

# Homework 11

## Problem I

Read the following codes and fill the given table

```
#include <stdio.h>
int a = 3;
int array[2];
void foo(int arg)
{
    static int b = 1;
    int tmp = b + arg;
    printf("%d\n", tmp);
}
```

1. Indicate the location of the following symbols (.data, .bss, stack etc.)

| Symbol       | Location              |
|--------------|-----------------------|
| <b>a</b>     | <b>.data</b>          |
| <b>array</b> | <b>.bss</b>           |
| <b>foo</b>   | <b>.text</b>          |
| <b>b</b>     | <b>.data</b>          |
| <b>tmp</b>   | <b>stack</b>          |
| <b>%d\n</b>  | <b>.rodata</b>        |
| <b>arg</b>   | <b>stack/register</b> |

## Problem II

Read the following codes and fill the given table

| main.c                                                                                | foo.c                                                                                                                                                                                        |
|---------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>char *me = "I am best" void foo()  int main() {     foo();     return 0; }</pre> | <pre>#include &lt;stdio.h&gt; extern char *me; int n = 1314; static char *s = "I love ipads";  void foo() {     printf("%s %d", s, n); }  static void foo2() {     printf("%s", me); }</pre> |

Indicate the type of the following symbols (defined global, referenced global or local)

| File   | Symbol | Type              |
|--------|--------|-------------------|
| main.c | me     | defined global    |
|        | foo    | referenced global |
| foo.c  | me     | referenced global |
|        | n      | defined global    |
|        | foo    | defined global    |
|        | foo2   | local             |
|        | s      | local             |

## Problem III

```
/* file: hw.c */
#include<stdio.h>
```

```
extern int Fun(void);
static int iNum = 1;
int *pNum = &iNum;
```

```
void fun2(int n)
{ ; }
```

```
void fun3()
{
    fun2(Fun() + *pNum);
}
```

Disassembly of section .text:

00000000 <fun2>:

```
0: 55          push    %ebp
1: 89 e5       mov     %esp,%ebp
3: 5d         pop     %ebp
4: c3         ret
```

00000005 <fun3>:

```
5: 55          push    %ebp
6: 89 e5       mov     %esp,%ebp
8: 83 ec 08    sub     $0x8,%esp
b: e8 fc ff ff ff  call   c <fun3+0x7>
10: 89 c2       mov     %eax,%edx
12: a1 00 00 00 00  mov    0x0,%eax
17: 8b 00       mov     (%eax),%eax
19: 01 d0       add     %edx,%eax
1b: 83 ec 0c    sub     $0xc,%esp
1e: 50          push    %eax
1f: e8 fc ff ff ff  call   20 <fun3+0x1b>
24: 83 c4 10    add     $0x10,%esp
27: c9         leave
28: c3         ret
```

Disassembly of section .data:

00000000 <iNum>:

```
0: 01 00          add     %eax, (%eax)
...
```

00000004 <pNum>:

```
4: 00 00          add     %al, (%eax)
...
```

Complete the following relocation records:

| Relocation Records for [.text]: |            |       |
|---------------------------------|------------|-------|
| OFFSET                          | TYPE       | VALUE |
| 0000000c                        | R_386_PC32 | Fun   |
| 00000013                        | R_386_32   | pNum  |
| 00000020                        | R_386_PC32 | fun2  |
| Relocation Records for [.data]  |            |       |
| 00000004                        | R_386_32   | pNum  |

If Fun is relocated to 0x08048418 and fun3 is relocated to 0x080483d0, what will the underlined instruction be changed to after linking?

**e8 30 00 00 00**