<<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：9787121119910

10位ISBN编号：7121119919

出版时间：2011-1

出版时间：电子工业出版社

作者：斯托林斯

页数：719

<<密码编码学与网络安全>>

内容概要

本书系统介绍了密码编码学与网络安全的基本原理和应用技术。
全书主要包括五个部分：对称密码部分讲解传统加密技术、高级加密标准等；非对称密码部分讲解数论、公钥加密、RSA；第三部分讨论了加密哈希函数、消息认证、数字签名等主题；第四部分分析了密钥管理、用户认证协议；网络与Internet安全部分探讨的是传输层安全、无线网络安全、电子邮件安全及IP安全的问题。
最后，两个附录给出了各章的项目练习和一些例子。
配套网站包含大量的延伸性内容。
本书可作为高校计算机专业、网络安全专业、通信安全专业等相关专业的本科生和研究生的教材，也可供相关技术人员参考使用。

作者简介

作者：（美国）斯托林斯（William Stallings）

<<密码编码学与网络安全>>

书籍目录

章节摘录

插图：There are numerous Web sites that provide information related to the topics of this book. In subsequent chapters, pointers to specific Web sites can be found in the Recommended Reading and Web Sites section. Because the addresses for Web sitestend to change frequently, the book does not provide URLs. For all of the Web siteslisted in the book, the appropriate link can be found at this book's Web site. Othe rlinks not mentioned in this book will be added to the Web site over time.Newsgroups and ForumsA number of USENET newsgroups are devoted to some aspect of cryptography ornet work security. As with virtually all USENET groups, there is a high noise-to-signalratio, but it is worth experimenting to see if any meet your needs. The most relevan tare as follows.

<<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5版)(英文版)》：在全球实现了电子化连接，充满病毒、黑客、电子窃听、电子欺诈的年代，安全是一个极其重要的主题《密码编码学与网络安全:原理与实践(第5版)(英文版)》针对密码编码学和网络安全，从原理和实践两方面提供了实用的知识。
《密码编码学与网络安全:原理与实践(第5版)(英文版)》适合用作密码编码学、计算机安全、网络安全专业的本科生或研究生一学期课程的教材。
在讲解密码编码学和网络安全的实用知识时，《密码编码学与网络安全:原理与实践(第5版)(英文版)》还为教师和学生提供了大量的支持材料。
涵盖最新的主题，扩充了分组密码模型的内容，包含认证加密优化并扩展了AES的讲解扩展了伪随机数发生器的内容新增联邦身份（federated iderltity）、HTTPS、SSH以及无线网络安全的内容全面重写并更新了1Psec新增关于法律和伦理的一章使用Sage计算机代数系统演示密码编码学算法关于密码编码学算法的全面比较对认证和数字签名的完整比较统一、全面地论述了相互信任的主题，比如密钥管理和用户认证针对电子邮件安全同时介绍了PGP和S／MlME

<<密码编码学与网络安全>>

版权说明