Assembly Questions

Question Responses for Assignment 3

Chris Klassen & Alex Kabak

2016

# Question A

# Question B

# Question C

# Question F

# Question G

## Pass by Value Function

mov eax, DWORD PTR \_number$[ebp]

push eax

call ?plusOne@@YAHH@Z

add esp, 4

mov DWORD PTR \_number$[ebp], eax

## Pass by Reference Function

lea eax, DWORD PTR \_number$[ebp]

push eax

call ?plusOneRef@@YAHAAH@Z

add esp, 4

mov DWORD PTR \_number$[ebp], eax

## Differences

When passing by value, the assembler moves the value **number** to eax and then pushes it to the stack so that it can be used by the function. After the function returns, the number is pulled out of eax (where it was returned to) and assigned to **number** once again.

When passing by reference, the assembler retrieves the address of **number** and pushes it to the stack. This address is then pushed to the stack to be used by the function in retrieving the actual value of the number. After the function returns, the return value is assigned to **number** normally.

# Question H

## Function Code

?timesTwo@@YAHXZ PROC

push ebp

mov ebp, esp

sub esp, 192 push ebx

push esi

push edi

lea edi, DWORD PTR [ebp-192]

mov ecx, 48

mov eax, -858993460

rep stosd

mov eax, 12

pop edi

pop esi

pop ebx

mov esp, ebp

pop ebp

ret 0

?timesTwo@@YAHXZ ENDP

## Inline Code

mov DWORD PTR \_numberB$[ebp], 12

## Differences

In the function code, quite a bit of overhead work must be done besides the very simple mathematical calculation. The function must store the existing base pointer, and also update the base pointer and stack pointer and other registers on the CPU. Then, it can calculate the result and put it in eax to be returned. After this is done, cleanup must be done to ensure that when the function returns, the program can continue properly.

In the inline code, the assembler simply puts the mathematical result into **numberB** and continues on its way, with far less overhead.