**Lab8 Reverse Engineering Exercises – Simple**

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. **实验原理**
3. **task1**
4. 通过IDA Freeware得到task1.exe的反汇编代码，如图1和图2所示。

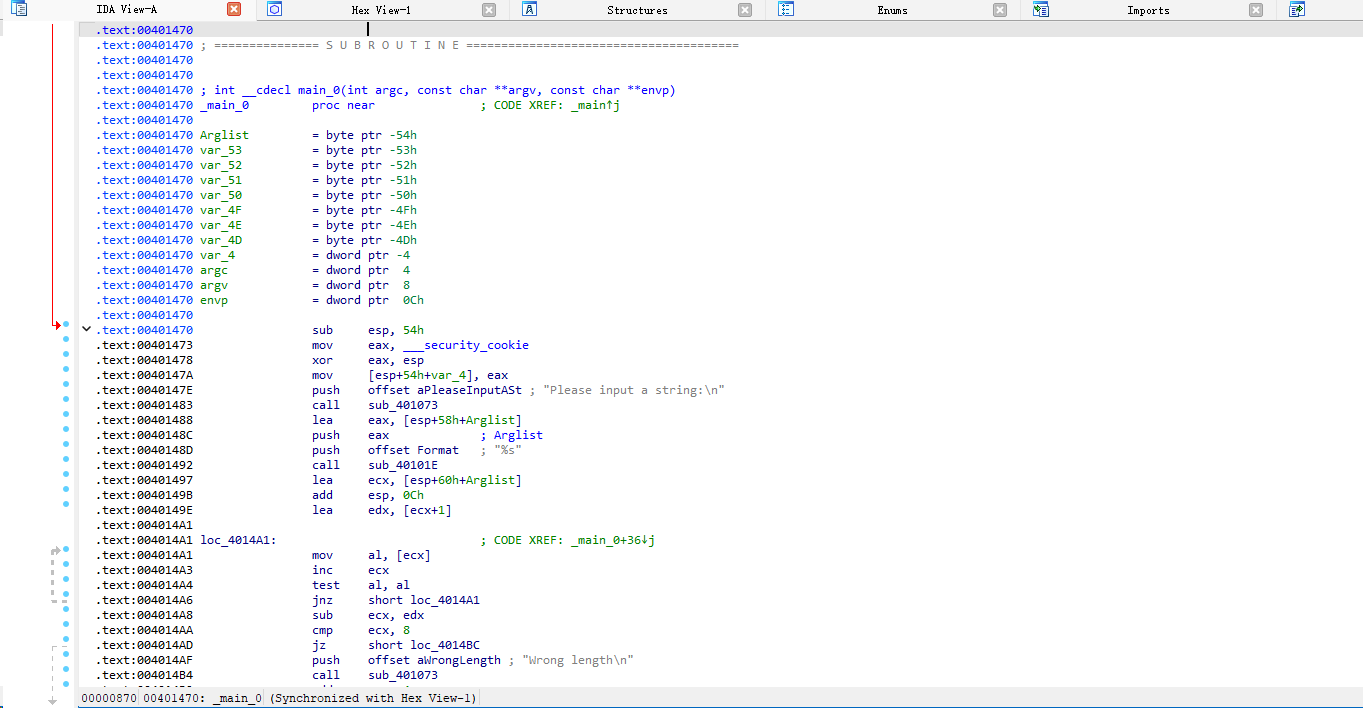


图 1 task1.exe的反汇编代码

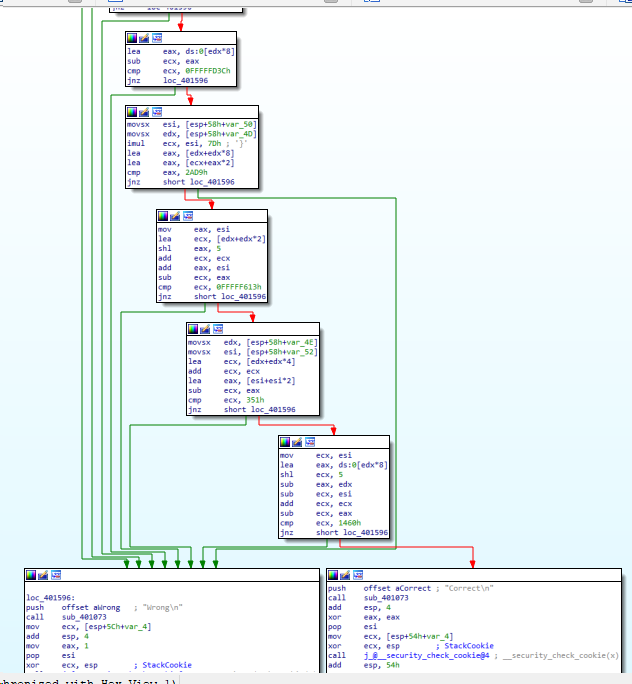


图 2 task1.exe反汇编代码的图形化显示

1. 对反汇编代码和计算过程、条件判断、分支结构等信息进行分析，逆向推出程序的正确输入数据，完成逆向分析挑战。

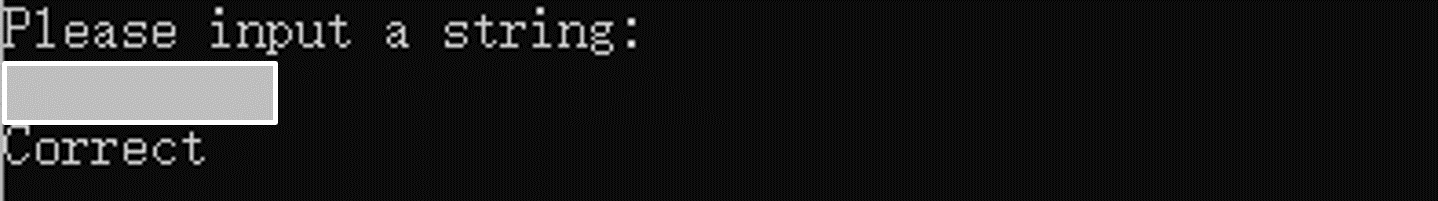


图 3 逆向分析，完成task1练习

1. **task2**
2. 通过IDA Freeware得到task2.exe的反汇编代码，如图4和图5所示。

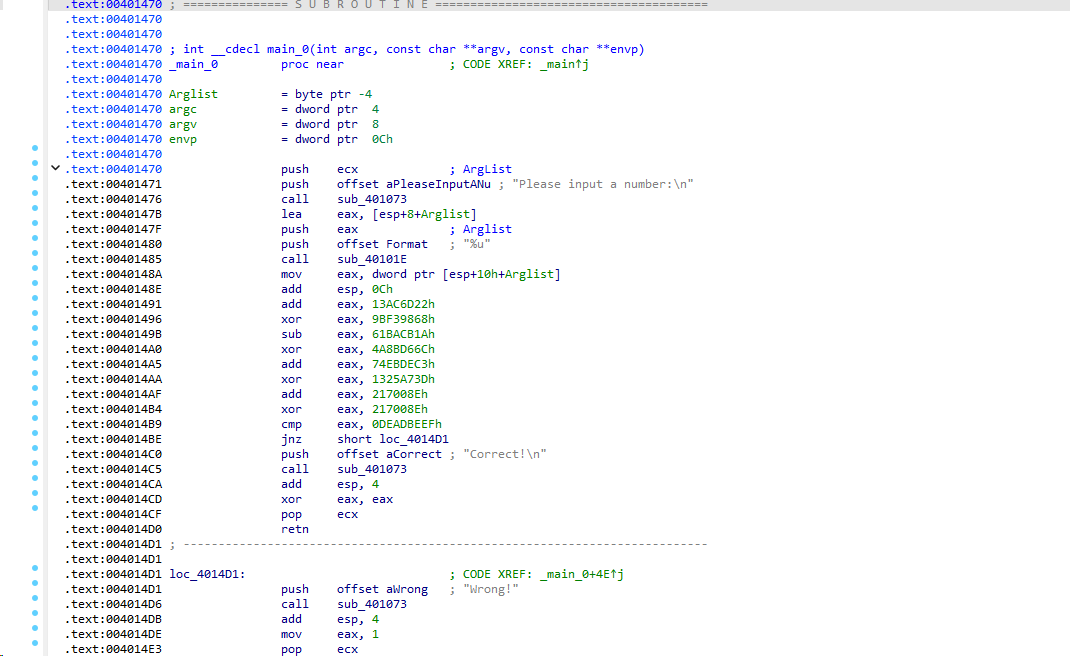


图4 task2.exe的反汇编代码

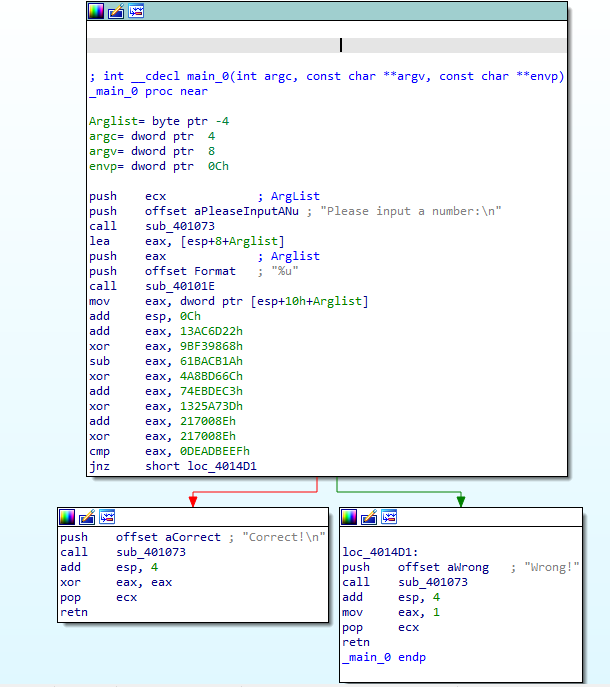


图 5 task2.exe反汇编代码的图形化显示

1. 对反汇编代码的计算过程、条件判断、分支结构等信息进行分析，逆向推出程序的正确输入数据，完成逆向分析挑战。

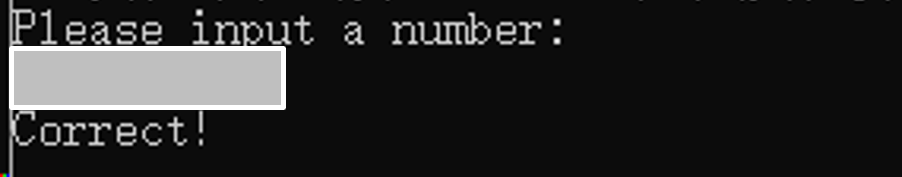


图 6 逆向分析，完成task2练习

1. **实验报告**
2. 分别针对task1、task2使用IDA Freeware，获得二进制代码的反汇编代码，提供截图。
3. 分别针对task1、task2反汇编代码的计算过程、数据结构、条件判断、分支结构等信息进行逆向分析，在实验报告中记录逆向分析的详细过程，并画出程序流程图。
4. 分别运行程序task1、task2，根据提示输入逆向挑战的结果，获得“Correct”输出，提供截图。