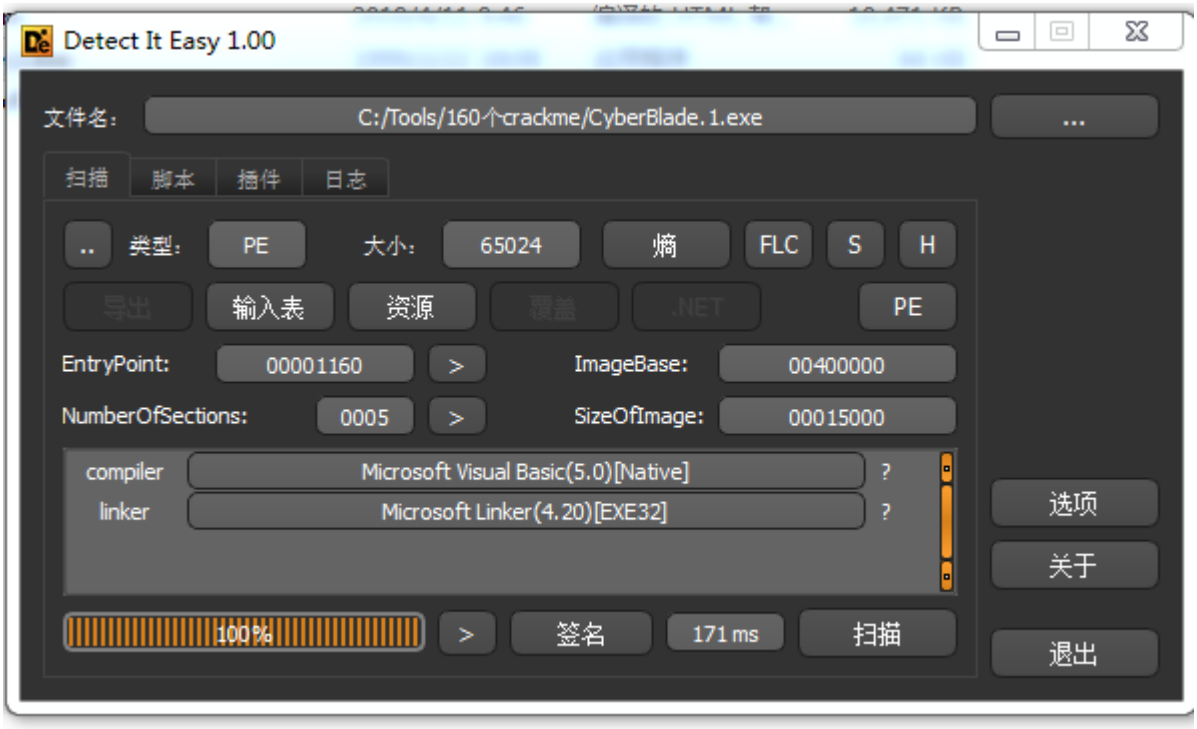
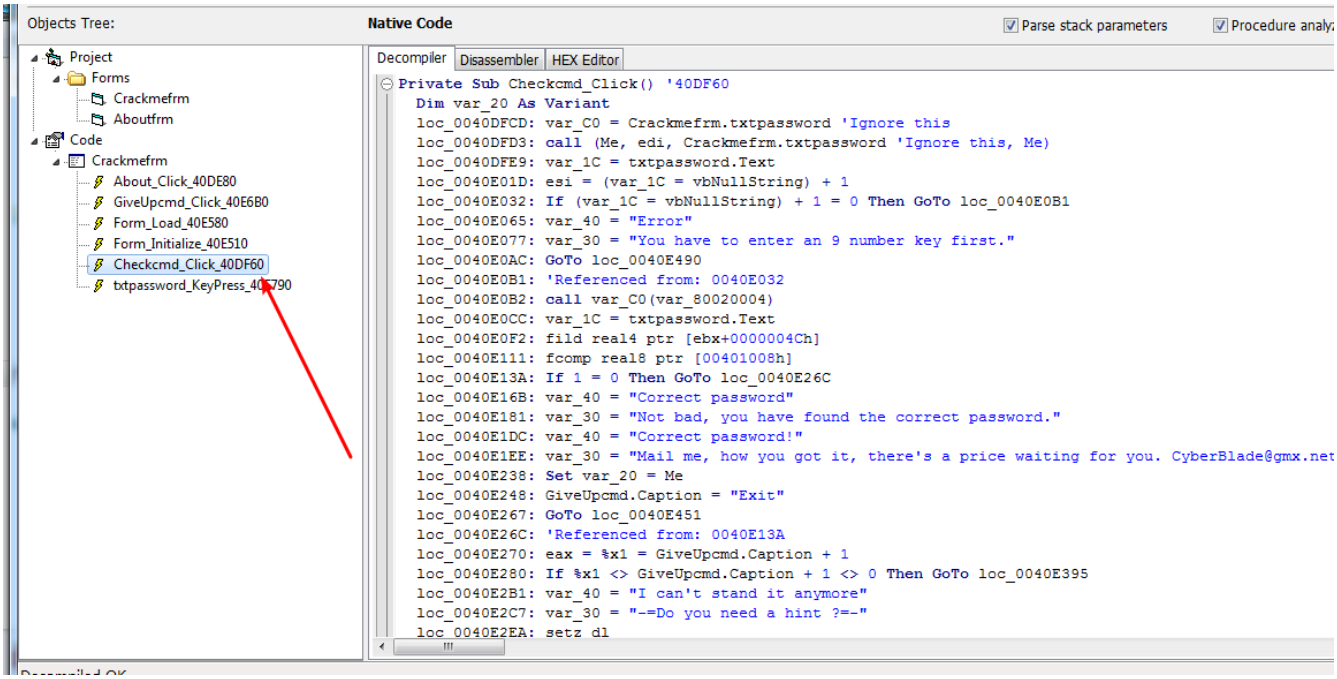
查壳



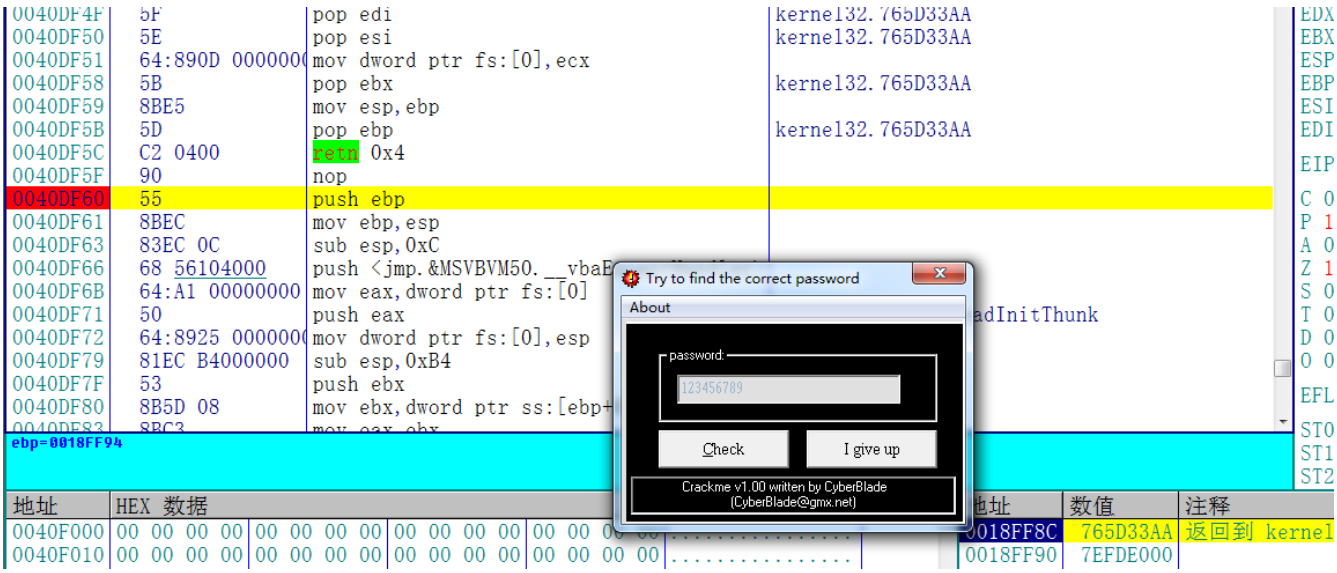
目标程序是用VB N-Code方式编译的，难度为一颗星，采用序列号保护方式

分析程序

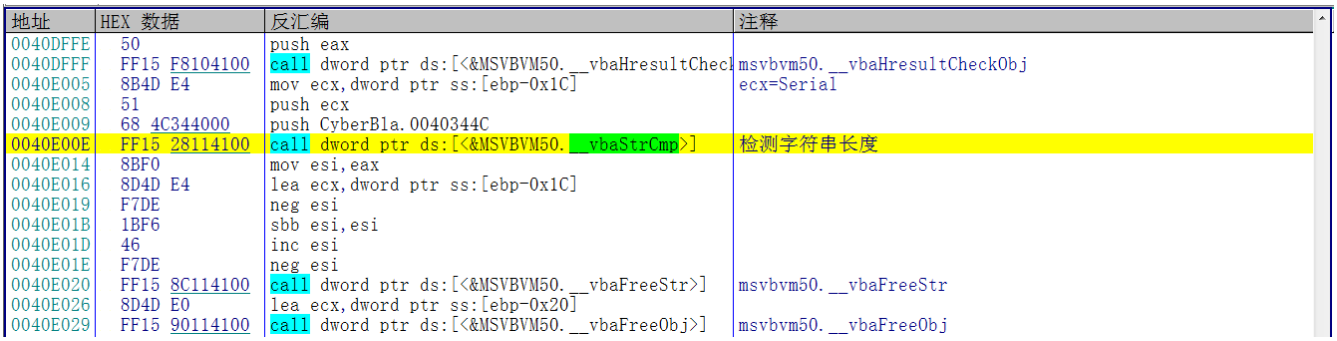
这个程序的序列号保护方式是有算法的，单纯追踪注册码比较困难，所以直接用VB反编译工具查看按钮点击事件的RVA



直接在40DF60的位置下断点，随便输入一个序列号



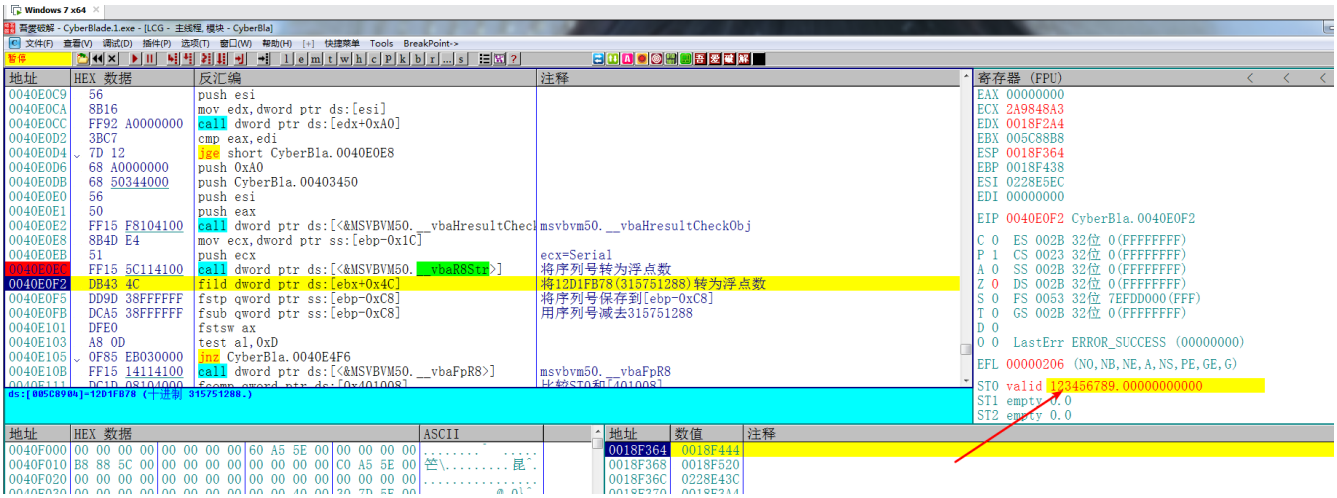
校验过程如下



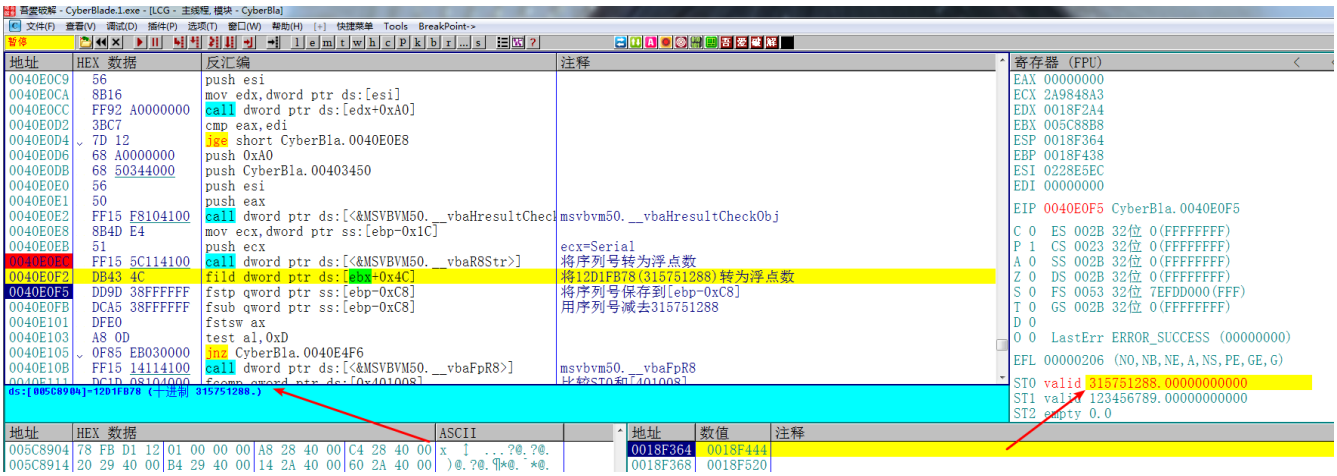
首先检测字符长度是否匹配，不满足则提示错误

```
0040E039   BB 04000280      mov ebx,0x80020004
0040E03E   897D A0          mov dword ptr ss:[ebp-0x60],edi
0040E041   897D B0          mov dword ptr ss:[ebp-0x50],edi
0040E044   8B3D 78114100    mov edi,dword ptr ds:[<&MSVBVM50.__vbaVarDup>] msvbvm50.__vbaVarDup
0040E04A   BE 08000000      mov esi,0x8
0040E04F   8D55 80          lea edx,dword ptr ss:[ebp-0x80]
0040E052   8D4D C0          lea ecx,dword ptr ss:[ebp-0x40]
0040E055   895D A8          mov dword ptr ss:[ebp-0x58],ebx
0040E058   895D B8          mov dword ptr ss:[ebp-0x48],ebx
0040E05B   C745 88 EC34400  mov dword ptr ss:[ebp-0x78],CyberBla.004034EC  UNICODE "Error"
0040E062   8975 80          mov dword ptr ss:[ebp-0x80],esi
0040E065   FFD7             call edi
0040E067   8D55 90          lea edx,dword ptr ss:[ebp-0x70]
0040E06A   8D4D D0          lea ecx,dword ptr ss:[ebp-0x30]
0040E06D   C745 98 9434400  mov dword ptr ss:[ebp-0x68],CyberBla.00403494  UNICODE "You have to enter an 9 number key first."
0040E074   8975 90          mov dword ptr ss:[ebp-0x70],esi
0040E077   FFD7             call edi
0040E079   8D55 A0          lea edx,dword ptr ss:[ebp-0x60]
0040E07C   8D45 B0          lea eax,dword ptr ss:[ebp-0x50]
0040E07F   52               push edx
```

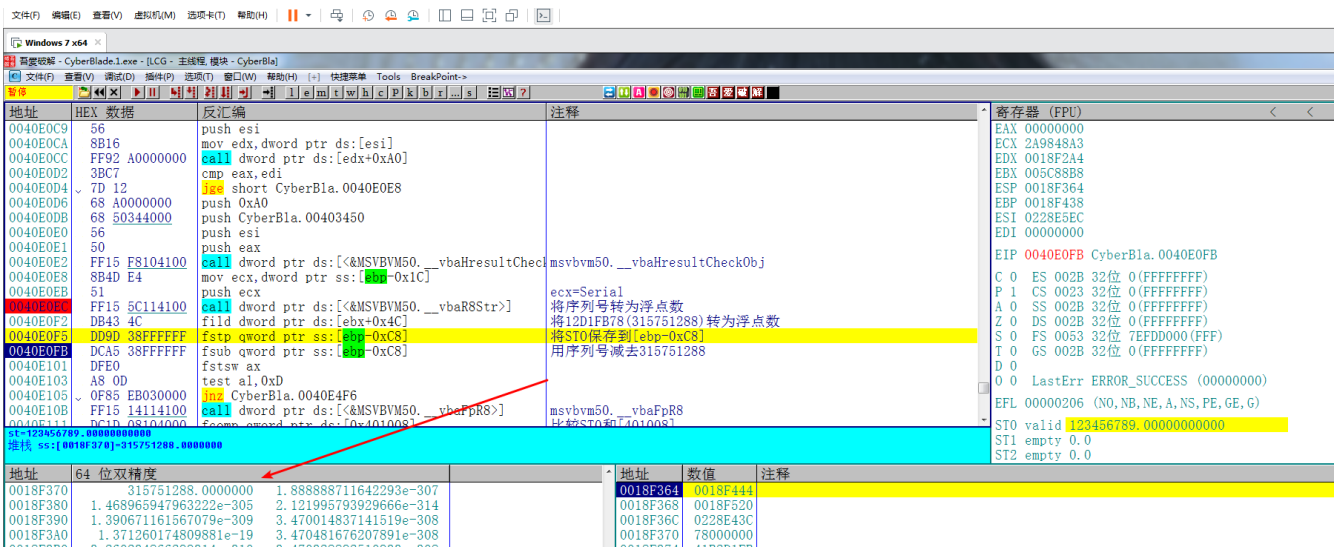
必须为9个字符



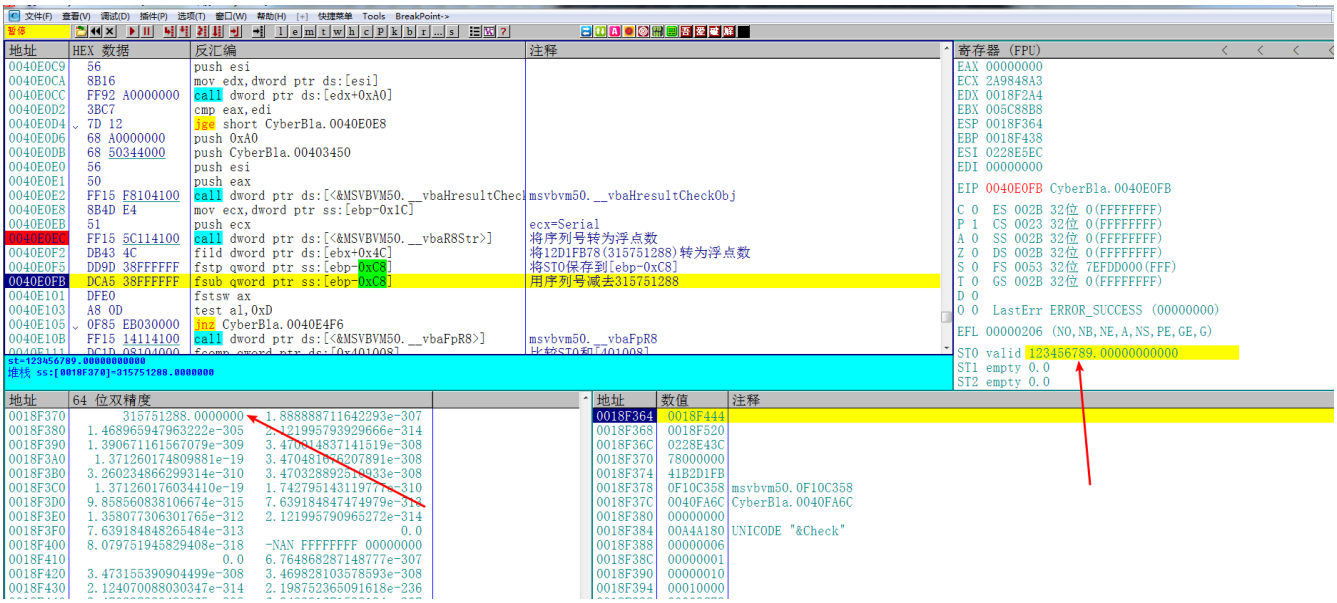
然后将输入的序列号转为浮点数



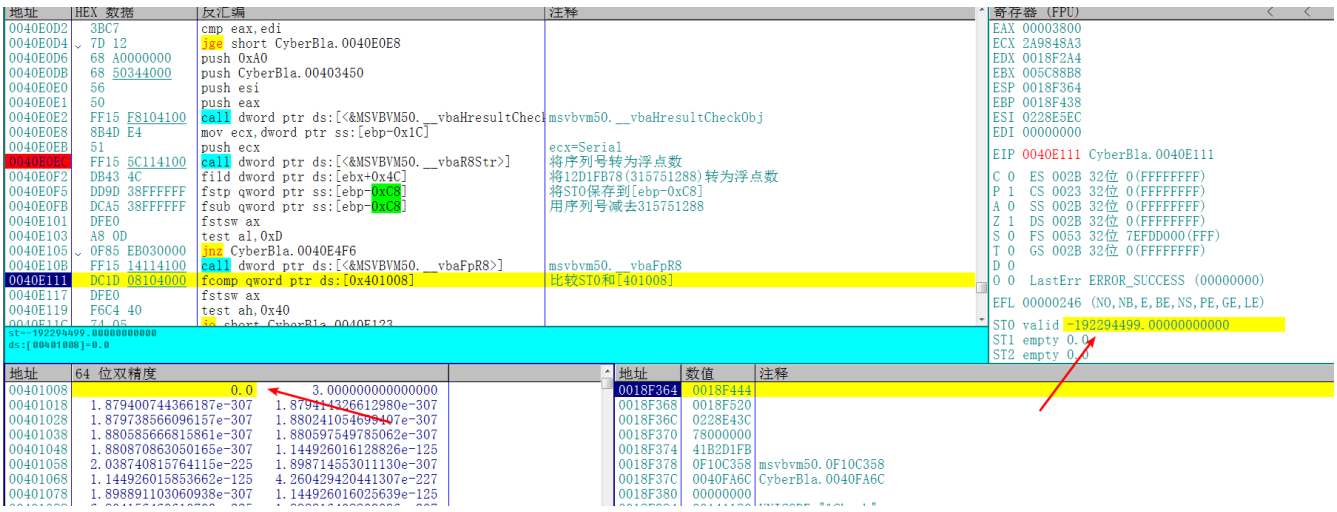
然后将315751288转为浮点数



接着保存315751288到内存



然后用序列号减去315751288

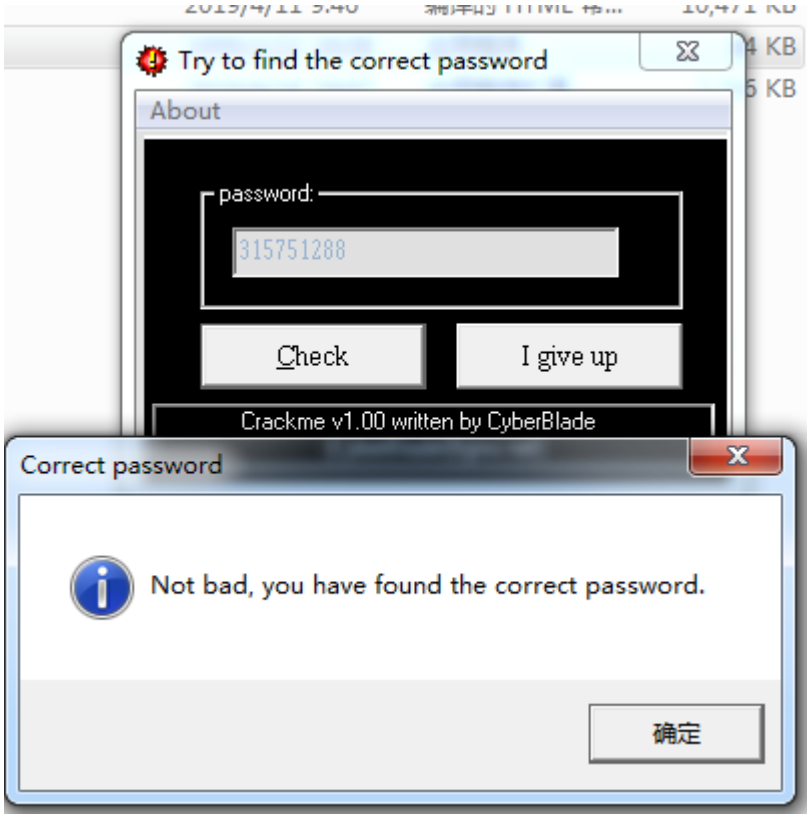


将两个数相减的结果和0进行比较，根据比较的结果提示是否正确注册。

结论：注册码很明显就是315751288了。

验证结果

输入315751288，



提升正确，破解完成。需要相关文件可以到我的Github下载:

https://github.com/TonyChen56/160-Crackme