主管领导审核签字

哈尔滨工业大学 2022 年春季学期

计算机系统（A）　答题卡

题号	一	二	三	四	五	六	七	总分
得分								
阅卷人								

片纸鉴心　诚信不败

授课教师　姓名　学号　院系　密　封

一、单项选择题（每小题 1 分，共 10 分）

1（ A ） 2（ D ） 3（ A ） 4（ D ）5（ C ）
6（ B ） 7（ C ） 8（ A ） 9（ C ）10（ D ）

二、填空题（ 每空 1 分，共 10 分 ）

11、 ① gcc hello.c -o hello
② objdump hello -D > 1.txt
12、 jobs
13、 16
14、 ①栈 ② 寄存器
15、 寄存器
16、 ①%rdi ② %rsi ③%rax

三、判断对错（每小题 1 分，共 10 分，正确打 √、错误打×）

17（√×）是指“指整数值”的描述有歧义，答案放宽
18（√）19（√）20（√）21（×）
22（√）23（×）24（√）25（√）26（√）

四、系统分析题（30 分）

27 题(5 分)

①寄存器%edx 赋值 0

②内存%rdi+%rdx*8 处的 8 字节数值与寄存器%rax 数值相加，结果保存在%rax 中

③将寄存器%rdx 的数值+1

④比较指令，用%rdx-%rsi 的结果设置标志位

⑤如果小于，则跳转至.L3

按对应的 C 语言的语句来解释，也给分。

28 题(5 分)

答：

```
long myproc0(long x[], long n){
    long val = 0;
    long i;

    for(i=0;i<n; i++){
        val += x[i];
    }
    return val;
}
```

29 题—（1）（5 分）

答：CC 是 0x4 或 100，PC、%rbx、%rdx 的数值分别是 0x014、0x123、0x210，组合逻辑是 addq %rdx,%rbx 这条指令的结果状态。

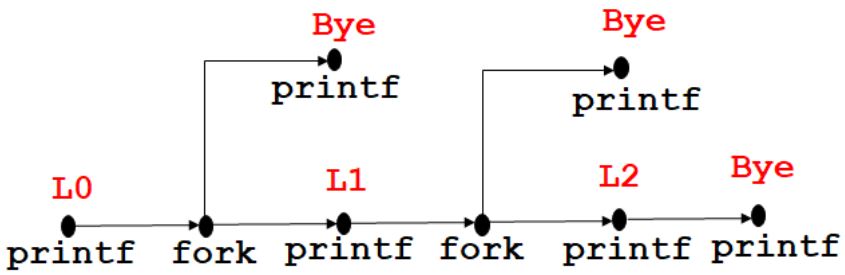
29 题—（2）（5 分）

答：组合逻辑包括 ALU、控制逻辑、读(内存、数据/指令内存、寄存器文件)

时序逻辑包括写寄存器、写内存。

组合逻辑的状态不用等待时钟上升沿触，就能快速更新；时序逻辑，例如寄存器，在数据更新/写入时，需要时钟上升沿触发，才能将更新的数值写入。

30 题—（1）进程图（5 分）



30 题—（2）可能的输出数列（5 分）

答对一列即可 5 分，答对一列的一部分，视情况给分。

L0	L0	L0	L0	L0
L1	L1	L1	Bye	Bye
L2	Bye	Bye	L1	L1
Bye	L2	Bye	L2	Bye
Bye	Bye	L2	Bye	L2
Bye	Bye	Bye	Bye	Bye

五、综合设计题（10 分）

31 题—(1)

2^{14} 、 19 、 14

31 题—(2)

块偏移是（3）位，组索引的位数是（3）位、标记的位数是（13）位。

31 题—(3)

组索引：2， 标记位数值: 0xC54、能命中、0x75
上述数值写成十进制也可以：分别是 2、3156、117

六、简答题（32 题～36 题，每小题 6 分，共 30 分）

32 题

答：每个正确的知识点 1 分，包括但不限于：
1) 全局符号中：有初值的全局变量、函数是强符号，无初值的全局变量是若符号
2) 根据强弱符号类别，确定被引用的符号在哪里
3) 根据各目标文件的段落大小、系统代码等信息，合并同类型的段，并计算可执行文件各段的大小，
4) 根据程序的内存映像，确定被引用的符号在程序运行时的内存地址
5) 根据在磁盘上的可执行文件中，各段落的大小，确定符号引用的位置
6) 根据上述信息，计算符号引用处应该采用的数值，并写入文件。

按教材和讲义中“解析过程”的描述、或者符号解析的解释来回答，也酌情给分。

33 题

答：
攻击原理：
1）向程序输入缓冲区写入特定的数据，例如在 gets 读入字符串时，使位于栈中的缓冲区数据溢出，用特定的内容覆盖栈中的内容，例如函数返回地址等；
2）函数 gets 读入字符串结束，返回（ret 指令）时，从栈中读取的返回地址将是被修改的错误地址，导致返回到特定的位置，执行特定的代码，达到攻击的目的。
防范方法：
1）代码中避免溢出漏洞：例如使用限制字符串长度的库函数。
2）随机栈偏移：程序启动后，在栈中分配随机数量的空间，将移动整个程序使用的栈空间地址。
3）限制可执行代码的区域
4）进行栈破坏检查——金丝雀

34 题

答：答对一点就给 1 分，包括但不限于：采用循环展开、增加累积量、运算

重组等手段

1） 减少数据依赖
2） 提高并发程度
3） 充分利用流水线（灌满）
4） 充分利用 CPU 中的多个计算单元
5） 减少循环开销

35 题

答：

1) 处理器生成一个虚拟地址 VA，并将其传送给 MMU
2) MMU 生成 PTE 地址(PTEA)，并从高速缓存/主存请求得到 PTE
3) 高速缓存/主存向 MMU 返回 PTE
4) MMU 将物理地址传送给高速缓存/主存
5) 高速缓存/主存返回所请求的数据字给处理器

36 题

答：每点 1 分，包括但不限于以下内容：

1) shell 接收命令
2) 用 fork 创建子进程
3) execve 函数加载进程
4) 执行时如何如何会产生缺页异常/中断
5) 利用 VA 访存的过程
6) 缺页中断后的页面换入的方法、如何恢复运行
7) printf 函数涉及的动态链接库的动态链接
8) 调用 printf 函数涉及的"Hello World"字符串的获取
9) hello 运行完毕后产生 SIGCHLD 的信号
10) 父进程对其回收、资源释放等
11) ……