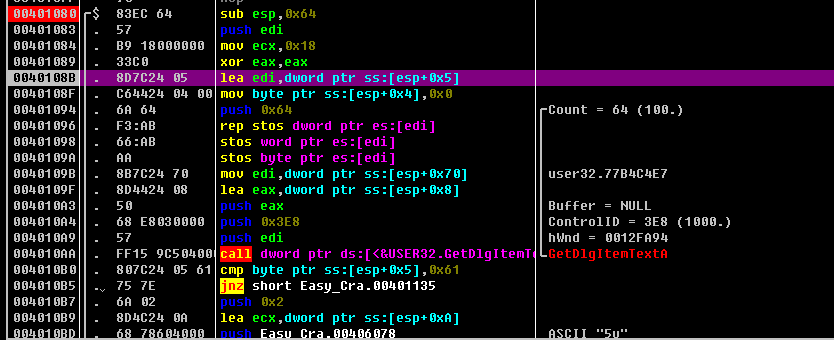
目录

**未找到目录项。**

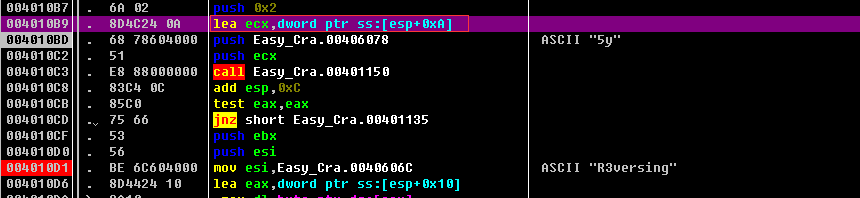
# EasyCrackMe



这段代码是读取对话框中输入的字符串，分配一个100字节的buffer。



判断第二个字符为“a”



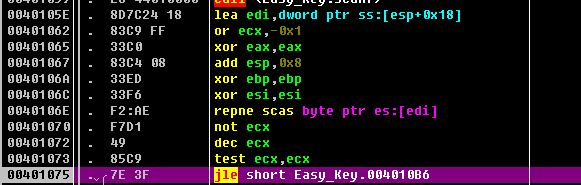
Lea 传递字符串地址。



比较“E”

Flag ==”Ea5yR3versing”

# EasyKeygen



即：repnz scasb（32位地址操作）。扫描es:edi指向的一系列字节数据，扫描长度由ecx指定，当遇到与al中的数据相等时停止扫描。

最经典的求字符串长度的代码，strlen()在VC优化编译模式是这段代码。

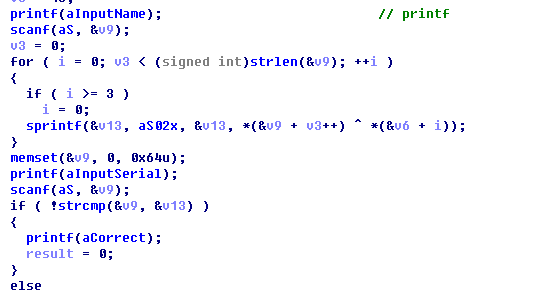
得到的字符串最后存放在ecx中。

总结：该段代码是strlen的汇编代码，返回值存放在ECX中。

JLE跳转是 <= 跳转。该段代码的功能是当strlen() <= 0 时，跳转代码。



注册机验证函数：

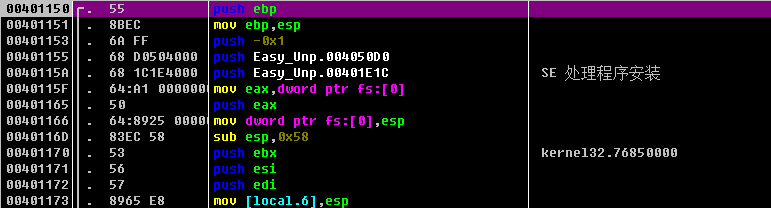


跑出的结果是K3yg3nm3

# Easy\_UnpackMe



上图为解密之后的jmp。跳转之后是常见函数入口。



# Easy\_ELF

# RePlace

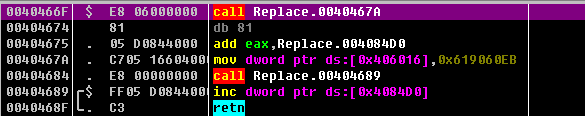


401000地址出的函数为主要函数。



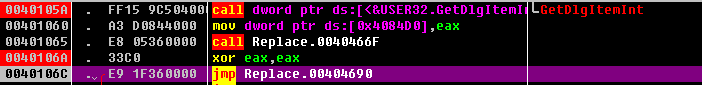
函数读取对话框中输入的数字。（按整数格式读取）。





EAX读取的值 + 0x6015cb，得到的数存放在4084d0地址处。





Jmp到404690处。





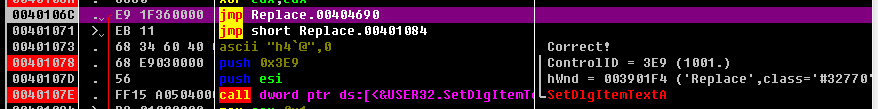
4084d0地址存放的数据自增1.



将40466f处的指令修改为c39000c6.，也就是将[EAX]=601605cc 修改成Nop



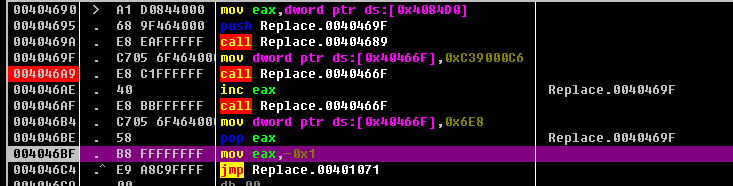
解题思路：



1．输入数据，然后程序运行到00401071，跳转到4046a9,eax=0x601605cb+输入的数据，这个值必须要等于0x100401071。然后这个eax值

（0040466F $ C600 90 mov byte ptr ds:[eax],0x90 ）也就是该中的eax值，程序会把eax也就是00401071中的指令修改为nop.

2,运行到004046AE。eax+1=00401072，在运行到004046af.程序会把eax也就是004010712中的指令修改为nop





所以2687109798即为最后的结果。