考试中心填写：

___年 ___月___日
考试用

湖南大学课程考试试卷

课程名称：计算机组成与结构 B(2016 春)；试卷编号：A；考试时间：120 分钟

专业班级：

学号：

姓名：

题号	一	二	三	四	五	六	七	八	九	十	总分
应得分	10	40	20	30							100
实得分											
评卷人											评分：

一、单项选择题（每小题 2 分，共 10 分）

1、关于 IA-32 与 x86-64 的不同，以下说法正确的是 （ ）。

(a) x86-64 不可能遭受缓冲区溢出攻击

(b) IA-32 具有调用者保存及被调用者保存寄存器使用惯例，x86-64 没有此惯例

(c) 在 x84-64 机器中，任何针对 32 位操作数的指令都是非法的

(d) 以上都不是

2、在 64 位系统中，子程序 RETQ 指令执行前% rsp 寄存器的值为 0x7fffff0000，请问在执行 RETQ 之后% rsp 的值为 （ ）。

(a) 0x7fffff0008

(b) 0x7fffff0004

(c) 0x7fffff0000

(d) 0x7ffffefff8

3、以下表述中哪个最符合 X86 汇编指令 TEST （ ）。

(a) 同 SUB 指令完全一样

(b) 类似于 SUB 指令，但不保留结果（仅设置标志位）

(c) 同 AND 指令完全一样

(d) 类似于 AND 指令，但不保留结果（仅设置标志位）

4、在 IEEE 浮点格式中，如果分配更多位数给指数部分，将会导致（ ）。

(a) 可表示的数值个数减少，但能表达更大的数

(b) 可表示的数值个数不变，但具有更多的小数位数

(c) 表数范围增大，但表数精度降低

(d) 先前可表达的一些数可能会被舍入为无穷大

5、32 位补码表示的最小整数值是 （ ）。

(a) -232 (b) -232 + 1

(c) -231 (d) -231 +1

二、(40 分)以下有三段完整或者不完整的 C 程序段，题目给出了它们对应的汇编代码，请利用你掌握的 C 语言和汇编语言知识，采用逆向工程的思维，回答下面的问题。

(1) 某程序的 C 代码及其汇编代码如下：(14 分)

```
int  lolwut (char *s)
{
    int  i, n;
    n = 0;
    for (i = ; _____;  i++)
    {
        if (_____)
        {
            return  -1;
        }
        n = _____;
    }
    return _____;
}
```

gcc 编译后，汇编代码如下：

```
lolwut:
    pushl   %ebp
    movl    %esp, %ebp
    subl    $16, %esp
    movl    $0, -8(%ebp)
    movl    $0, -4(%ebp)
    jmp .L2
```

```
.L6:
    movl    -4(%ebp), %eax
    addl    8(%ebp), %eax
    movzbl  (%eax), %eax
    cmpb    $47, %al
    jle .L3
    movl    -4(%ebp), %eax
    addl    8(%ebp), %eax
    movzbl  (%eax), %eax
    cmpb    $57, %al
    jle .L4
.L3:
    movl    $-1, %eax
    jmp .L5
.L4:
    movl    -8(%ebp), %edx
    movl    %edx, %eax
    sall    $2, %eax
    addl    %edx, %eax
    addl    %eax, %eax
    movl    %eax, %edx
    movl    -4(%ebp), %eax
    addl    8(%ebp), %eax
    movzbl  (%eax), %eax
    movsbl  %al,%eax
    leal    (%edx,%eax), %eax
    subl    $48, %eax
    movl    %eax, -8(%ebp)
    addl    $1, -4(%ebp)
.L2:
    movl    -4(%ebp), %eax
    addl    8(%ebp), %eax
    movzbl  (%eax), %eax
    testb   %al, %al
    jne .L6
    movl    -8(%ebp), %eax
.L5:
    leave
    ret
```

① 请将上面这段缺失的 C 代码填写完整（8 分）。

② 在进入函数时执行了两条指令

```
pushl   %ebp
movl    %esp, %ebp
```

在退出时的 leave 指令等价于：

```
movl    %ebp, %esp
popl    %ebp
```

请解释这些指令的意义。（6 分）

(2) 有如下 C 语言程序，请在空格处填充适当的整数，使程序运行后仅输出“I am a HNUer”字符串。(18 分)

```
#include <stdio.h>
void foo()
{
    int a,*p;
    p=(int*)((int)&a+ ①  );
    *p+= ②  ;
}

int main()
{
    int i='e';
    int j='p';
    foo();
    printf("不能被打印的内容\n");
    i+=2;
    j+= ③  ;
    printf("I am a HNU");
    printf("%c",i);
    printf("%c\n",j);
    return 0;
}
```

在用 objdump 查看对应的目标文件时，main 函数块的内容如下：

```
08048472 <main>:
8048472:   55                    push   %ebp
8048473:   89 e5                   mov    %esp,%ebp
8048475:   83 e4 f0                and    $0xfffffff0,%esp
8048478:   83 ec 20                sub    $0x20,%esp
804847b:   c7 44 24 1c 65 00 00    movl   $0x65,0x1c(%esp)
```

```
8048482:   00
8048483:   c7 44 24 18 70 00 00    movl   $0x70,0x18(%esp)
804848a:   00
804848b:   e8 c4 ff ff ff             call   8048454 <foo>
8048490:   c7 04 24 a0 85 04 08    movl   $0x80485a0,(%esp)
8048497:   e8 e8 fe ff ff             call   8048384 <puts@plt>
804849c:   83 44 24 1c 02          addl   $0x2,0x1c(%esp)
80484a1:   83 44 24 18 ??          addl   $0x?,0x18(%esp) //?代表一个数字
80484a6:   b8 b9 85 04 08          mov    $0x80485b9,%eax
80484ab:   89 04 24                mov    %eax,(%esp)
80484ae:   e8 c1 fe ff ff             call   8048374 <printf@plt>
80484b3:   8b 44 24 1c             mov    0x1c(%esp),%eax
80484b7:   89 04 24                mov    %eax,(%esp)
80484ba:   e8 95 fe ff ff           call   8048354 <putchar@plt>
80484bf:   b8 c4 85 04 08          mov    $0x80485c4,%eax
80484c4:   8b 54 24 18             mov    0x18(%esp),%edx
80484c8:   89 54 24 04             mov    %edx,0x4(%esp)
80484cc:   89 04 24                mov    %eax,(%esp)
80484cf:   e8 a0 fe ff ff             call   8048374 <printf@plt>
80484d4:   b8 00 00 00 00          mov    $0x0,%eax
80484d9:   c9                      leave
80484da:   c3                      ret
```

请根据以上内容作答：

①处应填整数_____(2 分)，因为_____

_____

_____。(4 分)

②处应填整数_____(2 分)，因为_____

_____

_____。(4 分)

③处应填整数_____(2 分)，因为_____

_____

_____。(4 分)

(3) 考虑下面数组访问的 C 程序：

```
#include "stdio.h"
#define H   ?  //定义常数 H
#define J   ?  //定义常数 J

int array1[H][J];
int array2[J][H];
void f (int x, int y) {
```

```
array1[x][y] = x+1;
array2[y][x]=y-1;
}

int main( )
{
    return 0;
}
```

经过 gcc 汇编后，得到的函数 f 汇编代码如下：

```
f:
    pushl   %ebp
    movl    %esp, %ebp
    pushl   %ebx
    movl    8(%ebp), %edx
    movl    12(%ebp), %ebx
    movl    8(%ebp), %eax
    leal    1(%eax), %ecx
    movl    %edx, %eax
    sall    $3, %eax
    addl    %edx, %eax
    addl    %ebx, %eax
    movl    %ecx, array1(,%eax,4)
    movl    12(%ebp), %edx
    movl    8(%ebp), %ebx
    movl    12(%ebp), %eax
    leal    -1(%eax), %ecx
    movl    %edx, %eax
    sall    $4, %eax
    subl    %edx, %eax
    addl    %ebx, %eax
    movl    %ecx, array2(,%eax,4)
    popl    %ebx
    popl    %ebp
    ret
```

问：值 H 和值 J 分别为多少？（8 分）

H = _____

J = _____

三、（20 分）假设我们有一个具有如下属性的系统：存储器是按字节寻址和访问的。地址位宽为 12 位。高速缓存是两路组相联结构（E=2），块大小为 4 字节（B=4），有四个组（S=4）。高速缓存内容如下，所有地址、标记和值都以十六进制表示。

组索引	标记	有效位	字节 0	字节 1	字节 2	字节 3
0	00	1	40	41	42	43
	83	1	FE	97	CC	D0
1	00	1	44	45	46	47
	83	0	-	-	-	-
2	00	1	48	49	4A	4B
	40	0	-	-	-	-
3	FF	1	9A	C0	03	FF
	00	0	-	-	-	-

A. 请给出 12 位主存地址的组成（即给出标志位、组索引和偏移量）；

B. 请问读写 0X409 和 0X831 地址时，是否命中？读出的值是什么？能否写入新值？（请分别给出读写的分析过程）

四、（30 分）若有如下所示代码：

```
#include “csapp.h”
int main() {
        int x=1;
        if (fork()==0)
            printf(“printf1:    x=%d\n”, ++x);
        printf(“printf2:    x=%d\n”, --x);
        exit(0);    }
```

① 此段包含 fork 函数的程序最终会输出什么？**为什么**？（6 分）

② 若有内核发送一个 SIGCHILD 信号，即表示一个子进程停止或终止，此时父进程会做什么工作（简述所调用函数）？什么情况下父进程无法进行该工作，会发生什么？（6 分）

③ **从虚拟内存的角度**，简述 fork 函数创建带有自己独立虚地址空间的新进程的过程（*建议绘制示意图*）。（8 分）

④ 若系统包含页表、TLB，简述 MMU 的地址翻译硬件如何将虚地址翻译到物理地址（设若包括 Cache 和主存）的过程，及对发生不命中时的处理。 （10 分）