**Lab9 Reverse Engineering Exercises – Advanced**

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. **实验原理**
3. **task3**
4. 通过IDA Freeware得到task3.exe的反汇编代码，如图1和图2所示。

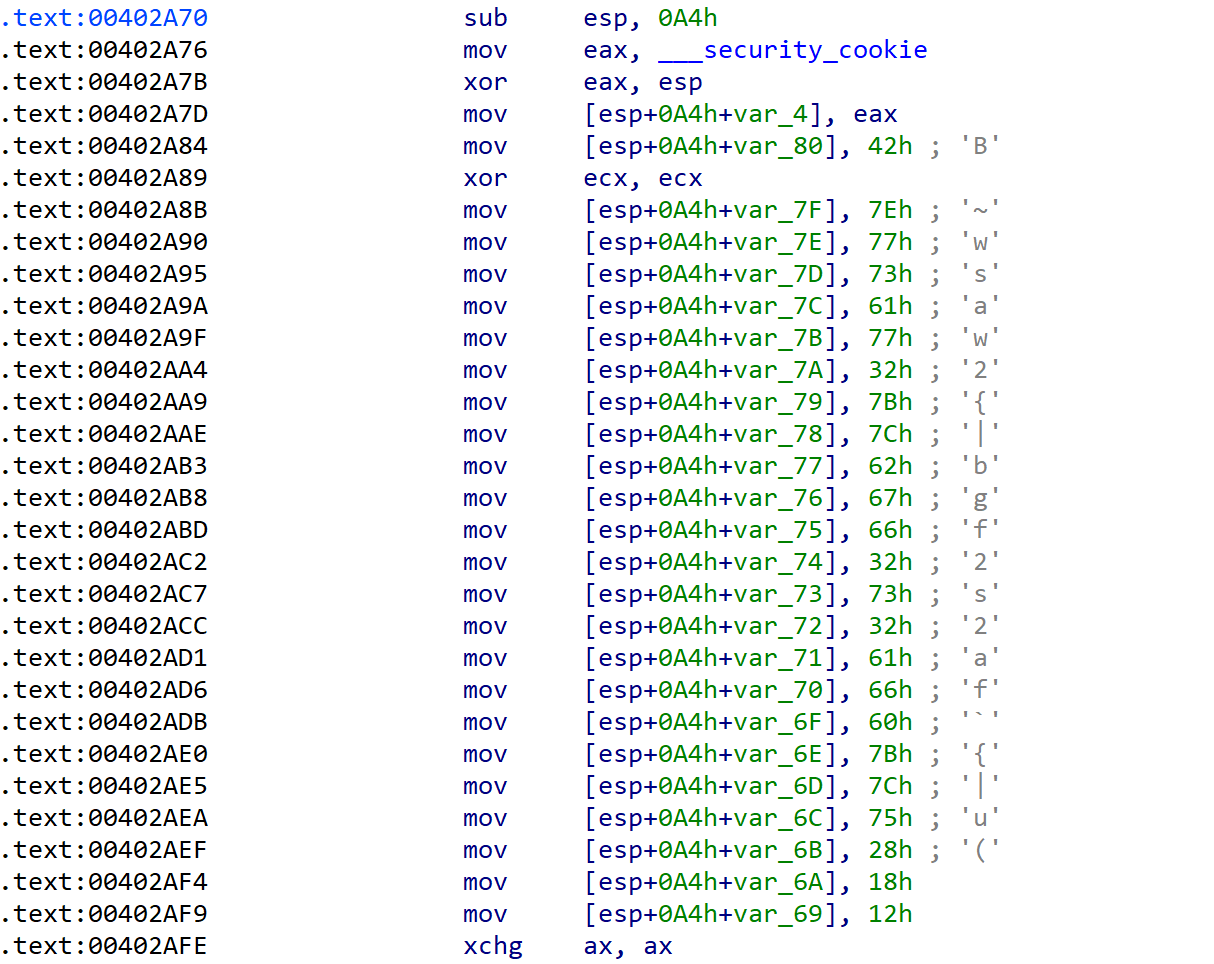


图1 task3.exe的反汇编代码

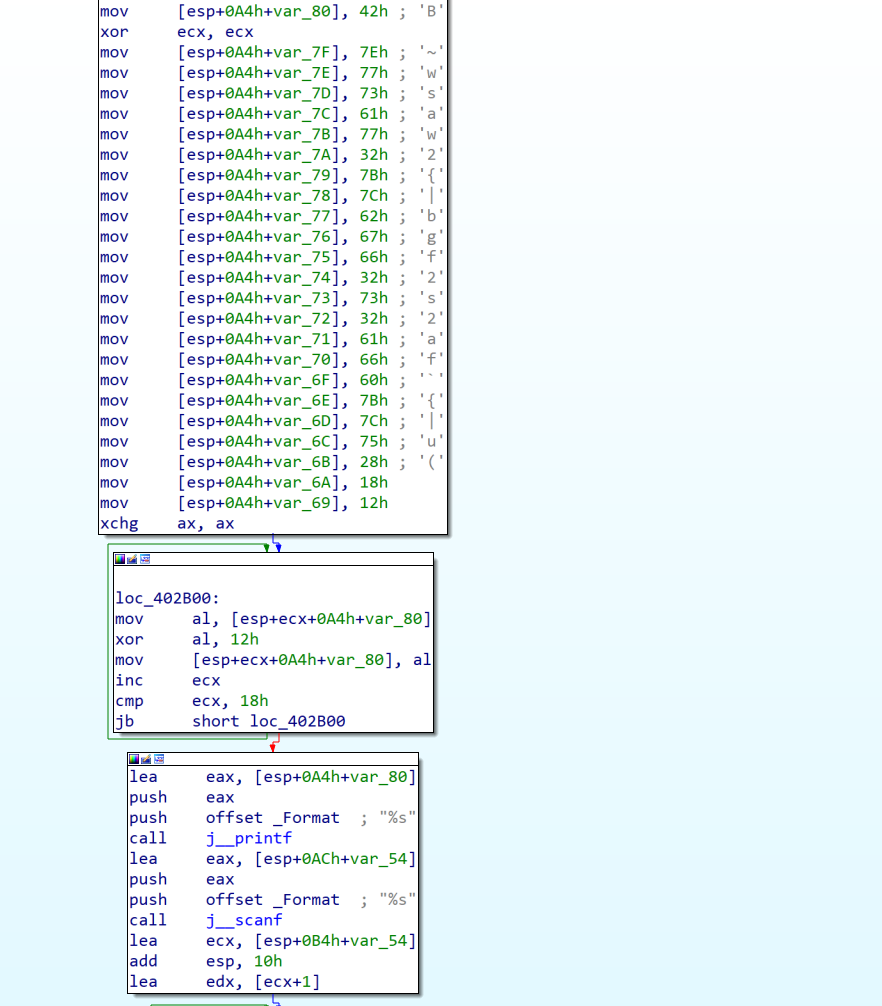


图 2 task3.exe反汇编代码的图形化显示

1. 使用IDA的反编译功能（F5快捷键）得到伪代码，如图3所示。

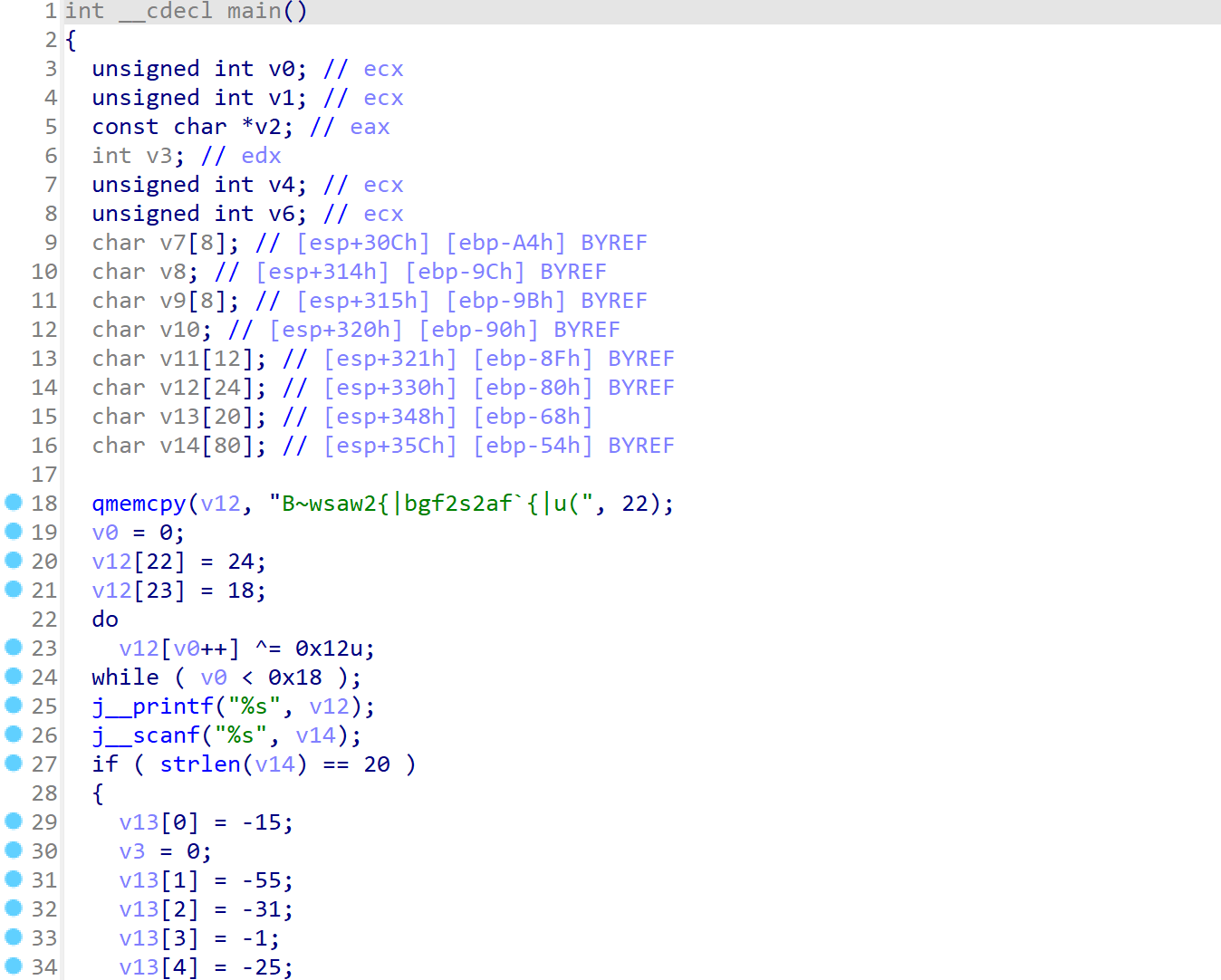


图 3 task3.exe的反编译伪代码

1. 通过对反汇编命令及反编译伪代码的分析，逆向推理出待输入字符串的计算公式
2. 使用熟悉的编程语言（C++、Java、Python等）对待输入字符串进行计算，完成逆向分析挑战。

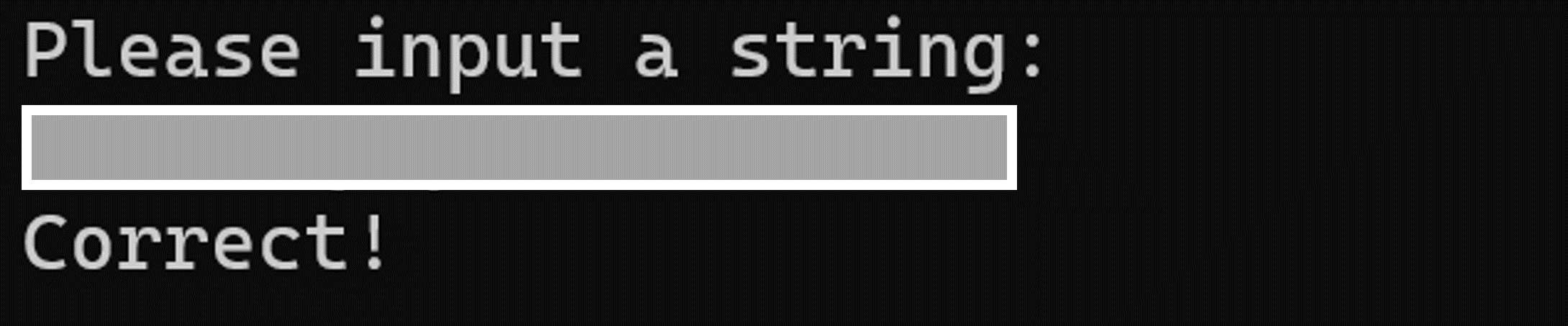


图 4 逆向分析，完成task3练习

1. **task4**
2. 通过IDA Freeware得到task4.exe的反汇编代码，如图5和图6所示。

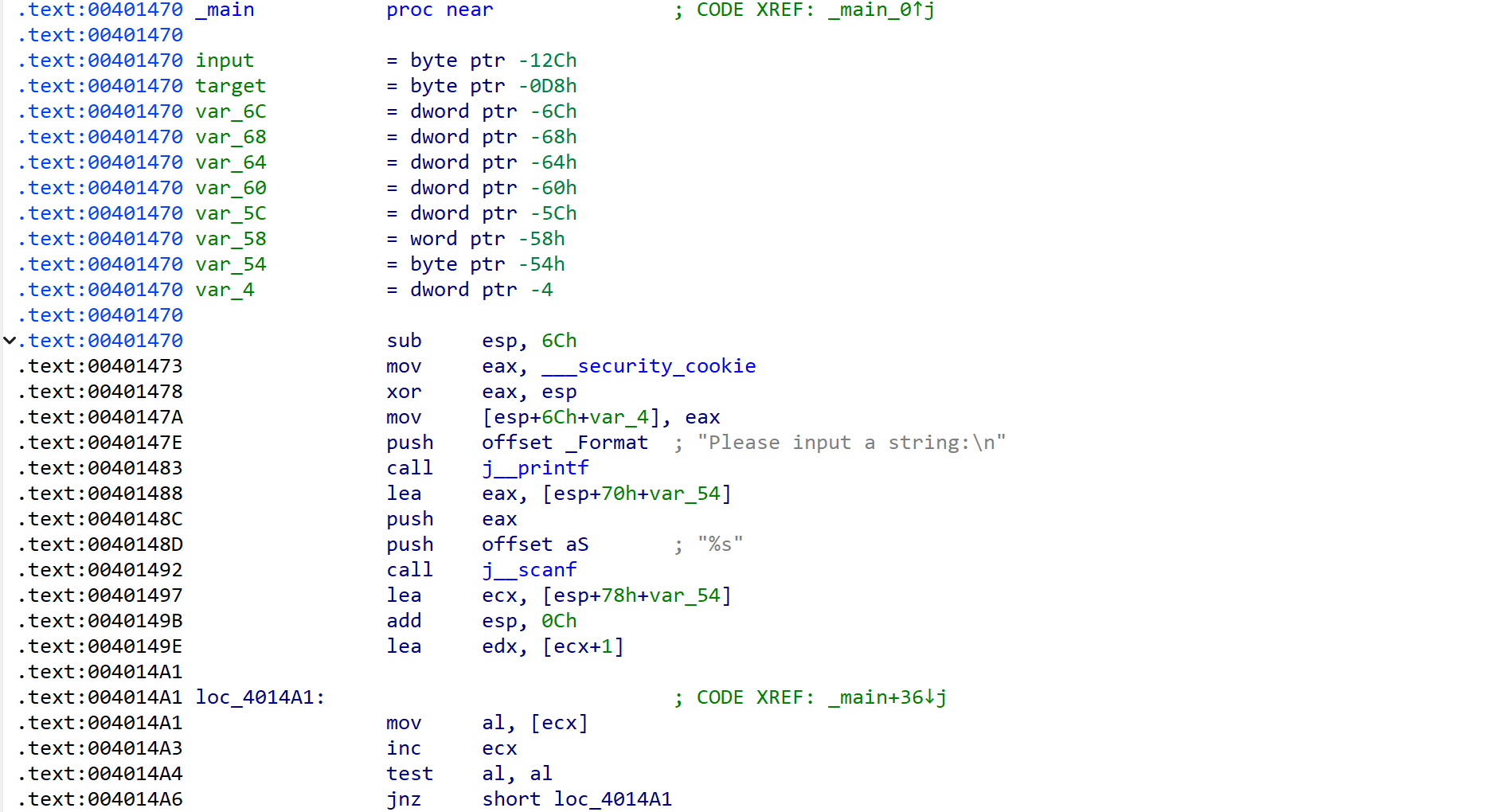


图 5 task4.exe的反汇编代码

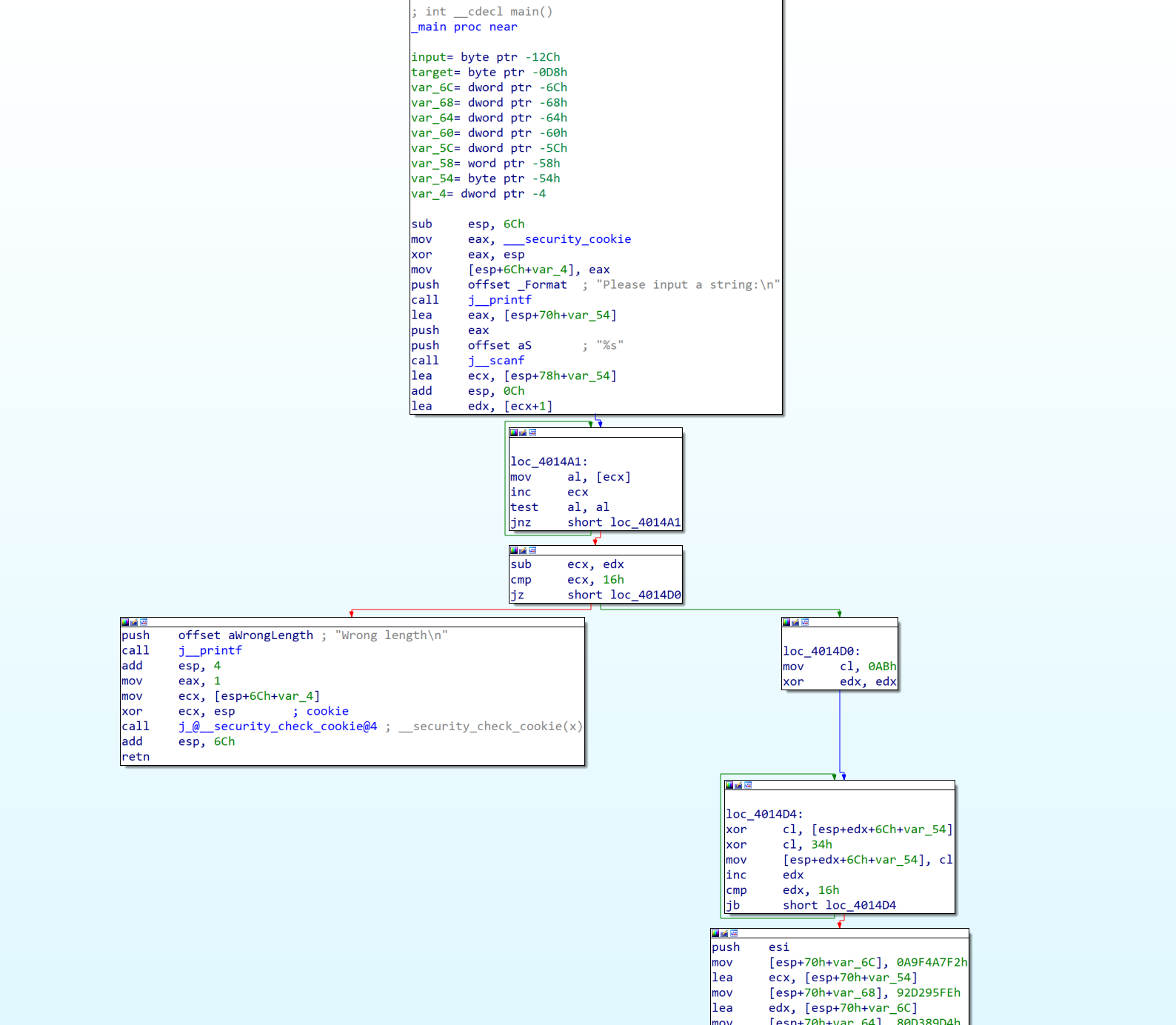


图6 task4.exe反汇编代码的图形化显示

1. 使用IDA的反编译功能（F5快捷键）得到伪代码，如图7所示。右键点击数字对象可实现数制转换。

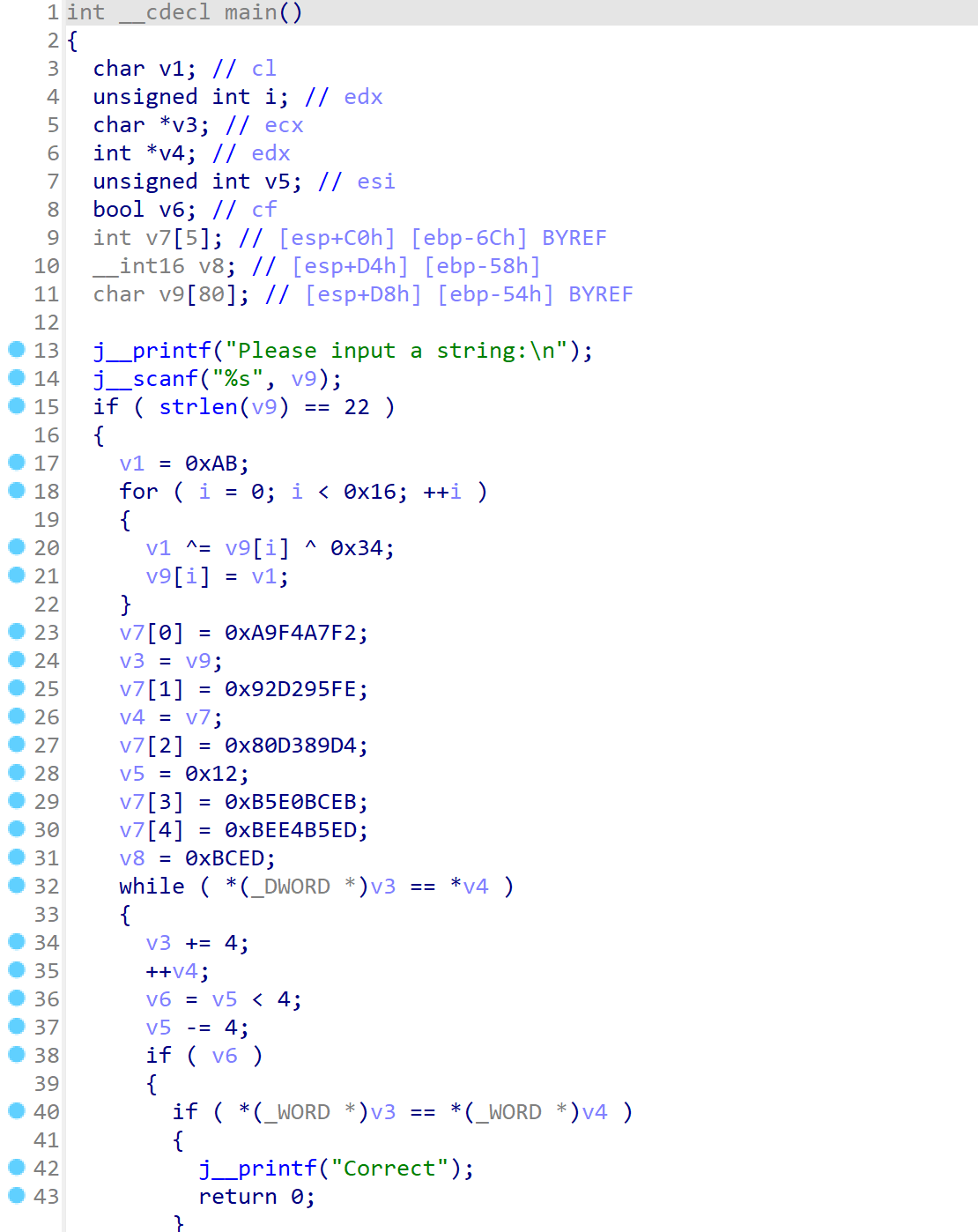


图7 task4.exe的反编译伪代码

1. 通过对反汇编命令及反编译伪代码的分析，逆向推理出待输入字符串的计算公式
2. 使用熟悉的编程语言（C++、Java、Python等）对待输入字符串进行计算，完成逆向分析挑战。



图8 逆向分析，完成task4练习

1. **实验报告**
2. 分别针对task3、task4使用IDA Freeware，获得可执行文件的反汇编代码及反编译伪代码，提供截图。
3. 分别针对task3、task4反编译伪代码的计算过程、数据结构、条件判断等信息进行逆向分析，列出正确输入字符串的计算公式。
4. 使用熟悉的编程语言，分别针对task3、task4编写脚本，计算出正确的字符串，提供脚本输出结果的截图
5. 分别运行程序task3、task4，输入计算得到的字符串进行验证，获得“Correct”输出，提供截图。