**Lab6 RE Challenge #2**

**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、伪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；
   4. 运用熟悉的编程语言，实现简单的脚本编写。
2. **实验原理**

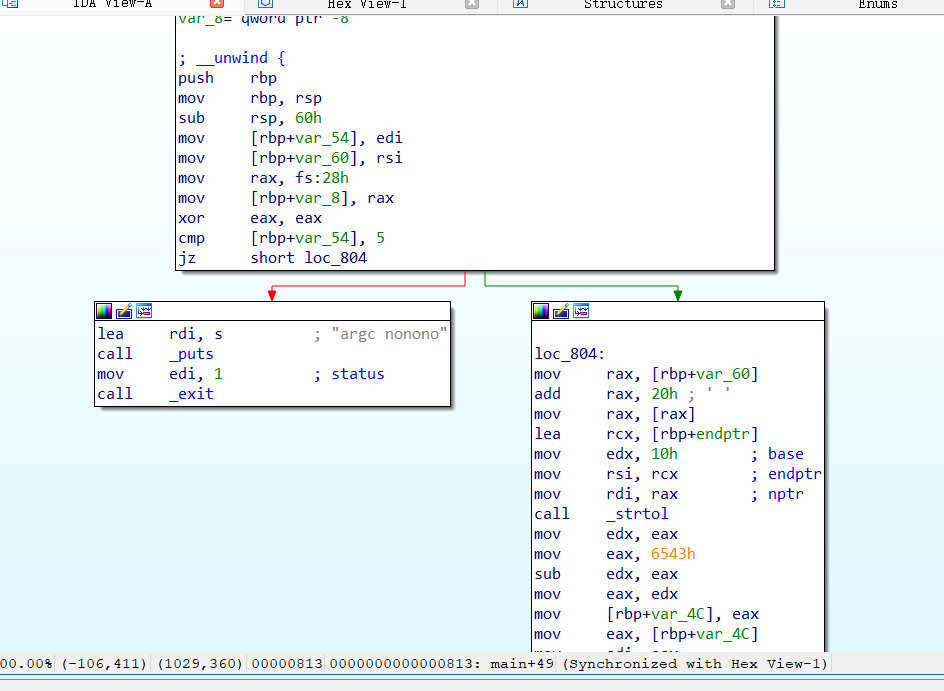
1.通过IDA Freeware得到ELF文件的反汇编代码

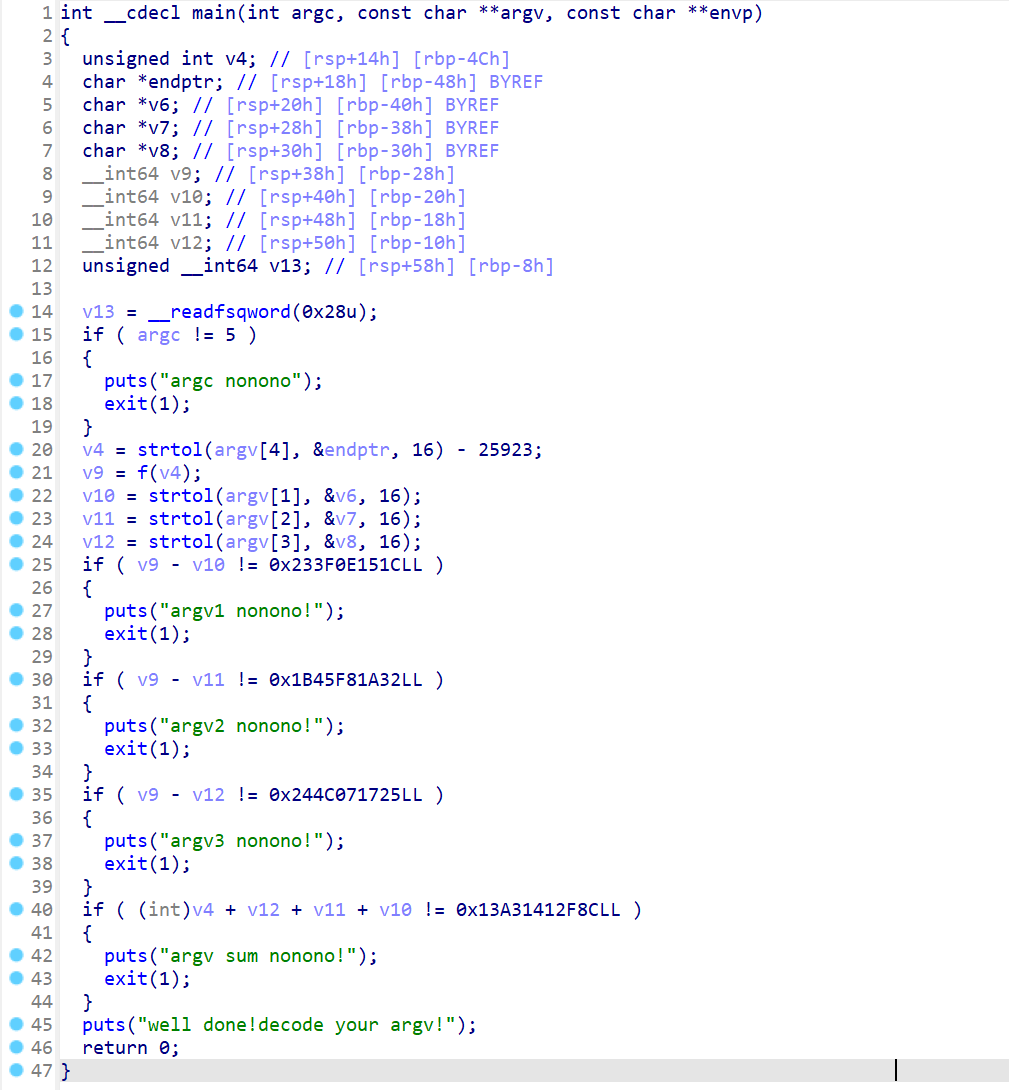
2.使用IDA的反编译功能（F5）得到伪代码

3.对汇编代码和反编译伪代码的计算过程、条件判断、分支结构等信息进行分析，逆向推出待解方程组。

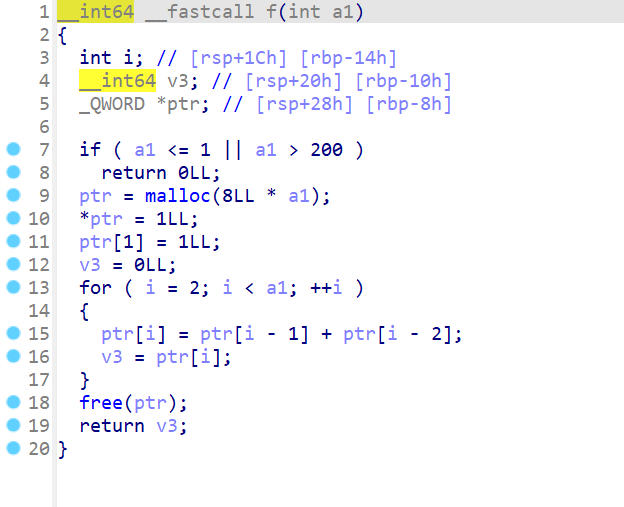
4.编写脚本实现暴力破解，解出方程组，得到参数“V9”、“V10”、“V11”、“V12”的正确取值，完成逆向分析挑战！

1. **获取反汇编代码**





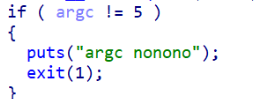
1. **逆向分析过程：**

****

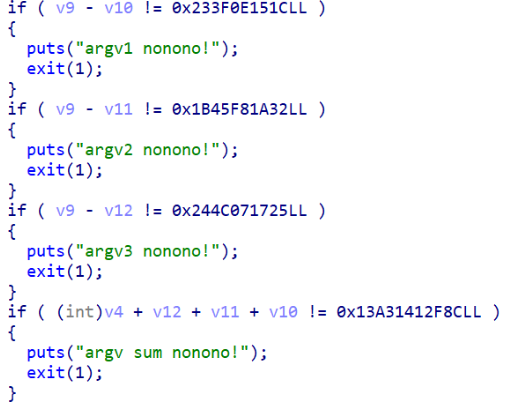
可知，f函数是生成斐波那契数

挑战成功需要经过5个判断：

分别是



故，argc=5



**可以得到一个关系式子：**

3\*v9+v4= 0x233F0E151C + 0x1B45F81A32 + 0x244C071725 + 0x13A31412F8C

其中：v9=f(v4)

且：

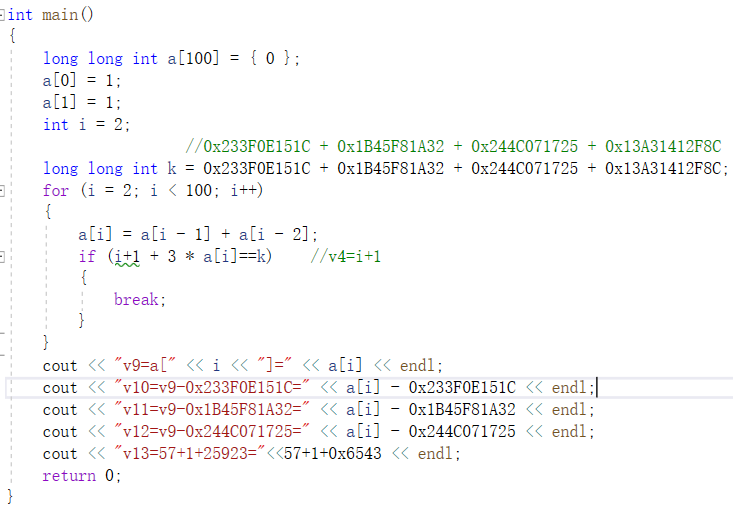
v10=v9-0x233F0E151C

v11=v9-0x1B45F81A32

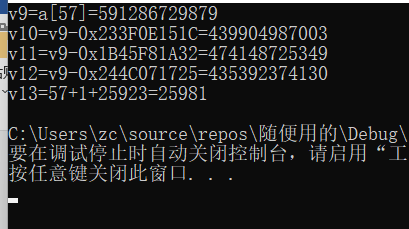
v12=v9-0x244C071725

1. **脚本暴力破解：**

用C++程序暴力求解：

* 

程序结果如下：



将其转为16进制：

Argv[1]=666C61677B

Argv[2]=6E65776265

Argv[3]=0x655F686572

Argv[4]=657D