

<<应用密码学教程>>

图书基本信息

书名：<<应用密码学教程>>

13位ISBN编号：9787121005244

10位ISBN编号：7121005247

出版时间：2005-1

出版时间：电子工业出版社

作者：胡向东,魏琴芳

页数：284

字数：480000

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>

## <<应用密码学教程>>

### 内容概要

本书是作者根据多年的教学和科研工作实践，在学习、总结众多国内外有关网络信息安全和应用密码学文献基础上，特别从教学适用性角度，遵从学习规律编写而成。

本书全面介绍了应用密码学的基本概念、基本理论和典型实用技术，专门为教学编排和设计。

全书共14章，语言简练，内容重点突出，算法经典实用，逻辑性强，便于读者花少量时间尽快掌握应用密码学的精髓。

本书最后介绍的应用密码学在电子商务支付安全、数字通信安全和工业网络控制安全这三个典型领域的应用方法和技术，也是本书的一大亮点。

本书可作为高等院校密码学、信息安全、通信工程、计算机、信息管理、电子商务、检测技术、控制理论与控制工程等专业高年级本科生和研究生教材，也可供从事网络和通信信息安全相关领域应用和设计开发的研究人员、工程技术人员参考。

## 书籍目录

第1章 绪论 1.1 网络信息安全概述 1.1.1 网络信息安全问题的由来 1.1.2 网络信息安全问题的根源 1.1.3 网络信息安全的重要性和紧迫性 1.2 密码学在网络信息安全中的作用 1.3 密码学的发展历史 1.3.1 古代加密方法（手工阶段） 1.3.2 古典密码（机械阶段） 1.3.3 近代密码（计算机阶段） 1.4 网络信息安全的机制和安全服务 1.4.1 安全机制 1.4.2 安全服务 1.5 安全性攻击的主要形式及其分类 1.5.1 安全性攻击的主要形式 1.5.2 安全性攻击形式的分类 思考题和习题第2章 密码学基础 2.1 密码学相关概念 2.1.1 惟密文攻击（Ciphertext only） 2.1.2 已知明文攻击（Known plaintext） 2.1.3 选择明文攻击（Chosen plaintext） 2.1.4 选择密文攻击（Chosen ciphertext） 2.1.5 选择文本攻击（Chosen text） 2.2 密码系统 2.2.1 密码系统的定义 2.2.2 柯克霍夫（Kerckhoffs）原则 2.2.3 密码系统的安全条件 2.2.4 密码系统的分类 2.3 安全模型 2.3.1 网络安全模型 2.3.2 网络访问安全模型 2.4 密码体制 2.4.1 对称密码体制（Symmetric Encryption） 2.4.2 非对称密码体制（Asymmetric Encryption） 思考题和习题第3章 古典密码 3.1 隐写术 3.1.1 诗情画意传“密语” 3.1.2 悠扬琴声奏响“进军号角” 3.1.3 显微镜里传递情报 3.1.4 魔术般的密写术 3.1.5 网络与数字幽灵 3.1.6 “量子”技术隐形传递信息 3.2 代替 3.2.1 代替密码体制 3.2.2 代替密码的实现方法分类 3.3 换位 思考题和习题第4章 密码学数学引论 第5章 对称密码体制第6章 非对称密码体制第7章 HASH函数和消息认证第8章 数字签名第9章 密钥管理第10章 序列密码第11章 密码学与电子商务支付安全第12章 密码学与数字通信安全第13章 密码学与工业网络控制安全第14章 密码学的新进展——量子密码学思考题和习题

<<应用密码学教程>>

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>