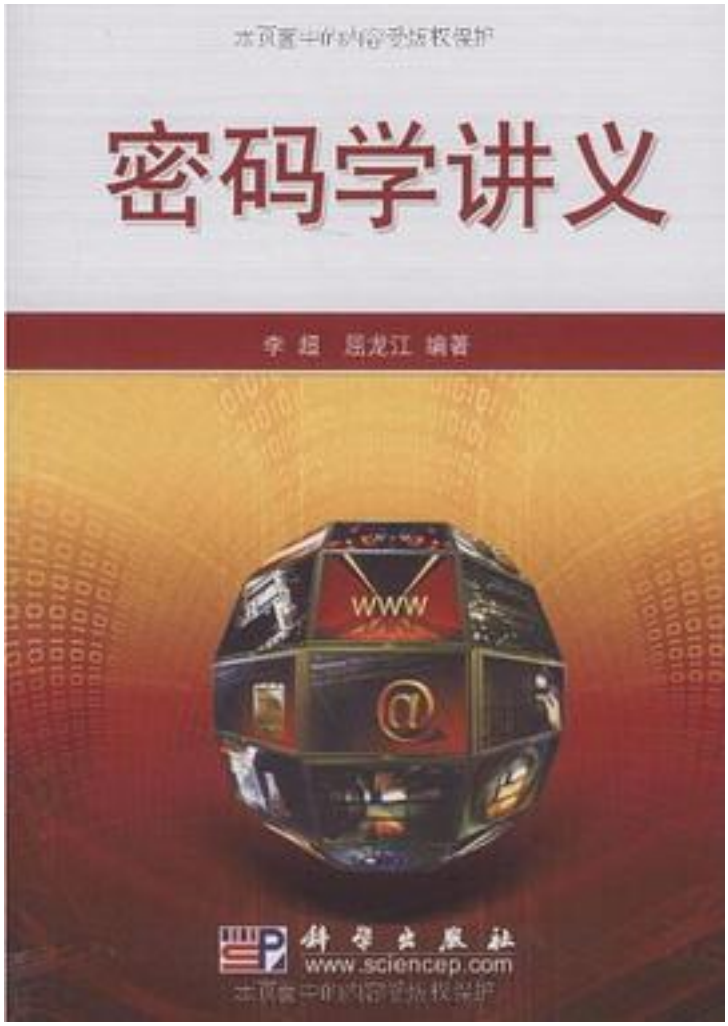
密码学讲义



密码学讲义_下载链接1_

著者:李超//屈龙江

出版者:科学

出版时间:2010-2

装帧:

isbn:9787030263858

《密码学讲义》从数学的角度较为系统地介绍了序列密码、分组密码和公钥密码的基本

理论与方法，利用周期序列的幂级数表示、根表示和迹表示研究了线性反馈移位寄存器序列及其变种的密码学性质；利用图论和组合数学等工具研究了非线性反馈移位寄存器序列的状态图性质，重点介绍M序列的存在性、构造与计数；介绍了五类典型分组密码算法的加解密流程、分组密码的设计原理以及一些常见的分析方法；讨论了RSA体制和椭圆曲线密码体制的基本原理及其相关的数学问题。

《密码学讲义》可以作为密码学与信息安全专业的本科生和研究生的教学用书，也可以作为从事密码学和信息安全研究的科技人员的参考书。

作者介绍:

目录: 前言第1章 绪论 1.1 密码学的基本概念 1.2 序列密码概述 1.3 分组密码概述 1.4 公钥密码概述第2章 线性反馈移位寄存器序列 2.1 序列的母函数表示 2.2 LFSR序列的数学描述 2.3 LFSR序列的周期分布 2.4 LFSR序列的线性复杂度分布 2.5 序列的采样特性 2.6 m序列 2.7 Berlekamp-Masseyr算法 习题2第3章 线性反馈移位寄存器序列的扩展形式 3.1 序列的根表示与迹表示 3.2 前馈序列 3.3 非线性组合序列 3.4 钟控序列 习题3第4章 非线性反馈移位寄存器序列 4.1 反馈移位寄存器的非奇异性 4.2 反馈移位寄存器的状态图性质 4.3 M序列 4.4 非线性反馈移位寄存器序列的综合 习题4第5章 分组密码的设计原理 5.1 分组密码的设计原则 5.2 分组密码的结构特征 5.3 S盒的设计准则 5.4 P置换的设计准则 5.5 轮函数和密钥扩展算法的设计准则 5.6 分组密码的工作模式 5.7 分组密码的测试方法 习题5第6章 典型分组密码算法 6.1 DES算法 6.2 IDEA算法 6.3 AES算法 6.4 Camellia算法 6.5 SMS4算法 习题6第7章 分组密码的分析方法 7.1 分组密码分析概述 7.2 差分密码分析 7.3 线性密码分析 7.4 Square攻击 7.5 代数攻击 习题7第8章 公钥密码算法及其相关问题 8.1 RSA算法 8.2 离散对数问题和ElGamal体制 8.3 椭圆曲线密码体制 8.4 大整数分解和素性测试 习题8参考文献索引
・・・・・・(收起)

密码学讲义_下载链接1_

标签

科学

密码学讲义

评论

密码学讲义_下载链接1_

书评

密码学讲义_下载链接1_