******华中科技大学计算机科学与技术学院2023~2024第一学期**

解答内容不得超过装订线

**“ 计算机系统基础 ”考试试卷(B卷)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **考试方式** | **闭卷** | **考试日期** | **2024-3-18** | **考试时长** | **150 分钟** |
| **专业班级** |  | **学 号** |  | **姓 名** |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **题号** | **一** | **二** | **三** | **四** | **五** | **总分** | **核对人** |
| **分值** | 20 | 20 | 20 | 20 | 20 | 100 |  |
| **得分** |  |  |  |  |  |  |  |

|  |  |
| --- | --- |
| **分 数** |  |
| **评卷人** |  |

1. **数据的存储表示和访问（共20分）**
2. 数据的存储表示（10分）

void func1()

{

int x = 10;

int y[2] = { 20,32 };

char msg[6] = "abcde";

int\* p = &x;

short z = \*(short\*)(msg + 1);

int u = \*(int\*)(msg + 1);

}

设 x的地址(&x) 为：0xffffd508； y[0]的地址为：0xffffd50c； msg[0] 的地址为：0xffffd51a；

p的地址(&p) 为：0xffffd514； z 的地址为：0xffffd518； u的地址为：0xffffd520。

在函数func1执行结束返回前，以字节形式观察内存内容。以16进制的形式填写程序用到的内存单元内容（无关的字节中的内容不要填写，打XX）。

0xffffd508 \_0A\_\_ \_00\_\_ \_00\_\_ \_00\_\_ \_14\_\_ \_00\_\_ \_00\_\_ \_00\_\_

0xffffd510 \_20\_\_ \_00\_\_ \_00\_\_ \_\_00\_ \_08\_\_ \_d5\_\_ \_ff\_\_ \_ff\_\_

0xffffd518 \_62\_\_ \_63\_\_ \_61\_\_ \_62\_\_ \_63\_\_ \_64\_\_ \_65\_\_ \_00\_\_

0xffffd520 \_62\_\_ \_63\_\_ \_\_64\_ \_65\_\_ \_xx\_\_ \_xx\_\_ \_xx\_\_ \_xx\_\_

评分标准：前两个变量，每个1分；后四个变量，每个2分。

2、调试一个C程序时，在函数的反汇编中看到源程序语句与对应的反汇编语句如下。根据观察到的信息填空。（10分）

*int a[2][5];*

*int i = 1;*

movl $1, -0x2c(%ebp)

i 的地址为 0x0019feb8， ebp = 0x \_\_0019fee4\_\_\_\_\_\_

*int j = 3;*

movl $3, -0x30(%ebp) &j = 0x\_0019feb4\_\_\_\_\_\_\_\_\_

*a[i][j] = 10;*

imul $0x14, -0x2c(%ebp), %eax

执行后，eax = \_\_0x14\_\_\_\_\_\_\_\_

eax中值的含义是\_二维数组a前i行所占字节数\_\_\_

lea -0x28(%ebp, %eax, 1), %ecx

ecx中存放的值的含义是\_a[2][0]的地址\_\_

mov -0x30(%ebp), %edx

movl $0xa, (%ecx, %edx, 4)

指令中的 edx 乘4的原因是\_每个int元素占4字节\_\_\_

a[0][0] 的地址表达形式是 \_-0x28(%ebp)\_\_\_\_;

*global[i] = 18;*  global 为一个全局整型数组

mov -0x2c(%ebp), %eax

movl $0x12, 0x417120(, %eax, 4)

global 数组的起始地址是\_0x417120\_\_\_\_,

*int\* p = &global[1];*

mov $4, %eax

shl $0, %eax

add $0x417120, %eax

mov %eax, -0x34(%ebp)

变量p 中的值是 0x\_417124\_\_­­­\_\_\_\_\_\_

*\*p = 19;*

mov -0x34(%ebp), %eax

movl $0x13, (%eax)

第二条汇编语句访存的寻址方式是\_\_寄存器间接寻址\_\_\_\_

评分标准：每空1分。第四空填“第一行长度”；第五空填“a[1][0]的地址”均给分。

|  |  |
| --- | --- |
| **分 数** |  |
| **评卷人** |  |

1. **程序运行的基本过程（共20分）**

1、在对某程序进行调试时，看到如下一段信息（10分，每空1分）：

① 设当前 eip 为 0x00411650，该处指令为“83 7D FC 00 cmpl $0, -4(%ebp)”，在取出该指令并进行译码后，eip = \_\_\_\_\_\_；

② 在0x00411654处，有指令 “7E 08 jle 0041165E”，综合前一条指令，就是在\_\_\_\_条件下，将0x0041165E →eip ,计算出该地址值的方法是 ；

③ 在0x0041165C 处，有jmp指令“EB 08”，该指令对应的反汇编语句是：\_\_\_\_\_；执行该指令时，会\_\_\_\_\_（有、无）条件跳转到 0x00411666处；

④ 在0x00411666处，有一子程序直接调用指令“E8 65 FC FF FF callq 004112D0”。由此推断子程序的入口地址是 ；指令中 FFFFFC65的含义是是 ；执行该call指令时，CPU会将 0x 压入堆栈中；

⑤ 在0x00411672处，有指令“FF 55 F4 callq -0xc(%ebp) ”，得到子程序入口地址的方法是 ；

⑥ 执行RET指令时，CPU会 →eip。

评分标准：每空1分

2、函数调用（10分）

在Linux环境下，对一个C语言程序进行编译、链接、调试运行，程序片段如下。

int fmax(int a, int b) {

004115A5 push %ebp

004115A6 mov %esp,%ebp

004115A8 sub $0x10,%esp

***int result;***

***if (a > b)***

004115A9 mov 0x8(%ebx), %eax

004115AC cmp 0xc(%ebp), %eax

004115AF jle fmax+19h (04115B9h)

***result = a;***

004115B1 mov 0x8(%ebp), %eax

004115B4 mov %eax, -0x4(%ebp)

004115B7 jmp fmax+1Fh (04115BFh)

***else result = b;***

004115B9 mov 0xc(%ebp), %eax

004115BC mov %eax, -0x4(%ebp)

***return result;***

004115BF mov -0x4(%ebp), %eax

}

004115C2 mov %ebp,%esp

004115C4 pop %ebp

004115C5 ret

void main( ) { ………

int x = fmax(10, -10);

00413863 push $0xfffffff6h

00413865 push $0xa

00413867 call 004115A5

0041386C add $8, %esp

0041386F mov %eax, -0x4(%ebp)

………

}

设执行main函数中的 call 004115A5 之前，esp= 0xffffd500; ebp= 0xffffd510.

|  |  |
| --- | --- |
|  | 0xffffd4f0 |
|  | 0xffffd4f4 |
|  | 0xffffd4f8 |
|  | 0xffffd4fc |
| XXXXXXXX | 0xffffd500 |

填写刚进入函数fmax 时（执行push %ebp 之前），堆栈中相关单元的内容。

函数参数 a的地址（即&a）是 0x\_\_\_\_。

局部变量 result的地址是 0x\_ \_\_\_\_。

评分标准：每空2分

|  |  |
| --- | --- |
| **分 数** |  |
| **评卷人** |  |

1. **C语句的转换 （共20分）**

**1、阅读下面的程序，回答问题 （10分，每小题2分）。**

void func ()

{ unsigned short us\_x = 0x8000;

unsigned int ui\_x;

short s\_x = -0x8000;

int i\_x;

int u = 0, v = 0; // ①

ui\_x = us\_x;

i\_x = s\_x; // ②

if (ui\_x > 0) u = -1;

if (i\_x > 0) v = -1; // ③

ui\_x = ui\_x >> 1;

i\_x = i\_x >> 1; // ④

ui\_x = ~ui\_x;

i\_x = -i\_x; // ⑤

}

**⑴ 执行完** ① 处语句后，

us\_x = 0x \_\_\_\_\_\_ s\_x = 0x \_\_\_\_\_（2个字节的16进制数）

**⑵ 执行完** ② 处语句后，

ui\_x = 0x \_\_\_\_\_ i\_x = 0x \_ \_\_\_\_\_\_\_\_（4个字节的16进制数）

ui\_x =us\_x; 对应的机器指令： \_\_\_ us\_x, %eax 、 mov %eax, ui\_x

i\_x =s\_x; 对应的机器指令： \_\_\_ s\_x, %eax 、 mov %eax, i\_x

**⑶ 执行完 ③** 处语句后，

u = \_\_\_\_\_\_\_\_\_\_\_ v = \_\_\_\_\_\_\_\_\_\_\_\_

if (ui\_x >0) u=-1; 对应的机器指令： cmp $0, ui\_x、 \_\_\_\_ process2、

mov $-1, u、 process2:…

if (i\_x >0) v=-1; 对应的机器指令： cmp $0, i\_x、 \_\_\_\_ process3、

mov $-1, v、 process3:…

**⑷ 执行完 ④** 处语句后，

ui\_x = 0x \_\_\_\_\_\_ i\_x = 0x \_ \_\_\_\_\_\_\_\_\_\_\_\_\_ （4个字节的16进制数）

ui\_x = ui\_x >> 1; 对应的机器指令： \_\_\_ $1, ui\_x

i\_x = i\_x >> 1; 对应的机器指令： \_\_\_ $1, i\_x

**⑸**  **执行完**  ⑤ 处语句后，

ui\_x = 0x \_\_\_\_\_\_\_\_\_\_\_\_\_\_ i\_x = 0x \_\_\_\_\_\_ （4个字节的16进制数）

ui\_x = ~ui\_x; 对应的机器指令： \_\_\_\_ ui\_x

i\_x = -i\_x; 对应的机器指令： \_\_\_\_ i\_x

评分标准：每小题两分。指令没写后缀不扣分。

1. **程序优化 （10分）。**

设有如下一段C语言程序，请写出完成相同功能、执行速度尽可能快的汇编语言程序代码片段，并指出优化中利用了CPU中的哪些特性。

int a[5],i,sum=0;

……

for (i = 0;i < 5;i++) sum += a[i];

评分标准：程序段6分，优化特性每条2分。

|  |  |
| --- | --- |
| **分 数** |  |
| **评卷人** |  |

**四、程序阅读与理解（20分）**

**1、阅读下面的程序，回答问题 （10分）。**

**.section .data**

**array: .long -1, -2, 11, -9, 5, 100**

**length = (. -array)/4 # length 为array中元数的个数，= 6**

**format: .ascii "%d\n\0"**

**.section .text**

**.global \_start**

**\_start:**

**mov $0, %eax**

**mov $length, %ecx**

**mov $0, %esi # ①**

**lp\_1:**

**cmpl $10, array( , %esi, 4)**

**jg lp\_2 # ②**

**inc %eax**

**lp\_2:**

**inc %esi**

**sub $1, %ecx # ③**

**jne lp\_1**

**push %eax**

**push $format**

**call printf**

**mov $1, %eax # 程序正常退出**

**mov $0, %ebx**

**int $0x80**

1. 上述程序的功能是什么？运行后，屏幕上显示的是什么？（2分）
2. 若标号 lp\_1 写到 **①**处语句前，程序运行的结果是什么？为什么？（3分）
3. 若将 **②** 处的语句改为 “ja lp\_2”,程序运行的结果是什么？(2分)
4. 若漏写了 ③ 处的语句 ，程序运行会出现或什么现象？为什么？（3分）

评分标准：第4问，若只填“死循环”给1分。

**2. 程序填空（10分，每空 1分）**

将一个以0结束的字符串中所有的大写字母转换为对应的小写字母，并将转换后的字符串、以及修改的字母个数输出。

……

.section .data

format: .ascii "%s %d\n\0"

buffer: .ascii "Computer System Foundation \n\_\0\_\_\_"

.section .text

.global \_start

\_start:

mov \_\_\_\_\_\_\_\_\_, %ebx # ebx 存放buffer 数组元素的下标

mov \_\_\_\_\_\_\_\_, %ecx # ecx 存放修改字母的个数

loop\_begin:

mov buffer(%ebx), %al

cmp $0, %al

\_\_\_\_\_\_\_\_\_\_\_\_\_

cmp $‘A’, %al

\_\_\_\_\_\_\_\_\_\_\_\_\_

cmp $’Z’, %al

\_ \_\_\_\_\_\_\_\_\_\_\_\_\_

add \_\_\_\_\_\_\_\_\_\_\_, %al

mov %al, \_ \_\_\_\_

\_inc \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

next\_char:

\_\_\_\_\_\_\_\_\_\_\_\_\_

jmp loop\_begin

loop\_over:

push %ecx

pushl $buffer

pushl $format

call printf

mov $1, %eax # 程序正常退出

mov $0, %ebx

int $0x80

评分标准：每空1分。第6空，若计算具体值，计算错误扣0.5分。

|  |  |
| --- | --- |
| **分 数** |  |
| **评卷人** |  |

1. **问答题（20分）**
2. 可重定位目标文件中有哪些节？各节中主要有什么信息？什么是符号解析？链接的过程是什么？（10分）

评分标准：每问得分分别是3分、2分、2分、3分

1. 在一个程序的运行过程中（如正在执行一个二维数组求累加和），用户按了键盘上的某个键，计算机系统会做出哪些响应（即一系列的处理过程）？中断分哪几类？请举例说明各类中断在何种情况下产生。（10分）

评分标准：第一问5分，每个关键词1分。第二问3分，第三问2分。