16.317: Microprocessor Systems Design I

Fall 2012

Homework 3

Due **Wednesday, 10/31/12, by the end of class (8:50 AM)**

1. *(60 points)* Write a subroutine for each of the operations listed below. Note that:

   - Subroutine arguments are passed on the stack, and can be accessed within the body of the subroutine starting at address EBP+8.
   - At the start of each subroutine:
     - Save EBP on the stack
     - Copy the current value of the stack pointer (ESP) to EBP
     - Create space within the stack for each local variable by subtracting the appropriate value from ESP. For example, if your function uses four integer local variables, each of which contains four bytes, subtract 16 from ESP.
     - Local variables can then be accessed starting at the address EBP-4.
   - A subroutine's return value is typically stored in EAX.

See Lecture 18 for more details on subroutines, the x86 architecture, and the conversion from high-level concepts to low-level assembly.

a. `int fact(int n)`

   Given a single integer argument, `n`, return n! = n × (n – 1) × (n – 2) × … × 1

b. `int max(int v1, int v2)`

   Given two integer arguments, return the largest of the two values.

c. `void swap(int *a, int *b)`

   Given two memory addresses, `a` and `b`, swap the contents of those addresses. You may assume `a` and `b` are offsets into the data segment.

2. *(40 points)* Assume the 80386 is running in protected mode with the state given below. Note that each memory location shown contains a single segment descriptor.

GDTR = 001631A00037
LDTR = 0010
DS = 000E
ES = 001B
SS = 0015

EDI = 0000444A
EBX = 0000F000
EBP = 0000F010

Memory	Address

Base = 030010F0
Limit = 020F
	00163170

Base = 12300020
Limit = 0007
	00163178

Base = A0331010
Limit = 0027
	00163180

Base = FE002200
Limit = FFFF
	00163188

Base = 12340000
Limit = 00FF
	00163190

Memory	Address

Base = AC000000
Limit = 0317
	00163198

Base = 01610200
Limit = 03F7
	001631A0

Base = 00163170
Limit = 0027
	001631A8

Base = 00163180
Limit = 001F
	001631B0

Base = 05000120
Limit = C00F
	001631B8

What address does each of the following instructions access?

a. `MOV DX, [40H]`
b. `XOR ES:[DI], CX`
c. `BSF AX, WORD PTR [BX+100H]`
d. `ADD SS:[BP-16], AX`