

FoxPRO 对 DBF 文件的低级加密法

李桂根 (山西财经学院 030012)

在用 FoxPRO 开发 MIS 时,须考虑的重要内容之一就是数据的加密,如 MIS 允许使用的不同人员的登录的口令数据,从而提高系统和数据的安全性。庆幸的是, FoxPRO 2. X FOR DOS 同 C、汇编语言一样,也具有低级文件的读写功能,使得 FoxPRO 对常用的 DBF 文件可按低级文件处理方式实现数据的加密处理,既简化了文件的加密处理方法,又提高了数据的破解难度。

1. FoxPRO 的低级文件操作函数

FoxPRO 2. X For DOS 对低级文件的读写操作,即直接按照文件的物理结构而进行的读写操作,是以函数的方式实现的,可完成文件的建立、打开、关闭、测试、读写、移动读写指针等功能,其主要函数的名称和用法见表 1。详细用法限于篇幅,在此不作详细说明,读者可参考有关书籍。

表 1

类别	名称及格式	功能概要	执行结果
开文件	FCREATE(<字符串>[, <属性>]) FOPEN(<文件名>[, <属性>])	建立文件 打开文件	文件号 文件号
关文件	FCLOSE(<文件号>)	关闭文件	真假值
读文件	FGETS(<文件号>[, <字符串长度>]) FREAD(<文件号>[, <字符串长度>])	按行读文件 读文件	所读字节数 所读字节数
写文件	FPUTS(<文件号>, <字符串>[, <字符串长度>]) FWRITE(<文件号>, <字符串>[, <字符串长度>])	按行写文件 写文件	所写字节数 所写字节数
移指针	FSEEK(<文件号>, <移动字节长度>[, <移动方式>])	移动读写指针	指针位置
测试	FEOF(<文件号>) FERROR()	测试遇文件尾否 测试文件操作错否	真假值 错误类型号

2. DBF 文件的物理结构简介

若想对 DBF 文件以低级文件方式进行数据加密,就必须了解其物理结构,现简介如下:

从物理结构看, DBF 文件的内容分两大部分, DBF 文件库结构描述数据和库中的每条记录数据。对于位于文

件开始处的库结构描述数据又分为占用 32 个字节、用二进制表示的文件描述数据和 ASCII 码表示的所有字段描述数据,其含义见如下表 2 和表 3:文件开始的 32 个字节为文件描述数据,其字节含义为(如表 2 所示):

之后的每 32 个字节为一个字段的描述数据,其字节含义为:

表 2

字节	字节含义
1	此字节为 03H 时表示不含 Memo 字段,为 83 时有 Memo 字段。
1~3	库文件的最后修改日期。存放顺序为年、月、日。
4~7	当前文件所含记录个数。低位在前,高位在后。
8~9	库结构描述数据长度。
10~11	每条记录的长度。
12~31	保留。通常为 0。

表 3

字节	字节含义
0~9	此 10 个字节为 ASCII 码表示的字段名称。
11	此字节为 ASCII 码表示的字段类型。
16	此字节为字段长度。
17	此字节字段的小数点位数。

其余字节保留,通常为零。

整个库结构描述数据由 0DH 表示结束。故此部分

内容长度为:

32 + 字段个数 * 32 + 1(字节)

在库结构描述数据之后,依次为按记录号顺序排列的每条记录数据,且由占一个字节删除标志(无删除时标志为 20H,删除时为 2AH)开始时数据内容不论其字段类型如何,均以 ASCII 形式存放数据中的每一位字符。最后由 1AH 表示整个文件的结束。

3. FoxPRO 对 DBF 文件的低级加密法

在明确了 FoxPRO 对低级文件的读写方法和 DBF 文件的物理结构之后,就可以用 FoxPRO 实现对 DBF 文件任意记录任意字段内容的加密。用 FoxPRO 对 DBF 文件进行低级加密时,须考虑两个问题:

- (1)对于指定记录号的指定字段的指针定位问题;
- (2)对字段内容加密时,是否受字段类型影响。

对于前者,用 FoxPRO 下的 FSIZE() 和 RECSIZE() 函数得到所有字段的长度和每条记录的长度后,再联想到 DBF 的物理结构后,则很容易算出任一指定字段的偏移地址。对于后者,因不论 DBF 文件的字段类型如何,其内容均以 ASCII 码存放,且用 FoxPRO 的低级文件读写法读写字段内容时,只关心字段中的每个符号,即字节中的 ASCII 码值,并不涉及此字段的类型,所以在修改字节内容以实现字段的加密时,是不受字段类型影响的,并且此低级加密法使得非字符型字段也能存放字符符号,从而彻底破坏了 DBF 文件的正常显示规律,故有较好的加密效果。此加密方法的另一好处是能够保证记录与记录之间的保密性。具体加密方法请见所附程序清单。

```
*****
* 程序名称:FoxPRO 下 DBF 文件低级加密程序 *
* 程序功能:在 FoxPRO 下对 DBF 文件的指定字段加密 *
* 运行环境:FoxPRO 2.x For DOS *
*****
```

```
SET TALK OFF
CLEAR
ACCEPT[请输入数据库名(<filename>):]TO F-DBF
F-DBF = F-DBF + [.DBF]
IF .NOT. FILE([&F-DBF])
    ? [所给文件不存在!]
ELSE && 打开所给文件
    USE &F-DBF R = RECCOUNT() && 取文件的记录个数
```

```
FCOU = FCOUNT() &&
R-LEN = RECSIZE() &&
STORE 1 TO R-NO, F-NO
@ ROW() + 1, 0 SAY [:]GET R-NO RANGE 1, R
@ ROW() + 1, 0 SAY[:]GET F-NO RANGE 1, FCOU
READ
H-BYTE = 32 + FCOU * 32 + 1 &&
R-BYTE = (R-NO - 1) * R-LEN &&
F-BYTE = (R-NO - 1) * R-LEN &&
F-BYTE = 1
F = 1
DO WHILE F < F-NO &&
    FNAME = FIELD(F) &&
    F-BYTE = F-BYTE + FSIZE([&FNAME]) &&
    F = F + 1
ENDDO
FNAME = FIELD(F)
CF-BYTE = FSIZE([* FNAME]) &&
USE &&
FH = FOPEN([&F-DBF], 2) &&
IF FH = -1
    ? [!]
ELSE
    = FSEEK(FH, H-BYTE + R-BYTE + F-BYTE) &&
    JM-FIELD = FREAD(FH, CF-BYTE) &&
    = FSEEK(FH, - CF-BYTE, 1) &&
    DO WHILE LEN(JM-FIELD) > 0 &&
        JM = SUBSTR(JM-FIELD, 1, 1)
        JM-FIELD = SUBSTR(JM-FIELD, 2)
        J = ASC(JM)
        JM = INT(J/16) + (J - INT(J/16) * 16) * 16
        JM = CHR(JM) &&
        = FWRITE(FH, JM, 1) &&
    ENDDO
    = FCLOSE(FH) &&
ENDIF
ENDIF
RETURN
```

本文所提供的程序仅作 DBF 文件低级加密法的说明,为了便于读者理解,密钥的选择采用了字节内容循环右移四位的方法,故对同一字段内容重复加密时,可实现字段的解密。读者可在此程序的加密处用适当的方法加以修改。本程序的执行不受 DBF 文件的库结构限制,并在 DOS 6.2、FoxPRO 2.5 For DOS 下运行通过。