Lab6 Reverse Engineering Challenge

一、 实验目的

1、熟悉静态反汇编工具 IDA Pro；

2、熟悉反汇编代码的逆向分析过程；

3、掌握反汇编语言中的数学计算、数据结构、条件判断、分支结构的识别和逆向分析

二、 实验原理

1. 通过 IDA Pro 可以得到二进制代码的反汇编代码，如图 1 和图 2 所示。

```
.text:00401000 ; ===========================================================================
.text:00401000
.text:00401000 ; Segment type: Pure code
.text:00401000 ; Segment permissions: Read/Execute
.text:00401000 _text           segment para public 'CODE' use32
.text:00401000                 assume cs:_text
.text:00401000                 ;org 401000h
.text:00401000                 assume es:nothing, ss:nothing, ds:_data, fs:nothing, gs:nothing
.text:00401000
.text:00401000 ; =============== S U B R O U T I N E =======================================
.text:00401000
.text:00401000
.text:00401000                 public start
.text:00401000 start           proc near
.text:00401000                 push    offset Format   ; "Please enter a challenge: "
.text:00401005                 call    ds:printf
.text:0040100B                 add     esp, 4
.text:0040100E                 push    offset Str
.text:00401013                 push    offset aS       ; "%s"
.text:00401018                 call    ds:scanf
.text:0040101E                 add     esp, 8
.text:00401021                 push    offset Str      ; Str
.text:00401026                 call    ds:strlen
.text:0040102C                 add     esp, 4
.text:0040102F                 cmp     eax, 6
.text:00401032                 jb      loc_40110D
.text:00401038                 push    offset aPleaseEnterThe ; "Please enter the solution: "
.text:0040103D                 call    ds:printf
.text:00401043                 add     esp, 4
.text:00401046                 push    offset dword_4030AD
.text:0040104B                 push    offset dword_4030A9
.text:00401050                 push    offset dword_4030A5
.text:00401055                 push    offset word_4030A1
.text:0040105A                 push    offset aUUUU    ; "%u-%u-%u-%u"
.text:0040105F                 call    ds:scanf
.text:00401065                 add     esp, 14h
.text:00401068                 cmp     eax, 4
.text:0040106B                 jb      loc_40111D
.text:00401071                 movzx   eax, byte_4030B2
.text:00401078                 movzx   ecx, byte_4030B4
.text:0040107F                 add     eax, ecx
.text:00401081                 movzx   ecx, byte_4030B5
.text:00401088                 add     eax, ecx
.text:0040108A                 cmp     eax, dword ptr word_4030A1
.text:00401090                 jnz     loc_40111D
00000400 00401000: start
```

图 1　challenge.exe 的反汇编代码

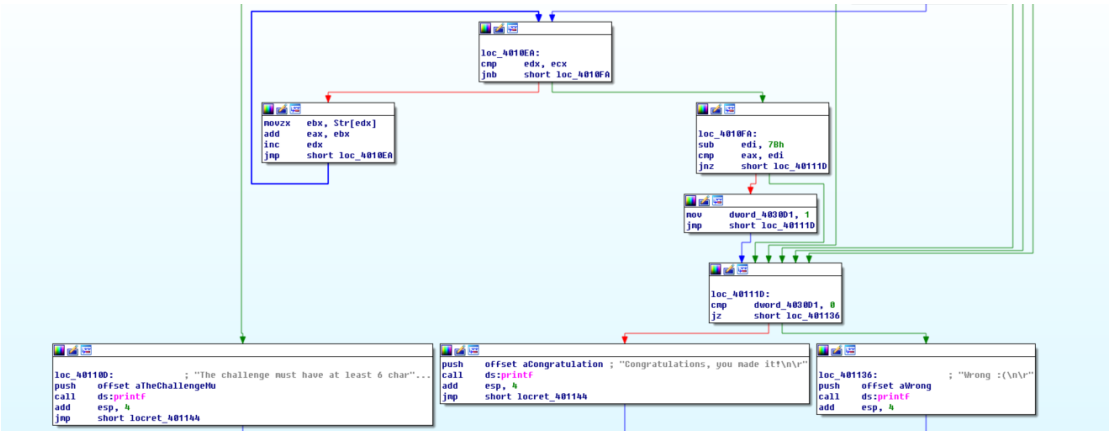

图 2 challenge.exe 的反汇编代码的图形化显示

2. 不修改二进制代码，分析汇编代码的计算过程、条件判断、分支结构等信息，逆向推理出程序的正确输入数据，完成逆向分析挑战。

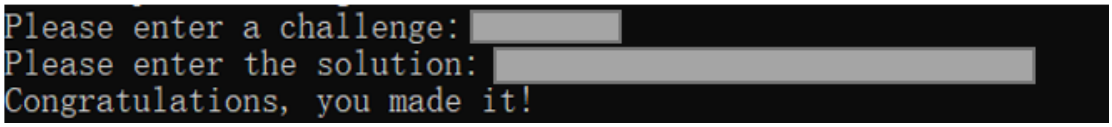

图 3 逆向分析，完成挑战

三、 实验报告

1. 使用 IDA Pro，获得二进制代码的反汇编代码，提供截图。
2. 逆向分析二进制代码的计算过程、数据结构、条件判断、分支结构等信息，在实验报告中记录逆向分析的详细过程。
3. 运行程序，根据提示输入字符串和逆向挑战的结果，获得“Congratulations，you made it！”输出，将成功的截图复制到实验报告中。