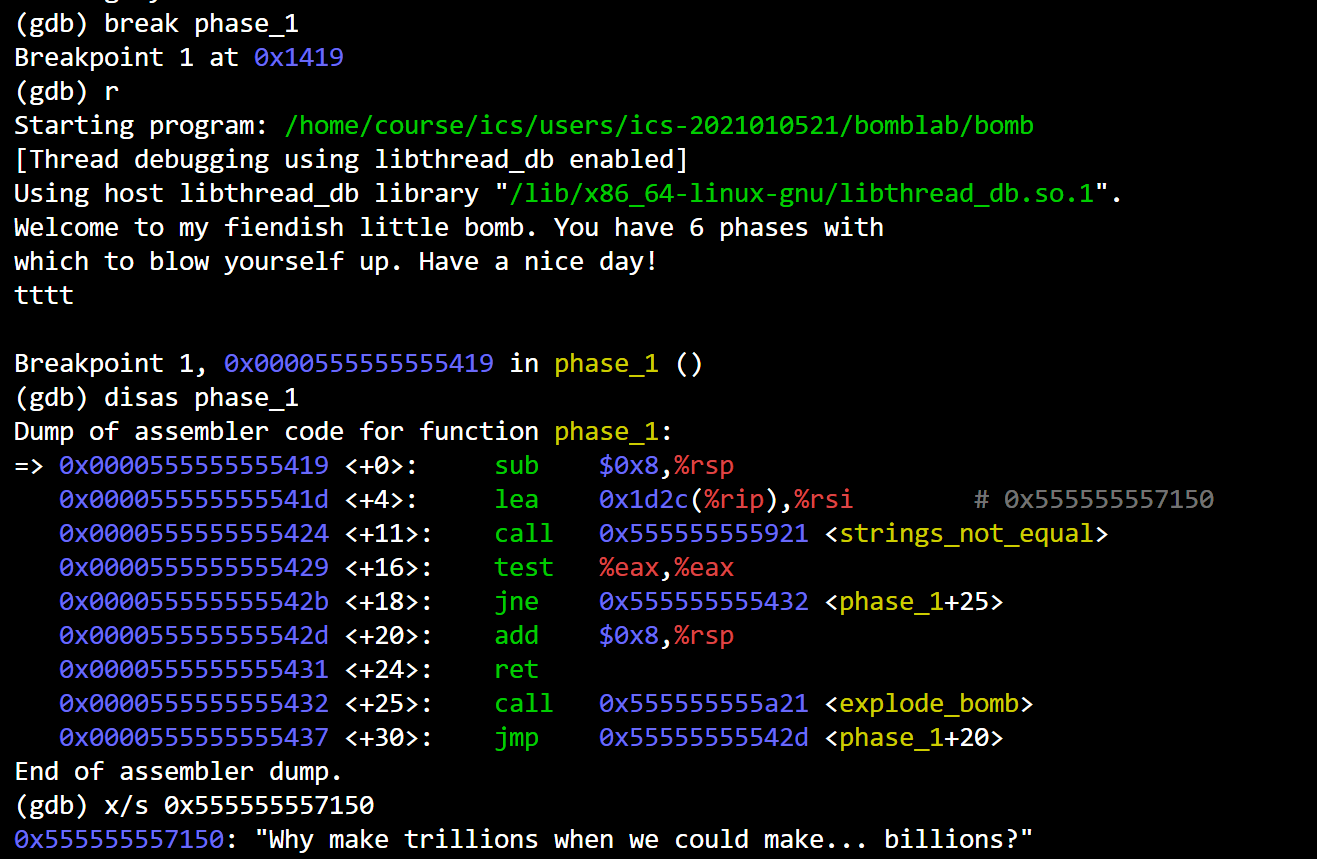
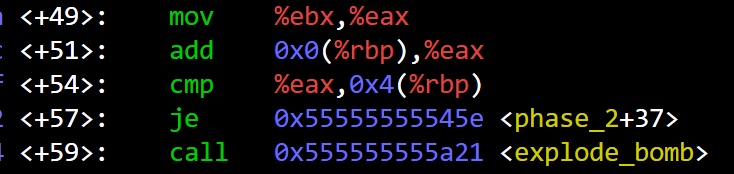
Phase\_1



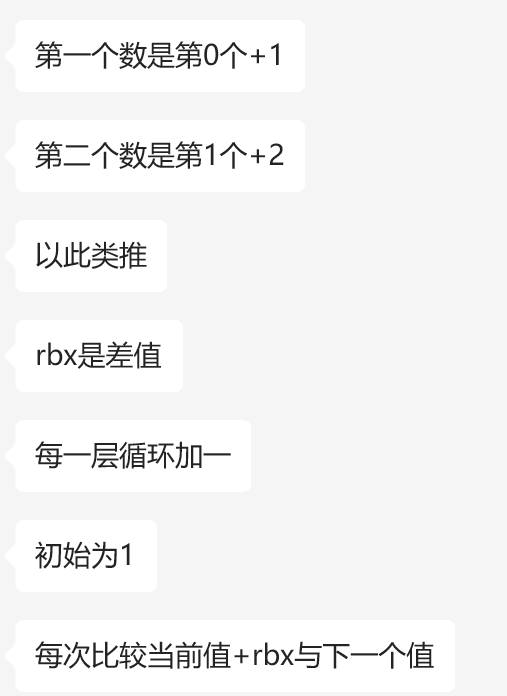
Phase\_2

rdx/ebx是用来存当前是第几个数的

关键几行：

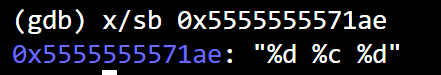






Phase\_3

输入格式：



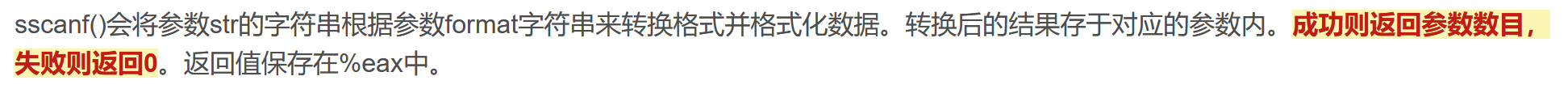
rdi : input

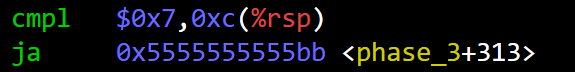
rsi : “%d %c %d”

rdx :

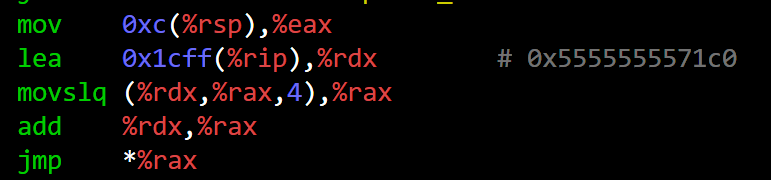
rcx :

r8 :

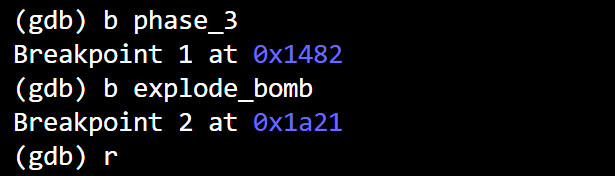


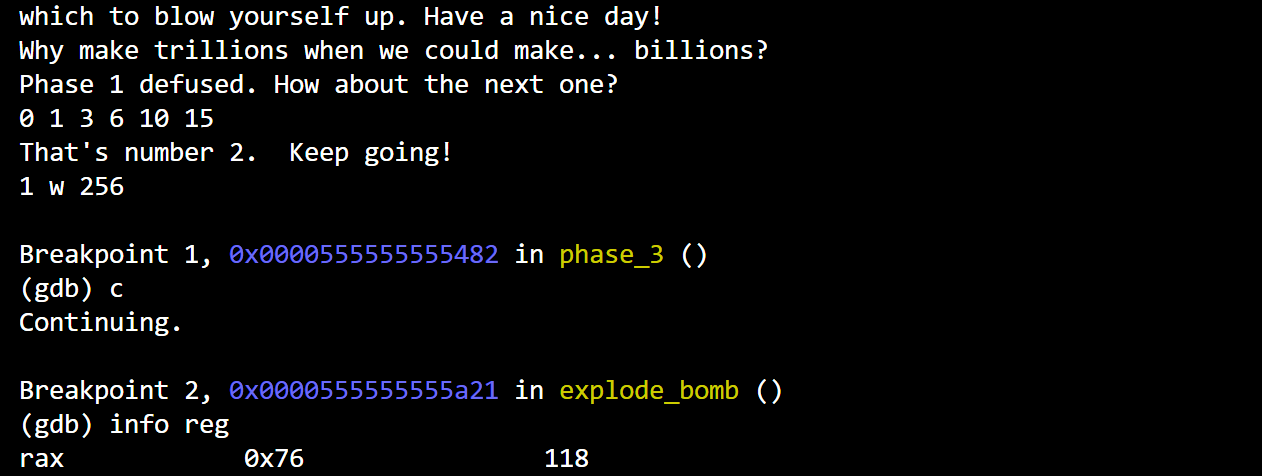
  
说明rdx小于7

Switch-case:

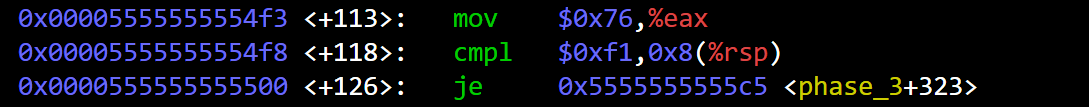


调试信息：

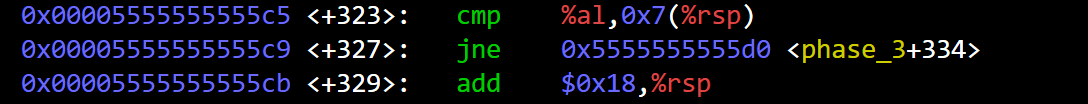




所以是汇编代码跳到：



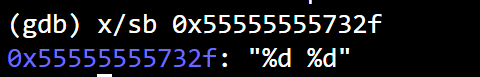
r8 = 0xf1 = 241

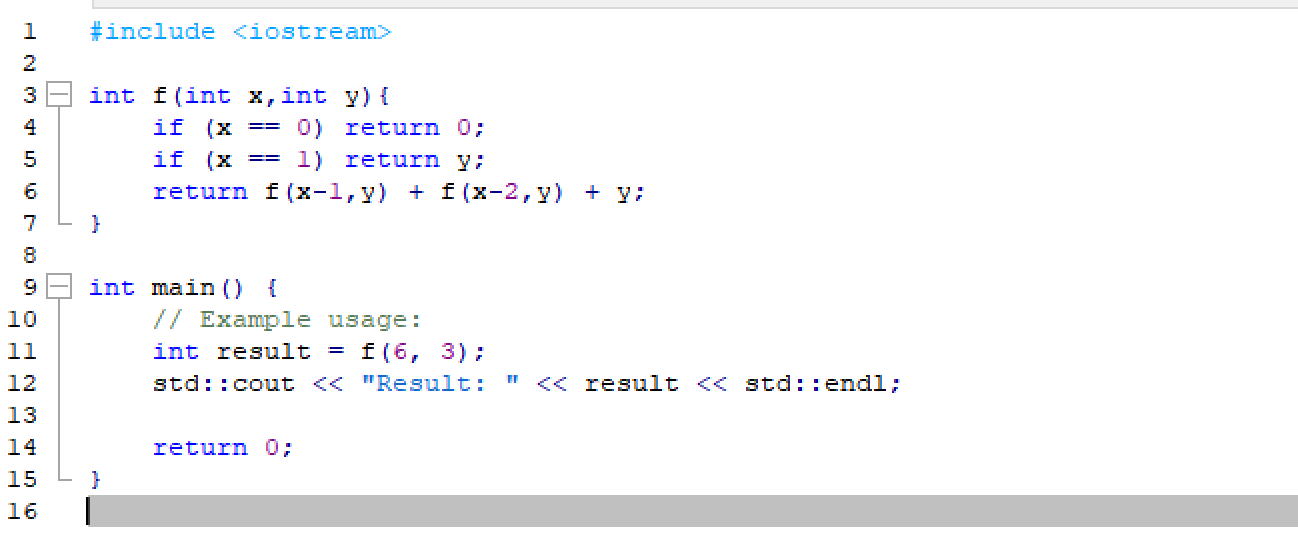


rcx的ACSII码为0x76即118

Phase\_4

格式：



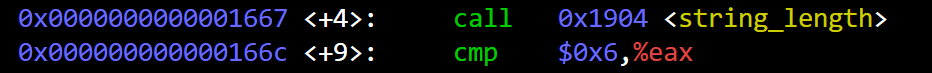


递归

eax = func4(6, rcx)

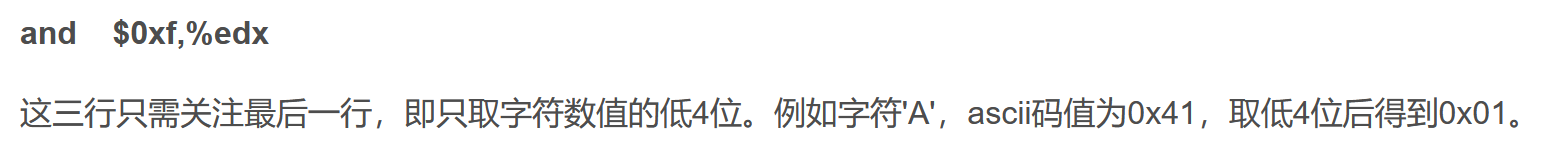
edx = eax

Phase\_5

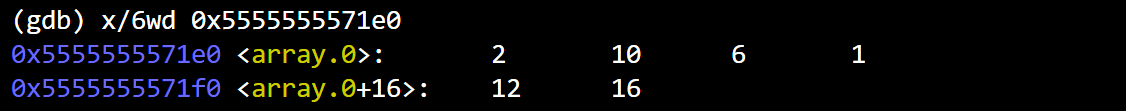


输入的字符串长度为6

cmp $0x32,%ecx  
最后ecx要等于0x32即50







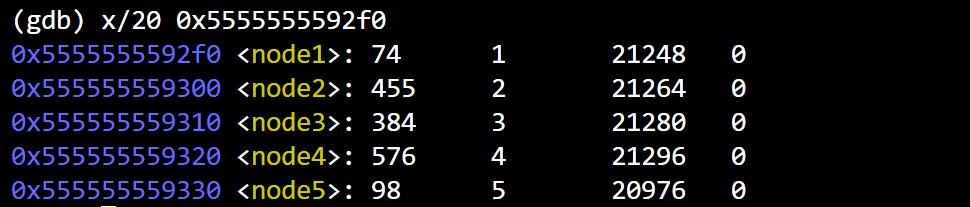
取数组中的值使得和为50：

50=16+16+12+2+2+2

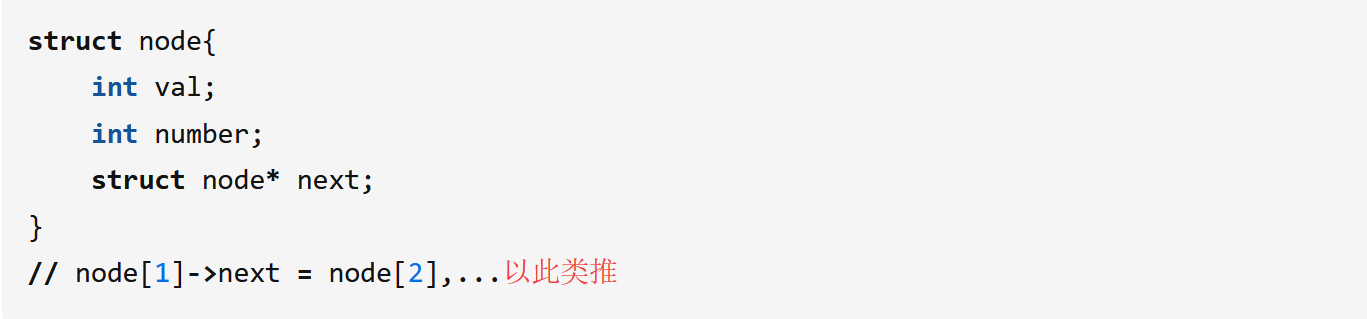
对应的数组下标偏移量为5 5 4 0 0 0

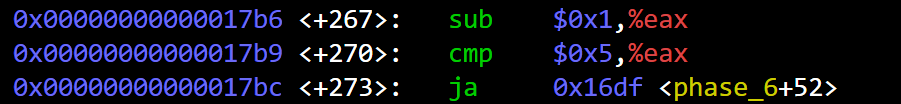
可以取eedppp（利用ASCII码）

Phase\_6



是个链表：





eax减1后≤5，所以输入的数均≤6

笔记见goodnotes

参考：

<https://wdxtub.com/csapp/thick-csapp-lab-2/2016/04/16/>

<https://blog.csdn.net/qq_37500516/article/details/113789606>

<https://cloud.tencent.com/developer/article/1957972>

<https://zhuanlan.zhihu.com/p/472178808>