Due date passed
X

(https://swayam.gov.in) (https://swayam.gov.in/nc_details/NPTEL)

umar97faruk@gmail.com

NPTEL (https://swayam.gov.in/explorer?ncCode=NPTEL) » C Programming and Assembly Language (course)

Announcements (announcements) **About the Course (https://swayam.gov.in/nd1_noc19_cs44/preview)**

Ask a Question (forum) Progress (student/home) Mentor (student/mentor)

Unit 5 - Week 3

Register for Certification exam (http://nptelonlinecourses.iitm.ac.in/)

Course outline

How to access the portal?

Pre-Requisite Assignment

Week 1

Week 2

Week 3

- ● Lecture 11 (unit?unit=18&lesson=19)
- ● Lecture 12 (unit?unit=18&lesson=20)
- ○ Lecture 13 (unit?unit=18&lesson=21)
- ○ Lecture 14 (unit?unit=18&lesson=22)

Assignment 3

Assignment not submitted **Due date: 2019-08-21, 23:59 IST.**

Instructions:

- Ignore any syntax errors, if any. All programs are assumed to compile successfully
- The focus in this assignment is on the PROLOGUE and EPILOGUE of functions
- Mnemonics that you fill should necessarily be one from the list below.

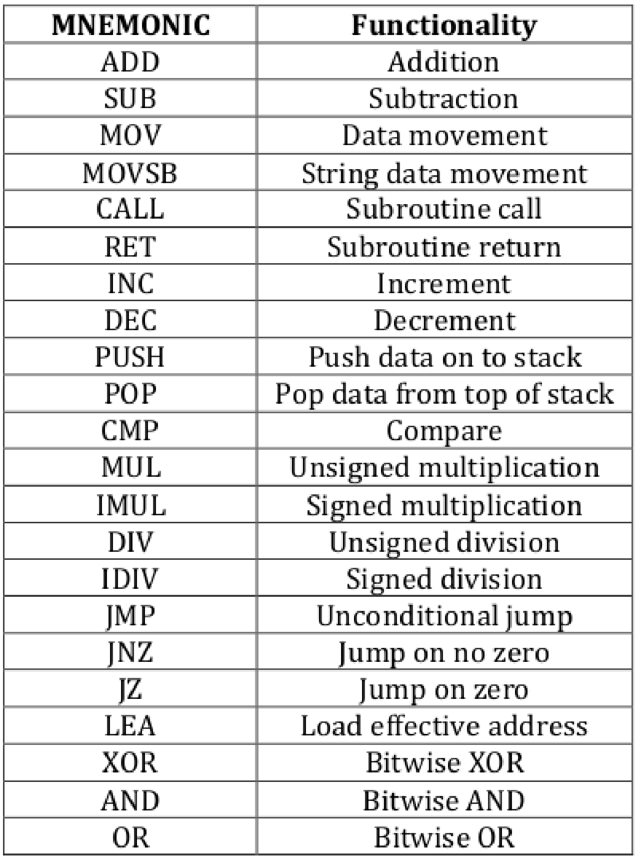
○ Lecture 15 (unit?unit=18&lesson=23)

○ **Quiz : Assignment 3 (assessment?name=40)**

○ Week 3 Feedback : C Programming and Assembly Language (unit?unit=18&lesson=41)

Week 4

DOWNLOAD VIDEOS



MNEMONIC	Functionality
ADD	Addition
SUB	Subtraction
MOV	Data movement
MOVSB	String data movement
CALL	Subroutine call
RET	Subroutine return
INC	Increment
DEC	Decrement
PUSH	Push data on to stack
POP	Pop data from top of stack
CMP	Compare
MUL	Unsigned multiplication
IMUL	Signed multiplication
DIV	Unsigned division
IDIV	Signed division
JMP	Unconditional jump
JNZ	Jump on no zero
JZ	Jump on zero
LEA	Load effective address
XOR	Bitwise XOR
AND	Bitwise AND
OR	Bitwise OR

Section-1- Answer the following True/False questions:

1) The calling conventions __cdecl is used when the calling function cleans up the stack and __stdcall is used when stack clean up happens within the function *1 point*

● True

○ False

2) Double Indirect addressing i.e. [[EAX-4]] is possible in the x86 architecture? *1 point*

○ True

● False

3) When a function call is made using CALL instruction, before transferring the control to the new location, the return address is pushed onto the stack. *1 point*

● True

○ False

4) For every operation on ESP, a counter operation must be performed, on ESP, failing which execution will resume from a random location when RET is called. *1 point*

● True

○ False

5) When a member variable is set inside a member function of a C++ class, the object loses the value once you return to the calling function where the object is instantiated *1 point*

○ True

● False

Section-2- Answer the following Multiple Choice/ Select Questions:

6) If a function **f2( )** is called from **main( )** function and if the declaration of **f2( )** is missing from the file that is being compiled, what kind of error is generated if any? ***1 point***

● Compiler Error
○ Linker Error
○ Assembler Error
○ None!! Calling a function is an implicit form of declaration

7) Assuming that the declaration of the function **f2( )** exists in the above question, however,the definition of the function **f2( )** does not exist in any file that was compiled, what kind of error is generated, if any? ***1 point***

○ Compiler Error
● Linker Error
○ Assembler Error
○ None!!

8) What are the operations performed by the RET N instruction? ***1 point***

□ Adds the value of N to ESP.
□ Pops out the value of EBP, so as to return to its initial value (value before the function call)
☑ Pops top of the stack to Instruction Pointer so as to return to the caller
☑ Copies the value of N to EAX before returning to the callee

9) Local variables in a function can be accessed as ***1 point***

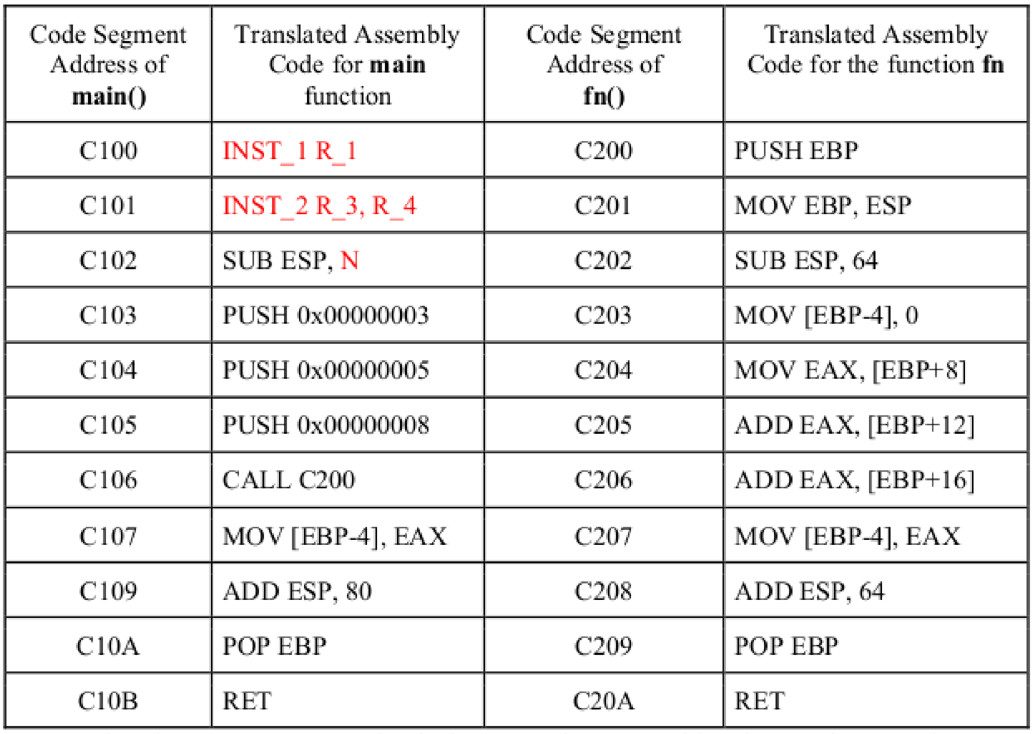
○ [ESP-N]
○ [ESP+N]
● [EBP-N]
○ [EBP+N]

10)A function with NO return value i.e. a void function ***1 point***

□ Does not require the RET instruction
□ Does not require a PROLOGUE
☑ Requires an EPILOGUE
☑ Requires the RET instruction

The following C program is compiled to the assembly equivalent code shown below. The values/ instructions in RED are missing and needs to be identified by you. Answer questions 11-20

```
/************** C Program ****************/
int fn(int x, int y, int z)
{
    int a = 0;
    a = x+y+z;
    return a;
}
void main()
{
        1. int z;
        2. z = fn(N1, N2, N3);
}
/*********** C Program End **************/
```



Code Segment Address of **main()**	Translated Assembly Code for **main** function	Code Segment Address of **fn()**	Translated Assembly Code for the function **fn**
C100	INST_1 R_1	C200	PUSH EBP
C101	INST_2 R_3, R_4	C201	MOV EBP, ESP
C102	SUB ESP, N	C202	SUB ESP, 64
C103	PUSH 0x00000003	C203	MOV [EBP-4], 0
C104	PUSH 0x00000005	C204	MOV EAX, [EBP+8]
C105	PUSH 0x00000008	C205	ADD EAX, [EBP+12]
C106	CALL C200	C206	ADD EAX, [EBP+16]
C107	MOV [EBP-4], EAX	C207	MOV [EBP-4], EAX
C109	ADD ESP, 80	C208	ADD ESP, 64
C10A	POP EBP	C209	POP EBP
C10B	RET	C20A	RET

Assume that the operating system loads the EIP with C100 and hands over the control to the following program. EIP is treated as a 16 bit address for brevity by dropping the high 16 bits which are all zeros.

In Line 2 of the C Program in **main( )**, which calls the function **fn( )**, as fn(N1, N2, N3).The decimal values of N1, N2 and N3 are:

11)N1 value = __________ ?

8

1 point

12)N2 value = _________ ?

5

1 point

13)N3 value = ________ ?

3

1 point

In the PROLOGUE of **main( )**, the instrction at C100 is

14)nstruction INST_1 = __________?

PUSH

Hint

Choose one mnemonic from the list given initially

1 point

15)Register R_1 = ________ ?

EBP

1 point

In the PROLOGUE of **main( )**, the instrction at C101 is

16)nstruction INST_2 = _______ ?

MOV

Hint

Choose one mnemonic from the listgiven initially

1 point

17)Register R_3 = ________ ?

EBP

1 point

18)Register R_4 = ________ ?

ESP

1 point

19)n the PROLOGUE of **main( )**, the instrction at C102 - SUB ESP, N, the value of N is =______ ?

40

1 point

20)ndicate a problem that may be encountered during the execution of the program, if any ***1 point***

- ● The base pointer of the caller is not saved when entering **fn( )**
- ○ Effect of pushing function parameters on to stack when calling **fn( )** is not undone
- ○ Local variable space is not allocated in **fn( )**
- ○ The program does NOT suffer any problem during execution

21)Which register is used by the function **fn( )** to return the integer value to to the caller function? ***1 point***

- ● EAX
- ○ EBX
- ○ ECX
- ○ EDX

22)The local variable z in main() is stored in location [EBP-K]. K=_____ ?

4

1 point

23)Assume that the microprocessor has just executed the instruction at C106 then EIP = 0x______ ?

C20A

Hint

Exclude the “0x” prefix. Enter only the lower 16 bits of the hexadecimal answer

1 point

24)Assume that the microprocessor has just executed the instruction at C106 then value on the top of stack i.e. [ESP] = 0x______ ?

64

Hint

1 point

25)Value of the local variable z when the EIP reaches C10B = ___________ ?

16

1 point

You may submit any number of times before the due date. The final submission will be considered for grading.

Submit Answers