

23

64

遗忘 CCED 文件加密口令的一种处理方法

关世奇[△] 尚杰[△] TP317

摘 要 本文介绍通过破译主密码,使用户可用变异口令而将加密的 CCED 文件打开一种切实有效的方法。

主题词 解密 口令 主密码 密码组 CCED 文件 加密 排版软件

加密后的 CCED 文件,在打开该文件时必须严格输入加密时所用的口令。此功能可以保护我们的文件不被他人非法阅读或修改,但是忘记口令的事情时有发生,致使用户无法打开自己加密后的文件。

一、加密原理

CCED 的口令经一定的加密算法处理,生成一个单字节的主密码和与口令等字节长的密码组,并保存在加密后的 CCED 文件中。对明文的加密是通过用主密码与明文进行一定的运算来完成的。找到这个主密码,也就找到了打开加密文件的钥匙。

二、CCED 加密文件的结构

由于 CCED 使用特殊的文件结构,所以我们先了解 CCED 加密后的文件结构,从中找到主密码进行加密文件的解密。文件的前 34 个字符 CCED 文件的标志,位数固定(如表一, "WARN;Don't modify ths file!");第 35 位为主密码,固定一位(如表一, "6c");后面几位为加密后的口令,位数不固定,但与口令的位数相同(如表一, "29 22 c2");口令以回车符为结束标志,固定两位;口令之后是加密后的密文内容(如表一,)。

三、解密方法及过程

我们只要将主密码破译即可到达解密的目的,表二就是主密码与破译后的单一字符(变异口令)对照表。

具体步骤如下:

假设有一 CCED 加密文件 WJ1, TXT, 口令未知。

c:debug wj1.txt

-d

21BC:0100 07 07 57 41 52 4E 20 3A-20 44 6F 6E 27 74 20 6D

21BC:0110 6F 64 69 66 79 20 74 68-69 73 20 66 69 6C 65 20
21BC:0120 21 20 6C 29 22 C2 0D 0A-60 7E E9 EF B4 FA OD OA
;察看主密码(6c) 密码组(29 22 c2)
-e 123; 将密码组用零替换
29.00 22.00 c2.00
- n wj2.txt ;以 wj2.txt 重新存盘
- w
- q

此时 wj2.txt 即为破译后的 CCED 加密文件 wj1.txt 的拷贝,口令为 'A' (查表二,由主密码 6c 得变异口令为 A)。

附表:

表 1

16 进 制 码	ASCII 字符
21BC:0100 07 07 57 41 52 4E 20 3A-20 44 6F 6E 27 74 20 6D	.. WARN Don't
21BC:0110 6F 64 69 66 79 20 74 68-69 73 20 66 69 6C 65 20	modify this file;
21BC:0120 21 20 6C 29 22 C2 0D 0A-60 7E E9 EF B4 FA OD OA)'...'~....
.....

表 2

主密码	20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36
变异口令	-,./)(+ * % \$ ' & ! AA # " = < ? > 9 8 :
主密码	37 38 39 3A 3B 3C 3D 3E 3F 4D 50 51 53 56 60 61 62 63 64 65 66 67 68
变异口令	,54761032') ~(MLONIHKJE
主密码	69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F
变异口令	DGFA@CB) - ^ YX[ZUTWVQPRS

(收稿日期:99 年 1 月 12 日)

关世奇 抚顺石油学院 113001
尚杰 抚顺石油学院 113001