

<<应用密码学>>

图书基本信息

书名：<<应用密码学>>

13位ISBN编号：9787111127819

10位ISBN编号：7111127811

出版时间：2003-8

出版时间：机械工业出版社

作者：王衍波/薛通编

页数：213

字数：345000

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>>

内容概要

本书讲解了现代密码学的教学基础知识和基本概念，DES、IDEA、AES等对称密码算法，RSA、NTRU等公钥密码算法，ElGamal、DSS等数字签名算法及序列密码学的基础。

还讲解了现代密码学的三个新的重要研究方向：椭圆曲线密码学、混沌密码学、量子密码学的基本原理和方法。

最后讲解了几个典型的密码协议。

本书可用作信息安全专业本科生的教材，也可作为其他信息技术专业的研究生、科技工作者的参考用书。

书籍目录

第1章 初等数论基础 1.1 素数与因式分解 1.2 同余式理论 1.3 Euler定理 1.4 平方剩余 1.5 素性检验与模幂算法 1.6 指数与原根 1.7 习题 1.8 实验题第2章 近世代数基础 2.1 群论初步 2.2 域论初步 2.3 有限域中的计算 2.4 习题 2.5 实验题第3章 密码学基本概念 3.1 密码技术发展简介 3.2 密码系统的概念 3.3 密码分析 3.4 数字签名与认证 3.5 计算复杂性理论 3.6 传统密码举例 3.7 习题第4章 对称密码算法 4.1 美国数据加密标准DES 4.2 国际数据加密算法IDEA 4.3 美国高级数据加密标准AES 4.4 欧洲密码标准 4.5 习题 4.6 实验题第5章 公钥密码算法 5.1 引言 5.2 RSA密码体制 5.3 Rabin公钥密码体制 5.4 ElGamal公钥密码体制 5.5 MH背包公钥密码体制 5.6 概率公钥密码体制 5.7 NTRU公钥密码体制 5.8 公钥密码标准 5.9 习题 5.10 实验题第6章 数字签名方案与散列函数 6.1 数字签名方案 6.2 散列函数 6.3 散列函数标准SHS 6.4 习题 6.5 实验题第7章 序列密码 7.1 序列密码模型 7.2 序列的随机性概念 7.3 线性反馈移位寄存器 7.4 m序列及其随机性 7.5 周期序列的线性复杂度 7.6 习题第8章 椭圆曲线密码学 8.1 引言 8.2 椭圆曲线的概念 8.3 椭圆曲线群的结构 8.4 有限域 F_{2^m} 上的算术运算 8.5 椭圆曲线上密码体制 8.6 习题第9章 混沌理论在密码学中的应用 9.1 混沌的基本概念 9.2 混沌序列的产生及其随机序列 9.3 逆混沌密码体制 9.4 示例 9.5 实验题第10章 量子密码理论 10.1 引言 10.2 Heisenberg测不准原理 10.3 BB84协议 10.4 习题第11章 密码协议 11.1 引言 11.2 公证协议 11.3 密钥协议 11.4 秘密共享 11.5 网络游戏 11.6 电子投票协议 11.7 习题 11.8 实验题参考文献

<<应用密码学>>

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>