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。

2.举例说明对数据库安全性产生威胁的因素。

答：例如未授权访问，弱密码，SQL 注入攻击等等。

4.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。

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。

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

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。

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。

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。

5.什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，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查用户的存取权限,防止不合法用户对数据库的存取。

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。

6. 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。

答：GRANT ALL PRIVILEGES ON TABLE 学生 班级 TO U1 WITH GRANT OPTION;

(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。

答：GRANT SELECT,UPDATE (家庭住址) ON TABLE 学生 TO U2;

(3) 将对班级表查看权限授予所有用户。

答：GRANT SELECT ON TABLE 班级 TO PUBLIC;

(4) 将对学生表的查询、更新权限授予角色 R1。

答：GRANT SELECT UPDATE ON TABLE 学生 TO R1;

(5) 将角色 R1 授予用户 U1 并且 U1 可继续授权给其他角色。

答：GRANT R1 TO U1 WITH ADMIN OPTION;

7.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 SOL 的 GRANT 和 REVOKE 语(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

答：GRANT SELECT ON TABLE 职工,部门 TO 王明;

(2)用户李勇对两个表有 INSERT 和 DELETE 权限
答：GRANT INSERT,DELETE ON TABLE 职工,部门 TO 李勇;
(3)每个职工只对自己的记录有 SELECT 权限
答：GRANT SELECT ON TABLE 职工 WHEN USER()= NAME TO ALL;
(4)用户刘星对职工表有 SELECT 权限，对工资字段具有更新权限。
答：GRANT SELECT,UPDATE(工资) ON TABLE 职工 TO 刘星;
(5)用户张新具有修改这两个表的结构的权限。
答：GRANT ALTER TABLE ON TABLE 职工,部门 TO 张新;
(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。
答：GRANT ALL PRIVILEGES ON TABLE 职工,部门 TO 周平 WITH GRANT OPTION;
(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：CREATE VIEW 部门工资 AS
SELECT 部门,名称,MAX(工资),MIN(工资),AVG(工资)
FROM 职工,部门
WHERE 职工.部门号=部门.部门号
GROUP BY 职工.部门号;
GRANT SELECT ON TABLE 部门工资 TO 杨兰;

8.对习题 7 中~的每一种情况,撤销各用户所授予的权限。

(1)答：DREVOKE SELECT ON TABLE 职工,部门 FROM 王明;
(2)答：REVOKE INSERT,DELETE ON TABLE 职工,部门 FROM 李勇;
(3)答：REOVKE SELECT ON TABLE 职工 WHEN USER()= NAME FROM ALL;
(4)答：REVOKE SELECT,UPDATE ON TABLE 职工 FROM 刘星;
(5)答：REVOKE ALTER TABLE ON TABLE 职工,部门 FROM 张新;
(6)答：REVOKE ALL PRIVILEGES ON TABLE 职工,部门 FROM 周平;
(7)答：REVOKE SELECT ON TABLE 部门工资 FROM 杨兰;
DROP VIEW 部门工资;

9.理解并解释 MAC 机制中主体、客体敏感度标记的含义。

答：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。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。

10.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,如下表所示(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:
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
仅当主体的许可证级别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。

11.什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。