八+九章

大纲：

第八章

1、软件工程

软件危机，软件的生命周期。

2、信息系统

关系数据库，E-R图

第九章

1、网络安全

网络安全定义，病毒、木马的定义及预防方法；

2、信息加密

加密，明文，密文，对称、非对称加密

3、网络检测

防火墙，入侵检测；其它提高网络安全的方法；

4、**计算机病毒**

概念，计算机病毒特征，病毒预防；

5、职业道德与规范

计算机人员职业道德，软件知识产权，计算机犯罪及预防；

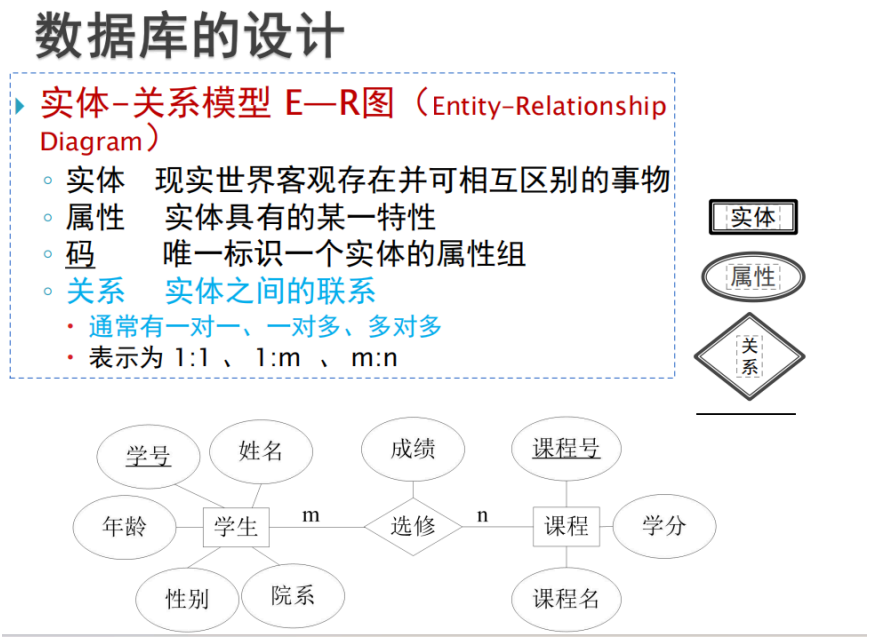
第八章：

1.关系数据库

常见的关系数据库

◦ Oracle、SQL Server、Access、IBM DB2、Sybase

2.数据库的设计



3.软件工程

软件危机：指在计算机软件的开发和维护过程中遇到的一系列严重问题。

软件危机的典型表现是：

（1）软件开发成本和进度无法预测。

（2）用户对已完成的软件系统不满意。

（3）软件可靠性没有保证。

（4）软件没有适当的文档资料。

（5）软件维护费用不断上升。

如何克服软件危机?

用软件工程的概念、原理、技术和方法进行计算机软件的开发、管理、维护和更新。

软件生命周期：一个软件从提出开发要求开始，到开发完成投入使用，直至废弃为止的整个时期

第九章

1.网络安全

定义：网络安全是指为保护网络不受任何损害而采取的所有措施的综合，一般包含网络的保密性、完整性和可用性。

病毒定义：计算机病毒是一种人为蓄意制造的、以破坏为目的的程序。//它寄生于其他应用程序或系统的可执行部分，通过部分修改或移动程序，将自我复制加入其中或占据宿主程序的部分而隐藏起来，在一定条件下发作，破坏计算机系统。

病毒特征：

1.破坏性

2.隐蔽性

3.传染性

4.潜伏性

5.非授权可执行性

木马定义：木马（全称为特洛伊木马）是在执行某种功能的同时进行秘密破坏的一种程序。//木马可以完成非授权用户无法完成的功能，也可以破坏大量数据。

预防方法：

不使用来历不明的程序或软件；在使用移动存储设备之前应先杀毒；安装防火墙，防止网络上的病毒入侵；安装最新的杀毒软件，并定期升级，实时监控；养成良好的电脑使用习惯，定期优化、整理磁盘，养成定期全面杀毒的习惯；对于重要的数据信息要经常备份，以便在机器遭到破坏后能及时得到恢复。

2.信息加密

加密：使用数学方法来重新组织数据，使得除了合法的接受者之外，其他任何人都不能恢复原先的信息。

明文：加密前的信息；密文：加密后的信息。

对称加密：

在对称加密中，信息的加密和解密使用同一密钥。

优点：安全性高、加密速度快。

缺点：管理的密钥多；密钥的传递存在风险。

常用的对称加密算法有DES和IDEA。

非对称加密：

在非对称加密中，信息的加密和解密使用不同密钥，参与加密过程的密钥公开，称为公钥，参与解密过程的密钥为用户专用，称为私钥，两个密钥必须配对使用。

常用的非对称加密算法有RSA、背包算法等。

3.网络检测

防火墙是一种用来加强网络之间访问控制的特殊网络互联设备，它对网络之间传输的数据包和链接方式按照一定的安全策略进行检查，以此决定网络之间的通信是否被允许。

入侵检测是指主动地从计算机网络系统中的若干关键点收集信息并分析这些信息，确定网络中是否有违反安全策略的行为和受到攻击的迹象，并有针对性地进行防范。**入侵检测技术主要基于特征检测和异常检测。**

4.职业道德与规范

计算机专业技术人员的道德责任：

原则一：计算机从业人员应当以公众利益为最高目标。

原则二：客户和雇主在保持与公众利益一致的原则下,计算机从业人员应注意满足客户和雇主的最高利益。

计算机软件著作权保护

发表权，即决定软件是否公之于众的权利；
开发者身份权，即表明开发者身份的权利以及在其软件上署名的权利；
使用权，即在不损害社会公共利益的前提下，以复制、展示、发行、修改、翻译、注释等方式使用其软件的权利。
使用许可权和获得报酬权，即许可他人以上述方式使用其软件的权利和由此获得报酬的权利；
转让权，即向他人转让上述使用权和使用许可权的权利。

计算机犯罪防范对策

（1）完善计算机立法。

（2）加强惩治计算机犯罪的应对机制。

（3）加强计算机安全技术研究，提高计算机系统本身的技术防御能力。

（4）加强管理与教育。