第一图书网, tushu007.com

<<信息安全基础>>

图书基本信息

书名：<<信息安全基础>>

13位ISBN编号：9787040201963

10位ISBN编号：7040201968

出版时间：2006-12

出版时间：高等教育

作者：徐茂智

页数：125

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

内容概要

《信息安全基础》介绍信息安全事先防护理论和技术的基础知识，不追求大而全，而把目标确定为使学生学到结构化的知识和对信息安全有一个系统的了解。
《信息安全基础》由基本概念、基本算法、基础密码协议、安全模型、应用技术和基础设施共六章组成。
前四章为《普通高等学校信息与计算科学专业系列丛书：信息安全基础》的重点，内容包括基本概念、基本算法与模型的详细讨论。
第五章对繁杂的实用技术进行了介绍，主要包括Web安全、数据库安全、电子交易安全三个重要的应用技术的介绍，而对操作系统安全、数据库安全、病毒防护、防火墙、VPN及入侵检测等系统安全方面的知识仅做了概念性的介绍。
第六章围绕密钥安全和授权体系对PKI、SKI、PMI的基本知识进行讲述。
《信息安全基础》适用于数学、计算机、通信、电子和信息专业的本科高年级学生和研究生一学期课程使用。

<<信息安全基础>>

书籍目录

第1章 基本概念1 因特网与网络环境下的信息安全1.1.1 安全攻击的基本类别1.1.2 常用的信息安全防护技术和产品1.1.3 信息安全研究的基本内容2 安全服务1.2.1 机密性1.2.2 完整性1.2.3 身份识别1.2.4 访问控制1.2.5 防抵赖1.2.6 权利保护3 安全机制简介1.3.1 加密1.3.2 数字签名1.3.3 消息鉴别1.3.4 身份识别1.3.5 访问控制1.3.6 公证与可信第三方1.3.7 通信量填充、信息隐藏与路由控制1.3.8 数据备份1.3.9 恢复1.3.1 0事件检测与安全审计1.3.1 1捕杀恶意程序习题1第2章 基本算法1 密码学简介2.1.1 传统密码系统2.1.2 公钥密码系统2 传统密码算法2.2.1 DES加密算法2.2.2 A5加密算法2.2.3 其他加密算法2.2.4 密码算法与数据机密性3 传统密码技术2.3.1 分组密码使用模式2.3.2 通信加密2.3.3 存储加密4 公钥加密算法2.4.1 公钥密码思想2.4.2 RSA加密算法2.4.3 Diffie.Hellman密钥交换算法2.4.4 EIGamal加密算法5 数字签名算法2.5.1 RSA数字签名2.5.2 E1Gamal数字签名6 HASH函数2.6.1 Hash函数SHA.1 2.6.2 数据完整性和Hash函数习题2第3章 基础密码协议1 安全协议概述2 密钥分发与认证协议3.2.1 密钥交换3.2.2 认证协议3 盲数字签名协议4 比特承诺5 密码协议的应用3.5.1 电子抛币3.5.2 电子投票6 安全多方计算3.6.1 百万富翁问题的多方计算协议3.6.2 平衡薪水问题的多方计算协议习题3第4章安全模型第5章应用技术第6章基础设施参考文献

编辑推荐

《信息安全基础》是在作者为北京大学数学和信息专业的本科高年级学生和研究生讲授信息安全课程讲义的基础上 编写成的。
为使学生较快对信息安全有一个系统的了解，《信息安全基础》力图对读者的基础做最低的要求，并且把重点放在基本概念、基本算法与模型的论述上面，同时也对一些重要的技术进行了介绍。
学生可以学到结构 化的知识、并了解最新技术动态。
内容选取主要集中在事先防护的安全理论和技术方面。
《信息安全基础》内容包括六章：基本概念；基本算法；安全协议；安全模型；应用技术；其它保障技术。
《信息安全基础》可供信息与计算科学、计算机科学以及通信专业的本科高年级学生和研究生课程的教材使用。

第一图书网, tushu007.com

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com