

## 第一章

- P13 信息安全三要素: CIA. 可控, 不可抵赖  
ISO安全体系 三大部分 安全机制  
五大安全服务
- P18 PDRR PDDR 两个安全模型
- P22 PCSIC 安全标准
- P23 CC标准  
我国标准的五个等级

## 第二章

古典密码与现代密码的区别

{ 对称加密机制

常见对称加密算法

非对称加密机制:

常见非对称加密算法

- P67 密钥管理技术 什么结构 层次结构  
会话密钥  
主密钥

P73 密钥分配


P74 密钥分配方案图 集中式/分布式 ★ 流程:

## 第四章

P81 哈希函数 特点

P84~P85 数字签名完整过程 (签名和验证)  
数字签名如何体现三个特性

P89 认证技术 (3-4种)

P94 Kerberos 过程 

## 第五章

P98 PKI { 什么是PKI  
PKI提供哪些安全服务 ☆ P99  
以上服务用什么机制体现 ☆  
PKI组成 ☆ P100

P104 PKI解决什么  
数字证书 一般放什么  
X.509通用证书格式

P101 CRL里放什么

## 第六章

什么是漏洞  
攻击的第一个部分 - 信息收集 信息收集方法

P123 ARP欺骗 { 什么是ARP  
图 P124  
ARP欺骗为什么会成功:

P125 社工学攻击目标: 人

P128 口令密码的攻击 { 主动 { ...  
被动 { ...

P133 DOS, DDOS

第5章

什么是恶意代码

蠕虫、木马、计算机病毒 ☆

访问控制技术 { 访问控制三种策略 P151

P152 防火墙 ☆ DMZ ☆!!

三种类型防火墙 { 包过滤 ☆☆ 超重点  
状态检测 包过滤规则  
代理网关

P155 防火墙不能防范什么 {  
- -  
- -  
- -  
- -

防火墙按 顺序优先 匹配规则

P175 入侵检测

P177 检测技术

P179

# 第九章

P107 什么是VPN

P189 VPN隧道方式

VPN网络建立方式

Host → Host

Host → VPN网关

VPN网关 → VPN网关

Remote User → VPN网关