P.154 1、4、6、7(1-4-6-7)、11

1. 什么是数据库的安全性

   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. 叙述是现实数据库安全性控制的常用方法和技术

   - 用户标识和鉴别：系统提供一定方式让用户标识自己的名字和身份，每次进入系统时由系统进行核对，鉴定后再提供系统的使用权。
   - 存取控制：通过用户权限定义和合法权检查确保只有合法权限的用户访问数据库，所有未授权的人员无法存取数据。
   - 视图机制：为不同的 用户定义视图，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，从而自动地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。
   - 数据加密：对存储和传输的数据进行加密处理，从而使得不知道解密算法的人无法获知数据的内容。

3. 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语句完成下列授权功能。

   - 授予用户U1对两个表的所有权限，并可以给其他用户授权。

     ```
     GRANT ALL PRIVILEGES
     ON TABLE 学生,班级
     TO U1
     WITH GRANT OPTION;
     ```

   - 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。

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

   - 将对班级查看权限授予所有用户。

     ```
     GRANT SELECT
     ON TABLE 班级
     TO PUBLIC
     ```

   - 将对学生表的查询，更新权限授予角色R1。

     ```
     GRANT SELECT, UPDATE
     ON TABLE 学生
     TO R1;
     ```

   - 将角色R1授予用户U1，并且U1可以继续授权给其他角色。

     ```
     GRANT R1
     TO U1
     WITH ADMIN OPTION;
     ```

4. 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)

   使用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。

   - 用户王明对两个表有SELECT权限

     ```
     GRANT SELECT
     ON TABLE 职工,部门
     TO 王明
     ```

   - 用户刘星对职工表有SELECT权限，对工资字段具有更新权限

     ```
     GRANT SELECT, UPDATE(工资)
     ON TABLE 职工
     TO 刘星
     ```

   - 用户周平具有对两个表的所有权限(读，插，改，删)，并具有给其他用户授权的权限。

     ```
     GRANT ALL PRIVILIGES
     ON TABLE 职工,部门
     TO 周平
     WITH GRANT OPTION;
     ```

   - 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。

     ```
     CREATE VIEW 工资信息 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 工资信息
     TO 杨兰
     ```

5. 什么是数据库的审计功能，为什么提供审计功能。

   - 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，DBA 可以根据审计跟踪的信息，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。