2023 年春季：X86 汇编程序设计第一次实验作业

1. 建立 DOSBox 环境，至少包含 edit, masm, link, debug。建立好后，dir BIN 目录下的文件，截屏。命名：”MASM 编程环境截屏.JPG”——**参看第 4 章的讲义 2**
2. 用 EDIT 修改样例程序 exp41.asm，保存更名为 TTTT.asm，在程序中 Name 后将“Zhang Wuji”修改为“XXXX YYYY”。XXXX 是你的班号学号，YYYY 是你的姓名的全拼音；汇编、连接，运行，截取完整汇编、连接、运行及显示结果的屏幕，命名为：“TTTT 汇编连接及运行.JPG”。
3. 在 DEBUG 下，跟踪执行 TTTT.exe——**DEBUG 使用请参看 DEBUG 指导**
   (1) 在 DEBUG 下，修改要排序的表，合适位置放入字“XXYY”（水印），XX 为小班号，YY 为学号；
   (2) 在 DEBUG 下，修改 JBE 为 JAE，将升序排序改为降序排序。
   (3) 单步执行，先执行至排序前，找到数据区，显示数据段，截屏；再执行至排序结束，找到数据区，显示数据段，截屏；将两个截屏文件放入 Word 文件，解读“水印”在排序前后数据段内的地址，标示出来。此 Word 文件命名为：“TTTT 降序排序前后水印位置”文档，并转换为 PDF 文件，提交“TTTT 降序排序前后水印位置.PDF”。
4. **（选做题）**
   (1) 在 DEBUG 下，将 ADD1 修改为长度为 32 位的“班号学号”双字水印，如 11223434h(根据你的班号学号改)，显示数据区，指出 ADD1 地址及内容。
   (2) 改 CS：IP 至 JMP DWORD ADD1，截取单步执行此命令后的屏幕，在后面的文档中解读 CS：IP 的值及含义。
   (3) 改 CS：IP 至 CALL DWORD ADD1，截取单步执行此命令后的屏幕，显示堆栈段的栈顶处， 截取堆栈栈顶数据区屏幕，在后面的文档中解读栈顶值及含义。
   (4) 在 WORD 下粘贴上述三个截屏文件，分别解读截屏中的“水印”地址及内容；解读 JMP DWORD ADD1 执行后的 CS:IP 值；解读 CALL DWORD ADD1 执行后栈顶数据区的地址及内容（SS：[SP]处的双字）、含义,CS:IP 值。存

成 Word 文档，并转换为 PDF 文件，提交“段间转移及调用指令解读.PDF”。

5. 将作业文件打包为“XXXXYYYY_第一次实验作业”（XXXX 为班号学号，YYYY 为姓名汉字），**上传至北航在线教学平台**。