Exam 3 Study Guide

Show how to pass argument by reference on stack

```
push   ebp
mov    ebp , esp
sub    esp , 4
lea    eax , [ebp - 4 ]  ;  eax = address of local variable
```

Show how to pass argument by value on stack

```
push   ebp
mov    ebp , esp

mov    eax , [ebp + 8 ]   ; eax = arg1
mov    ecx , [ebp +12 ]   ; ecx = arg2
```

Show how to create a local variable in a procedure

```
push   ebp
mov    ebp , esp
sub    esp , 8

mov    [ ebp - 4 ] , 5    ;  local var1  = 5
mov    [ ebp - 8 ] , 10   ;  local var2 = 10
```

Show how to create a stack frame

```
push ebp
mov ebp, esp
```

Show how to restore the caller's stack frame

```
mov esp, ebp
pop ebp
```

What is enter instruction

It is used to create a stack frame in a procedure
- push EBP on stack
- set EBP to the base of the stack frame
- reserve space for local variables

What is leave instruction

It terminates the stack frame in the procedure
- free local space

What is lea instruction

stores the address of a local variable into a register

What is recursion

a procedure that calls itself

A procedure X calls procedure Y the Y calls X

What are cld, std

cld clear the direction flag

std set the direction flag

The direction flag controls the inc or dec of ESI and EDI

What are movsb, movsw, and movsd instructions and what do they do?

copy data at the address pointed by esi into the address pointed by edi

After the operation esi and edi automatically increment or decrement, based on the DF, by 1, 2, and 4 respectively

What are cmpsb, cmpsw, and cmpsd instructions and what do they do?

Compare the address pointed by esi to the address pointed by edi

What are scasb, scasw, and scasd instructions and what do they do?

Compare a value in AL | AX | EAX to a byte, word, dword, respectively, addressed in EDI

search for a specific element in a string or array

What are stosb, stosw, and stosd instructions and what do they do?

store the value in AL | AX | EAX respectively into the address pointed by EDI

What are lodsb, lodsw, and lodsd instructions and what do they do?

load a byte, word, dword into AL/AX/EAX respectively from the address offset pointed by esi

What is struct?

a preprocessor marco

a collection of data

What is string? Why does string have to be null terminated?

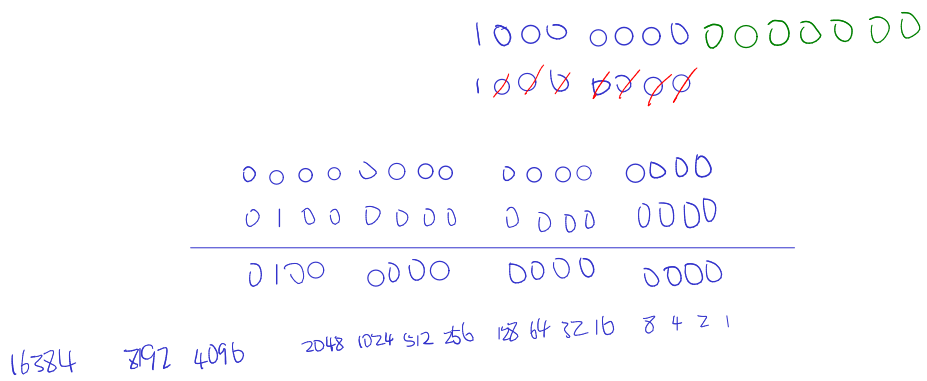
String is an array of characters

Null at the of the string marks the end of the string Many operations can check for the Null so they know when to stop

Binary Multiplication

128 x 128

= 16384



93 x 45 = 4185