数据库作业四

1. 什么是数据库的安全性?

答：

数据库的安全性是指保护数据库以防止不合法的使用所造成的数据泄露、更改或 破坏。

1. 举例说明对数据库安全性产生威胁的因素。

答：

（1）**非授权用户对数据库的恶意存取和破坏。**一些黑客和犯罪分子在用户存取数据库时猎取用户名和用户口令，然后假冒合法用户偷取、修改甚至破坏用户数据。（2）**数据库中重要或敏感的数据被泄露。**黑客和敌对分子千方百计盗窃数据库中的重要数据，一些机密信息被暴露。（3）**安全环境的脆弱。**操作系统安全的脆弱，网络协议安全保障的不足等都会造成数据库安全性的破坏。

1. 试述实现数据库安全性控制的常用方法和技术。

答：

实现数据库安全性控制的常用方法和技术有以下几种。

**（1）用户身份鉴别：**系统提供多种方式让用户标识自己的名字或身份。用户要使用数据库系统时，由系统进行核对，通过鉴定后才可以使用数据库。

**（2）多层存取控制：**系统提供用户权限定义和合法权限检査功能，用户只有获得某种权限 才能访问数据库中的某些数据。

**（3）视图机制：**为不同的用户定义不同的视图，通过视图机制把要保密的数据对无权存取 的用户隐藏起来，从而自动对数据提供一定程度的安全保护。

**（4）审计：**建立审计日志，把用户对数据库的所有操作自动记录下来放入审计日志中，审 计员可以利用审计信息重现导致数据库现有状况的一系列事件，找出非法存取数据的人、时间和内容等。

**（5）数据加密**：对存储和传输的数据进行加密处理，从而使不知道解密算法的人无法获知数据的内容。

1. 什么是数据库中的自主存取控制方法和强制存取控制方法？

答：

（1）**自主存取控制方法：**定义各个用户对不同数据对象的存取权限。当用户对数据库访问时 首先检査用户的存取权限。防止不合法用户对数据库的存取。自主存取控制中自主的含义是：用户可以将自己拥有的存取权限“自主”地授予别人, 即用户具有一定的“自主”权。

（2）**强制存取控制方法：**每一个数据对象被（强制地）标以一定的密级，每一个用户也被（强制地）授予某一个级别的许可证。系统规定只有具有某一许可证级别的用户才能存取某一 个密级的数据对象。

1. 对下列两个关系模式：

学生（学号，姓名，年龄，性别，家庭住址，班级号）

班级（班级号，班级名，班主任，班长）

使用GRANT完成下列授权功能：

①授予用户U1拥有对两个表的所有权限，并可给其他用户授权；

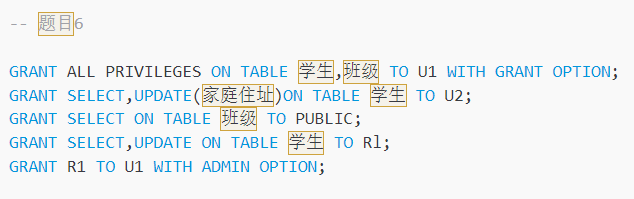
②授予用户U2对学生表具有查看权限，对家庭住址具有更新权限；

③将对班级表查看权限授予所有用户。

④将对学生表的查询、更新权限授予角色Rio

⑤将角色R1授予用户U1,并且U1可继续授权给其他角色。

答：



1. 今有两个关系模式：

职工（职工号，姓名，年龄，职务，工资，部门号）

部门（部门号，名称，经理名，地址，电话号）

请用SQL的GRANT和REVOKE语句（加上视图机制）完成以下授权定义或存取控制功能：

①用户王明对两个表有SELECT权限。=

②用户李勇对两个表有INSERT和DELETE权限。

③\*每个职工只对自己的记录有SELECT权限；

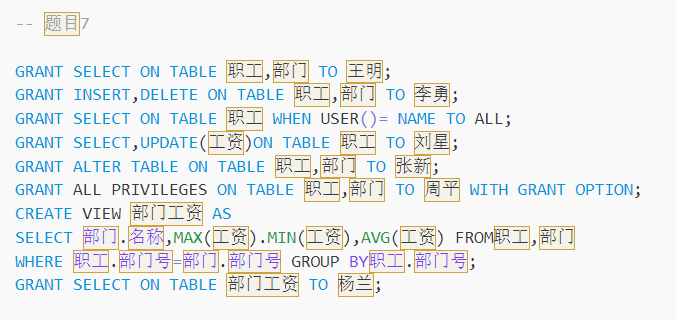
④用户刘星对职工表有SELECT权限，对工资字段具有更新权限。

⑤用户张新具有修改这两个表的结构的权限。

⑥用户周平具有对两个表所有权限（读，插，改，删数据），并具有给其他用户授权的 权限。

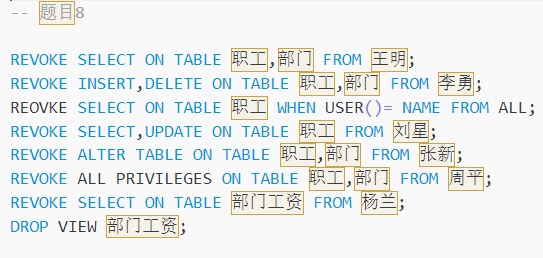
⑦用户杨兰具有从每个部门职工中SELECT最高工资、最低工资、平均工资的权限，他不能查看每个人的工资。

答：



1. 把习题7中①〜⑦的每一种情况，撤销各用户所授予的权限。

答：



1. 理解并解释MAC机制中主体、客体、敏感度标记的含义。

答：

1. 主体是系统中的活动实体，既包括DBMS所管理的实际用户，也包括代表用户的各进程。（2）客体是系统中的被动实体，是受主体操纵的，包括文件、基本表、索引、视图等。（3）对于主体和客体，DBMS为它们每个实例（值）指派一个敏感度标记。敏感度标记被分成若干级别，如绝密、机密、可信、公开等。主体的敏感度标记称为许可证级别，客体的敏感度标记称为密级。
2. 举例说明强制存取控制机制是如何确定主体能否存取客体。

答：

假设要对关系变量S进行强制存取控制，为简化起见，假设要控制存取的数据单元是元组，则每个元组标以密级，如下表示（4 =绝密，3 =机密,2 =秘密）。

SNO SNAME STATUS CITY CLASS

S1 Smith 20 London 2

S2 Jones 10 Paris 3

S3 Clark 20 London 4

假设系统的存取规则是：

① 仅当主体的许可证级别大于或等于客体的密级时才能读取相应的客体；

② 仅当主体的许可证级別小于或等于客体的密级时才能写相应的客体。

假定用户U1和U2的许可证级别分别为3和2,则根据规则用户U1能读元组S1和S2, 可修改元组S2；用户U2只能读元组S1,修改元组S1。

1. 什么是数据库的审计功能，为什么要提供审计功能？

答：

审计功能是指DBMS的审计模块在用户对数据库执行操作的同时，把所有操作自动记录到系统的审计日志中。

因为任何系统的安全保护措施都不是完美无缺的，蓄意盗窃破坏数据的人总可能存在。利用数据库的审计功能，审计员可以根据审计日志中记录的信息，分析和重现导致数据库现 有状况的一系列事件，找出非法存取数据的人、时间和内容等。