Homework 7

Problem 1

What's the output of the following C program? (on a 32-bit machine)

```
#include <stdio.h>
int main()
{
    static char daytab[3][13] = {
        {100, 111, 32, 121, 111, 117, 32, 119, 97, 110, 116, 32, 97},
        {32, 109, 105, 100, 116, 101, 114, 109, 32, 101, 120, 97, 109},
        {0}
    };
    static char ans[] = "abcdefghijklmnopqrstuvwxyyz";
    printf("%s?\n", daytab);
    printf("%c%c%c!\n",
           (char)(((char **)ans)[3]),
           (char)(((char *)ans)[4]),
           (char)(ans[18]));
    return 0;
}
```

Problem 2

Consider the following declaration:

```
short S[5];
short *T[4];
int **U[3];
double V[2];
char *W[3];
```

And fill in the following blanks:

Array	Size of Element	Size of Array	Start Address	Address of i-th Element
S	2	10	s	s+2*i
T			t	
U			u	
V			v	
W			w	

Problem 3

Consider the following declaration:

```
short S[5][6];
int T[4][2];
float U[3][1];
char *V[2][0];
char*(*(*W[3][4])())[5];
```

And fill in the following blanks:

Array	Size of Element	Size of Array	Start Address	Element	Element addr
S	2	60	s	S[i][j]	s+2*(i*6+j)
T			t		t+20
U			u	U[1][0]	
V			v	/	/
W			w	W[2][1]	

Problem 4

Given a C function

```
1 int proc(void)
2 {
3  int x, y;
4  scanf("%x %x", &y, &x);
5  return x-y;
6 }
```

GCC generates following assembly codes:

```
1 proc:
2     pushl %ebp
3     movl %esp, %ebp
4     subl $24, %esp
5     addl $-4, %esp
6     leal -4(%ebp), %eax
7     pushl %eax
8     leal -8(%ebp), %eax
9     pushl %eax
10 pushl $.LC0 ;Pointer to string "%x %x"
11 call scanf
12 movl -8(%ebp), %eax
13 movl -4(%ebp), %edx
14 subl %eax, %edx
15 movl %edx, %eax
16 leave
17 ret
```

Assume stack pointer register and frame pointer register value are set as follows at the beginning of proc():

%esp 0x800040

%ebp 0x800060

And scanf reads 0x46 and 0x53 from stdin. String %x %x is stored at 0x300070 in memory.

Questions:

A. In line 3, what value is assigned to %ebp

B. Where are local variables x and y stored (Indicate their addresses)

C. What is the value of %esp after line 10

D. Draw a diagram to illustrate the stack frame after scanf returns (p.s. from %ebp to %esp)

E. Indicate the unused stack frame of proc(). (p.s. these areas are allocated to improve the performance of high-speed cache)