23K-0019

COAL ASSIGNMENT 2

Date

Q1

(i) CMP performs subtraction without modifying any of the operands. It updates the required flags. CMP is a non-destructive instruction. On the other hand, SUB performs actual subtraction and stores the result in the destination operand.

Example:

```
CMP eax,3
jz zero ; jumps if eax-3=0.
SUB eax,2 ; eax = eax-2.
```

(ii) 1) Runtime stacks are used as temporary storage for registers.
2) Return addresses for CALLS are saved in stacks.
3) To pass function arguments.
4) To store local variables.

(iii) JMP doesn't keep track of where to return. It just jumps to the target label without knowing where to return afterwards.

(iv) LAHF loads the status flags into the AH register.
SAHF restores the flags values from the AH register.

(v) POP instruction will immediately remove the return address from the stack causing the program to crash.

(vi) Calling a user-defined procedure without using RET instruction will likely crash the program due to uncontrolled execution.

Date

Q2

(a) a: AL = EFh
b: AL = 30h
c: AL = DBh
d: AL = 18h
e: AL = B7h

(b) AX = FFFEh
CX = 0Fh ; IS push AX onto stack
; LOOP execution.
AX = FFEFh
DX = FFFEh

Q3:

(a)
```
.data
    val1  SDWORD  ?
    x     SDWORD  ?
.code
    main PROC
    CMP  val1, ecx
    jle  else_cond
    CMP  ecx, edx
    jle  else_cond
    MOV  x, 1
    else_cond:
        MOV  x, 2
```

(b) ESP = 00001FFBh