

## 实验四 二进制程序逆向工程

### 实验内容：

- 1 二进制炸弹实验的内容、方法和基本步骤；
- 2 程序机器级表示、分析与调试基本知识和方法的应用。

### 实验目标：

- 1 加深对程序的机器级表示、汇编与反汇编、二进制程序分析与调试、逆向工程等方面知识的理解和掌握；
- 2 从程序员角度认识计算机系统，分析高级语言对应的机器行为及其对程序执行结果和性能的影响，解决计算机系统设计、程序开发过程中的关键问题。
- 3 掌握各种开源的编译调试工具。

### 实验任务：

- 1 学习 MOOC 内容

<https://www.icourse163.org/learn/NJU-1449521162>

#### 第五周 二进制程序逆向工程

- 第 1 讲 二进制炸弹实验：概述
- 第 2 讲 二进制炸弹实验：字符串比较
- 第 3 讲 二进制炸弹实验：浮点数表示
- 第 4 讲 二进制炸弹实验：课后实验

- 2 完成实验

详见二进制逆向工程实验文档

- 2.1 字符串 phase0
- 2.2 浮点数表示 phase1
- 2.3 循环 phase2（选做）

注意：本实验提供的代码和 MOOC 视频讲解内容不完全相同，需要根据代码中的实际内容完成作业。

- 4 提交报告

实验报告（word 格式）、程序代码拷贝到一个文件夹中，命名为：

实验 n

其中， $n=1\cdots 6$  为第 n 次实验

课程结束时，将这 6 个文件夹拷贝到同一个文件夹中，命名为如下格式：

班号-学号-姓名

以班为单位一起提交。