

[**Offensive Hacking Tractical And Stratagic**](https://courseweb.sliit.lk/course/view.php?id=3250)

BIGBANG THEORY

*I.L.Basnayake*

*IT16064164*

Sheldon1 is opened via the GDB. phase\_2 calls a function by the name of read\_6\_numbers. It looks the input has six integers in it, each separated by a space. our answer takes the format a b c d e f where a-f are integers. The function is looping over its input. After %eax is compared to (%esi, %ebx, 4) at <+54>, %ebx gets incremented and, as long as its less than 5, the function jumps back to above the comparison so that it can do it again. This means that our input integers will probably be a pattern of some sort, where <+46> is where the math that increments the pattern happens. Key found was 1 2 6 24 120 720. The steps which I obtained the key is below with the workings.



