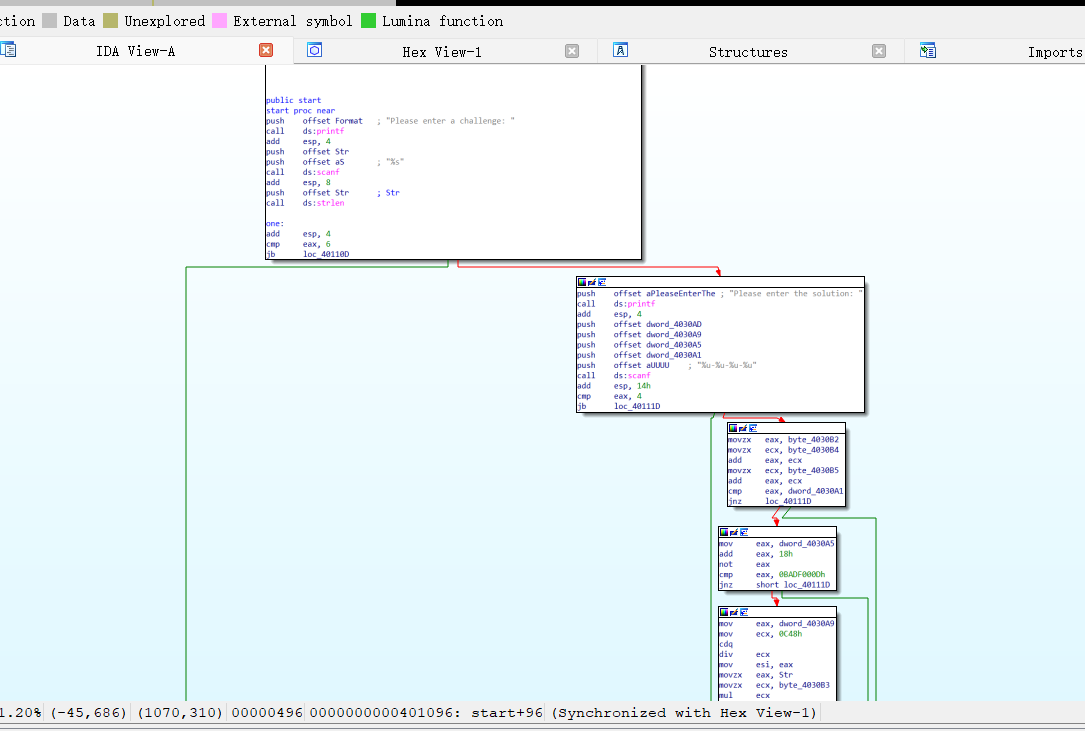
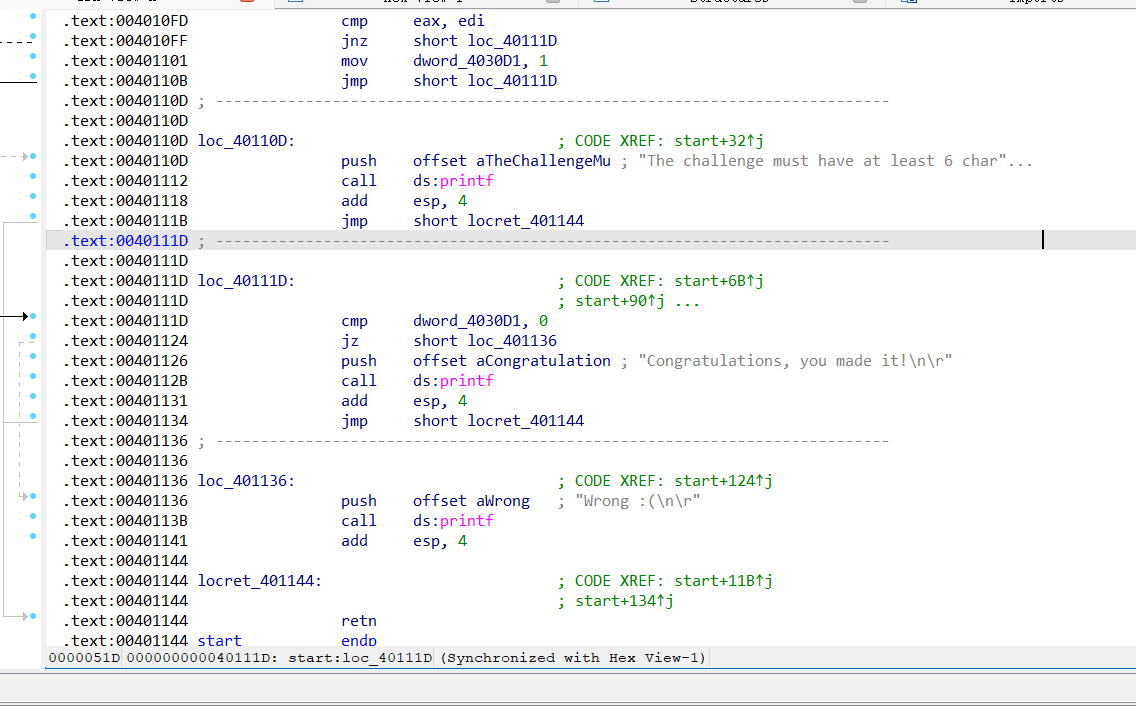
**Lab5 Reverse Engineering Challenge**

**学号：2113662 姓名：张丛**

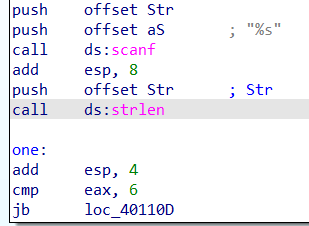
1. **实验目的**
   1. 熟悉静态反汇编工具IDA Freeware；
   2. 熟悉反汇编代码的逆向分析过程；
   3. 掌握反汇编语言中的数学计算、数据结构、条件判断、分支结构的识别和逆向分析
2. **实验步骤：**
3. 通过IDA可以得到二进制代码的反汇编代码。
4. 不修改二进制代码，分析汇编代码的计算过程、条件判断、分支结构等信息，逆向推理出程序的正确输入数据，完成逆向分析挑战。
5. **获取反汇编代码：**





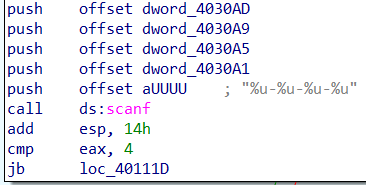
1. **逆向分析过程：**

（1）要求输入字符串长度不小于6



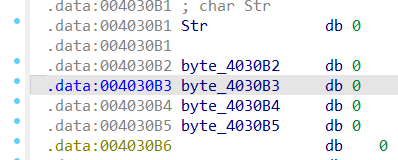
否则输出“The challenge must have at least 6 characters”后结束

（2）要求输入四个十进制无符号整数（%u）,以“-”隔开



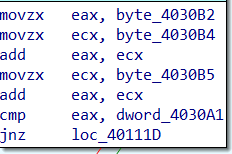
否则dword\_4030D1默认为0，跳转输出“Wrong”后结束

(3)



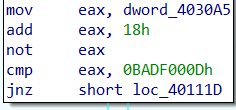
由上图知，B2、B3、B4、B5分别储存了Str字符串的第2、3、4、5位的ASCII值

（4）



dword\_4030A1应为输入challenge的2、4、5位的ASCII码值的和,否则输出“Wrong”后结束

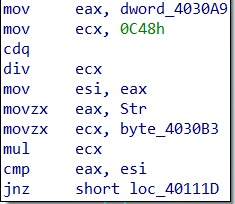
（5）



4030A5+18h后按位取反，应等于0BADF000h,否则“Wrong”;

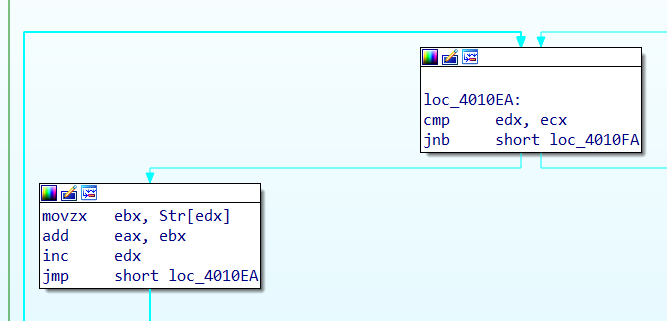
可以得出，4030A5的值为4520FFDAh=1159790554

(6)

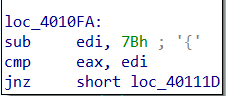


A9/0C48应等于Str字符1、3位ASCII的积，即A9=3144\*B1\*B3

（7）



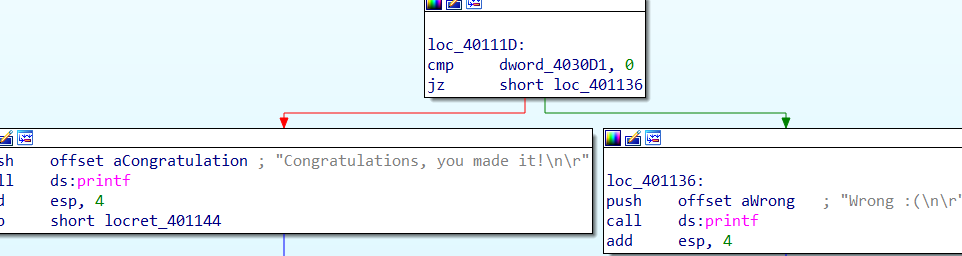
进行循环，循环结束后，eax储存Str每一位ASCII值的和；



4030AD xor 31337h 应等于 Str每一位ASCII值求和后再加7Bh，Xor为按位异或操作

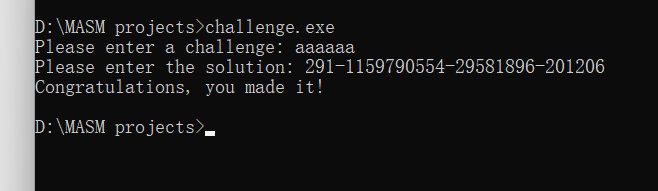
可得，4030AD = (ASCII值的和+7Bh) xor 31337h

（8）



4个值输入无误，则将4030D1的值赋1，跳转输出“Congratulations, you made it!”后结束，挑战完成

1. **结果截图：**



**291=97+97+97**

**29581896=97\*97\*3144**

**201206=（97\*6+123）xor 31337h**

1. **实验心得：**

**学习了逆向分析的相关知识，并且在反汇编语言中，复习或是新学到了一些代码，受益匪浅。**