

**汇编语言与逆向工程实验报告**

**实验九：Reverse Engineering Exercises – Advanced**

****

学 院 网络空间安全学院

专 业 信息安全

学 号 2212046

姓 名 王昱

班 级 信息安全班

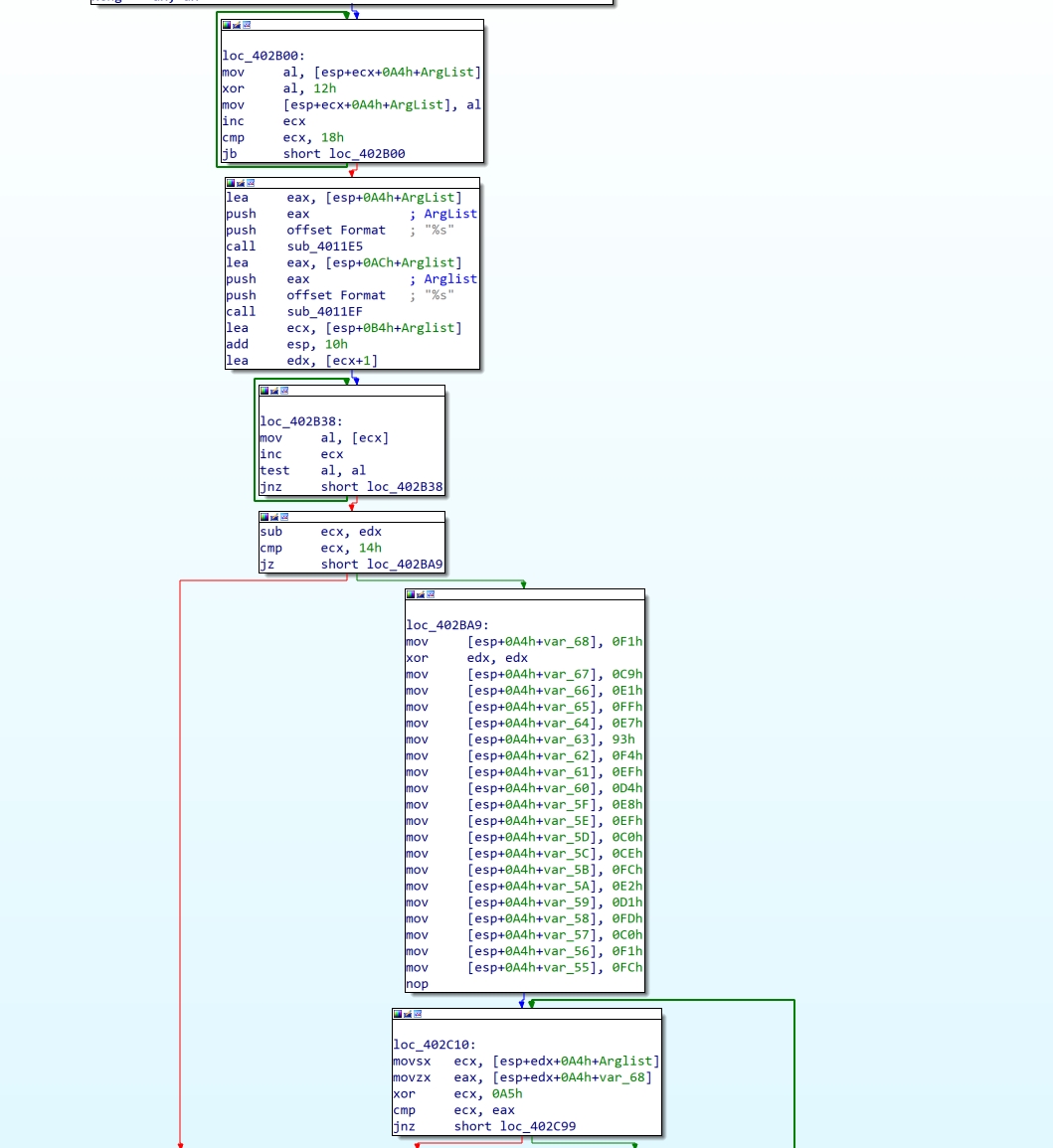
1. **实验目的**
   1. 进一步熟悉静态反汇编工具IDA Freeware；
   2. 熟悉将反汇编代码进行反编译的过程；
   3. 掌握对于反编译伪代码的逆向分析；
   4. 运用熟悉的编程语言，实现简单的脚本编写。
2. **实验工具**

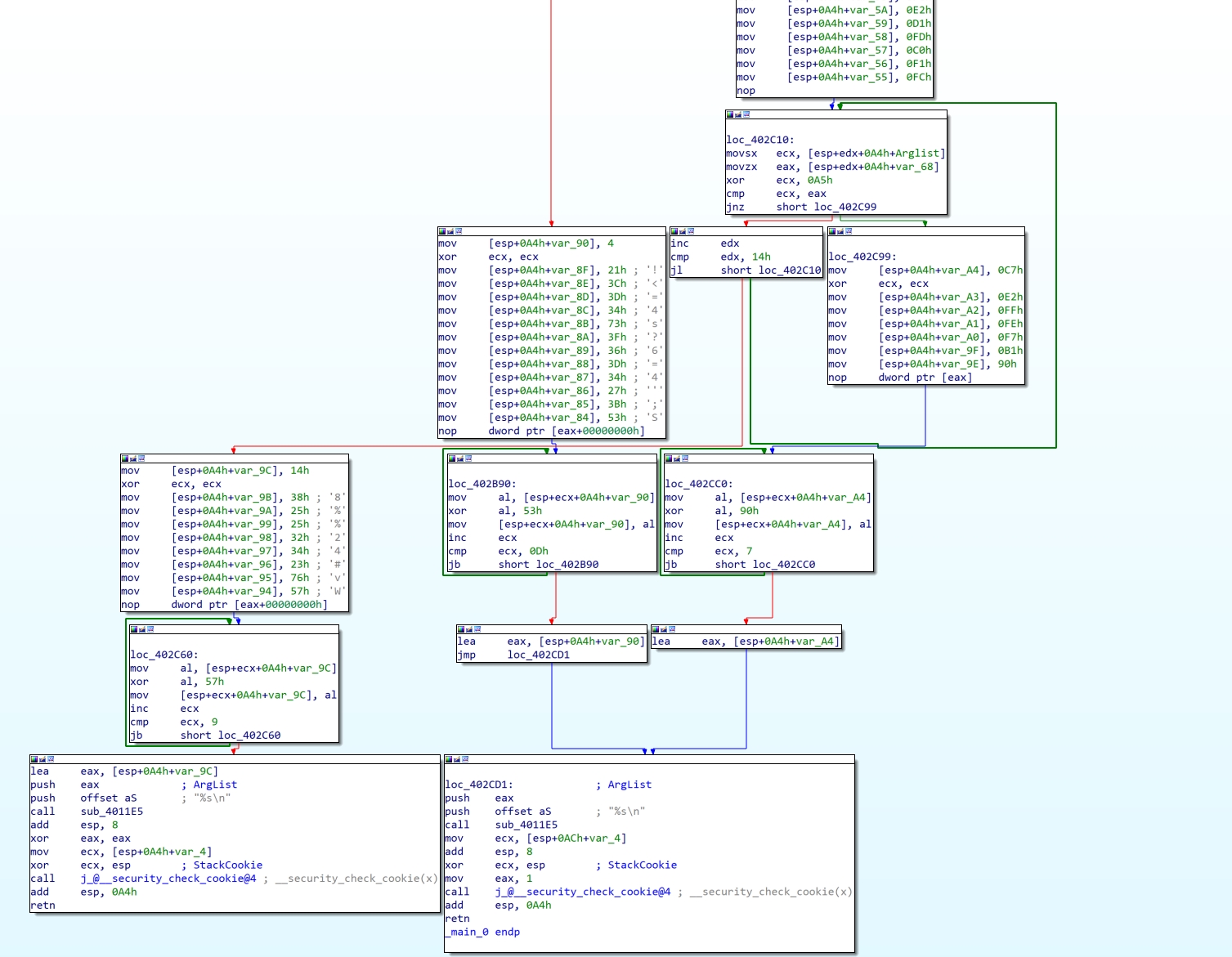
**IDA Freeware**

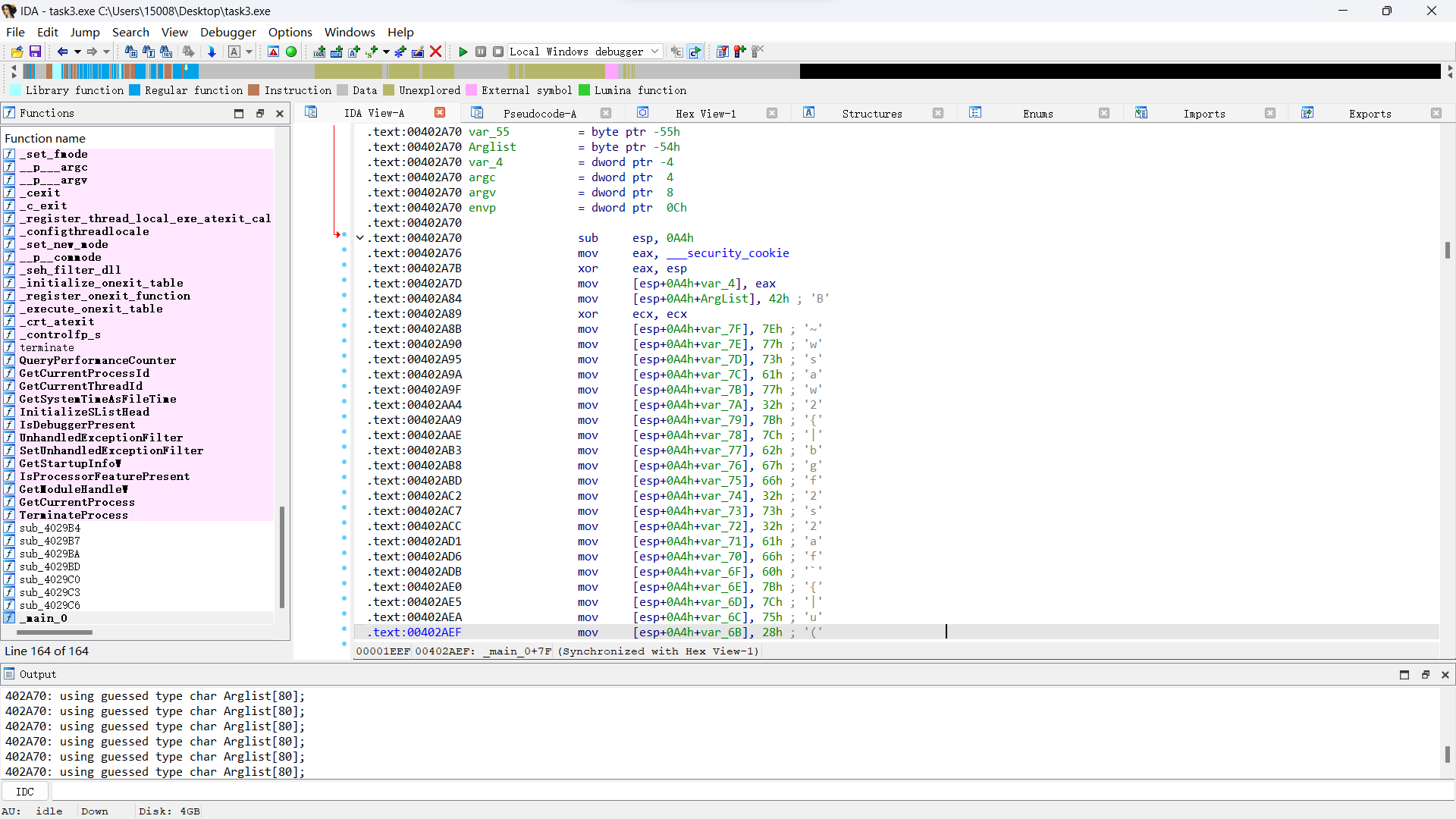
1. **实验过程**

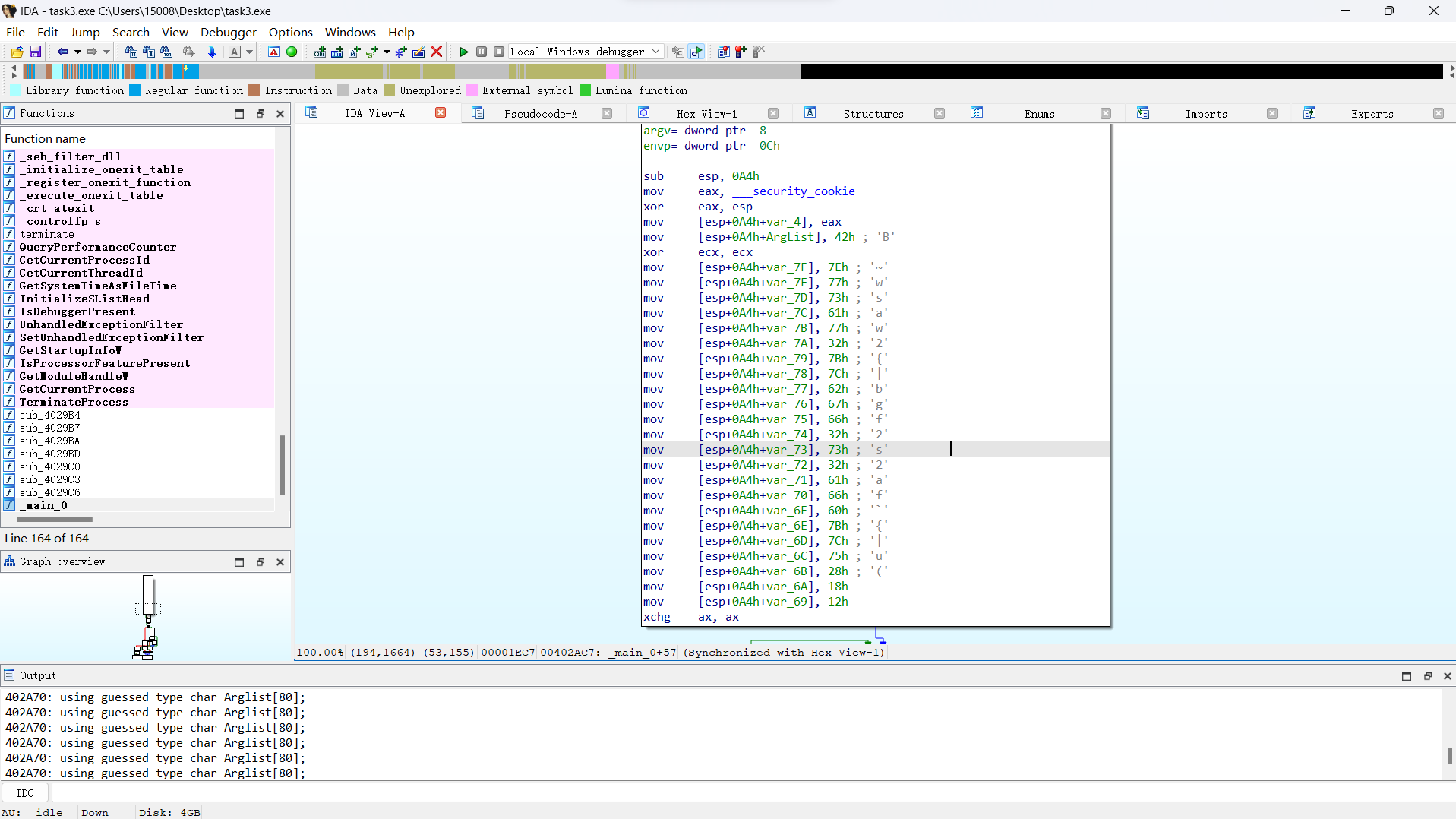
**（一）task3：**

**1.IDA Freeware得到task3.exe的反汇编代码**

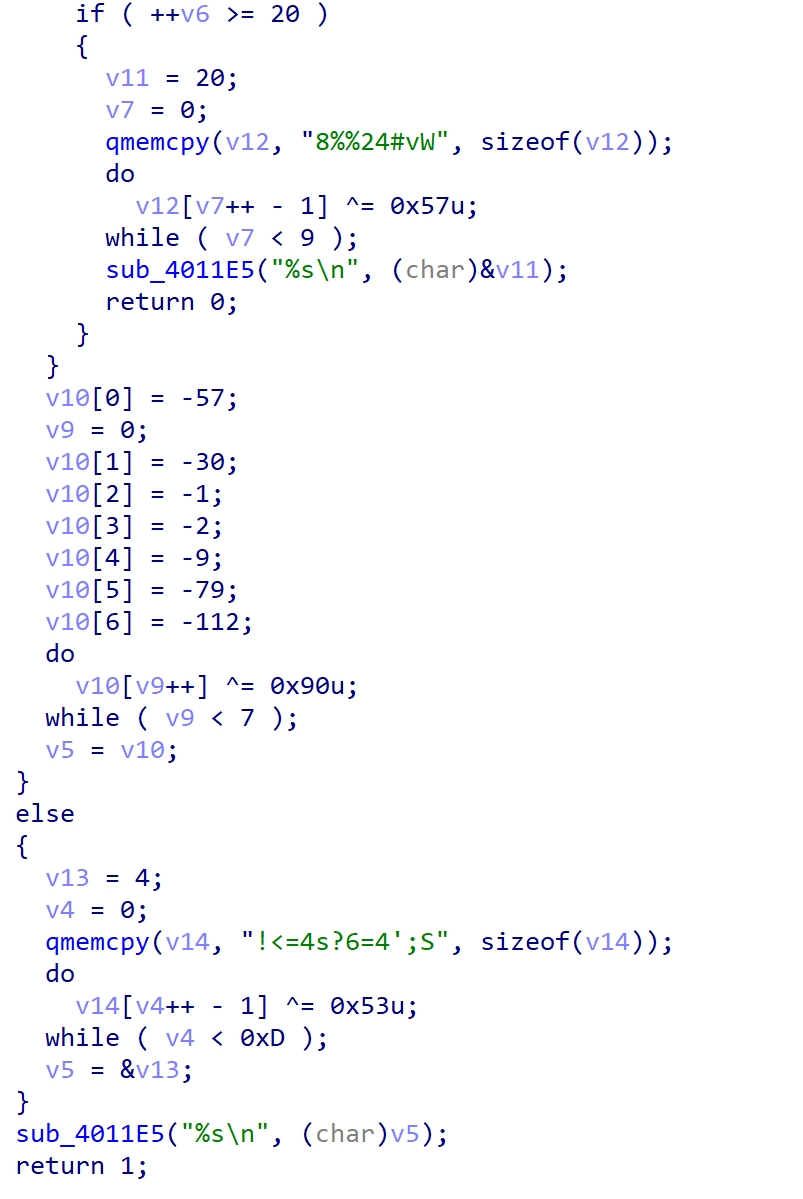
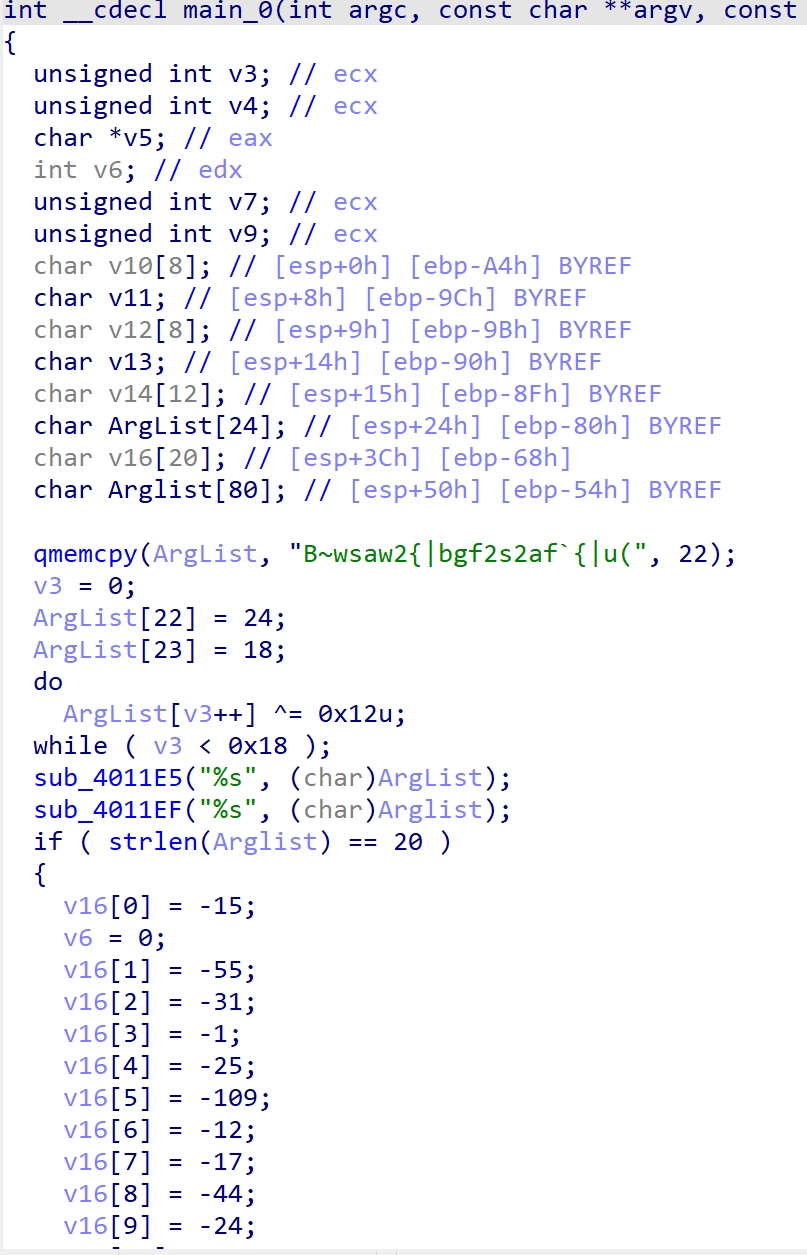
****

****

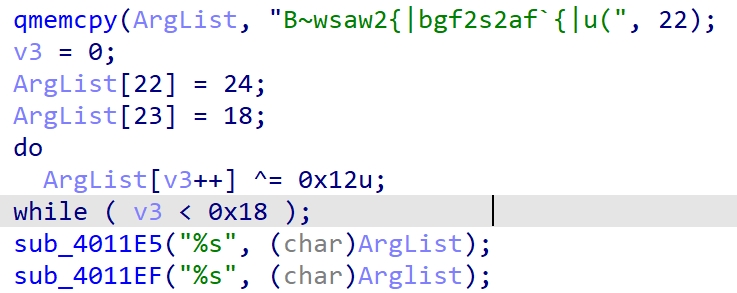
****



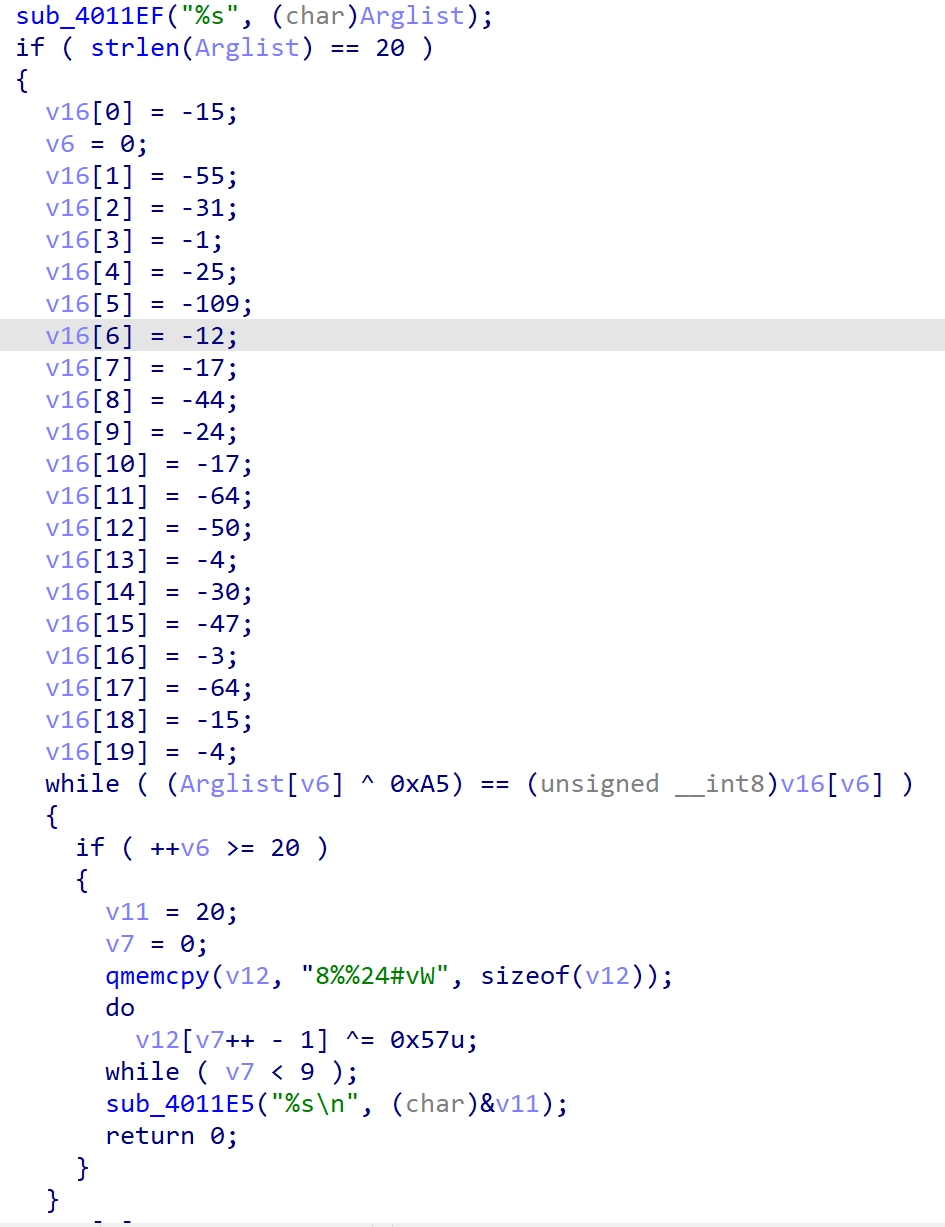
**2.使用IDA的反编译功能（F5快捷键）得到伪代码**

****

**3.正确字符串计算公式**

****

这段代码的目的是将"B~wsaw2{|bgf2s2af`{|u("这个字符串复制到ArgList中，并将其转换为"Please input a string:"这个字符串。qmemcpy是C标准库中的一个函数，用于将一个内存区域的内容拷贝到另一个内存区域。

****

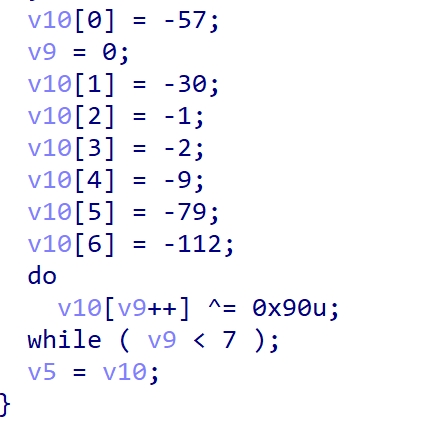
利用函数sub\_4011EF输入字符串，存入Arglist中。

首先判断输入字符串的长度是否为20，然后通过索引v6遍历Arglist中的元素，如果其中前20个元素均满足与0xA5异或后的值等于v16中对应的值，此时v16=19，++v16=20，进入if语句中。

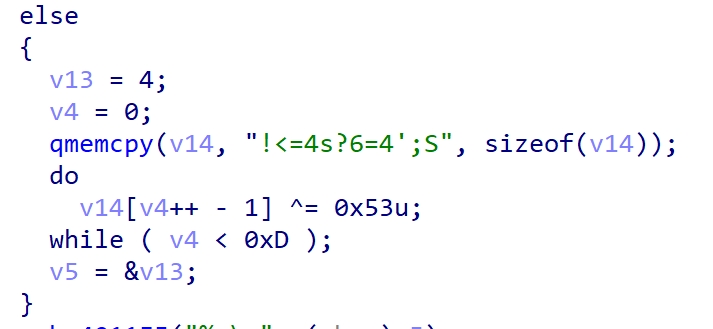
If语句中将8%%24#vW存入v12中，将其中每个元素与0x57异或，因为从v12[-1]开始，所以v7<9（保护v12中的最后一位0，不被异或）；最终输出从v11所在的地址开始输出，直到遇到v12字符串中的0（v11和v12地址相邻），输出结束。将输入的字符串中的每一位与0xA5进行异或后与常量数组中的对应位进行比较，如果每一位都相同的的话v6会大于20，就会输出“Correct!”字符

结果输出“correct!”。

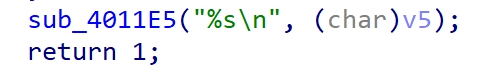
根据异或反推得出应输入的Arglist为“TlDZB6QJqMJekYGtXeTY”

****

若前19个元素有一个不满足与0xA5异或后的值等于v16中对应的值，那么将跳出while,进入到以上代码，利用v9作为索引，遍历v10中七个元素，使其每一个与0x90异或，将最终结果存入v5，用于后续输出。内容为“Wrong！”

****

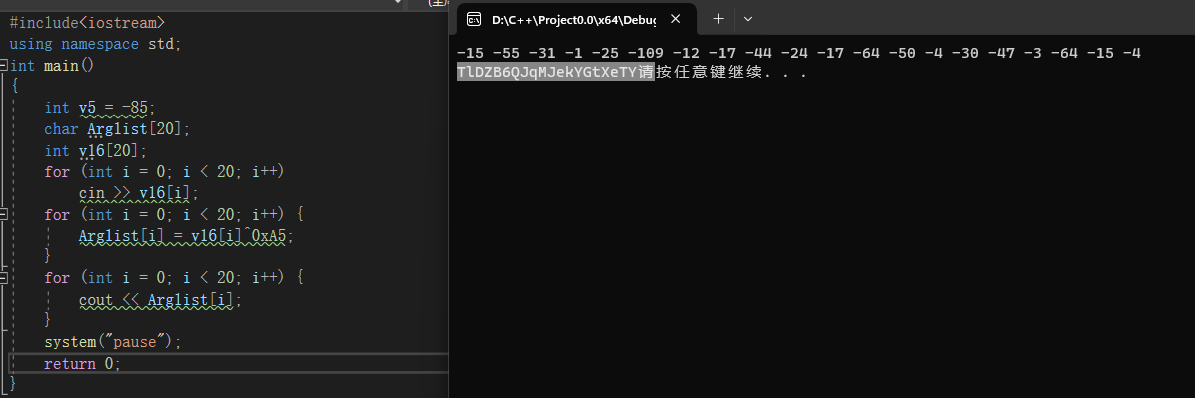
若字符串长度不是20，则进入else，将!<=4s?6=4';S存入v14，遍历v14中前12个元素，每一个元素与0x53异或（保护v14中的最后一位0，不被异或）**，**将13的地址存入v5，v5最终输出从v13所在的地址开始输出，直到遇到v14字符串中的0（v13和v14地址相邻）。结果输出“Wrong length”

****

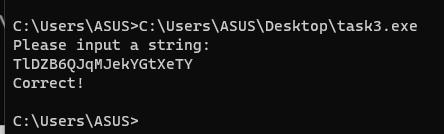
最终实现v5的输出“Wrong！”或者“Wrong length”

公式：Arglist[i]=v16[i]^0xA5

**4.脚本及脚本结果输出**

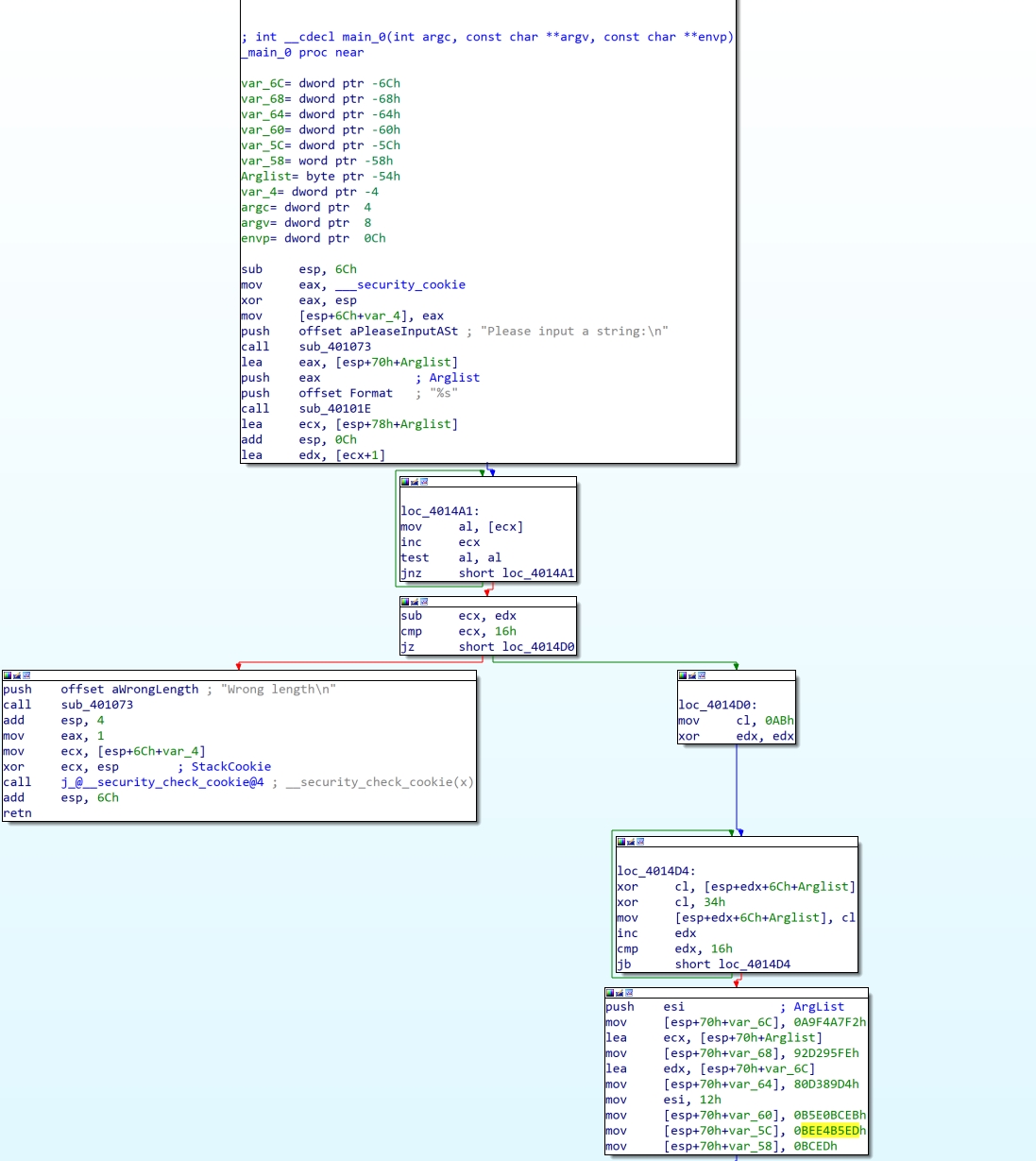
对每一个常数进行与0xA5的异或操作，得到最终正确的字符串输出

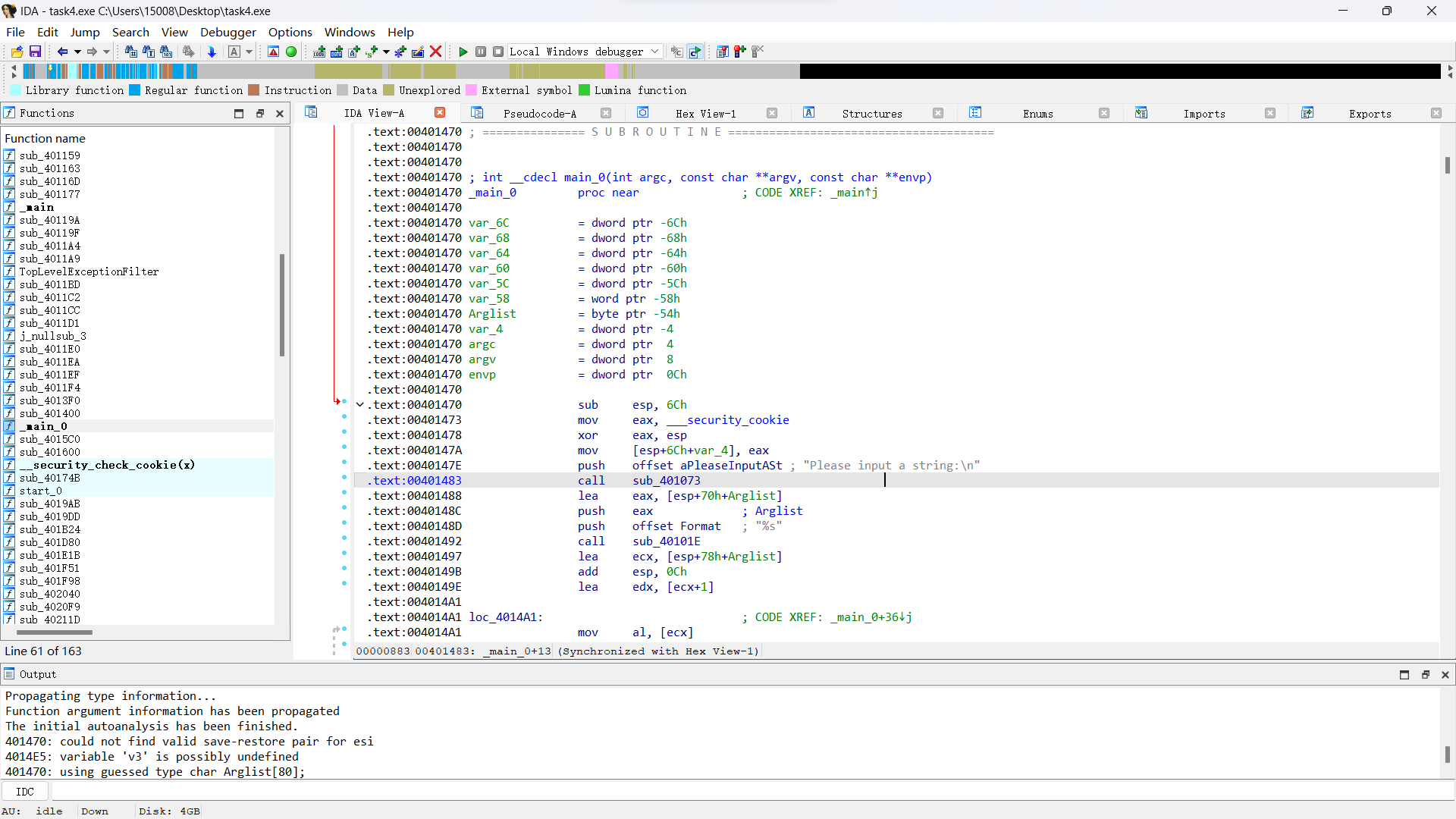
**5.运行结果**



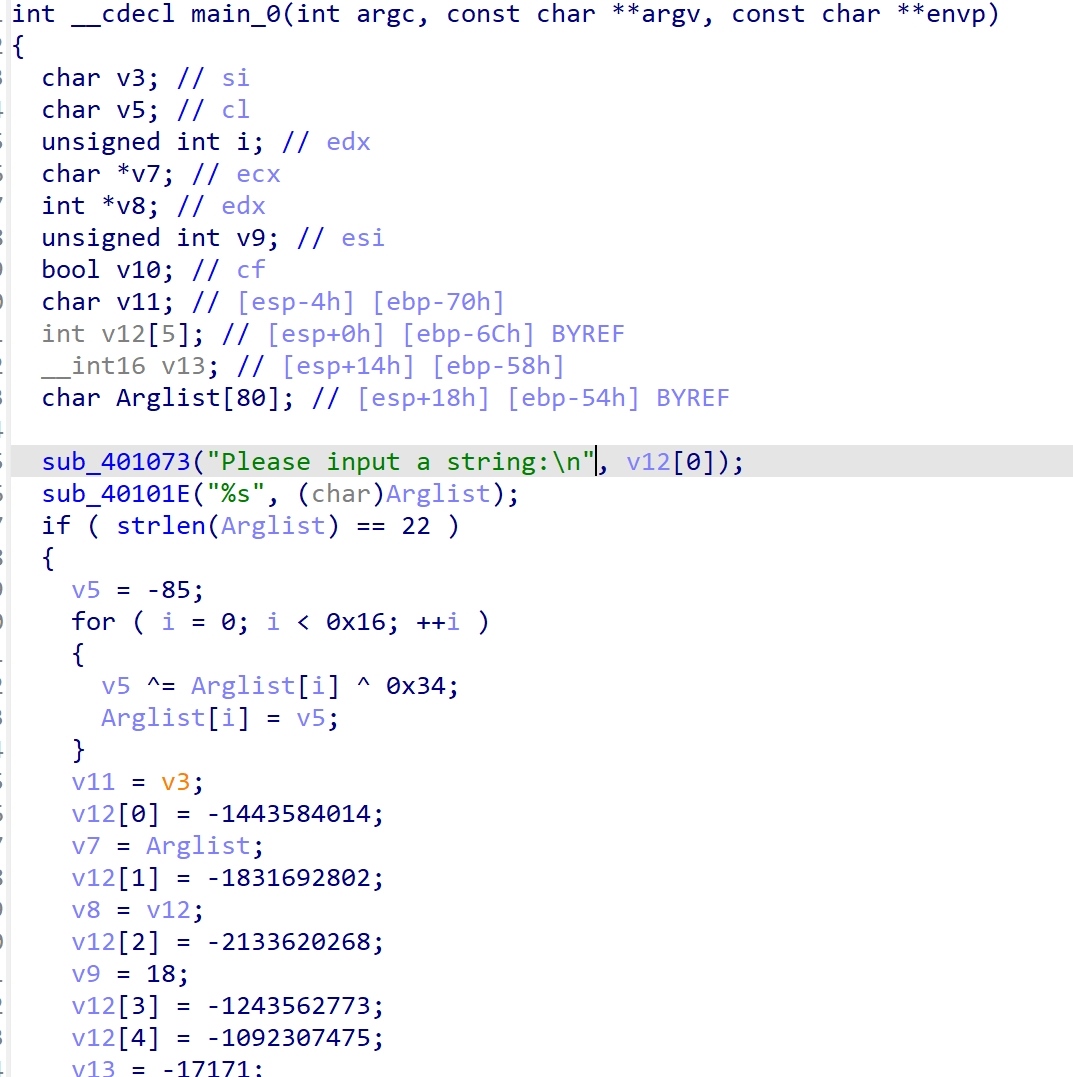
**（二）task4：**

1.IDA Freeware得到task3.exe的反汇编代码

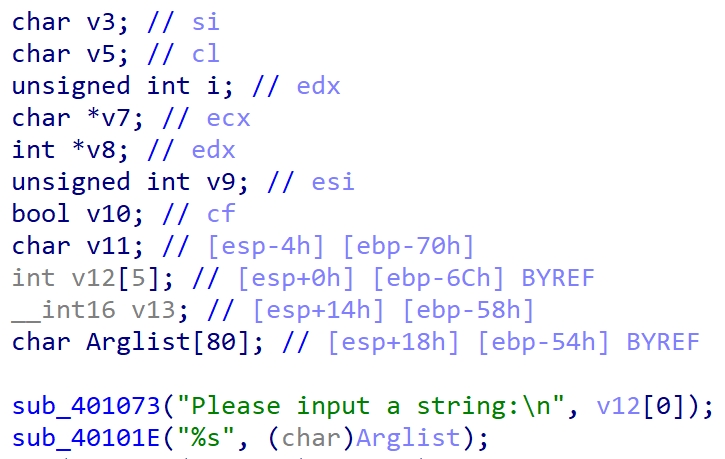
****

****

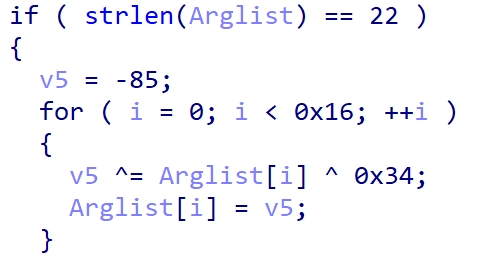
2.使用IDA的反编译功能（F5快捷键）得到伪代码

****

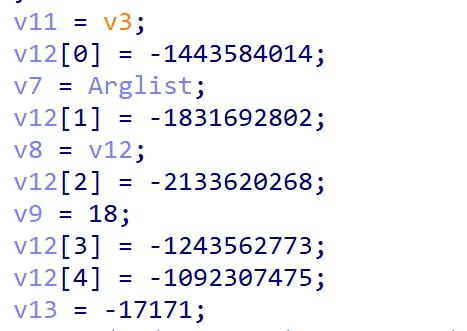
3.正确字符串计算公式

****

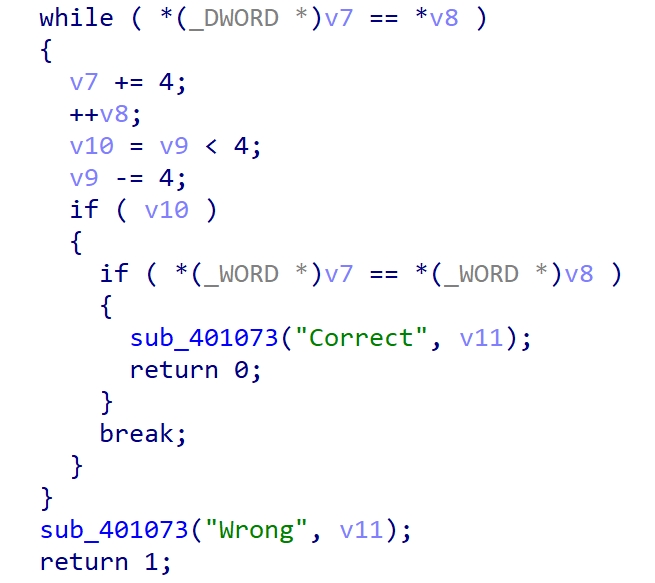
首先定义了一些后面要用到的常量

****

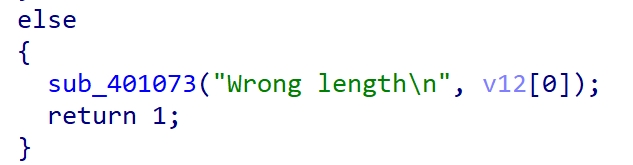
如果输入字符串的长度等于22，那么就进入if中，利用for循环将字符串的前22位与v5，0x34异或，结果存入v5中，再将v5的值存入字符串中对应的字符。

****

将字符串的值更新后，把v12的前五位分别赋值，将v7指向Arglist的地址，将v8指向v12的地址，将v9赋值18，作为后面循环终止的标志。

****

这段代码的目的是比较Arglist和v12的值是否相等，如果相等则进入循环，否则输出“Wrong”。Arglist是一个字节数组，v12是一个dword数组，它们的长度都是22个字节。

****

如果输入字符串的长度不是22，那么输出“Wrong length”。

经过以上逆向分析，能够输出“correct”的Arglist为“magic\_string\_challenge”

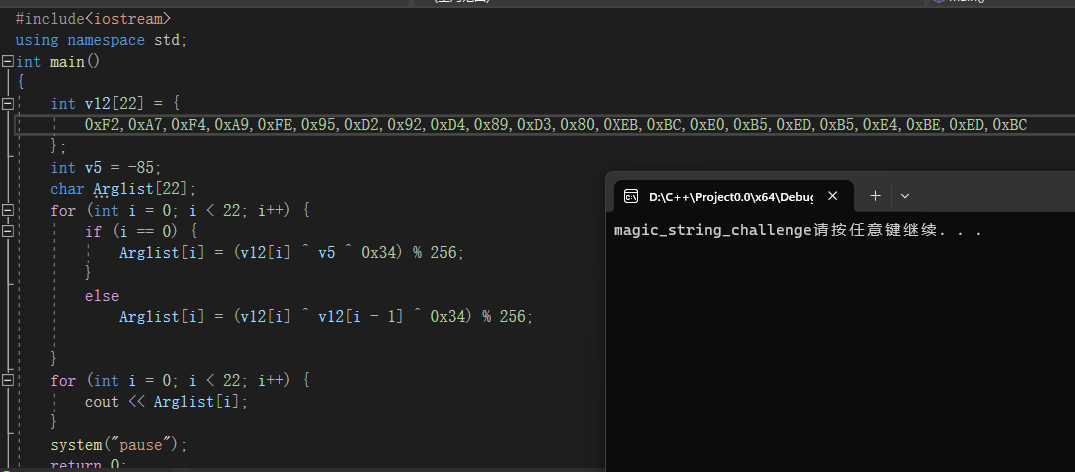
公式： y0=-85^x0^0x34

yi=yi-1^xi^0x34

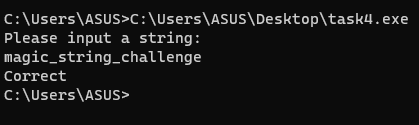
0≤i≤4, y4\*i+3 y4\*i+2 y4\*i+1 y4\*i=zi

y21y20=z5

4.脚本及脚本结果输出



**5.运行截图**



**以上就是本次实验全部内容。**