

《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：9787121027673

10位ISBN编号：7121027674

出版时间：2006-07-01

出版社：电子工业出版社

作者：William Stallings

页数：680

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《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：

对称密码部分讨论了对称密码的算法和设计原理；

公钥加密和散列函数部分讨论了公钥密码的算法和设计原理、报文鉴别码和散列函数的应用等；

网络安全应用部分讨论了系统层的安全问题，包括电子邮件安全、IP安全以及Web安全等；

系统安全部分讨论了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等。

第四版与第三版相比，新增了Whirlpool、CMAC、DDoS以及CCITSE等内容，并对简化的AES、PKI等内容做了扩充。此外，对于基本内容的讲述方法也有许多变化和更新，并新加了100多道习题。

本书可作为信息类专业高年级本科生与低年级研究生的教材，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。

《密码编码学与网络安全》

作者简介

作者：(美)斯托林斯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，五次获得教材和作家协会颁发的优秀计算机科学与工程教材奖。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。

William Stallings获得了麻省理工学院计算机科学博士学位。他在Prentice Hall出版的著作都可以从Prentice Hall的网站<http://WWW.prenhall.com/stallings>上找到。张焕国：教授、博士生导师，武汉大学计算机科学与技术学院副院长。主要从事信息安全、容错计算和计算机应用方面的教学和科研工作。现任中国密码学会理事，中国计算机学会容错专业委员会委员，湖北省电子学会副理事长，湖北省暨武汉市计算机学会理事。

《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DES3.2 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 $GF(2^n)$ 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》

编辑推荐

《密码编码学与网络安全:原理与实践》(第4版英文版)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《密码编码学与网络安全:原理与实践》(第4版英文版)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。

《密码编码学与网络安全》

精彩短评

- 1、经典中的经典啊，内容深入浅出啊
- 2、应付选修课买的...
- 3、这本书的内容很详尽，呵呵，就是因为是英文版的，读起来，可能要费解些。
- 4、国外经典计算机著作，我们网络安全课指定教材，没说的了。中文版的翻译有的不正确，还是看原版的好。
- 5、这书当年是看过的。。。现在退化得。。。openssl的文档都看不懂了
- 6、网络安全的根本其实就是密码编码 不会这个说自己懂安全 都不怕被别人鄙视死吗。。。
- 7、课本
- 8、我算一个计算机比较老的菜鸟。本着计算机，英语和数学一起学习的念头买了本书以及其中文版。送货挺快的（我在四川南充，距离苏州近2000公里）。这也是我在亚马逊第7次买东西，只希望配送费能够少点。

《密码编码学与网络安全》

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:www.tushu000.com