

⑦  
34-36

## CCED 加密文件密码的再现

于富强 王国庆

(河北师范大学西校区物理系)

齐 兰

(河北省科学院应用数学研究所)

TP391

【摘要】 本文详细介绍 CCED 软件中密码的形成过程,密码的再现原理,并附一简单的密码还原程序。

文字处理软件,

【关键词】 密码, 偏移量, 特征码

CCED 软件, 加密,

现在有许多文字处理软件可以对编辑的文件进行加密,如 WPS、CCED 等,这样对自己的文件进行保密,但由于忘记了密码,作者自己也不能打开此文件,这样是一很大的损失,别无选择,只能是“望它兴叹”了。本文介绍用一程序能够对被加密文件的密码自动测试,能够重新获得密码。

笔者对 CCED 文件进行大量研究,对 CCED 文件总结如下:

用 CCED 对文件加密(不是加密压缩方式),被加密的文件格式如下:

XXXX;0000 07 07 57 41 52 4E 20 3A-20 44 6F 6E 27 74 20 6D	.. WARN:Don'tm
XXXX;0010 6F 64 69 66 79 20 74 68-69 73 20 66 69 6C 65 20	odify this file
XXXX;0020 21 20 29 21 25 2D 71 0D-0A 21 0D 0A 22 0D 0A 23	!)!%-q..!..". #
XXXX;0030 0D 0A 24 0D 0A 24 0D 0A-25 0D 0A 26 0D 0A 26 0D	.. \$.. \$..%..&..&.
XXXX;0040 0A 27 0D 0A 27 2F 0D 0A-28 0D 0A 29 0D 0A 1A FF	..'. ' /..(..)....

偏移量:00H—21H 为加密文件的文件头,所有加密文件相同。

偏移量:22H—“0D0A”为密码区。密码区的长度为 2 至 10 个字节,根据密码数而定,密码从偏移 22H 开始,至第一个“0D0A”止,共有密码数加 1 个字节。密码区后为文件的内容。

特征码:密码区第一个字节,我们可以称之为特征码,它在加密文件中起到决定性的作用,文件的内容包括特征码后的密码,都和特征码进行操作,形成加密后的内容。

密码:从特征码后至第一个“0D0A”,其为密码的 ASCII 码与特征码进行操作而形成。密码是由键盘上输入的,一些只有扫描码而没有 ASCII 码的键,不能当做密码,并且字母的大小写一律转换成大写存放,空格也不能为密码,这样能为密码的键只能是 ASCII 码为 21H~60H 和 7BH~7EH 的键。

数据区:从密码区后至“1A”之间。此数据是加密前数据的 ASCII 按列与特征码进行不同的处理。

## 1 特征码的形成

我们既然知道了特征码在此文件中的地位,我们着重研究一下特征码,经过大量的研究分析发现,特征码是由各个密码的 ASCII 码相异或,形成一个字节,此字节与 2DH 相异或,如果此字节小于 20H,那么再和 20H 相或一次,这样形成了特征码。

## 2 密码的再现原理

被加密的 CCED 文件被 CCED 调用时,首先向用户询问密码,如果用户所给密码与文件中记载的密码相符,那么 CCED 则根据特征码把文件的内容还原。如果我们把密码区中的内容抹成零,调用文件时,任何密码都可进入,但 CCED 则根据新密码形成的特征码还原文件内容,这样还原后的内容当然不是文件的真实内容,但我们输入与老密码的特征码相同的新密码,则还原的文件仍是原来的真实内容,这样文件的真实内容又重新呈现在我们的眼前了。

## 3 密码再现实例

把下面程序 CCED JM.C 经编译后形成 CCEDJM.EXE 文件。

```
1; #include<stdlib.h>
2; #include<stdio.h>
3; main()
4; {
5; char file[8];
6; char i, ch, chh, tl, time;
7; char bc[9] = {0x21, 0x21, 0x47, 0x46, 0x45, 0x44, 0x43, 0x42, 0x41}; //密码的前两位可以
   变化,后面几位固定
8; FILE *fp;
9; printf("\n\tPlease input a filename:");
10; scanf("%s", file);
11; if((fp=fopen(file, "rb+"))==NULL)
12;     {printf("\7\n\tCannot open file !!!");
13;     exit(0);
14;     }
15; if(fgetc(fp) != 7 && fgetc(fp) != 7)
16;     {printf("\7\n\tThe file hasnot password!");
17;     exit(0);
18;     }
19; fseek(fp, 7L, 0);
20; if (fgetc(fp) == 0x5a && fgetc(fp) == 0x69 && fgetc(fp) == 0x70)
21;     {printf("\7\tThe file is cced-Zip-file");
22;     exit(0);}
23; fseek (fp, 34L, 0);
24; ch=fgetc(fp);          \读特征码
25; time=0;               \time 为密码个数
26; while((tl=fgetc(fp)) != 0x0d)
27; time++;
```

```

28: i=time;
29: fseek(fp,35L,0);
30: for(;i>0;i--){putc(0x00,fp);\\密码区中除特征码外其它置 0
31: if(time==1)bc[1]=0x60;\\如只有一个密码的话外循环执行一次
32: for(;bc[1]<=0x60;bc[1]++)
33:     for(bc[0]=0x21;bc[0]<=0x60;bc[0]++)
34:     { t1=0;
35:         for(i=0;i<time;i++)t1=t1^bc[i];
36:         chh=(t1^0x2d);
37:         if(chh<0x20)chh=chh+0x20;
38:         if(chh==ch)
39:             {printf("\\nThe file's password is:");
40:                 for(i=time;i>0;i--){printf(" %c",bc[i-1]);
41:                     }
42:             }
43: fclose(fp);
44: return 0;
45: }

```

操作如下:

A. 先把被解密文件的只读属性去掉。

C:\CCED>ATTRIB-R<被解密文件>

B. 运行上面程序

C:\CCED\CCEDJM

键入被解密文件名,则密码则可以再现

说明:A. 本程序给出的密码与原来密码特征码相同,并非一定为原来密码,所以不一定只有一种,往往是一组,只要从中找出其一便可。

B. 如果用所得密码进入编辑状态,请马上修改密码或修改存盘模式,否则存盘后数据混乱。

C. 本程序只适合 CCED 中的加密文件,不适合加密压缩方式。

D. 本程序经过 Turbo C++3.0,编译连接成功,对 CCED 5.03 测试无误。

## RECOVERING THE PASSWORD IN THE CCED'S FILE

Yu Fuqiang Wang Guoqing Qi Lan

**ABSTRACT** This paper introduces the process that the password is produced in the CCED's file, and principle of the password recovering. This paper gives a program for recovering the password in the CCED's file.

**Key words** Password, Offset, Special code