第五届“强网杯”青少年专项wp

> 战队名称：听话让我康康flag
> 战队排名：第46名
> 答题情况：Misc-签到、Crypto-Crypto2、Reserve-Lihua's for

Crypto

Crypto2

> 答题人：全嘉政

1.下载附件后得到五个数据：

```
n1=20663949646446787716947370247427064802032290773674573417491154934657966734874
24103630763356769517513101484061720805193175347622314965242713348516077106899407
35664316529692439622901168983453371897049748338173351353919744977546703224301596
24252007005736522065638860351992074099453212550475552692645688800084354832716662
14286041315836902000583009504998880793179473687656329391652532817481272651462602
91035066078131866909095858701153646009691484826170838172739100207223549232440936
24032174432568413187131385994452769295894606345768596899824635672699945050103814
68155398101991755266779451480435950010894710223437672600932 9
n2=23260834024376640092536888922041147168387702014814910549469730354688848760379
27420308871664960967544993623473252877855704170152498120036899631006458447965704
20984261643662866701153920158658538928169838855303120740733964223010095131062586
55315791720535737587913264728919869055970993613641008348186263870234072422880033
88286460343890707086427147048369172970542154714362330505553233910777731431097694
73928333951809223242432447840189647368262350183884985164386129621235629777369246
74510730898077787055367234786519915374446506561992135856904927351307275140543635
15277167041021123570228382278241297164609258464675810776606 1
c1=20522772249591436865905796103232542494211695376973377722875606678999899690405
48080923167134648982187805035438059199993596079588848366447395220729850419620383
05432084772291621776485866839578310166645692425387759287280096993001453558184172
33892295367828930893733774091897666206696635744262884229680137381841581000794056
15684281258305710347276448660802202863828816125642493652344497481572776462063417
41124746122389920611869376131718786359034557006368945705043761534826000576554806
54731180740098435209814585459376319844315388048636156465832997913885636776523217
18860404021673213710899744478715700766565271855301342434764 9
c2=18715009944766815149492560645051626329204114049927707292306481018724323433701
97025354149509024478737882656954988548049176405752682853142903337814342627224894
02564324239399778052467422878862818534846966254865225350427944032881993934329000
65504766428665320682811338887618389589263597065738414638013423594446322359052784
84261975505309402805024532563769867844463286009751008183207784261071604247369747
84162139158054817045378846111260699078126217508179012788033263047840571459167216
93930579344441283586458621033705530309835431139751025999089707480829034535026967
77944137906242625403831093086321518888866235713399790868873 6
e=65537
```

由题目提供的数据来看，应该是属于RSA的解密。其中，n为q*p乘积，c为密文，e为加密质数数值。观察后将其分为两组，其中e的值相同。n与c的值显然不同，分为两组后可求出n1与n2的最大公因数p。接下来通过Python脚本使用 `gmpy2` 和 `binascii` 库来解密：

```
import gmpy2
import binascii
p=gmpy2.gcd(n1,n2) # 求得最大公因数p
q=n1//p
phi=(p-1)*(q-1)
d=gmpy2.invert(e,phi)
m=gmpy2.powmod(c1,d,n1)
print(binascii.unhexlify(hex(m)[2:]))
```

可得前半段flag：`flag{afb1e6f2-9acb-efde-ad`

然后，分别将q,m改为：

```
q=n2//p
m=gmpy2.powmod(c2,d,n2)
```

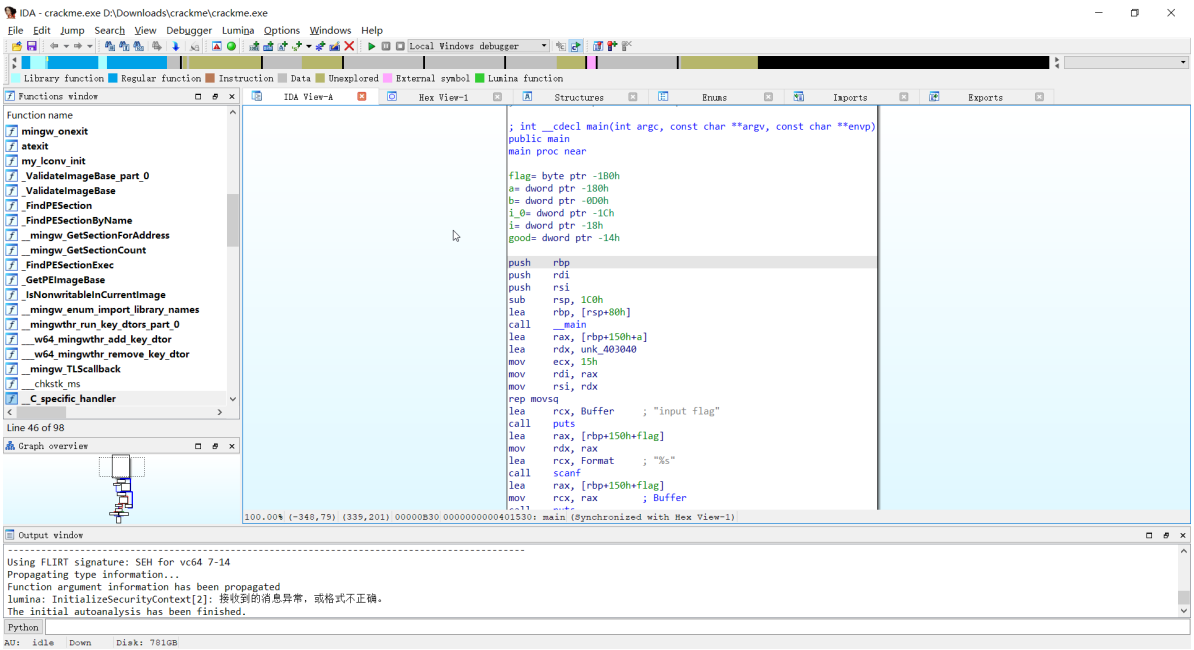
可得后半段flag:`7c-246a99d8f1fd}`
拼接之后，即可得到flag。

Reserve

Lihua's for

> 答题人：陈睿豪

在确定程序没有加壳之后，进IDA逆向，查看程序结构：



发现`main`函数中即使程序的核心代码：

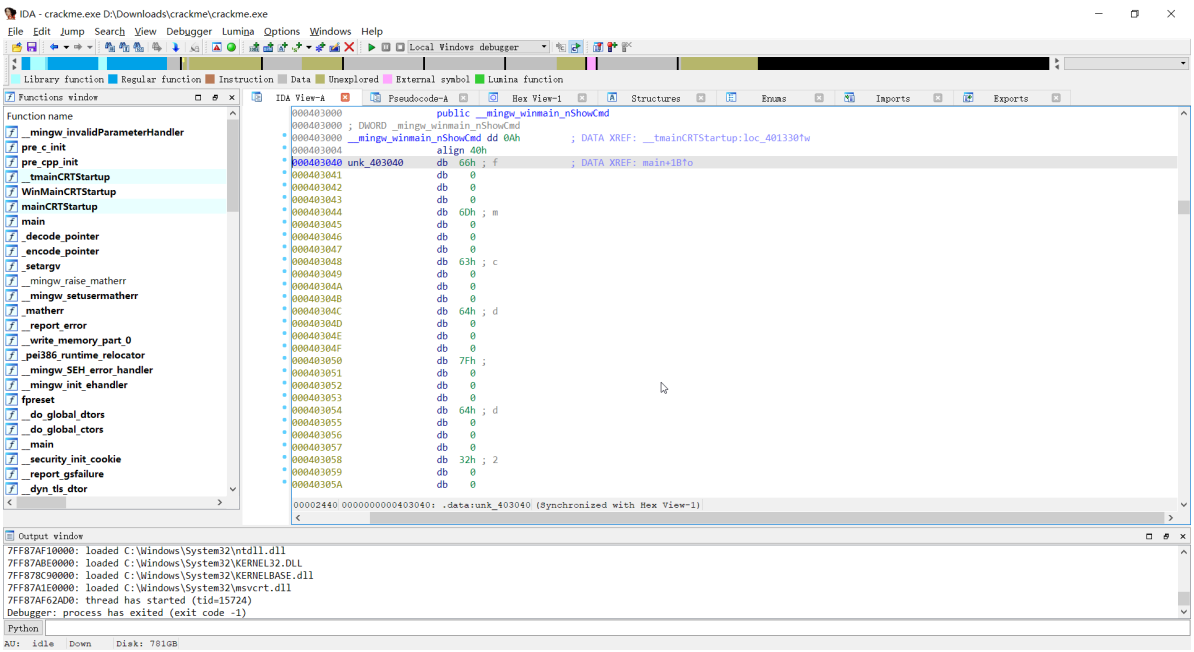
```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char flag[42]; // [rsp+20h] [rbp-60h] BYREF
  int a[42]; // [rsp+50h] [rbp-30h] BYREF
  int b[42]; // [rsp+100h] [rbp+80h]
  int i_0; // [rsp+1B4h] [rbp+134h]
  int i; // [rsp+1B8h] [rbp+138h]
  int good; // [rsp+1BCh] [rbp+13Ch]
```

```
  _main();
  qmemcpy(a, &unk_403040, sizeof(a));
  puts("input flag");
  scanf("%s", flag);
  puts(flag);
  for ( i = 0; i <= 41; ++i )
    b[i] = i ^ flag[i];
  for ( i_0 = 0; i_0 <= 41; ++i_0 )
  {
    if ( a[i_0] != b[i_0] )
    {
      good = 0;
      break;
    }
    good = 1;
  }
  if ( good == 1 )
    printf("good~");
  else
    printf("error!");
  return 0;
}
```

根据伪代码判断，输入的数据会依位与循环次数进行异或，之后与`a`字符串进行比较，那么只需字符串`a`的值与循环次数再进行异或，便可以得到flag。并且由语句：

```
qmemcpy(a, &unk_403040, sizeof(a));
```

便可以定位到`&unk_403040`就是`a`数据的来源



在提取`&unk_403040`的HEX数据之后，使用脚本处理：

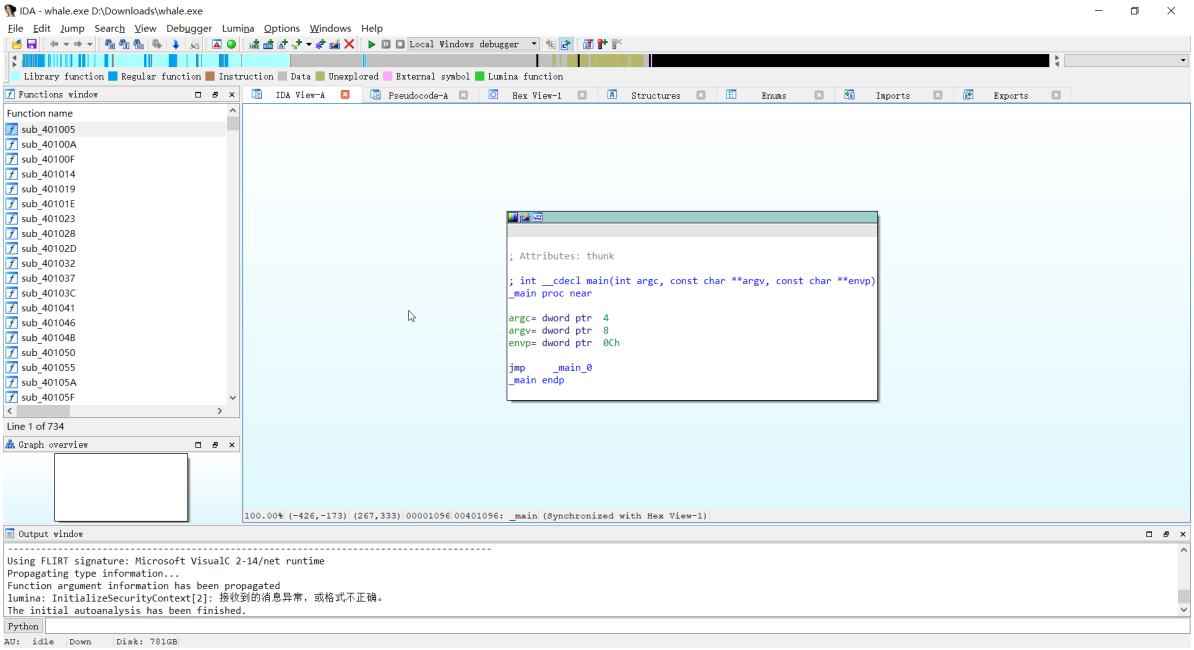
```
import math
s1=
[0x66,0x6D,0x63,0x64,0x7F,0x64,0x32,0x36,0x6A,0x6C,0x3E,0x3D,0x39,0x20,0x6F,0x3A
,0x20,0x77,0x3F,0x27,0x25,0x27,0x22,0x3A,0x7A,0x2E,0x78,0x7A,0x31,0x2F,0x29,0x29
,0x16,0x40,0x44,0x45,0x12,0x47,0x47,0x41,0x1A,0x54]
print(len(s1))
i:int=0
while i<=41:
    print(chr(i^s1[i]),end="")
    i+=1
```

Misc

签到

> 答题人：陈睿豪

附件下载后，拖进IDA逆向看一下程序结构：



Shift+F12看一下变量列表，即可发现flag：