

Homework4

Problem 1: Suppose a 32-bit little endian machine has the following memory and register status. Fill in the blanks using 1 byte size and hex. (Value means the evaluated result of the operand. For example, `mov $264, %xxx`, what is stored in `%xxx` now?)

Memory status:

Address	Value
0x100	0x12345678
0x104	0x87654321
0x108	0xaabbccdd
0x10c	0xabcddcba
0x110	0x22446688
0x114	0x77553311

Register status:

Register	Value
%eax	0x102
%ebx	0x2
%ecx	0x4
%edx	0x80

Fill the blanks:

Operand	Value
\$264	0x08(0x108)
0x108	0xdd
%eax	0x02(0x102)
(%eax)	0x34
(%eax, %ebx)	0x21
(%eax, %ebx, 4)	0xbb
0x100(%ebx, %ecx, 2)	0xbb
16(%ecx, %edx, 2)	0x11

Problem 2: Suppose the following C code and assembly code are executed on a **32-bit** little endian machine. 0x08048374 is the starting address of this code and “a” is stored at 0x8(%ebp) while “b” is stored at 0xc(%ebp).

```
void exchange(int *a, int *b)
{
    int tmp = *a;
    *a = *b;
    *b = tmp;
}
```

0x08048374<exahange>:

Line1	08048374	:55	push %ebp
Line2		:89 e5	mov %esp,%ebp
Line3		:83 ec 04	sub \$0x4,%esp
Line4		:8b 45 08	mov 0x8(%ebp),%eax
Line5	__0x0804837d_	:8b 00	mov __(%eax), %eax
Line6		:89 45 fc	mov %eax,-0x4(%ebp)
Line7		:8b 55 08	mov 0x8(%ebp),_%edx_
Line8		:8b 45 0c	mov 0xc(%ebp),%eax
Line9	__0x08048388_	:8b 00	mov (%eax),%eax
Line10		:89 02	mov %eax,(%edx)
Line11		:8b 55 0c	mov _12(%ebp),%edx
Line12		:8b 45 fc	mov -0x4(%ebp),%eax
Line13		:89 02	mov %eax,__(%edx)_
Line14		:c9	leave
Line15		:c3	ret

Suppose the value of %ebp is 0xbffff6a8 and the value of %esp is 0xbffff684 before the instruction Line1 executed, please answer the following questions:

1. After the instruction Line3 is executed, value of %ebp = **0xbffff680** and %esp = **0xbffff67c**.
2. The local variable tmp is stored in **-0x4(%ebp)**.