

<<ICSA密码学指南>>

图书基本信息

书名：<<ICSA密码学指南>>

13位ISBN编号：9787111142300

10位ISBN编号：7111142306

出版时间：2004-6

出版时间：机械工业出版社

作者：尼科尔斯 编

页数：527

译者：吴世忠

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>

## <<ICSA密码学指南>>

### 内容概要

本书详细介绍密码学在保护商业信息资源方面应用，并详细描述了ICSA的信息安全产品认证过程。本书很好地将古典密码学历史和密码分析学结合到现代公钥密码产品领域，展现了密码分析学在先进计算机安全体系中的应用，探讨了生物学加密的前景，强调了密码安全产品在计算机系统中的正确实现。

内容涉及过程、产品、协议、密钥管理、实现错误、产品认证等诸多方面。

本书面向信息技术的实践者，内容丰富，适合企业的CIO、网络管理人员、安全管理人员等专业人员阅读。

## <<ICSA密码学指南>>

### 作者简介

尼科尔斯先生是本书的主编，他是国际计算机安全联盟密码学和生物统计学方面的技术主管，同时也是ICSA密码学和生物统计学产品联盟的资料密码技术主管。

本书是尼科尔斯先生关于密码学方面的第三著作。

尼科尔斯先生是密码分析学和古典密码学领域的专家，并已经编写了古典密

## <<ICSA密码学指南>>

### 书籍目录

译者序译者简介作者简介序前言第一部分 密码学发展史 第1章 引言 第2章 第一原则和概论 第3章 历史上的密码系统1 第4章 历史上的密码系统2 第5章 代码和机器密码 第6章 数据加密标准 (DES) 和信息论 第二部分 商用密码系统 第7章 公钥 (非对称) 密码术 第8章 算法 第9章 万维网中的标识、鉴别和授权 第10章 数字签名 第11章 硬件实现 第12章 证书机构 第三部分 实现和产品认证 第13章 实现错误 第14章 ICSA产品认证 第四部分 实用密码学 第15章 因特网密码学 第16章 安全:策略、隐私权与协议 第17章 智能卡 第18章 IP安全与安全的VPN 第19章 电子商务系统中的密码学 第20章 基于角色的密码学 第五部分 密码学的发展方向 第21章 密码分析与系统识别 第22章 生物特征加密 第六部分 附录 附录A 标准 附录B 外国加密数据 附录C 复杂度理论的简要指南 附录D 数论的简短贯 附录E ICSA采用的算法清单 附录F 椭圆曲线及密码学 (ECC) 附录G 密码机的发展 附录H 美国法定和政府控制密码技术的政策 密码术语和互用性词汇表 参考资料目录和资源 关于原书光盘

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>