Short Notes Chapter 10 (Lecture 28-29):

The three flags not used for mathematical operations are:

1. the direction flag,
2. the interrupt flag and
3. the trap flags

If the **trap flag is set**, the after every instruction a type 1 interrupt will be automatically generated. This is named as the single step interrupt. This is like the divide by zero interrupt which was never explicitly invoked but it came itself. The debugger is made using this interrupt.

INT 1 function: It allows one instruction to be executed and then return control to us. It has its display code and its code to wait for the key in the INT 1 handler. Therefore, after every instruction the values of all registers are shown and the debugger waits for a key.

Another interrupt used by the debugger is **the break point interrupt INT 3**.

INT 3 has a single byte opcode so it can replace any instruction. To put a breakpoint the instruction is replaced with INT 3 opcode and restored in the INT 3 handler. The INT 3 opcode is placed again by a single step interrupt that is set up for this purpose after the replaced instruction has been executed.

Note: There is no instruction to set or clear the trap flag like there are instructions for the interrupt and direction flags.

PUSHF and POPF:

We use two special instructions PUSHF and POPF to push and pop the flag from the stack.

We use PUSHF to place flags on the stack, change TF in this image on the stack and then reload into the flags register with POPF. The single step interrupt will come after the first instruction after POPF.

The interrupt mechanism automatically clears IF and TF otherwise there would an infinite recursion of the single step interrupt.

The TF is set in the flags on the stack so another interrupt will come after one more instruction is executed after the return of the interrupt.

👉 Also Recommended: CS401 SHORT NOTES CHAPTER 1-7 Midterm