 'Hammer was the mouth of the ball, only issued
            continue
        if l1l == '3':
            print "You must give me the flag , or you can't save
            print 'But I must know who are you , give me your ke
            key = raw_input()
            flag = raw_input('Now , give me your flag:')
            l_l = flag[-4:-1]
            if l_l != key:
                print 'Unknown key!'
                print '(You are taken as an intruder, captured a
                exit()
            f = open('1.jpeg', 'r')
            f.seek(1024, 0)
            o = f.read(1)
            o = o_0(o)
            f.seek(512, 1)
            oo = f.read(1)
            oo = o_0(oo)
            f.seek(256, 1)
            ooo = f.read(1)
            ooo = o_0(ooo)
            f.seek(128, 1)
            ooo0 = f.read(1)
            ooo0 = o_0(ooo0)
            print 'Pay attention, The program may be abnormal'
            if o != '0d61f8370cad1d412f80b84d143e1257':
                print 'Error flag!'
                print '(You are taken as an intruder, captured a
                exit()
            if oo != 'cfcd208495d565ef66e7dff9f98764da':
                print 'Error flag!'
                print '(You are taken as an intruder, captured a
                exit()
            if ooo != '8277e0910d750195b448797616e091ad':
                print 'Error flag!'
                print '(You are taken as an intruder, captured a
                exit()
            if ooo0 != 'e4da3b7fbbce2345d7772b0674a318d5':
                print 'Error flag!'
                print '(You are taken as an intruder, captured a
                exit()
            o_l = o + oo + ooo + ooo0
            o_1 = flag[6:15]
            if l11_l(o_1) != 'RnVjazFuZzEx':
                print 'Error flag5!'
                print '(You are taken as an intruder, captured a
                exit()
            print 'Yeah! You got it!'
            flag233 = 'hgame{' + o_1 + '_' + o_l + '_' + l_l + '
            print flag233
            continue
```

flag分为3个部分，唯一的难度就是变量名丑。

第1部分o_1: base64

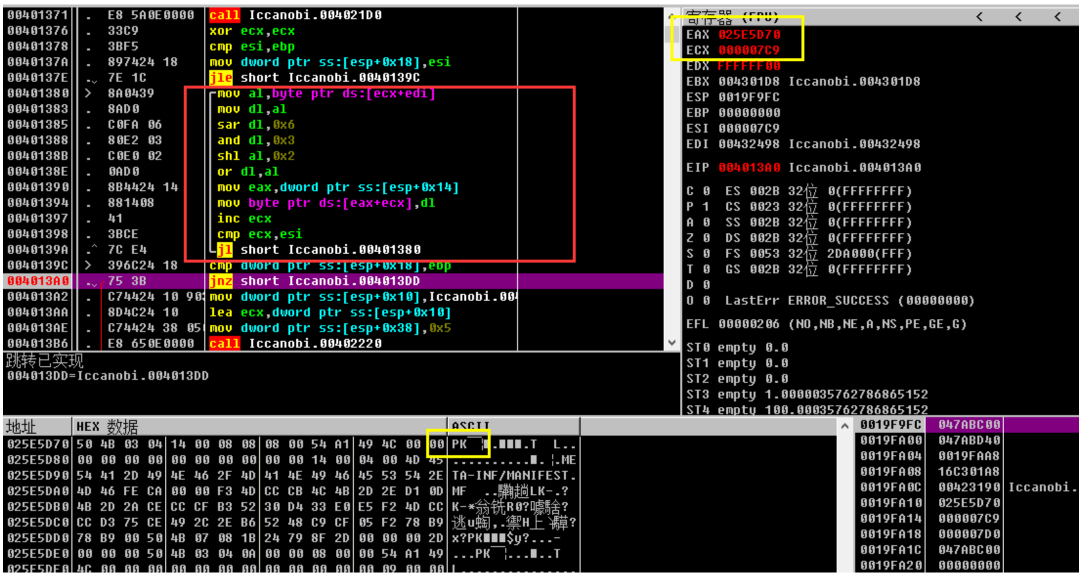
第2部分o_l: md5
第3部分l_l: 'orz'

flag:

```
hgame{Fuck1ng11_C0d5_orz}
```

0x02 Iccanobif

上一题是py2exe，这题是jar2exe。字符串中很多java字样。
还是工具题，这次我们下手搞。
先获取RCDATA的VA，在OD中下硬件访问断点，F9来到Decode循环。



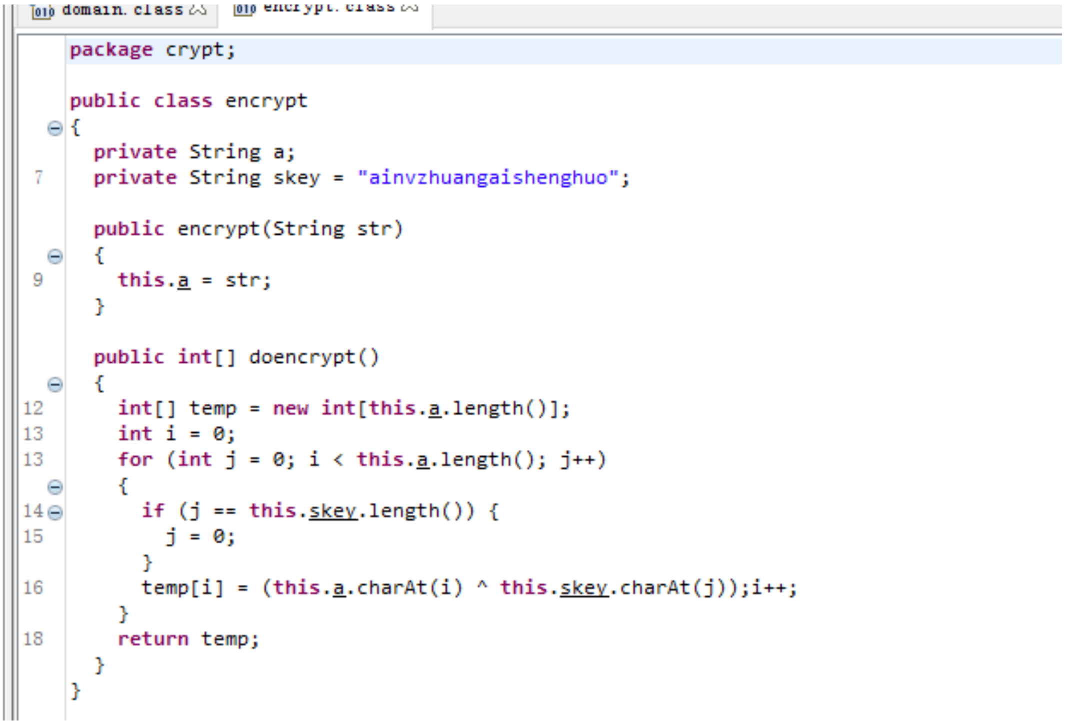
```
00401371  .  E8 5A0E0000   call Iccanobi.004021D0
00401376  .  33C9          xor ecx,ecx
00401378  .  3BF5          cmp esi,ebp
0040137A  .  897424 18     mov dword ptr ss:[esp+0x18],esi
0040137E  .~ 7E 1C         jle short Iccanobi.0040139C
00401380  >  8A0439        mov al,byte ptr ds:[ecx+edi]
00401383  .  8AD0          mov dl,al
00401385  .  C0FA 06       sar dl,0x6
00401388  .  80E2 03       and dl,0x3
0040138B  .  C0E0 02       shl al,0x2
0040138E  .  0AD0          or dl,al
00401390  .  8B4424 14     mov eax,dword ptr ss:[esp+0x14]
00401394  .  881408        mov byte ptr ds:[eax+ecx],dl
00401397  .  41            inc ecx
00401398  .  3BCE          cmp ecx,esi
0040139A  .^ 7C E4         jl short Iccanobi.00401380
0040139C  >  396C24 18     cmp dword ptr ss:[esp+0x18],ebp
004013A0  .~ 75 3B         jnz short Iccanobi.004013DD
004013A2  .  C74424 10 90: mov dword ptr ss:[esp+0x10],Iccanobi.00
004013AA  .  8D4C24 10     lea ecx,dword ptr ss:[esp+0x10]
004013AE  .  C74424 38 05( mov dword ptr ss:[esp+0x38],0x5
004013B6  .  E8 650E0000   call Iccanobi.00402220
跳转已实现
004013DD=Iccanobi.004013DD
```

```
寄存器 (FPU)
EAX 025E5D70
ECX 000007C9
EDX FFFFFF00
EBX 004301D8 Iccanobi.004301D8
ESP 0019F9FC
EBP 00000000
ESI 000007C9
EDI 00432498 Iccanobi.00432498

EIP 004013A0 Iccanobi.004013A0

C 0  ES 002B 32位 0(FFFFFFFF)
P 1  CS 0023 32位 0(FFFFFFFF)
A 0  SS 002B 32位 0(FFFFFFFF)
Z 0  DS 002B 32位 0(FFFFFFFF)
S 0  FS 0053 32位 2DA000(FFF)
T 0  GS 002B 32位 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000206 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 1.0000035762786865152
ST4 empty 100.00035762786865152
```

```
地址      HEX 数据                                         ASCII
025E5D70  50 4B 03 04 14 00 08 08 08 00 54 A1 49 4C 00 00  PK  .■■■.T   L..
025E5D80  00 00 00 00 00 00 00 00 00 00 14 00 04 00 4D 45  ..........■. ¦.ME
025E5D90  54 41 2D 49 4E 46 2F 4D 41 4E 49 46 45 53 54 2E  TA-INF/MANIFEST.
025E5DA0  4D 46 FE CA 00 00 F3 4D CC CB 4C 4B 2D 2E D1 0D  MF   ..黼趟LK-.?
025E5DB0  4B 2D 2A CE CC CF B3 52 30 D4 33 E0 E5 F2 4D CC  K-*翁铳R0?噱骀?
025E5DC0  CC D3 75 CE 49 2C 2E B6 52 48 C9 CF 05 F2 78 B9  逃u蚼,.霁H上 孅?
025E5DD0  78 B9 00 50 4B 07 08 1B 24 79 8F 2D 00 00 00 2D  x?PK■■■$y?...-
025E5DE0  00 00 00 50 4B 03 04 0A 00 00 08 00 00 54 A1 49  ...PK ¦...■..T
025E5DF0  4C 00 00 00 00 00 00 00 00 00 00 00 00 09 00 00  L...............
```

```
0019F9FC  047ABC00
0019FA00  047ABD40
0019FA04  0019FAA8
0019FA08  16C301A8
0019FA0C  00423190  Iccanobi.
0019FA10  025E5D70
0019FA14  000007C9
0019FA18  000007D0
0019FA1C  047ABC00
0019FA20  00000000
```

eax为Decode地址，
ecx为Decode大小。
用hex编辑工具把这部分挖出来，保存为jar文件，可以拿到class文件。
反编译，源码Get，里面只是个异或



```
package crypt;

public class encrypt
{
  private String a;
  private String skey = "ainvzhuangaishenghuo";

  public encrypt(String str)
  {
    this.a = str;
  }

  public int[] doencrypt()
  {
    int[] temp = new int[this.a.length()];
    int i = 0;
    for (int j = 0; i < this.a.length(); j++)
    {
      if (j == this.skey.length()) {
        j = 0;
      }
      temp[i] = (this.a.charAt(i) ^ this.skey.charAt(j));i++;
    }
    return temp;
  }
}
```

flag:

```
hgame{nvzhuang_zhen_hao_wan}
```