第 7章 数据库系统安全作业

一、填空题

1、数据库安全是保证数据库信息的 机密性、完整性 、可用性 、可控性 和 隐私性， 防止系统软件及其数据遭到破坏、更改和泄漏

2、数据库的结构分为 内模式、概念模式、外模式 。

3、数据库系统一般分为两个部分： 数据库，DBMS 。

4、数据库加密分为 库内加密和 库外加密。

5、安全审计的分析方法包括：潜在违规分析 ， 基于异常检测的描述，简单攻击试探法 ，复杂攻击试探法 。

二、选择题

1、以下描述是正确的是（B ）

A.数据库在执行事务处理时，先操作数据库，再写日志；

B.数据库在执行事务处理时，先写日志，再操作数据库；

C．数据库在执行事务处理时，只需要操作数据库，不需要写日志；

D.数据库在执行事务处理时，操作数据库和写日志同时进行。

2、用户访问数据库时，涉及以下哪些安全内容（ABCE ）

A.授权规则；B.语义完整性检查；C.用户登录鉴别；D.数据加密；E.审计追踪

3、根据数据库的特点和实际需求，数据库加密必须满足以下要求（ BCE）

A.对数据库加密对原有系统功能的影响不大；

B.加解密的速度必须足够快，特别是对解密的速度要求更高；

C.加密机制在理论上和计算上都具有足够的安全性；

D.加密后的数据库存储量不增加，不能破坏字段长度的限制；

E.加解密对数据库的合法用户是透明的。

4、数据库加密的粒度可以分为以下哪几类（ ABCEF）

A.数据库；B.表；C.记录；D.页面；E.字段；F.数据项

三、简答题

1.数据库加密应具备哪些要求？

由于数据库中的记录保存时间相对较长，因此加密算法强度要求高。

数据库加密以后，明密文数据长度相同或者相当，不应明显增加，

避免数据库管理系统有较大变动。

对于大型数据库系统而言，数据库最常见的使用方式是随机访问，

所以加解密速度要足够快，对数据操作响应时间的影响应在用户可

接受的范围内。

加密算法应该能够直接对记录或者字段进行加密。

1. 操作系统安全威胁和数据库安全威胁分别是什么？为什么不同？

操作系统安全威胁：病毒，蠕虫，木马，逻辑炸弹，隐蔽通道，天窗

数据库安全威胁：软威胁，硬威胁，传输威胁，人为错误，物理环境威胁。

与OS不同，数据库安全威胁是指针对数据安全而言，主要影响数据安全的都可以称为数据库安全威胁。OS不是没有物理安全威胁，而是统统划归物理安全中，这是因为，OS是安装在物理平台上的，硬件平台的安全就是OS的物理安全，所以不需要另外再描述。

四、问答题

1.什么是数据库系统的安全策略？它包括哪几个方面，目的分别是什么？

数据库安全策略是组织、管理、保护和处理敏感信息的规则，包括安全管理策略、信息流控制策略和访问控制策略。

安全管理策略的目的是定义用户共享数据和控制它的使用。

信息流控制策略主要考虑如何控制一个程序去访问数据。

访问控制策略是数据库安全策略的重要组成部分，一般分为：集中式控制和分布式控制。

1. 数据库的恢复技术包含哪些，各有什么特点

数据库的恢复技术包括：事务故障的恢复，系统故障的恢复，介质故障的恢复。

事务故障恢复：在不影响其他事务运行的情况下，强行回滚该事务。

系统故障恢复：让所有非正常终止的事务回滚，强行撤销所有未完成的事务，重做（REDO）所有已提交的事务，从而保证数据库恢复到一致性状态。

介质故障的恢复：介质故障的恢复不仅要使用日志，还要借助于数据库备份。