

<<密码学导引>>

图书基本信息

书名：<<密码学导引>>

13位ISBN编号：9787302160144

10位ISBN编号：7302160147

出版时间：2007-10

出版时间：清华大学

作者：何德全 编

页数：310

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>

<<密码学导引>>

内容概要

《密码学导引：原理与应用》主要从两个方面介绍密码学的知识：第一部分介绍了经典密码学中的对称密码体制、非对称密码体制及相关的密码协议，重点讨论了模代数学和以模代数学为基础的非对称密码。

第二部分从Shannon经典的信息论工作出发，分析了概率算法和单向函数的安全性，并给出了基本的安全性定义。

在此基础上，对公钥加密和签名方案的可证明安全性做了详细的分析。

另外，在附录中，《密码学导引：原理与应用》还完整地介绍了密码学中需要用到的代数数论和概率信息论的基础知识。

《密码学导引：原理与应用》可作为信息安全领域的大学生与研究生的相关课程的教材，也可作为密码学和信息安全领域的研究人员的参考书。

书籍目录

1. Introduction
 1.1 Encryption and Secrecy
 1.2 The Objectives of Cryptography
 1.3 Attacks
 1.4 Cryptographic Protocols
 1.5 Provable Security
 2. Symmetric-Key Encryption
 2.1 Stream Ciphers
 2.2 Block Ciphers
 2.2.1 DES
 2.2.2 Modes of Operation
 3. Public-Key Cryptography
 3.1 The Concept of Public-Key Cryptography
 3.2 Modular Arithmetic
 3.2.1 The Integers
 3.2.2 The Integers Modulo n
 3.3 RSA
 3.3.1 Key Generation and Encryption
 3.3.2 Digital Signatures
 3.3.3 Attacks Against RSA
 3.3.4 The Secure Application of RSA Encryption
 3.4 Hash Functions
 3.4.1 Merkle's Meta Method
 3.4.2 Construction of Hash Functions
 3.4.3 Probabilistic Signatures
 3.5 The Discrete Logarithm
 3.5.1 ElGamal's Encryption
 3.5.2 ElGamal's Signature Scheme
 3.5.3 Digital Signature Algorithm
 3.6 Modular Squaring
 3.6.1 Rabin's Encryption
 3.6.2 Rabin's Signature Scheme
 4. Cryptographic Protocols
 4.1 Key Exchange and Entity Authentication
 4.1.1 Kerberos
 4.1.2 Diffie-Hellman Key Agreement
 4.1.3 Key Exchange and Mutual Authentication
 4.1.4 Station-to-Station Protocol
 4.1.5 Public-Key Management Techniques
 4.2 Identification Schemes
 4.2.1 Interactive Proof Systems
 4.2.2 Simplified Fiat-Shamir Identification Scheme
 4.2.3 Zero-Knowledge
 4.2.4 Fiat-Shamir Identification Scheme
 4.2.5 Fiat-Shamir Signature Scheme
 4.3 Commitment Schemes
 4.3.1 A Commitment Scheme Based on Quadratic Residues
 4.3.2 A Commitment Scheme Based on Discrete Logarithms
 4.3.3 Homomorphic Commitments
 4.4 Electronic Elections
 4.4.1 Secret Sharing
 4.4.2 A Multi-Authority Election Scheme
 4.4.3 Proofs of Knowledge
 4.4.4 Non-Interactive Proofs of Knowledge
 4.4.5 Extension to Multi-Way Elections
 4.4.6 Eliminating the Trusted Center
 4.5 Digital Cash
 4.5.1 Blindly Issued Proofs
 4.5.2 A Fair Electronic Cash System
 4.5.3 Underlying Problems
 5. Probabilistic Algorithms
 5.1 Coin-Tossing Algorithms
 5.2 Monte Carlo and Las Vegas Algorithms
 6. One-Way Functions and the Basic Assumptions
 6.1 A Notation for Probabilities
 6.2 Discrete Exponential Function
 6.3 Uniform Sampling Algorithms
 6.4 Modular Powers
 6.5 Modular Squaring
 6.6 Quadratic Residuosity Property
 6.7 Formal Definition of One-Way Functions
 6.8 Hard-Core Predicates
 7. Bit Security of One-Way Functions
 8. One-Way Functions and Pseudorandomness
 9. Provably Secure Encryption
 10. Provably Secure Digital Signatures
 A. Algebra and Number Theory
 B. Probabilities and Information Theory
 References
 Index

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>