第一图书网, tushu007.com

<<基于案例的网络安全技术与实 >

图书基本信息

书名：<<基于案例的网络安全技术与实践>>

13位ISBN编号：9787302302452

10位ISBN编号：7302302456

出版时间：2012-12

出版时间：清华大学出版社

作者：朱宏峰　等编著

页数：372

字数：608000

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

第一图书网, tushu007.com

内容概要

《21世纪高等院校计算机网络工程专业规划教材：基于案例的网络安全技术与实践》主要介绍了研究和掌握网络安全技术必备的基本数学方法、安全协议以及相关的网络安全典型知识，主要内容包括密码学数学基础、古典密码、计算密码、物理密码、基本安全协议、N方安全协议、网络安全体系结构、网络实体安全、网络安全协议、访问控制与VPN、防火墙与隔离网闸、入侵检测技术、计算机病毒等方法与技术，并同步介绍了这些方法与技术在实际应用中的典型案例。

《21世纪高等院校计算机网络工程专业规划教材：基于案例的网络安全技术与实践》适用于计算机专业本科生以及对当前密码学与网络安全感兴趣的技术人员。

第一图书网, tushu007.com

书籍目录

第一篇 引言
第1章 网络安全概述
1.1 计算机网络安全的概念
1.1.1 计算机网络安全的定义
1.1.2 计算机网络安全的含义
1.2 计算机网络安全的攻击与防御
1.2.1 潜伏者——谁是主要威胁
1.2.2 层次化网络安全的核心问题
1.2.3 网络安全的攻防体系
1.2.4 影响网络安全的因素
1.3 计算机网络安全的宏观层次
1.3.1 安全立法
1.3.2 安全管理
1.3.3 安全技术措施
1.4 计算机网络安全的法律和法规
1.4.1 国外的相关法律和法规
1.4.2 我国的相关法律和法规
1.5 小结
1.6 习题
第2章 数学基础
2.1 数论基础
2.1.1 整除及辗转相除
2.1.2 算术基本定理
2.1.3 同余式
2.1.4 费马小定理和欧拉定理
2.2 抽象代数基础
2.3 离散概率基础
2.4 信息论基础
2.5 计算到底有多难：复杂性理论基础
2.5.1 基本概念
2.5.2 计算模型与判定问题
2.5.3 复杂性类
2.6 计算困难问题及其假设
2.6.1 大整数因子分解问题和RSA问题
2.6.2 离散对数和Diffie-Hellman问题
2.6.3 椭圆曲线和双线性对问题
2.7 小结
2.8 习题
第二篇 密码学——奠基之石
第3章 古典密码
3.1 一些有趣的解谜实例
3.2 密码演化：从艺术到完美
3.3 密码学基本概念
3.4 古典替换密码体制
3.4.1 古典单码加密法

第一图书网, tushu007.com

3.4.2 古典多码加密法
3.5 古典换位密码体制
3.6 隐写术：在敌人面前通信
3.7 小结
3.8 习题
第4章 计算密码
4.1 对称密钥密码
4.1.1 计算对称密码的特点
4.1.2 流密码基本概念
4.1.3 流密码实例
4.1.4 分组密码基本概念
4.1.5 分组密码实例：DES算法
4.2 公开密钥密码
4.2.1 从对称密码到非对称密码
4.2.2 实现：Diffie-Hellman密钥交换
4.2.3 中间人攻击
4.2.4 RSA密码系统：凑成欧拉定理
4.3 散列函数
4.3.1 我的“奶酪”完整么
4.3.2 鸽洞原理与随机预言
……
第三篇 安全协议——衔接之桥
第四篇 网络安全——应用之钥
附录
参考文献

第一图书网, tushu007.com

章节摘录

版权页： 插图： 量子密码学有广义和狭义之分。
狭义量子密码学主要指量子密钥分配等基于量子技术实现经典密码学目标的结果，广义量子密码学则是指能统一刻画狭义量子密码学和经典密码学的一个理论框架。
经典密码学和一切与量子性质有关的密码学结果可以统一在“量子信息密码学”框架下。
这里“量子信息”概念十分重要。
把量子态视为信息，对量子态提出信息论问题，是人类在信息概念上的巨大飞跃，是基于自然界基本定律对信息概念的自然推广，是量子信息科学的基石。
因为经典信息是量子信息的一个子集，在量子信息上建立的密码学才是一个自洽理论。
经典密码学和狭义量子密码学只是作为量子信息密码学这个普遍理论的两个退化形式而存在。
发展量子信息密码学的目的是研究量子信息的密码编码和密码分析问题，探索希尔伯特空间“量子信息密码学”的理论体系，一方面致力于对量子信息系统安全性问题的解决，一方面希望为有限域上传统的密码学开辟新的道路。
这与应用方面的理念完全不同。
想想从牛顿力学到狭义相对论的推广。
虽然至今建筑、水利、机械、航空航天等仍然只是应用牛顿力学，但铭刻在爱因斯坦墓碑上的那个不朽的公式在使人类长期受到毁灭威胁的同时，也给人类带来了无限的希望。
这就是理论的力量。
所以，理论上做一件事跟应用是完全不同的出发点，将来的作用也不一样。
发展量子信息密码学需要传统的密码学理论和方法，也需要量子信息和量子计算理论，如量子信息论和量子计算复杂性理论，但是这些可能还是远远不够的。
发展量子信息密码学必然涉及概念的创新，必须重新考察密码学的理论基础、研究对象和研究方法。
可以这么说，经典密码与量子密码首先是一个“+”的关系，然后再转变为“×”的关系；或者说是先是黑盒互相调用的关系，再逐步转变为白盒互相融合的关系；总之，经典密码与量子密码之间是辩证统一的。
5.2.2 量子密码的目标与特性 1.量子密码的目标 与传统密码一样，量子密码的目标也是为了实现保密和认证两大功能。
在保密方面，主要密码体制有：经典密码算法+量子密钥分配、量子密码算法+经典密钥分配、纯量子密码算法、基于量子计算复杂性理论的密码（又称为“后量子密码”或“抗量子计算机密码”）等方式。
在认证方面，已有研究成果涉及量子身份认证、量子消息确认、量子签名、量子信道认证、量子安全协议等。
在量子保密体制和认证系统中，量子密钥分配是一个重要课题。
一个量子密钥分配方案通常包括4个过程：量子信号传输、随机编码、秘密协商、保密加强。
物理实现上，量子密钥分配主要以3种模式实现：基于单光子（准单光子）信号、基于连续变量量子信号以及基于纠缠量子信号的实现方式。

第一图书网, tushu007.com

编辑推荐

《21世纪高等院校计算机网络工程专业规划教材:基于案例的网络安全技术与实践》适用于计算机专业本科生以及对当前密码学与网络安全感兴趣的技术人员。

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