1. 数据库安全性

（自定义函数权限的授权。回收。角色）

1. 计算机安全性概论

答：保护数据库以防止不合法使用所造成的数据泄露、更改或破坏

非法使用数据库的情况（4）

1. 数据库安全性控制

答：用户标识与鉴别，DBMS存取控制，数据加密，审计追踪

数据库安全性控制的常用方法：

用户标识和鉴定、存取控制、视图、审计、密码存储

1. 用户标识与鉴别（注意登录名和用户名的区别）

答：系统提供的最外层安全保护措施

登录名与用户名的区别：

登录名：

Sa：数据库管理员，数据库管理员在SQL Server中的用户名叫dbo

登录名只能进入服务器，未必能访问数据库

程序中连接字符串中的用户名也是指的登录名

一个登录名可以授权访问多个数据库

用户名：

一个或多个登录对象在数据库中的映射

一个登录名在每个数据库中能映射一次

1. 存取控制（自主存取控制方法、授权与回收、数据库角色）

答：

自主存取控制方法：

授权与回收：（在SQL中on后面不用写table）

Grant select on student

To u1;

//

Grant all privileges on student,course

To u2,u3;

//

Grant insert on sc

To u4

With grant option

//

Grant update(sno),select on student

On u5

//

Revoke update(sno) on student

From u4

//revoke select on sc

From public --所有用户

数据库角色：

被命名的一组与数据库操作相关的权限

角色是权限的集合

可以为一组具有相同权限的用户创建一个角色

简化授权的过程

//

Create role R1;

Grant select,update,insert on student

To R1;

Grant R1

To 张大，张二；

Revoke R1

From 张大；

1. 强制存取控制方法

答：保证更高程度的安全性

用户不能直接感知或进行控制

适用于对数据有严格而固定密级分类的部门

军事部门

政府部门

主体是系统中的活动实体

DBMS所管理的实际用户

代表用户的各进程

客体是系统中的被动实体，是受主体操纵的

文件

基表

索引

视图

1. 视图机制

答：

Create view cs1

As

Select \*

From student

Where sdept=’cs’;

Grant select on cs1

To 张大；

//grant all privileges on cs1

To 张二；

本章考核要求：

4.1 掌握：身份验证、存取控制、角色管理

4.2 了解：安全标准、强制存取控制、审计、数据加密

4.3 难点：身份验证、存取控制、角色管理

4.4 难点：身份验证、存取控制、角色管理