**四、各章知识点**

**第一章**

冯诺依曼型计算机五大功能部件；

计算机系统的层次化结构；

计算机系统的性能评价：响应时间（执行时间）和吞吐率；

MIPS、CPI等；

响应时间（执行时间）=时钟周期数\*时钟周期=指令数\*CPI\*时钟周期=指令数\*CPI/时钟频率；

**第二章**

十进制与二进制之间转换；

原码、补码、反码、移码转换；

补码的优点；移码的优点；

IEEE 754标准中单精度浮点、双精度浮点格式；

C语言中int、short、char、float等各种常见数据类型所占字节数；

大小端机器数据在内存中的存储顺序差别；

**第三章**

IA-32中通用寄存器的名称、宽度；

IA-32中EFLAGS、EIP的功能；

IA-32中各类寻址方式及有效地址的计算方式；

了解IA-32中各类传输指令功能，包括MOV、PUSH/POP、LEA、PUSHF/POPF等；

了解IA-32中各类定点算术运算指令的功能，包括ADD/SUB，INC/DEC、NEG、CMP、MUL/DIV、IMUL/IDIV；

了解IA-32中各类逻辑运算指令的功能，包括NOT、AND、OR、XOR、TEST等；

了解IA-32中各类移位指令的功能，包括SHL/SHR、SAL/SAR等。

了解IA-32中各类控制转移指令的功能，包括JMP、Jcc等；

了解IA-32中调用和返回指令的功能，包括CALL、RET等。

理解C语言中过程调用的执行步骤；

理解堆、栈、栈帧的概念，能画出过程调用中栈帧的变化；

牢记EAX是过程调用return的返回值；

牢记在栈帧中EBP+8一般是指向第一个入口参数；

理解过程调用中按值传递参数和按地址传递参数的本质区别；

了解常用C语言与汇编语言之间的对应关系：if else；switch；条件表达式；while；for等。

难点：能在C语言与汇编语言之间做手动转换，重点是读懂汇编程序，反汇编为对应的C代码。也能够根据C语言，手动汇编为对应的汇编程序。参考作业题：13和14等。

了解数组元素、结构体数据、联合体数据在存储空间中的存放方式及访问机制。

了解越界访问和缓冲器溢出攻击机器及其防范方法。

注意：不用记忆汇编语言格式，考试时会给出汇编指令功能提示，类似下面的表格（统一按AT&T格式给出）：

|  |  |
| --- | --- |
| 汇编指令 | 指令功能 |
| Movl %eax, %ebx | R[ebx]=R[eax] |
| Call Label | Push %eip  R[eip]=Label |
| sub $1, %edx | R[edx]=R[edx]-1 |
| cmpl %edx, %eax | 根据R[eax]-R[edx]减法结果改变EFLAGS，但R[eax]值不改写 |
| Mulb %bl | R[ax]=R[al]\*R[bl] |
| salw $2, %ax | R[ax]=R[ax]<<2 |
| cmpl %edx，%eax  jg Lable | 带符号整数%edx>%eax时跳转 |
| …… |  |

凡是考试中涉及的指令均会给出功能提示。

**第四章**

了解ELF可重定位目标文件的格式。

了解ELF可执行文件的格式。

了解静态链接与动态链接的概念。