

<<现代密码学>>

图书基本信息

书名：<<现代密码学>>

13位ISBN编号：9787302146094

10位ISBN编号：7302146098

出版时间：2007-4

出版时间：清华大学出版社

作者：杨波

页数：212

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>

<<现代密码学>>

内容概要

本书全面而详细地介绍现代密码学的理论和相关算法。

可帮助读者将所学知识应用于信息安全的实践中。

全书共分8章，第1章引言介绍现代密码学的基本概念，其余各章包括流密码、分组密码体制、公钥密码、密钥分配与密钥管理、消息认证和杂凑算法、数字签字和密码协议、网络加密与认证。

本书从教材使用的角度考虑，概念清晰、结构合理、通俗易懂、内容深入浅出，并充分考虑方便教师在教学过程中的实施，同时还注意与其他专业课教学的衔接。

本书取材新颖，不仅介绍现代密码学所涉及的基础理论和实用算法，同时也涵盖了现代密码学的最新研究成果，力求使读者通过本书的学习而了解本学科最新的发展方向。

本书可作为高等学校有关专业大学生和研究生的教材，也可作为通信工程师和计算机网络工程师的参考读物。

书籍目录

第1章 引言 1.1 信息安全面临的威胁 1.2 信息安全的模型 1.3 密码学基本概念 1.4 几种古典密码 习题
第2章 流密码 2.1 流密码的基本概念 2.2 线性反馈移位寄存器 2.3 线性移位寄存器的一元多项式表示
2.4 m序列的伪随机性 2.5 m序列密码的破译 2.6 非线性序列 习题第3章 分组密码体制 3.1 分组密码概
述 3.2 数据加密标准 3.3 差分密码分析与线性密码分析 3.4 分组密码的运行模式 3.5 IDEA 3.6 AES 算法
——Rijndael 习题第4章 公钥密码 4.1 密码学中一些常用的数学知识 4.2 公钥密码体制的基本概念 4.3
RSA算法 4.4 背包密码体制 4.5 Rabin密码体制 4.6 NTRU公钥密码系统 4.7 椭圆曲线密码体制 4.8 基于
身份的密码体制 习题第5章 密钥分配与密钥管理 5.1 单钥加密体制的密钥分配 5.2 公钥加密体制的密
钥管理 5.3 密钥托管 5.4 随机数的产生 5.5 秘密分割 习题第6章 消息认证和杂凑算法 6.1 消息认证码
6.2 杂凑函数 6.3 MD5杂凑算法 6.4 安全杂凑算法 6.5 HMAC 习题第7章 数字签字和密码协议 7.1 数字
签字的基本概念 7.2 数字签字标准 7.3 其他签字方案 7.4 认证协议 7.5 身份证明技术 7.6 其他密码协议
习题第8章 网络加密与认证 8.1 网络通信加密 8.2 Kerberos认证系统 8.3 X.509 认证业务 8.4 PGP 习题参
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>