主管院长签字

哈尔滨工业大学 2023 年春季学期

计算机系统（A） 试 题

题号	一	二	三	四	五	六	总分
得分							
阅卷人							

答案务必写在答题纸上，并标明题号。答在试题上无效。

片纸鉴心 诚信不败

授课教师 姓名 班号/学号 院系

一、 单项选择题（每小题 2 分，共 20 分）

1. 在 X86-64 机器中，有 C 代码：short x = -3；已知&x = 0x601018，则内存 0x601019 处的字节值(十六进制)是（ ）。
   A. FF B. FD C. 00 D. F3

2. 针对汇编指令（AT&T 格式）"addl 20(%edx,%esi,4), %eax"的叙述，错误的是（ ）。
   A. 目的操作数是%eax
   B. 20(%edx,%esi,4)是内存操作数
   C. 操作数 20(%edx,%esi,4)的地址是 20+%edx+%esi+2
   D. 操作数的宽度是 4 字节

3. 考虑以下 C 语言程序：

```
int x=-1;
printf("x = %u\n",x);
```

   则执行上述代码后的结果是（ ）。
   A. x = -1 B. x = 4294967295
   C. x =255 D. x = 1

4. 以下关于 X86-64 指令的叙述，错误的是（ ）。
   A. movq 指令可传送 64 位数据
   B. 当目的操作数是寄存器时，movl 会将目的寄存器的高 32 位清 0
   C. pushq 和 popq 分别对寄存器 esp 减 8 和加 8
   D. movabsq 能将 64 位立即数传送给寄存器操作数

5. 下列哪种情况能很好地发挥 Cache 的作用？（ ）。
   A. 程序中不含过多的 I/O 操作 B. 程序的大小不超过实际的内存容量
   C. 程序具有较好的访存局部性 D. 程序的指令间相关度不高

6. 下列异常事件中异常处理后处理器会重新执行引起异常的指令的是（ ）。
   A. 键盘输入异常 B. 存储保护异常
   C. 奇偶校验错误异常 D. 缺页异常

7. X86-64 中，某 C 程序定义了结构体

```
struct S {
    double v;
    int i[2];
    short s;
};
```

   则 sizeof(S)的值是（ ）。
   A.24 B.18 C.20 D. 8

8. 以下有关共享库的叙述中，错误的是（ ）。
   A. 共享库可以单独升级，比静态库更方便维护
   B. 可以在程序运行过程中通过编程指令进行动态链接
   C. 一个共享库如果被 n 个正在运行的进程使用，则会被载入到内存 n 次
   D. 共享库需要系统中的动态链接器来支持

9. 根据下面的反汇编代码，指出 je 指令的目标（即 xxxxxx 处的值，je 指令的机器码是 74）是（ ）。

```
4005c8: 74 03    je     xxxxxxx
4005ca: ff d0    callq  *%rax
```

   A.4005c8 B.4005ca
   C.4005cb D.4005cd

10. 下列事件中会导致进程终止的是（ ）。
    A. 执行 exit 函数 B. 执行 wait 函数
    C.时间片中断 D.上下文切换

二、填空题（每空 1 分，共 10 分）

11. 8 位整数的补码是 10101001，扩展 8 位成为 16 位后的十六进制表示为 0x____。
12. 汇编指令“movx %dx, (%rax)”中，操作数宽度后缀 x 应为____。
13. 在 x86-64 的 64 位 Linux 程序中，调用函数 int fun (long x, long y)时，保存参数 y 的寄存器是____。
14. 若主存物理地址 32 位，高速缓存总大小为 2K 行，块大小 16 字节，采用 4 路组相连，则标记位的位数是____。
15. C 语言中 float f1=-1.5 的 IEEE754 编码是 0x____。
16. 链接器经过符号解析和____两个阶段，将目标文件生成可执行文件。
17. Linux 进程在进行上下文切换时会____次进入内核模式。
18. 在 Linux Shell 中执行命令“ld -o p main.o p.o”时，Shell 通过函数 execve(argv[0],

argv，environ）加载 ld 程序，此时 argv 数组中非空指针的数量为（即 argc）____。

19. 虚拟内存将____作为磁盘空间的缓存，其工作是由操作系统和硬件共同管理的。

20. 某 CPU 使用 32 位虚拟地址和 4KB 大小的页面，虚拟内存采用单级页表时，页表中 PTE 的总数是____。

三、判断对错（每小题 1 分，共 10 分，在题前打√X 符号）

21. （ ）CPU 在进行算术运算时，不需要判断操作数是有符号或无符号数。
22. （ ）现代超标量 CPU 指令的平均周期通常小于 1 个时钟周期。
23. （ ）在汇编语言程序中，函数调用者必须将参数存放到栈中才能向被调用函数传递参数。
24. （ ）通过链接技术，可以实现一个程序多个模块的并行开发，如果程序只有一个模块，则不需要链接过程。
25. （ ）当工作集的大小超过高速缓存的大小时，会发生容量不命中。
26. （ ）当系统中出现 Cache 不命中时，操作系统将调用异常处理程序进行处理。
27. （ ）Linux Shell 在执行 execve()函数加载可执行目标文件时，可执行目标文件中的指令和数据即刻被读入进主存储器。
28. （ ）进程 P1 是进程 P11 的父进程，则 P1 与 P11 是并发执行的独立进程。
29. （ ）在分页式虚拟内存中，采用多级页表结构，不仅可以压缩页表大小，还可以压缩 PTE 的数量。
30. （ ）Linux 系统中的所有进程共有一个页表。

四、简答题（每小题 5 分，共 15 分）

31. 二进制文件 bomb 的部分反汇编代码如下图所示，其中 strings_not_equal 函数有两个参数，请问这两个参数分别保存在哪里，以及是什么内容？为了获得二进制文件 bomb 的反汇编代码，你采用的指令是什么？（5 分）

```
/* Hmm...  Six phases must be more secure than one phase! */
input = read_line();              /* Get input                  */
phase_1(input);                   /* Run the phase              */
phase_defused();                  /* Drat!  They figured it out!
                                   * Let me know how they did it. */
printf("Phase 1 defused. How about the next one?\n");
```



```
0000000000001174 <phase_1>:
  1174: 48 83 ec 08           sub    $0x8,%rsp
  1178: 48 8d 35 d1 14 00 00  lea    0x14d1(%rip),%rsi    # 2650
  117f: e8 32 04 00 00        callq  15b6 <strings_not_equal>
  1184: 85 c0                 test   %eax,%eax
  1186: 75 05                 jne    118d <phase_1+0x19>
  1188: 48 83 c4 08           add    $0x8,%rsp
  118c: c3                    retq
  118d: e8 30 05 00 00        callq  16c2 <explode_bomb>
  1192: eb f4                 jmp    1188 <phase_1+0x14>
```

32. 有如下 C 语言程序：

```
int getstr() {
   char buf[100];
   scanf("%s",buf); //从标准输入流读入字符串，保存到 buf 中
   return 0;
}
int main(){
  return getstr();
}
```

分析该程序存在什么安全隐患，并从编程和编译的角度阐述如何解决？（5 分）

33. 简述 Linux 处理信号的过程，试举例说明（5 分）

五、系统分析题（30 分）

34. 已知内存和寄存器中的数值情况如下：

内存地址	值
0x100	0x66
0x104	0xAB
0x108	0x13
0x10c	0x88

寄存器	值
%rbx	0x100
%rcx	0x1
%rdx	0x3

请填写下表，给出对应操作数的值（5 分）

操作数	值
%rbx	
(%rbx)	
9(%rbx,%rdx)	
0xfc(,%rcx,4)	
(%rbx,%rdx,4)	

35. 下面给出了一个函数的汇编源代码和对应的 C 语言代码框架，请在横线上解释左侧对应汇编指令的功能，并补全右侧 C 代码的语句。（5 分）

汇编代码：

```
proc:
    movl    %edi, %edx      ①
    movl    $0, %ecx
.L2:
    testl   %eax, %eax      ②
    je      .L4             ③
    movl    %eax, %ecx
    imull   %edi, %ecx      ④
    addl    %ecx, %edx
    subl    $1,   %eax
    jmp     .L2
.L4:
    movl    %edx, %eax
    ret
```

C 程序代码：

```
unsigned int proc(unsigned int x)
{
  unsigned int y, z;
  unsigned int w = 0;
  z = 1;
  y = x;
  while(y>0 )
  {
    z = x*y;
    w += z;
    y --;
  }
  return ⑤;
}
```

36. 考虑下面的程序，它由两个模块组成。（5 分）

```
/*main. c*/
#include <stdio.h>
unsigned x = 257;
short y,z = 2;
void p1(void);
int main()
{
    p1();
    printf("x=%u,z=%d\n",x,z);
    return 0;
}
```

```
/*p1.c*/
double x;
void p1()
{
    x=-1.5;
}
```

（1） 请指出 main.c p1.c 中哪些是强符号？哪些是弱符号？

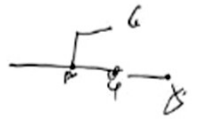
（2） 程序执行后的打印结果是什么？

37. 有如下 C 语言程序，请分别分析父进程与子进程的输出是什么？并给出可能的输出序列(5 分)。

```
int main()
{
    int  x=5;

    if (Fork() != 0)
        printf("x=%d\n",--x);

    printf("x=%d\n",++x);
    exit(0);
}
```



38. 下面是多项式 $a_0 + a_1 \times x + a_2 \times x^2 + \ldots + a_n \times x^n$ 求和的 C 语言函数。（10 分）

```
double poly(double a[], double x, long n)
{// a 是多项式系数数组，x 是值，n 是多项式次数
    long i,j;
    double result = 0;
    double xpwr;
    for (i = 0; i <= n; i++) {
        xpwr = 1;
        for(j=0;j<i;j++)
            xpwr *=x;
        result += (a[i]*xpwr);
    }
    return result;
}
```

（1）优化程序性能的一般性方法有哪些？请列举至少 5 种；

（2）对该程序进行速度优化，写出优化后的程序并说明采用的方法种类。

六、综合设计题（共 15 分）

某计算机系统的情况如下：

（1）内存是按字节寻址，字长为 2 字节（非 4 字节），采用小端模式存储；

（2）虚拟地址长度：24 位；

(3) 使用一级页表，页面大小是 2048 字节；
(4) 物理地址的位数是 19 位；
(5) TLB（翻译后备缓冲器）是 4 路组相连，共 16 个条目；
(6) L1 d-Cache 是物理寻址、直接映射（每组一行），行大小 8 字节，共 8 个组；
(7) TLB、Cache 的当前数值如表 1、表 2 所示。

表 1 TLB 数值表

组	标记位 PPN		有效位	标记位 PPN		有效位	标记位 PPN		有效位	标记位 PPN		有效位
0	0CD	09	1	AA1	00	1	3E0	62	1	C4C	48	1
1	312	45	0	010	75	1	987	3A	1	D39	3F	0
2	038	E3	0	0A7	13	0	188	52	1	49B	11	0
3	6C0	42	0	075	50	0	013	39	1	0F2	0D	0

表 2 L1 d-cache 的数值

索引	标记位	有效位	块 0	块 1	块 2	块 3	块 4	块 5	块 6	块 7
0	35E	1	42	A0	75	50	42	0	05	50
1	27B	1	08	E3	00	A7	13	00	88	52
2	C54	1	3F	75	AB	11	25	78	9A	00
4	A32	1	97	3A	91	D3	3F	12	86	22
5	C30	1	30	62	15	4C	48	A1	12	5C
6	B26	1	01	25	3E	62	1F	C4	85	12
7	01A	1	98	3A	12	D39	3F	3C	4D	5E

39. 回答以下问题(7 分，每空 1 分)：
(1) VPN 的位数是(13)位，页表条目 PTE 的总数量是 (2^{19}) 个。
(2) TLB 中，组索引是 (2) 位，标记 tag 的位数是 (11) 位。
(3) 在 L1 d-cache 中，块偏移的位数是 (3) 位，组索引的位数是 (3) 位、标记的位数是 (19) 位。

40. CPU 从虚拟地址 0x7C0515 读取一个字的数值，将虚拟地址翻译成物理地址、并获取数值的过程中，写出下表中各参数对应的数值(8 分，每空 1 分)。

参　数	数　值
虚拟地址	0x7C0515
虚拟页号 VPN	(1) 0x0F80
TLB 索引	(2) 0x00 或 0
TLB 标签 Tag	(3) 0x3E0 或 0x3E0
TLB 命中?(Y/N)	(4) Y
物理页号 PPN	(5) 0x62
物理地址	(6) 0x31515
Cache 命中?(Y/N)	(7) Y
读取的数值	(8) 39