## 2024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**
4. 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；
5. 在DEBUG下，修改JBE为JAE，将升序排序改为降序排序。
6. 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”。
7. **（选做题）**
8. 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。
9. 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。
10. 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。
11. 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”。
12. 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**](mailto:发送至masm2020@126.com)**在线教学平台**。