writeup

1. 题目给出一个windows可执行程序，运行可以发现是一个类似于魔塔的命令行游戏。
2. 通过交叉引用和字符串，可以发现在游戏通关时会检测一个计数器的值，需要等于5才能输出flag。
3. 对5处修改了计数器的位置进行分析，第一处是在判断按键处，通过一个状态机隐藏了一个whosyourdaddy指令，输入即可解锁第一个计数器，secret1为whosyourdaddy。
4. 第二个计数器在伤害计算处，需要伤害值的md5等于一个固定值，注意这里md5的长度是16，要在后面补零，爆破可以得到伤害为666，secret2即为666。
5. 第三个计数器需要触发一个隐藏事件，首先需要在商店购买特殊道具MAGIC BOX（需要修改金钱），然后在第二层一个空洞前按t键即可打开通道，走到尽头拿到secret3，secret3为空洞内的行进路径aaawaassassssaawwwwwwaaaassdd。
6. 第四个计数器需要进入隐藏地图，首先要在第7层打开开关得到隐藏钥匙，然后回到入口左下角进入隐藏房间。secret4是拿到钥匙的坐标+入口坐标+隐藏地图内传送门坐标+出口坐标，即38,8、10,13、32,6和26,7，secret为38,810,1332,626,7
7. 第五个计数器通关即可拿到，这里会计算文件text段的crc值并转为无符号int，计算可得secret为693666165。
8. 最后的flag通过rc4算法进行解密，key为五个secret相连，解密即可得到flag。
9. 除了手动解密flag密文之外，也可以使用修改器修改金钱和攻击力，然后手玩通关拿到flag，可见视频文件夹中的通关视频。