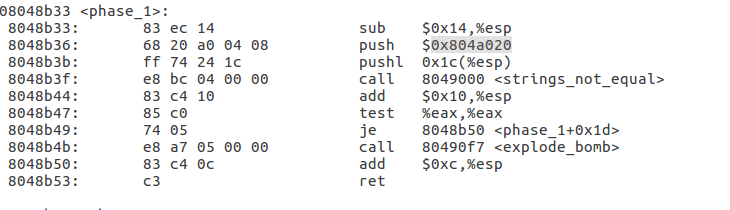
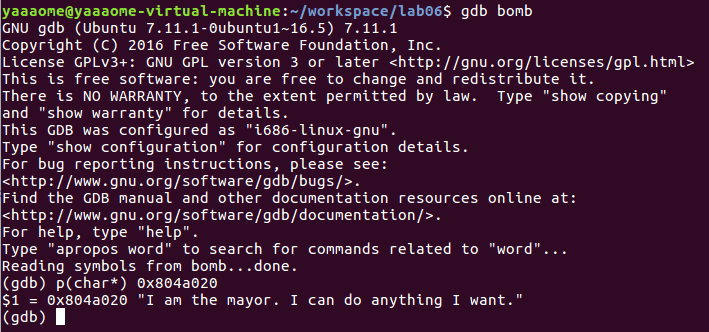
综合实验报告

吴紫航 171860659

Phase1

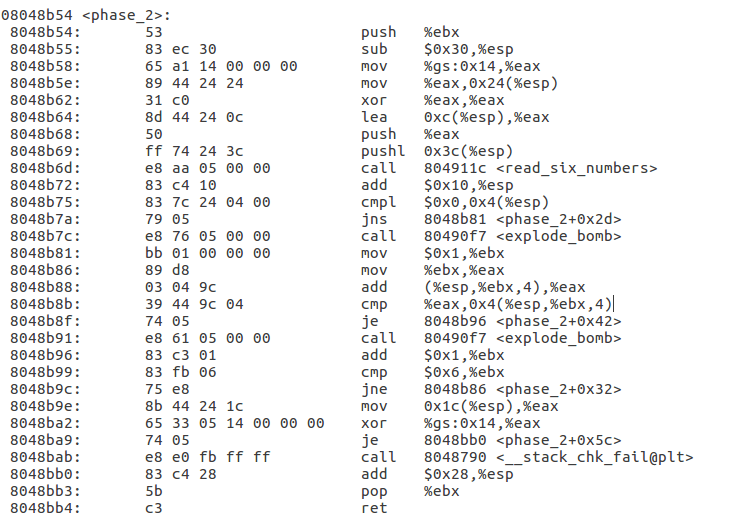
由汇编第二行的地址0x804a020，在gdb中输入p(char\*) 0x804a020可找到对应的字符串





所以phase1答案是I am the mayor. I can do anything I want.

Phase2



因为循环中每一项等于上一项加上本项的下标，第一项是0，所以第二项是0+1，第三项是1+2，第四项是3+3，第五项是6+4，第六项是10+5

所以phase2的答案是 0 1 3 6 10 15

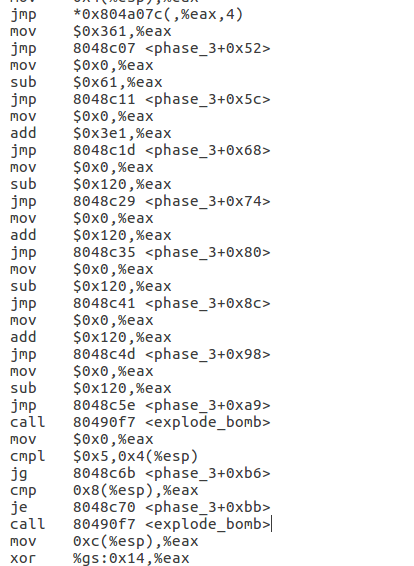
Phase3

由题意输入的第一个数要比1大比7小

跳转表由汇编代码为：

1. 0x(361-61+3e1-120+120-120+120-120)
2. 0x(-61+3e1-120+120-120+120-120)
3. 0x(3e1-120+120-120+120-120)
4. 0x(-120+120-120+120-120)
5. 0x(120-120+120-120)
6. 0x(-120+120-120)
7. 0x(120-120)
8. 0x(-120)

不妨取第一个参数是2，则第二个参数由表算出为3e1-120=2c1=2\*256+12\*16+1=705



所以phase3答案为2 705（不唯一）

Phase 4

由phase\_4代码部分可知道一共有两个参数输入，因为sscanf返回值是2，此外第二个参数得值要小于等于4，并且func4函数第一个参数是9，第二个参数设为n，由func4部分函数可以知道，该函数的c形式如下

Int func4(int a,int b)

{

If(a==0)return 0;

If(a==1)return n;

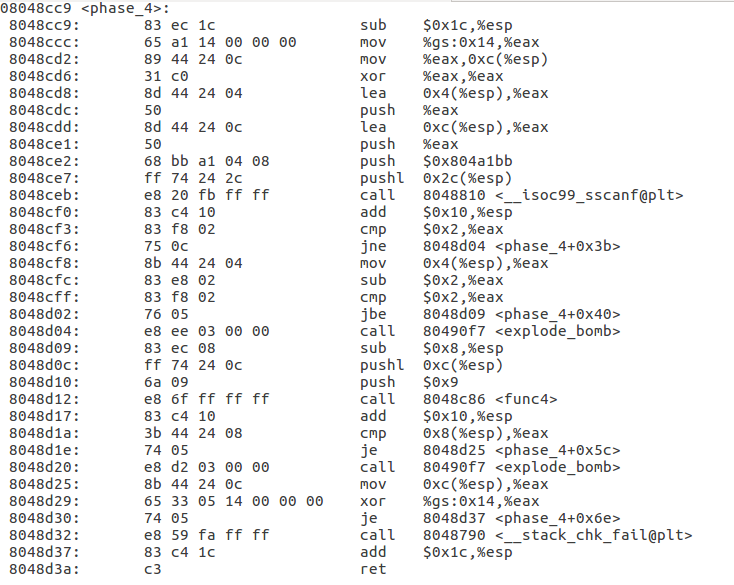
Return func(a-1,b)+func(a-2,b)+b;

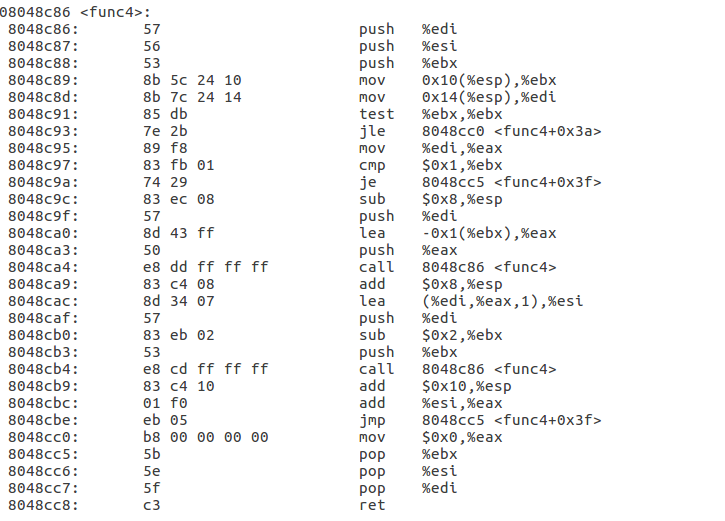
}

不妨取第二个参数是4，则带入运算func4（9，4）结果是352

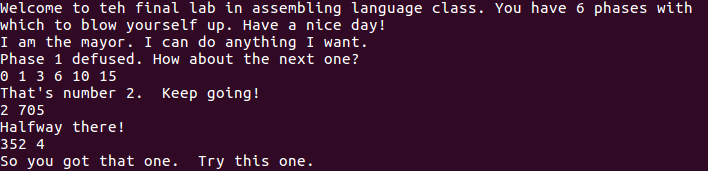
所以phase4的答案是352 4

（不唯一）





完成phase1-phase4，如图



Phase5、Phase 6、Secret phase未完成