

<<现代密码学基础理论与应用>>

图书基本信息

书名：<<现代密码学基础理论与应用>>

13位ISBN编号：9787564707170

10位ISBN编号：7564707178

出版时间：2011-4

出版时间：电子科技大学出版社

作者：张键红

页数：199

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>

## <<现代密码学基础理论与应用>>

### 内容概要

应用密码技术是电子安全系统的关键技术，它主要实现保密性、完整性和不可否认性。

《现代密码学基础理论与应用》包括密码算法、密码协议及使用方面的主要内容：密码学基础、公钥密码算法、数字签名、序列密码、密钥建立、密钥管理、电子邮件安全等。

每章附有阅读资料，部分章节配有习题。

《现代密码学基础理论与应用》是在讲授多年的讲义的基础上形成的，可以作为高等学校计算机科学、通信工程、信息安全等专业的本科教材，也可以供有关工程技术人员参考。

## 书籍目录

第1章 绪论1.1 密码学的历史1.2 密码学的基本概念简介1.3 密码系统设计的理论基础和攻击类型1.4 密码体制的分类第2章 密码学数学基础2.1 数论基础2.1.1 素数2.1.2 欧拉函数2.1.3 同余及模运算2.1.4 逆运算2.2 代数基础(群)2.3 中国剩余定理(Chinese Remainder Theorem)2.4 二次剩余(Quadratic Residue)2.5 计算机复杂性理论基础2.6 密码学的困难问题第3章 序列(流)密码3.1 序列密码原理3.1.1 流密码对密钥流的要求3.1.2 同步流密码3.1.3 自同步流密码3.1.4 流密码的工作模式3.1.5 序列的随机性3.1.6 有限状态自动机3.1.7 密钥流产生器3.2 线性反馈移位寄存器3.2.1 线性移位寄存器的一元多项式表示3.2.2 线性移位寄存器序列的周期性3.2.3 m序列的伪随机性3.2.4 m序列密码的破译3.2.5 B-M算法与序列的线性复杂度3.3 非线性序列3.3.1 非线性组合序列3.3.2 钟控非线性序列3.3.3 A5算法3.3.4 二元加法非线性组合流密码的相关攻击3.4 利用线性反馈移位寄存器的密码反馈第4章 公钥密码4.1 引言4.1.1 公钥密码体制的加密原理4.1.2 公钥密码体制的认证原理4.1.3 对公钥密码体制的要求4.1.4 公钥密码的作用4.1.5 公钥密码体制的优缺点4.1.6 单向陷门函数4.2 背包公钥密码4.2.1 背包算法4.2.2 超递增背包向量4.2.3 背包公钥密码系统4.2.4 背包公钥的安全性4.3 RSA公钥密码4.3.1 RSA密码系统的描述4.3.2 RSA的安全性分析4.3.3 RSA实现中的问题4.4 Rabin公钥密码体制4.5 ElGamal密码系统4.5.1 求离散对数问题的算法4.5.2 ElGamal密码体制原理4.6 MaEliece公钥密码4.7 椭圆曲线公钥体制4.7.1 椭圆曲线的概念4.7.2 有限域上的椭圆曲线4.7.3 椭圆曲线密码体制4.7.4 椭圆曲线密码的安全性及优点4.8 多变量公钥密码4.8.1 多变量公钥密码(Multivariate Public Key Cryptosystem, MPKC)产生的背景4.8.2 一般的多变量公钥密码体制的描述4.8.3 MI多变量公钥密码.....第5章 数字签名与认证第6章 密钥管理和密码协议第7章 电子邮件的安全

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>