两种解法

1. 直接根据关键函数猜测需要进入case4和case5一次即可得到flag字符串

写exp注意是小端序

2.linux下动态调试打补丁，因为主要学的是od，linux下的gdb不太懂怎么打补丁就用ida远程调试了，这次调试发现的有两点，动调补丁要调试后打不能静态打完补丁再调试，这样的话补丁会只停留再静态，动调的时候还是原来的样子，二是发现了撤销上一个补丁的按键