

<<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：9787121033414

10位ISBN编号：7121033410

出版时间：2006-11

出版时间：电子工业出版社

作者：斯托林斯

页数：486

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>

## <<密码编码学与网络安全>>

### 内容概要

William Stallings为读者提供了一本关于密码编码学与网络安全的最优秀书籍。

更新的第四版反映了该领域的最新发展趋势与进展，详尽讲述了密码编码学与网络安全的原理、技术与实践。

首先，本书系统地解释了加密的概念与标准、密码、对称与公钥加密、数字签名等内容；接着探讨了网络安全的实践，为鉴别、电子邮件安全、IP安全以及Web安全引入了最新的应用；最后，本书回顾了系统安全的挑战，涉及到了主要的攻击与当今的最佳防范措施。

像往常一样，本书提供了非常卓越的支持，包括大量的补充材料以及联机资源。

对学生、教师以及工程技术人员而言，本书仍是该领域的最佳资源。

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、报文认证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，并新增加了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。

## 作者简介

斯托林斯 (William Stallings) : 计算机网络与体系结构方面成就卓著。他六次荣获由“教材与大学作者协会”颁发的“年度最佳计算机科学与工程教材”奖, 作品包括《操作系统——精髓与设计原理》、《计算机组成与体系结构》、《数据与计算机通信》等。他是致力于密码学各个方面的学术期刊Cryptologia的编委会成员之一。目前他作为独立顾问为计算机硬件制造商、软件开发商和政府研究机构提供咨询服务。

## <<密码编码学与网络安全>>

### 书籍目录

第0章 读者导引第1章 引言第一部分 对称密码第2章 传统加密技术第3章 分组密码与数据加密标准第4章 有限域第5章 高级加密标准第6章 对称密码的其他内容第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 散列算法和MAC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

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>