#### 逆向分析

- 在软件开发的过程中,程序员会使用一些调试工具,以便高效地找出软件中存在的错误。
- 而在逆向分析领域,分析者也会利用相关的调试工具来分析软件的行为并验证分析结果。
- 调试逆向分为动态分析技术和静态分析技术。
  - 动态分析技术指的是使用调试工具加载程序并运行,随着程序运行,调试者可以随时中断目标 的指令流程,以便观察相关计算的结果和当前的设备情况。
  - 静态分析技术是相对于动态分析而言的。由于在实际分析中,很多场合不方便运行目标(例如病毒程序,设备不兼容,软件的单独某一模块)。那么这个时候静态分析技术就该上场了!
- OD (OllyDbg) 和IDA Pro这两款工具分别是调试逆向的倚天剑和屠龙刀。
- 虽然两者都兼容动态和静态的调试方式,但就动态调试而言,OD更为灵活和强大,而静态调试工具的王者理所应当是功能极为强大的IDA Pro。

## OD基本快捷键及功能

F2	下断点,也就是指定断点的地址
F3	加载一个可执行程序,进行调试分析
F4	程序执行到光标处
F5	缩小、还原当前窗口
F7	单步步入
F8	单步步过
F9	直接运行程序,遇到断点处,程序暂停
Ctrl+F2	重新运行程序到起始处,一般用于重新调试程序
Ctrl+F9	执行到函数返回处,用于跳出函数实现
Alt+F9	执行到用户代码处,用于快速跳出系统函数
Ctrl+G	输入十六进制地址,快速定位到该地址处

## 定位到系统函数

- Ctrl + G 输入MessageBoxA
- bp MessageBoxA 直接下断点

#### 数据类型

在学习16位汇编时,可以对内存单元进行长度修饰,比如: mov byte ptr [1000H], 1,表示1是一个字节类型数据, mov word ptr [1000H], 1,表示1是一个字类型数据。

在C++中,使用变量类型表示数据的大小,引用头文件windows.h

字节 BYTE 1字节 0-0xFF (unsigned char)

字 WORD 2字节 0-0xFFFF (unsigned short)

双字 DWORD 4字节 0-0xFFFFFFF (unsigned long)

# 问题

只能使用目前学过的汇编指令,最多使用4条指令,编程计算2的4次方。

 $1 \mod ax, 2$ 

2 add ax,ax

3 add ax,ax

4 add ax,ax