# 信息与信息技术

信息是什么？信息与“消息”“情报”“知识”区别。 P(4)

熵 P(8)

信息技术 P(10)

信息技术发展阶段，现阶段趋势 P(11、12)

信息安全是什么 P(14)

信息安全有哪些威胁（系统，网络，实体，数据，内容，安全管理）P(15-20)

为什么需要信息安全 P(21)

信息安全的应用场景（安全攻击中的主动攻击和被动攻击） P(22-26)

一些常见的攻击方式 P(27)

CIA安全模型（保密性，完整性，可用性） P(29-37)

信息安全的研究内容，基本观点 P(38、39)

绝对的安全是不存在的！！ P(40-结束)

# 加密解密

密码技术的发展（四阶段） P(45)

密码系统组成（明文空间，密文空间，密钥空间、加密算法，解密算法）P(50-53)

密码系统的分类 P(54-56)

密码系统的安全 P(58-61)

密码学研究（数学基础） P(62,63)

## 古典密码

塞塔式密码（置换密码） P(65-68)

替代密码（单表，同音，多表，多字母） P(69-73)

一次一密方案（OTP） P(74-76)

密码机 P(77)

## 现代密码技术

序列密码 P(79-81)

分组密码 P(82-85)

Feistel P(86-89)

DES P(90-104)

ECB P(105、106)

CBC P(107、108)

CFB P(109-111)

OFB P(112-114)

DES的安全性和DES的破译 P(115、116)

其他分组密码 P(117)

## 公钥密码体制

基本思想 P(118-119)

公钥密码体质基本条件 P(120)

公钥密码体制算法条件 P(121)

单向陷门函数 P(122-123)

RSA P(124-126)

# 数字签名

如何保证一份文件的真实特性？以及真实性内涵 P(128)

数字签名与消息认证区别 P(129)

手写签名的特性 P(130)

数字签名的设计目标 P(132)

数字签名的特性 P(133)

数字签名主要算法 P(134)

RSA数字签名 P(135-139)

DSS签名 P(140-141) 还没看！

RSA VS DSA P(142)

其他签名模式（不可否认签名，盲签名，群签名，代理签名、指定证实人签名）P(143-146)

# 区块链 （P148）

中心化弊端 P(153)

区块链起源：比特币诞生中本聪 P(151)

区块链特性：去中心化，不可篡改，可追溯。交易透明，双方匿名。开放共识。P(154-158)

区块链的种类和主要区别 P(159、160)

区块链的数据结构 P(161-175)

区块链网络 P(176,177)

区块链交易产生过程 P(178-181)

区块链基本原理-POW原理 P(182)

分叉解决机制 P(183)

51%攻击问题 P(184-188)

区块链的优势和劣势 P(187)

常用数字货币平台 P(188)

# 防火墙

防火墙的概念 P(190)

防火墙的特性

防火墙的作用

防火墙的性能指标

防火墙的优缺点 P(194,195)

防火墙的发展 P(196)

防火墙技术(包过滤技术，应用代理，状态检测技术) P(197)

包过滤技术 P(198-209)

包过滤特性 P(210-216)

包过滤技术的局限性 P(217)

代理技术 P(218)

代理技术：应用层网关 P(219,220)

代理技术：电路级网关 P(221,222)

状态检查技术 P(224)

地址翻译技术NAT P(225,226)

防火墙的体系结构 P(227)

屏蔽路由器，单宿，双宿，屏蔽字网体系主机网关P(228)

# 入侵检测

传统安全技术是否足够 P(236)

什么是入侵检测 P(237)

入侵检测的目的 P(238)

入侵检测的起源 P(239-240)

入侵检测系统的需求特性 P(241)s

入侵检测性能关键参数 P(242)

入侵检测的一般过程 P(243)

信息收集 P(244)

信息收集的来源 P(245)

3种信息分析(分析技术) P(246)

结果处理(响应) P(247)

入侵检测系统的通用模型 P(248)

入侵检测的分类 P(249)

基于主机的入侵检测HIDS P(250-252)

基于网络的入侵检测NIDS P(253-255)

两种IDS的比较 P(256)

入侵检测建模：异常检测 P(257-258)

异常检测的优缺点 P(259)

误用检测 P(260-262)

误用检测的优缺点 P(263)

误用检测和异常检测的比较 P(264)

网络入侵检测系统举例 P(265)

误用检测和异常检测的比较 P(266)

分析数据包 P(267)

模式匹配 P(268)

协议分析 P(269)