题目 1

阅读汇编代码，根据唯一的减法可以得到 x 与 c 分别被放置在 edx 和 eax 寄存器里，从而可以由指令后的 l 与 swl 得知它们的大小与所在地址。接着根据改变内存的这一行可以得到 p 和 d 的大小与所在地址。

参数	大小（字节）	地址
c	2	ebp+8
x	4	ebp+20
d	1	ebp+12
p	4	ebp+16

因为参数从右向左入栈，所以函数原型为 func(int x, char *p, char d, short c)

题目 2

（1）

寄存器	value
esp	0x7FFFFFC0
ebp	0x7FFFFFF4

（2）

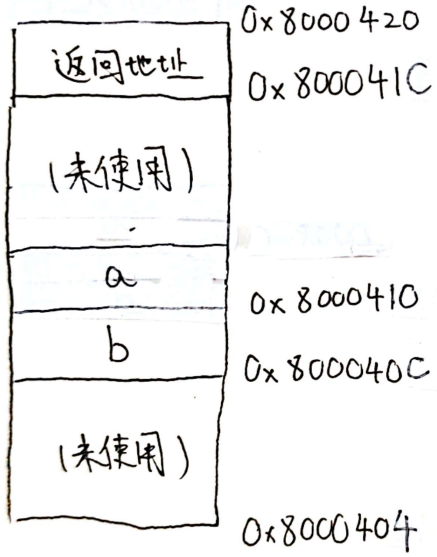
寄存器	value
esp	0x7FFFFFC0
ebp	0x7FFFFFC0

（3）

寄存器	value
esp	0x7FFFFFC4
ebp	0x7FFFFFC4

题目 3

```
int main{
    int a,b;
    scanf("%d %d",&a,&b);
    int c = a ^ b;
    printf("%d %d %d\n",c,b,a);
    return 0;
}
```



%edi = .LC1地址，指向 "%d %d %d\n"

%esi = a^b = c

%edx = b

%ecx = a

%rsp = 0x8000404