S10L3

Consegna:

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.

```
0×00001141 <+8>:    mov    EAX,0×20
0×00001148 <+15>:   mov    EDX,0×38
0×00001155 <+28>:   add    EAX,EDX
0×00001157 <+30>:   mov    EBP, EAX
0×0000115a <+33>:   cmp    EBP,0xa
0×0000115e <+37>:   jge    0×1176 <main+61>
0×0000116a <+49>:   mov    eax,0×0
0×0000116f <+54>:   call   0×1030 <printf@plt>
```

Esecuzione:

La consegna prevede la spiegazione delle funzioni in assembly riportate di sopra.

La prima riga usa la funzione mov, che è utilizzata per spostare un determinato dato o variabile in una determinata locazione di memoria o registro. In questo caso richiede di spostare il valore esadecimale 0x20 (che equivale a 32 in decimale) nel registro EAX.

Anche la seconda utilizza la funzione mov, tuttavia, vengono cambiati i parametri: più nello specifico richiede di spostare il valore esadecimale 0x38 (che equivale a 56) nel registro EDX.

La terza utilizza la funzione add che in assembly corrisponde alla funzione somma, in particolare somma il contenuto dei due registri EAX e EDX e li riporta in EAX. Abbiamo visto prima che i valori riportati sono 32 e 56 che sommati danno come risultato 88 (che convertito in esadecimale è uguale a 0x58).

La quarta richiede di spostare i valori di EAX su EBP portando il valore di EBP a 88.

La quinta fa riferimento all'istruzione cmp che controlla se il valore di due dati/variabili siano uguali, in base al risultato va a modificare dei flag del registro EFLAG, in questo caso non andrà a modificare nessun flag perché il valore attribuito a EBP, ovvero 88, è maggiore di a, che in esadecimale è 10.

La sesta utilizza l’istruzione jump che compie uno spostamento in un’altra sezione di memoria al verificarsi di determinate condizioni. Nel caso riportato la funzione è jge che si trasferisce nella sezione di memoria 0x1176 solamente nel caso in cui il primo parametro dell’istruzione precedente sia maggiore o uguale al secondo parametro. In questo caso 88>10 e quindi si compie il trasferimento della memoria.

La settima sovrascrive con 0 il valore di EAX.

L’ottava utilizza l’istruzione call che fa riferimento alla funzione printf che arriva alla cella di memoria 0x1030