ASSEMBLY

Dato il codice in Assembly per la CPU x86 allegato qui di seguito, identificare lo scopo di ogni istruzione, inserendo una descrizione per ogni riga di codice. Ricordate che i numeri nel formato 0xYY sono numeri esadecimali. Per convertirli in numeri decimali utilizzate pure un convertitore online, oppure la calcolatrice del vostro computer (per programmatori).

1. 0x00001141 <+8>: mov EAX,0x20
2. 0x00001148 <+15>: mov EDX,0x38
3. 0x00001155 <+28>: add EAX,EDX
4. 0x00001157 <+30>: mov EBP, EAX
5. 0x0000115a <+33>: cmp EBP,0xa
6. 0x0000115e <+37>: jge 0x1176 <main+61>
7. 0x0000116a <+49>: mov eax,0x0
8. 0x0000116f <+54>: call 0x1030 <printf@plt>

* **l'indirizzo esadecimale**, indica la posizione in memoria dell'istruzione a cui fa riferimento. Nel primo caso l'indirizzo è 0x00001141.
* **offset** o uno spostamento rispetto all'indirizzo di base. Nel primo caso, il +8 significa che l'istruzione a cui fa riferimento è situata a 8 byte dall'inizio del blocco di codice o della funzione.

I seguenti valori valori esadecimali sono stati convertiti dal convertitore di seguito riportato <https://www.rapidtables.org/it/convert/number/hex-to-decimal.html?x=0x20>

Scopo delle seguenti istruzioni:

1. mov EAX, 0x20: Copiail valore esadecimale 0x20 nel registro EAX. Imposta il valore 32 in EAX.
2. mov EDX, 0x38: Copia il valore esadecimale 0x38 nel registro EDX. Imposta il valore 56 in EDX.
3. add EAX, EDX: Copia il contenuto di EDX al registro EAX. Ora EAX contiene la somma di 32 e 56, che è 88.
4. mov EBP, EAX: Muove il valore contenuto nel registro EAX nel registro EBP. Ora EBP contiene 88.
5. cmp EBP, 0xa: Compara il valore contenuto nel registro EBP con il valore esadecimale 0xa (che è 10 in decimale).

L'istruzione CMP (compare) confronta due operandi senza effettuare alcuna modifica

Lo scopo del CMP è quello di vedere se i flag ZERO FLAG e CURRY FLAG vengano attivate, in base al risultato dell’operazione possono attivarsi o meno questi flag:

SATUS FALG: sono dei segnalini che servono a tener traccia di un operazione eseguita dalla CPU

ZERO FLAG: se il risultato dell’operazione è 0

CURRY FLAG: se nel risultato ci sono riporti

1. jge 0x1176 <main+61> Salta all'indirizzo 0x1176 se il risultato della comparazione precedente è maggiore o uguale.

I Salti Condizionali utilizzano il contenuto dei flags per determinare se «saltare» o meno ad una data locazione.

Jge salta in una locazione specifica se la destinazione è maggiore o uguale alla sorgente nell’istruzione cmp

<main+61> indica 61 byte più avanti della funzione main (princiaple)

1. mov eax, 0x0: Se la comparazione precedente (CMP) è falsa (il valore in EBP non è maggiore o uguale a 10), il programma imposta EAX a 0.
2. call 0x1030 <printf@plt>: indica che il programma sta chiamando la funzione printf per eseguire operazioni di stampa a schermo, e l'indirizzo 0x1030 è associato alla sua posizione nella tabella delle procedure di collegamento dinamico.

call dire al programma di eseguire un certo blocco di codice (una funzione) e poi tornare al punto da cui è stato chiamato una volta completato il suo compito.