<<密码编码学与网络安全>>

图书基本信息

书名：<<密码编码学与网络安全>>

13位ISBN编号：9787505393950

10位ISBN编号：7505393952

出版时间：2004-1-1

出版时间：电子工业出版社

作者：William Stallings

页数：494

字数：819000

<<密码编码学与网络安全>>

内容概要

本书系统地介绍了密码编码学与网络安全的基本原理和应用技术。
全书主要包括下列四个部分。
传统密码部分详细讨论了传统密码算法和设计原理，包括使用传统密码来保证秘密性。
公钥密码和hash函数部分详细讨论了公钥密码算法和设计原理、消息认证码和hash函数的应用，以及数字签名和公钥证书。
网络安全部分讨论了系统层的安全问题，包括入侵者和病毒造成的威胁及相应的对策、防火墙和可信系统的应用。
本书第三版与第二版相比，在继续广泛涵盖密码编码学与网络安全领域内容的同时，新增了有限域、高级加密标准（AES）、RC4密码、CTR模式等内容，并对椭圆曲线密码部分的内容做了很多扩充。此外，对于基本内容的讲述方法也有许多变化和更新。
本书内容全面，讲述深入浅出，便于理解，尤其适合于课堂教学和自学，是一本难得的好书。
特别是本书后面讨论的网络安全在现实世界中的应用，包括已经实现的和正在使用的提供网络安全的实际应用。

本书可作为研究生和高年级本科生的教材，也可供从事信息安全、计算机、通信、电子工程等领域的科技人员参考。

作者简介

William Stallings：在计算机网络和计算机体系结构领域作出了独特的、广泛的贡献。
他在18个专题方面编写出版了48本书籍，五次获得教材和著作家协会颁发的优秀计算机科学和工程教材奖。
他还作为独立顾问为计算机网络制造商、软件开发商、研究机构和计算机用户提供咨询服务

<<密码编码学与网络安全>>

书籍目录

第1章 引言 1.1 服务、机制和攻击 1.2 OSI安全框架 1.3 网络安全模型 1.4 本书概览 1.5 推荐读物 1.6 Internet和Web资源第一部分 对称密码 第2章 传统加密技术 2.1 对称密码的模型 2.2 代换技术 2.3 置换技术 2.4 转轮机 2.5 隐写术 2.6 推荐读物和网址 2.7 关键术语、思考题和习题 第3章 分组密码与数据加密标准 3.1 简化DES 3.2 分组密码原理 3.3 数据加密标准 3.4 DES的强度 3.5 差分分析和线性分析 3.6 分组密码的设计原理 3.7 分组密码的工作模式 3.8 推荐读物 3.9 关键术语、思考题和习题 第4章 有限域 4.1 群、环和域 4.2 模运算 4.3 Euclid算法 4.4 有限域GF（p） 4.5 多项式运算 4.6 有限域GF（2n） 4.7 推荐读物和网址 4.8 关键术语、思考题和习题 第5章 高级加密标准 5.1 高级加密标准的评估准则 5.2 AES密码 5.3 推荐读物和网址 5.4 关键术语、思考题和习题 附录5A 系数在GF（28）中的多项式 第6章 对称密码 6.1 三重DES算法 6.2 Blowfish算法 6.3 RC5算法 6.4 高级对称分组密码的特点 6.5 RC4流密码 6.6 推荐读物和网址 6.7 关键术语、思考题和习题 第7章 用对称密码实现保密性第二部分 公钥加密与hash函数 第8章 数论入门 第9章 公钥密码学与RSA 第10章 密钥管理和其他公钥密码体制 第11章 消息认证和hash函数 第12章 hash算法 第13章 数字签名和认证协议第三部分 网络安全应用 第14章 认证的实际应用 第15章 电子邮件安全 第16章 IP安全性 第17章 Web安全性第四部分 系统安全性 第18章 入侵者 第19章 恶意软件 第20章 防火墙附录A 标准和标准化组织附录B 用于密码编码学与网络安全教学的项目术语表参考文献

<<密码编码学与网络安全>>

版权说明