微机数据库信息加密

于功第 (西南交通大学)

摘要:本文从实用角度出发,介绍了目前微机数据库常用的信息安全机制,详细叙述了笔者研制的微机数据库信息加密控制方法的设计思想、原理和实现算法,进行了算法分析,最后给出了实用工具程序清单。

目前,随着微机数据库管理系统(如 dBASE、FoxBASE、Foxpro 等)的应用不断深入普及,各种应用微机管理信息系统陆续投入实用。从而使社会机密和财富信息越来越高度地集中于微机系统中,因此微机数据库管理系统的数据安全已成为迫切需要解决的问题之一。为此,发展安全可靠实用的微机数据库密码控制方法,已成为目前计算机信息保护学需要研究的分支课题之一。

一、微机数据库信息保护机制

目前,微机数据库系统信息保护机制的基础理论主要包括存取控制、加密控制和信息流向控制三种。

1.存取控制

是对存取信息的授权机制,它与存取信息的内容不相干。对微机数据库系统而言,目前的主要保护机制是存取授权控制。这是由于在微机数据库中有大量数据集中存放,并且可为用户直接共享。一般来讲,为了控制用户对数据库数据的存取范围,有效保证数据的安全,系统可以控制不同的用户对不同的数据有不同的使用权限,所以控制合法使用权是微机数据库安全性问题的主要内容。目前,在微机数据库系统中控制用户合法使用权常采用注册口令和存取授权两种方法:

(1)对于注册口令。是在用户向数据库管理系统注册时,让系统对用户进行真实性鉴别。鉴别的方法是要求用户给出口令,然后系统把它与存储在系统内的口令文件比较,以决定是否允许用户注册。为了保护口令文件的绝对安全性,它是利用一个单向函数建立的。迄今为止,此法仍是防止非法用户进入系统的有效方法。

(2)存取授权。它决定用户能否访问微机数据库以及用户的使用权限。如 ORACLE 数据库系统规定,表和视图的建立者是主人(OWNER)。主人拥有对这些表和视图的一切权力。其它用户要使用这些表和视图,必须由主人对他们作明确授权。目前存取授权一般采用分级授权(由数字表示),级别越高对数据库访问范围越大,存取控制能力越强。

2.加密控制

它使数据库信息内容更加难懂,以使不被窃取信息者识破。它与授权并无直接关系。目前常采用的加密控制方法主要是用利计算机密码学的理论和方法,将数据库信息明码文通过加密控制变成密码文,进行保存和传递,以确保信息的安全(本文下面将主要讨论加密控制的有关方法问题)。

3.信息流向控制

它一般涉及信息传递并非是权的转让。它主要解决某些人借机滥用授权,致使数据库信息流向失控的问题。

从目前情况看,在微机数据库系统保护机制中,存取控制主要控制用户访问信息的权限和范围;加密控制主要防止信息内容的失密,它使窃取者得到的信息无意义;而信息流向控制,主要解决数据库信息的传递安全问题。目前,对一般微机数据库系统信息和数据的安全性,主要受存取控制机制的保护,这也是微机数据库管理系统本身固有的安全机制。而加密控制则需要用户自己根据应用需要来研究设置。下面介绍笔者研制的一种加密控制方法。

二、实用加密控制的实现

1.设计思想

目前，微机关系数据库系统主要采用“二维表”视图形式描述数据库，而数据库物理表现形式为记录(Record)和域段(Field)，且一个记录由若干个域段组成，域段是数据库的基本信息单位。本文提出的加密控制方法主要考虑对微机数据库记录的域段内容作为基本信息单位进行加密控制。具体步骤为：

(1)对数据库记录中的某一指定域段内容进行加密。先顺序求出域段内容（明码文）中每个字符的ASCII码，加上密钥位移量，然后映射变成密码文字符，实现一对我射的位移替代变换，完成记录域段内容的横向加密。

(2)在加密过程中，每个数据库记录指定域段内容中每个字符加密完成后，立即进行下一个记录对应域段值内容的加密。循环反复直到数据库中所有记录中的指定域段内容全部变成密码文为止，即完成记录域段的纵向加密。

2.算法原理描述

首先定义数据库中某指定域段为M域段，记录1中对应域段为M1，记录2中对应域段为M_2，…，记录n中对应域段为M_n。

又定义：$M_1=m_{11}m_{12}\cdots m_{1t}$

；

$M_n=m_{n1}m_{n2}\cdots m_{nt}$

即：$M_i(i=1,2,\cdots,n)$的内容由七个字符串组成。

设：数据库域段M明码文为：

$$M=\begin{pmatrix} m_{11}m_{12}\cdots m_{1t} \\ m_{21}m_{22}\cdots m_{2t} \\ \vdots \quad\quad \vdots \\ m_{n1}m_{n2}\cdots m_{nt} \end{pmatrix}$$

数据库域段密码文：

$$M=E\begin{pmatrix} c_{11}c_{12}\cdots c_{1t} \\ c_{21}c_{22}\cdots c_{2t} \\ \vdots \quad\quad \vdots \\ c_{n1}c_{n2}\cdots c_{nt} \end{pmatrix}$$

密钥 $k=k_1k_2\cdots k_t$

则：加密变换 $Ek:C=E_k(M)$

解密变换 $Dk:M=D_k(C)$

又设：变换映射函数ASC为将字符变成ASCII码函数；CHR为将ASCII码转换成字符的函数。

加密关系式：

$$\left.\begin{aligned} C_{11}&=CHR(ASC(m_{11})+k_1)\\ C_{12}&=CHR(ASC(m_{12})+k_2)\\ &\vdots\\ C_{1t}&=CHR(ASC(m_{1t})+k_t) \end{aligned}\right\}\text{第一个记录 } M_1 \text{ 域段的字符串加密}$$

$$\left.\begin{aligned} C_{21}&=CHR(ASC(M_{21})+k_1)\\ &\vdots\\ C_{2t}&=CHR(ASC(M_{2t})+k_t) \end{aligned}\right\}\text{第二个记录 M2 域段的字符串加密}$$

$$\vdots$$

$$\left.\begin{aligned} C_{n1}&=CHR(ASC(M_{n1})+k_1)\\ C_{n2}&=CHR(ASC(M_{n2})+k_2)\\ &\vdots\\ C_{nt}&=CHR(ASC(M_{nt})+k_t) \end{aligned}\right\}\text{最后第 n 个记录对应域段 Mn 字符串的加密}$$

解密关系式：

$$\left.\begin{aligned} m_{11}&=CHR(ASC(c_{11})-k_1)\\ m_{12}&=CHR(ASC(c_{12})-k_2)\\ &\vdots\\ m_{1t}&=CHR(ASC(c_{1t})-k_t) \end{aligned}\right\}\text{第一个记录解密}$$

$$\left.\begin{aligned} m_{21}&=CHR(ASC(c_{21})-k_1)\\ m_{22}&=CHR(ASC(c_{22})-k_2)\\ &\vdots\\ m_{2t}&=CHR(ASC(c_{2t})-k_t) \end{aligned}\right\}\text{第二个记录解密}$$

$$\vdots$$

$$\left.\begin{aligned} m_{n1}&=CHR(ASC(c_{n1})-k_1)\\ m_{n2}&=CHR(ASC(c_{n2})-k_2)\\ &\vdots\\ m_{nt}&=CHR(ASC(c_{nt})-k_t) \end{aligned}\right\}\text{最后第 n 个记录解密}$$

3.算法分析

(1)此算法当数据库需加密记录为 n,域段信息长度为 t 时,其算法时间复杂性是 O(nt)阶的。当 n>>t 时,是 O(n)阶的。即与记录个数多少有关。

(2)其安全性、可靠性适中。当域段信息长度超过 10 时,密钥长度 t 为 10,如果不通过大量统计规律计算分析,要想在短时间内猜中密钥是不可能的。

三、工具软件清单

笔者利用 FoxBASE 语言编制了一个实现上述算法的软件程序(在 AST / COMPAQ 386 机上通过)。用户可将其嵌套进实用系统中,用于 FoxBASE 或 dBASE 数据库信息的加密控制(程序清单见后)。若要用于其数据库管理系统,用户可参照其设计思想和程序内容换成其它数据库管理系统支持语句即可。

附程序清单:

数据库加密程序:

```
set talk off
dimension k(20)
accept "请输入加密的库名:" to a
accept "请输入加密的字段名:" to f
input "请输入加密的字段长度" to m
j=1
do while j<=m
   input "请一个一个输入密钥:" to k(j)
   j=j+1
enddo
use &a
do while .no. eof()
   n=1
   cs=""
   do while n<=m
      c=substr(&f,n,1)
      b=asc(c)+k(n)
      c=chr(b)
      cs=cs+c
      n=n+1
   enddo
   replace &f with cs
   skip
enddo
set talk on
return
```

数据库解密程序:

```
set talk off
dimension k(20)
accept "请输入解密的库名:" to a
accept "请输入解密的字段名:" to f
input "请输入解密的字段长度" to m
j=1
do while j<=m
   input "请一个一个输入密钥:" to k(j)
   j=j+1
enddo
use &a
do while .nto.eof()
   n=1
   cs=""
   do while n<=m
      c=substr(&f,n,1)
      b=asc(c)-k(n)
      c=chr(b)
      cs=cs+c
      n=n+1
   enddo
   replace &f with cs
   skip
enddo
set talk on
end
```

参考文献:

[1]于功第"密码学在软件保护上的应用",中国计算机用户,92(8)

[2]于功第,路枝"计算机加密解密实用技术",微电子学与计算机,92(1)

[3]于功第"背包密码术的研究",西南交通大学学报,93(2)

[4]邓幼强"FoxBASE 十数据库语言与应用程序的自动生成工具与方法",成都出版社,1992