加密技术在航天器仿真平台数据库中的应用

何文会,廖 瑛
HE Wen-hui,LIAO Ying

国防科学技术大学 航天与材料工程学院,长沙 410073
College of Aerospace and Material Engineering,NUDT,Changsha 410073,China
E-mail:hwhcxm@sohu.com

HE Wen-hui,LIAO Ying.Application of encryption techniques in spacecraft simulation platform database.Computer Engineering and Applications,2007,43(35):210-212.

Abstract: In order to improve the security of database,the main encryption techniques applied to databases are studied.The algorithms of encryption and the main steps of algorithm implementation are discussed,and an example is given.At last,the key management and the encryption/unencryption influence on system functions of the database are expounded.The research results are valuable in the field of security of spacecraft simulation data.

Key words: spacecraft simulation platform;database encryption techniques;encryption/unencryption;key

摘 要:从提高数据的安全性出发,对航天器仿真平台中的数据库加密技术进行研究。详细论述数据库的加密算法及其算法实现的主要流程,并给出了某航天器仿真平台数据库管理系统加密实例;同时还阐述了密钥管理,加密解密对系统功能的影响。该研究结果对保证航天器仿真数据的安全具有一定的实用价值。

关键词:航天器仿真平台;数据库加密技术;加密/解密;密钥
文章编号:1002-8331(2007)35-0210-03 **文献标识码**:A **中图分类号**:TP309.7

随着计算机网络技术和网络仿真技术的广泛应用,网络之间信息传输量的急剧增大,网络传输的数据信息遭到不同程度的破坏,数据的安全受到严重威胁。

在分布交互式的航天器仿真系统中, 被仿真系统庞大,数学模型复杂,需要的参数多,仿真输出的结果类型也有所不同,而且仿真数据在网络中传输,共享数据的要求也更高,实时处理的速度要求快,数据交互访问较频繁,为了保证仿真数据信息的安全和保密,因此,必需对各种仿真数据进行加密处理。本文通过一个实例来验证对仿真数据库中的数据信息进行加密/解密,确保了仿真数据信息的安全性和完整性,也使数据库的安全性更加提高[1]。

1 数据库加密技术研究

一般的数据库系统采用密码识别的方法, 而常见的密码有:固定密码(一个口令)、简单加密的固定密码(进行变换)和加密变化的密码(数位的改变)。如对数据库系统进行数据的加密、身份认证以及登录用户的名称和口令、权限判断以及密钥的判断等。对用户信息进行多次验证,保证用户信息是正确、有效,确保数据库中数据信息的安全性和完整性。

特殊的数据库系统就要根据数据的保密要求和数据类型的复杂程度来进行相应的加密处理,利用一定的加密算法并编程实现该方法,增强数据库系统的安全性,数据信息的完整性和保密性。

1.1 数据库加密概述

对数据库进行加密,首先,要对数据库数据的加密粒度进行选择,由于数据库数据结构的不同,加密粒度通常有文件级、字段级、记录级和数据项级。加密单位越小,灵活性越强,适用范围越广,但实现难度就越大。

其次,要对数据的加密层次进行选择。数据库的加密层次主要有:操作系统(OS)层、DBMS 内核层和 DBMS 外围层。在操作系统 OS 层实现加密,由于无法辨认数据库文件中的数据关系,因而无法根据数据关系进行加密,只能对数据库文件进行文件加密,这对于大型数据库来说没有实际意义。在 DBMS 内核层实现加密,数据的加密和解密工作可以在物理存取之前完成,从而不影响数据库的各种操作,并且加密效率高,但需要有 DBMS 开发商的支持,实现非常困难。在 DBMS 的外围层实现加密,是将数据库加密系统做成 DBMS 的一个外层工具,在实现时既可以充分考虑数据库中的各种数据关系,又不需要开发商的支持,是一种切实可行的加密方法。

最后,在数据库加密之后,数据量不应明显增加,数据的长度也应该不会改变,加密和解密的速度要快,数据响应能够被用户所接受,而且要求数据库系统运行稳定、可靠和安全。

基金项目:航天支撑技术基金资助项目(No.2004GF01)。

作者简介:何文会(1977-),男,硕士研究生,主要研究方向为飞行器仿真平台的数据库设计和加密技术等;廖瑛(1961-),女,教授,博士生导师,主要研究方向为飞行器系统建模、控制与仿真等。

1.2　数据库加密算法及其实现

1.2.1　加密算法介绍

数据加密是保障数据库安全的最基本、最核心的技术支持和理论基础，数据加密过程由各种加密算法具体实施，它以很小的代价提供很大的安全保护。

目前，数据加密常用的算法为对称算法，以 DES、IDEA 为代表，加密、解密采用相同的密钥，其优点是加密、解密速度快，缺点是密钥分发困难。实际应用中往往采用非对称算法协助分发对称算法密钥的策略，其中以 RSA 算法最为常用。RSA 算法是 PKI 的基础核心，由于 PKI 的市场优势，选择 RSA 算法，系统部署会相对容易。

通过加密算法的简单介绍，利用 DES 和 RSA 加密算法可以很好地解决大多数数据库系统的加密要求。

1.2.2　DES 算法的实现

DES 使用相同的算法对数据进行加密和解密，所用的加密密钥和解密密钥也是相同的。而且 DES 加密算法适合于大量数据的加密，所以数据库数据的加密一般选择 DES 加密算法。

DES 加密算法的数据流程图如图 1 所示：

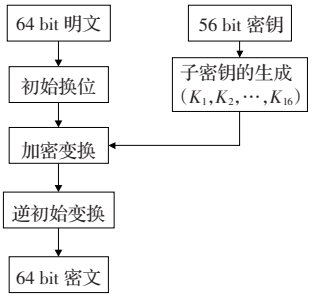

图 1　DES 数据流程图

该算法的输入是 64 bit 的明文，在 56 bit 的密钥控制下，通过初始换位 IP 变成 $T0=IP(T)$，再对 $T0$ 经过 16 层的加密变换，最后通过逆初始变换得到 64 bit 的密文。密文的每一位都是明文的每一位和密钥的每一位联合确定的。DES 的加密过程可以分为加密处理、加密变换以及子密钥的生成和解密等部分。

DES 算法采用了散布、混乱等基本技巧，构成其算法的基本单元是简单的置换、代替和模 2 加。由于 DES 的整个算法结构都是公开的，其安全性由密钥保证。

1.2.3　RSA 算法的实现

RSA 算法既能用于数据加密，也能用于数字签名，RSA 的理论依据为寻找两个大素数比较简单，而将它们的乘积分解开则非常困难。

在 RSA 算法中，包含两个密钥：加密密钥(e,n)和解密密钥(d,n)，在加密的时候，先把明文转换成$(0,n-1)$范围内的整数 M。当明文较长时，先分隔成适当的组，然后再进行变换。从 M 到密文 C 的加密方程和解密方程分别如下所示：

加密方程为：$C=M^e(\mathrm{mod}\ n)$

解密方程为：$M=C^d(\mathrm{mod}\ n)$

RAS 加密实施过程如下：

(1)设计密钥：选取 2 个互异的素数 P 和 Q，令 $r'=P\cdot Q$，$n=(P-1)(Q-1)$(r 为公开的加密密钥，其长度不少于 500 bit，一般为 1 024 bit)，必须对这 2 个素数加以保密；再找 2 个正整数 d 和 e，使之分别满足：n 与 d 互素，$e\cdot d\equiv 1(\mathrm{mod}\ n)$，这里的 e、r 就是公开的加密密钥。

(2)设计密文：要求把明文信息 M 数字化并分块，然后加密。加密公式为：

$C=M^e(\mathrm{mod}\ r)$

(3)解密密文：要求把密文转换成明文，就要对密文解密，即得到明文。解密公式为：

$M=C^d(\mathrm{mod}\ r)$

RSA 算法的优点是密钥空间大；缺点是加密速度慢。如果 RSA 和 DES 结合使用，则正好弥补 RSA 的缺点。即 DES 用于明文加密；RSA 用于密钥的加密。由于 DES 加密速度快，适合加密大量的数据，主要应用在计算机网络通信、电子资金传送系统、用户识别和用户文件的保护；而 RSA 可解决 DES 密钥的分配和管理问题。

1.3　密钥管理

由于密钥技术的核心内容是利用加密手段对大量数据的保护，最终归结为对若干核心参量密钥的保护。因此，数据库系统中密钥管理方案的选择成为系统是否安全的又一关键因素。密钥的管理也是很重要的，密码分析者经常会通过密钥管理来破译对称密码体制和公钥体制。好的密钥管理方案不但能增强系统的安全性，还能提高加密解密的运算效率。因此，通常采用多级密钥结构和动态密钥管理是数据库数据加密的良好选择。通过 DES 对数据库加密之后，利用 RSA 对密钥进行加密，实现了数据库加密的二级密钥管理。一级密钥为主密钥，二级密钥为工作密钥。主密钥的作用是对二级密钥加密生成工作密钥。工作密钥用于对数据库数据的加密解密。工作密钥的长度为 128 bit，前 112 bit 是记录名，需要带校验位存储在数据库表中。后 16 bit 是数据库表的列信息，它们是临时生成的。为了存储记录名数据，每个数据库表增加了一个记录名字段，在用户录入数据时，系统自动生成记录名数据，使每条记录都有一个记录名并做到各记录名数据互不重复。

假设一个表有 m 列、n 条记录，对于每一个加密单位都有一个对应的二级密钥信息 X_iX_j，组织方法如下：

$$\begin{array}{llll} x_1y_1 & x_1y_2\cdots & x_1y_j\cdots & x_1y_m \\ x_2y_1 & x_2y_2\cdots & x_2y_j\cdots & x_2y_m \\ x_3y_1 & x_3y_2\cdots & x_3y_j\cdots & x_3y_m \\ \vdots & \vdots & \vdots & \\ x_iy_1 & x_iy_2\cdots & x_iy_j\cdots & x_iy_m \\ \vdots & \vdots & \vdots & \\ x_ny_1 & x_ny_2\cdots & x_ny_j\cdots & x_ny_m \end{array}$$

其中，X_i 占 112 bit，X 序列的周期为 $2^{112}\approx 5\times 10^{33}$。$Y_j$ 占 8 bit，允许列编号 0~65 536，即一个数据库表最多允许 256 列数据。X_iX_j 的总长度为 128 bit。在数据需要加密解密时，将相应的 128 bit 二级密钥用主密钥进行加密即得到工作密钥，用工作密钥完成对数据的加密解密。

1.4　数据库加密的范围

通过数据库加密操作，很难找到明文和密文之间、密文和密钥之间的内在关系，也就是说经过加密的数据经得起来自 OS 和 DBMS 的攻击，大大提高数据库系统的安全性能。另一方面，数据库管理系统要完成对数据库数据信息的管理和使用，必须具有能够识别部分数据的条件。因此，只能对数据库中的部分数据进行加密。主要有以下内容：(1)索引字段不能加密。为了达到迅速查询的目的，数据库文件需要建立一些索引。不

论是字典式的单词索引,还是 B 树索引或 HASH 函数索引,它们的建立和应用必须是明文状态，否则将失去索引的作用;(2)关系运算的比较字段不能加密。数据库管理系统要组织和完成关系运算,参加并、差、积、商、投影、选择和连接等操作的数据一般都要经过条件筛选,这种“条件”选项必须是明文,否则数据库管理系统将无法进行比较筛选;(3)表间的外键字段不能加密。数据模型规范化以后,数据库中表之间存在着密切的联系,这种相关性往往是通过“外键”联系的,这些关键字段若加密就无法进行表与表之间的连接运算,降低系统的运行速度;(4)存储过程和触发器都不能加密。一旦加密,数据库的维护和修改就不能进行,而且数据的操作处理不能够完成。

1.5　数据库加密流程和解密流程

1.5.1　加密流程

加密前保证数据库中的数据是有效的,并且满足约束条件的数据才能够进行加密;如果数据信息是无效的,重新验证数据信息,直到数据信息正确为止。然后将明文数据加密转换为密文数据并存储于数据库。加密流程图如图 2 所示:

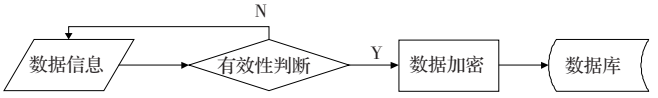

图 2　加密流程图

1.5.2　解密流程

数据解密是加密的逆过程，即将密文数据转变成明文数据。数据库中主要贮存密文数据,在数据的查询操作处理过程中,要求将数据库中的密文数据提取出来,并解密得到明文数据,便于用户的浏览、编辑和操作处理。解密流程如下图 3 所示:

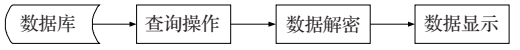

图 3　解密流程图

2　数据库加密对系统功能的影响

数据库加密之后,有些功能会受到一定的影响,不利于用户的操作使用。通过分析比较,在满足系统性能要求的前提下,对数据库的部分数据进行加密，既能达到系统运行速度的要求,也能保证数据的安全性和完整性。

目前大多数数据库管理系统的功能比较完备,特别像 SQL Server、Oracle、Sybase 这些采用 Client /Server 结构的数据库管理系统,具有数据库管理和应用开发等工具。但是,在数据库加密之后,数据库管理系统的一些功能将无法使用。例如 SQL 语言中 Select 语句中的 Group by、Order by、Having 子句分别完成分组、排序、分类等操作无法实现,SQL 语言中的内部函数不能进行正确计算,存储过程和触发器不能够实现数据的操作处理等。所以对数据库加密时,要确定好加密的对象和算法,然后进行加密,不然会影响数据库系统的性能和效能。

3　实例

下面以航天器仿真平台的数据库管理系统(简称仿真数据库系统)为例,进行仿真数据的加密和解密,并对算法实现的主要步骤进行详细的阐述。

因航天器系统的数学模型庞大,故相应的仿真数据库系统结构复杂,所涉及的表、数据类型、数据容量大和参数多的情况下,要实现仿真数据的全加密和解密过程是非常的困难。根据仿真数据库系统的基本要求,确保数据信息的完整性,在本例中,针对仿真数据库中的仿真数据信息表进行加密和解密过程的实现。

3.1　加密算法选择

根据仿真数据库系统的技术要求，在此选择 DES 和 RSA 混合加密的方法。DES 主要用来加密数据信息内容,RSA 是对 DES 加密后的数据信息进行二次加密,保证数据信息的安全和完整。为了查询的方便、快捷,提高操作仿真数据的效率,对表的索引、外键和 SQL 语句不加密。

3.2　加密/解密的实现

例如有一组仿真数据如下表 1 所示(m 行 3 列):

表 1　仿真数据表

X	Y	Z
0.01	0.03	0.01
0.02	0.01	0.02
0.03	0.02	0.02
…	…	…
0.0m	0.03	0.0m

DES 加密过程为:设初始密钥为用户名“张小峰”,按字转换成 ASCII 码为“-10811-12127-18459 ”。

(1)计算密钥表产生子密钥的目的是产生加密/ 解密过程所需的 16 个子密钥 K_1、K_2、…、K_{15}、K_{16}。

(2)初始置换是根据初始置换表(利用字符与 ASCII 代码对照表进行换算，如:A-65,B-66，……,Z-90,a-97,b-98,……,z-122;0-48,1-49,……)将输入的 64 bit 明文进行混乱后输出。逆初始置换根据逆初始置换表对乘积变换的结果进行混乱后形成 64 bit 密文。

(3)乘积变换是一个与密钥有关的加密运算,每个子密钥控制一次迭代过程。加密时子密钥序列为 K_1、K_2、…、K_{15}、K_{16},解密时子密钥序列为 K_{16}、K_{15}、…、K_2、K_1,记作 K_i,每个 K_i 是通过置换、选择和移位操作得到的。根据选择运算映射表将输入的 32 bit 信息转换成输出的 48 bit 结果与子密钥进行模 2 加法运算,然后把运算结果分为 8 组,每组 6 bit,分别用相应的选择函数 S_1~S_8 计算。产生 8 组,每组 4 bit,共 32 bit 结果,再通过置换运算和模 2 加法，产生 64 bit 乘积变换结果。如 0.01 通过 ASCII 转换后为:48 46 48 49，左移一位后为:84 64 84 94,然后与子密钥 K_1 进行模 2 加法运算,选择函数 S_1,再进行置换和模 2 加,产生的结果是 001。

DES 加密变换后的数据如表 2:

表 2　DES 加密变频后数据表

X	Y	Z
0001	0011	0001
0012	0001	0010
0011	0010	0013
…	…	…
0051	0012	0051

其次用 RSA 再对 DES 加密的密钥进行二次加密，得到最终的密钥。

RSA 加密实施过程如下:

(1)密钥设计:选取两个互异的素数 P 和 Q,令 $r=P\cdot Q$,$z=(P-1)(Q-1)$;再找 2 个正整数 d 和 e,使之分别满足:z 与 d 互素,$e\cdot d\equiv 1(\mathrm{mod}\ z)$,这里的 e、r 就是公开的加密密钥。例如 r 为

(下转 225 页)