

一、课程目标

课程目标 1：全面了解信息安全知识领域的体系结构，了解信息安全发展历史，了解信息安全技术产生与发展，了解信息安全问题对国家及社会的影响；

课程目标 2：理解密码的基本理论及应用方法，掌握身份认证及访问控制的基本方法，具有设计信息安全方案的初步能力，了解网络威胁的产生机理与网络防御的基本技术，具有解决信息安全问题的初步能力；

课程目标 3：了解信息安全系统、工程的技术标准及操作规范，明确有关信息安全的法律法规，建立初步信息安全工程素质和全面的信息安全法律意识。

二、课程内容要点

章节	教学内容	要求
1. 信息安全概述	<ul style="list-style-type: none">● 信息安全内涵与外延● 信息安全的发展历程● 信息安全威胁分类● 互联网的安全性● 面向目标的知识体系● 面向应用的层次型技术体系● 面向过程的保障体系	<ol style="list-style-type: none">1. 理解信息安全基本内涵和外延2. 了解网络空间的安全性3. 明确信息安全知识及技术体系
2. 密码学应用基础	<ul style="list-style-type: none">● 密码体制及分类● 古典密码（单表代替、多表代替）● 数据加密标准 DES● DH 秘钥交换算法● RSA 公开密钥算法● 消息认证	<ol style="list-style-type: none">1. 掌握密码体制设计的基本方法2. 掌握古典代替密码的基本原理及应用3. 掌握对称密钥密码的基本原理及应用4. 掌握公开密钥密码的基本原理及应用5. 掌握消息认证基本原理及应用及应用
3. 物理安全	<ul style="list-style-type: none">● 设备安全防护（防火、防盗、防静电、防雷击）● 电磁泄漏● 防窃听● 隔离，容错与容灾	<ol style="list-style-type: none">1. 理解物理安全的重要性2. 明确信息设备安全防护的注意事项3. 了解电磁泄漏及如何防窃听4. 了解网络隔离技术原理5. 理解容错与容灾的基本方法
4. 身份认证	<ul style="list-style-type: none">● 基于对称加密的认证协议● 基于公开密钥的认证协议● PKI 技术● X. 509	<ol style="list-style-type: none">1. 掌握身份认证的基本思想2. 掌握设计基于对称加密及非对称加密的认证协议的技术方法3. 理解 PKI 及 X. 509 等结构及原理
5. 访问控制	<ul style="list-style-type: none">● 自主访问控制● 强制访问控制● 基于角色的访问控制● windows 系统的安全管理	<ol style="list-style-type: none">1. 掌握访问控制的基本思想2. 掌握设计访问控制解决方案的技术方法3. 理解 windows 系统的安全管理
6. 网络威胁	<ul style="list-style-type: none">● 计算机病毒的原理与防治<ul style="list-style-type: none">■ 传统病毒■ 蠕虫■ 木马● 网络入侵原理与防范● 诱骗类威胁	<ol style="list-style-type: none">1. 理解网络威胁的基本分类2. 掌握计算机病毒的原理与防范技术3. 掌握网络入侵原理与防范技术4. 掌握诱骗类威胁原理与防范技术。
7. 网络防御	<ul style="list-style-type: none">● 防火墙原理及相关技术● IPtables/ Netfilter 技术原理● IDS 原理及相关技术● Snort 系统● VLAN, IPS 与 IMS	<ol style="list-style-type: none">1. 理解网络防御基本思想2. 理解防火墙原理及相关技术，掌握 IPtables/Netfilter 的技术原理3. 理解 IDS 原理及相关技术，掌握 Snort 系统的技术原理4. 理解 IPS 与 IMS 等的防御技术

8. 网络安全协议	<ul style="list-style-type: none"> ● IPSec 协议的体系结构及工作原理 ● SSL 协议 ● HTTPS 协议 ● 电子商务流程 ● SET 协议 	<ol style="list-style-type: none"> 1. 理解网络安全协议的分类 2. 理解掌握 IPSec、SSL、SET 协议的体系结构及工作原理 3. 掌握设计网络应用的安全协议的基本方法
9. 内容安全	<ul style="list-style-type: none"> ● 数字版权保护 <ul style="list-style-type: none"> ■ DRM 原理 ■ 数字水印 ● 网络信息内容监管技术 ● 垃圾邮件系统 	<ol style="list-style-type: none"> 1. 理解内容安全内涵与分类 2. 理解数字版权保护的基本原理,掌握设计版权保护系统的基本思路 3. 理解内容监管系统设计原理,掌握设计垃圾邮件处理系统的基本思路
10. 信息安全管理	<ul style="list-style-type: none"> ● 风险评估与风险控制 ● CC 标准, BS7799 ● 中国相关信息安全标准 ● 信息犯罪 ● 信息道德规范 ● 信息安全法律法规 	<ol style="list-style-type: none"> 1. 理解信息安全的内涵 2. 理解风险评估与风险控制,掌握基本评估及控制方法 3. 明确信息安全系统、工程的技术标准及操作规范 4. 明确有关信息安全的法律法规