考试形式：

9大题简答题—来源各章课后习题，每题可能有若干问

重点在：信息安全技术基本概念、基本方法（名词解释等），信息安全技术基本应用

例：

什么叫信息安全技术？（可能要举例）

第一章习题1.1：解释安全性完整性可用性等，最基本安全服务六个目标（举例）

信息安全技术应用解决实际问题：

如防火墙、PGP等（核心技术和信息系统的结合）

第一章：安全服务基本概念

信息安全核心技术—密码技术—三个大的模块—核心技术成分（对称密码技术AES，DES算法核心差别（feistel））（古典密码、卡塞密码等对称密码的核心技术）（第二章思考题）（什么是置换密码）

第三章和第五章：DES，对称密码构建衡量标准，混淆扩散，AES和DES差别

非对称密码：RSA/ECC（基于什么数学难题所设计）

对称密码和非对称密码最主要的差别、非对称密码的应用（实际应用更多两者一起用）、什么时候用对称密码什么时候用非对称密码

↑以实例形式理解

第六章和第七章：分组密码流密码的概念、理论模型

如何实现、应用分组密码，有若干种实现模式，典型例子，优缺点，为什么用现有商业密码而不是流密码

三大模块：对称密码，非对称密码，hash函数

Deffie-Hellman密钥交换协议—最基本模型，公钥密码体制理想环境下的密钥交换协议，漏洞为中间人攻击（举简单例子）

数学难题--离散对数问题

对称密码：每一对通信方分配对称密钥

非对称密码：每一方有两个密钥，公钥和私钥

什么是Hash函数，为什么要有hash函数—消息摘要，电子指纹，在密码技术的应用—完整性检验、抗抵赖、身份认证，实际应用中需要带有密钥的hash函数以防中间人攻击

第十二章：消息认证码

第十三章：数字签名，为什么还要DSS或DSA

第十四章和第十五章：密钥管理和用户认证，可结合十二章十三章

带有密钥的hash函数HMAC，对称密码和非对称密码怎么用hash函数进行消息认证和身份认证

Kerberos基于对称密码的身份认证模型，PKI数字证书（基于非对称密码）

主密钥、会话密钥

16-20章网络安全：网络访问控制和云安全

密码技术和网络技术的结合，基于TCPIP技术

访问控制（加密数据库管理）

SSL/SSH

PGP（没有物理载体）

附录三章：

恶意软件（病毒等）

IDS（入侵检测系统）

防火墙

重点在前12章

不做要求：

第四章（简单了解4.5）

第七章

第八章