

<<密码学与网络安全>>

图书基本信息

书名：<<密码学与网络安全>>

13位ISBN编号：9787302114901

10位ISBN编号：7302114900

出版时间：2005-9

出版时间：清华大学出版社

作者：卡哈特

页数：365

字数：598000

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>

## <<密码学与网络安全>>

### 内容概要

本书清晰易懂地介绍了密码学和网络安全的基本概念和实际问题，探讨了加密、解密、对称和不对称密钥，详细分析和解释了各种主要密码算法，包括数据加密标准（DES），国际数据加密算法（IDEA），RC5，Blowfish，先进加密标准（AES），RSA，数字签名算法（DSA）等，并讨论了主要用于机构的防火墙和虚拟私人网络（VPN）技术，数字证书，数字签名，公钥基础结构（PKI）和XML安全性，安全套接层（SSL），安全超文本传协议（SHTTP），安全电子交易（SET），3D安全、PGP，PEM，S/MIME等。

在无线安全方面研究了WAP、GSM、3G身份认证、单次登录（SSO）等技术。

本书还介绍了拒绝服务（DOS）攻击，联机银行交易等一些案例研究。

本书每章后面给出了多项选择、复习题、编程练习题等。

本书不仅对于普及IT专业人员的网络安全知识、提高普通用户的安全意识会大有裨益，也是本科生和研究生的一本不错的参考书。

## 作者简介

Atul Kahate在印度和世界IT业中已经有8年的工作经验，他取得了统计学学士学位和计算机系统专业的MBA学位。

这是他撰写的第二部IT专著，他过去曾为TataMcGraw-Hill出版公司与他人合成了“Web Technologies-TCP/IP to Inaternt Application Architectures”一书。

目前，他正

## 书籍目录

第1章 安全的基本概念 1.1 简介 1.2 安全需求 1.3 安全方法 1.4 安全原则 1.5 攻击类型 1.6 本书概述 1.7 本章小结 1.8 关键术语和概念 1.9 多项选择题 1.10 复习题 1.11 设计与编程练习 第2章 加密技术 2.1 简介 2.2 明文与密文 2.3 替换方法 2.4 变换加密技术 2.5 加密与解密 2.6 对称与非对称密钥加密 2.7 夹带加密法 2.8 密钥范围与密钥长度 2.9 攻击类型 2.10 本章小结 2.11 关键术语和概念 2.12 多项选择题 2.13 复习题 2.14 设计/编程练习 第3章 计算机对称密钥加密算法 3.1 简介 3.2 算法类型与模式 3.3 对称密钥加密法概述 3.4 数据加密标准 3.5 国际数据加密算法 3.6 RC5 3.7 Blowfish 3.8 高级加密标准 3.9 差分与线性密码分析 3.10 本章小结 3.11 关键术语和概念 3.12 多项选择题 3.13 复习题 3.14 设计/编程练习 第4章 计算机非对称密钥加密算法 4.1 简介 4.2 非对称密钥加密简史 4.3 非对称密钥加密概述 4.4 RSA算法 4.5 对称与非对称密钥加密 4.6 数字签名 4.7 背包算法 4.8 其他算法 4.9 本章小结 4.10 关键术语和概念 4.11 多项选择题 4.12 复习题 4.13 设计/编程练习 第5章 公钥基础设施 5.1 简介 5.2 数字证书 5.3 私钥管理 5.4 PKIX模型 5.5 公钥加密标准 5.6 XML、PKI与安全 5.7 本章小结 5.8 关键术语和概念 5.9 多项选择题 5.10 复习题 5.11 设计/编程练习 第6章 Internet安全协议 6.1 基本概念 6.2 安全套接层 6.3 安全超文本传输协议 6.4 时间戳协议 6.5 安全电子事务规范 ..... 第7章 用户鉴别机制 第8章 实现加密与安全 第9章 网络安全 第10章 加密与安全案例分析 附录A 数学知识 附录B 数字系统 附录C 信息理论 附录D 实际工具 附录E Web资源 附录F ASN、BER、DER简介 附录G 现代安全趋势 多项选择题答案 词汇表

## <<密码学与网络安全>>

### 编辑推荐

《密码学与网络安全》每章后面给出了多项选择、复习题、编程练习题等。

《密码学与网络安全》不仅对于普及IT专业人员的网络安全知识、提高普通用户的安全意识会大有裨益，也是本科生和研究生的一本不错的参考书。

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>