

修改 CCED.EXE 一个字节 实现对遗忘密码的文件编辑

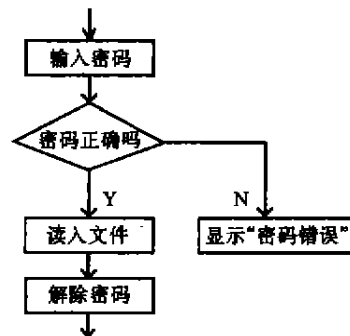
成都交通银行 胡毅

TP317

CCED 是许多计算机用户所喜爱的编辑软件。而且 CCED 具有给文件加解密的功能，增强了文件的保密性。但是用户一旦忘记了密码，则无法对文件进行操作。一般对加密文件进行解密的方法是：通过对加密的文件进行研究，找出其加密的方法。然后利用工具软件或编程将加密文件的密码找出，或编程将有密码的文件恢复为未加密的文件。这种方法往往比较繁琐，而且一旦加密的方法比较复杂，这种方法就无能为力了。笔者通过对 CCED 的跟踪发现了一种极其简单的方法，仅需修改一个字节，即可实现对遗忘密码的文件进行各种操作，且修改后不影响其他功能的使用。

下面叙述修改的原理及方法。笔者所用版本为 CCED 4.0。

首先简述一下 CCED 判别密码的过程。进入 CCED，输入文件名后，系统要求输入密码，密码输入后，系统判断此密码与加密的密码是否相同，若相同读入加密文件，对文件进行解密，若不同则显示密码错误。我们也正是修改判别密码的这一部分。其判别密码的流程如下：



对应于流程图中的判密码部分的汇编代码如下：

```

XOR AL,AL
REPNZ SCASB
SUB BX,CX
MOV CX,BX
  
```

```

MOV DI,SI
MOV SI,[BP+04]
REPZ CMPSB ;比较密码是否相同
MOV AL,[SI-01]
MOV BL,[DI-01]
XOR AH,AH
MOV BH,AH
SUB AX,BX ;如果 sub ax,bx 为 0,则说明密码相同;
JMP EE14 ;如果 sub ax,bx 不为 0,则说明密码不同。
POP DI ;以 ax 的值为密码判别结果传递给上一级程序。
POP SI
POP BP
RET
  
```

注意到上面的代码中 REPZ CMPSB 是用来比较二个密码是否相同，而 SUB AX, BX 是用来判断二密码是否相同，用 AX 的值作为返回上一级程序的参数。因此改法是将 sub ax, bx 换为 sub ax, ax 即可。sub ax, bx 的机器码为 2bc3，而 sub ax, ax 的机器码为 2bc0，因此仅需把 c3 改为 c0 即可。

读者可用 PCTOOLS 修改。本方法适用于 CCED 4.0。注意到 sub ax, bx 及其后面的四条指令的机器串为 2bc3eb005f5e5d，使用 find 功能，找字符串 2bc3eb005f5e5d，将其中的 c3 改为 c0 即可（注意使用 find 功能时用 hex 方式）。使用修改后的 CCED 时，当进入密码输入画面时，不要急于回车，可随意输入几个键，再回车，这时就可以进入编辑画面了。事实上由于仅修改了密码的判别部分，所以修改后不影响其他功能的使用。

G.33



科达电源

急您所急 想您所想

地址：(519000)珠海翠香二路 34 号红海工业楼三楼

电话：(0756)2220324

FAX：(0756)2231980