

<<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. Introduction1.1 Encryption and Secrecy1.2 The Objectives of Cryptography1.3 Attacks1.4 Cryptographic Protocols1.5 Provable Security2. Symmetric-Key Encryption2.1 Stream Ciphers2.2 Block Ciphers2.2.1 DES2.2.2 Modes of Operation3. Public-Key Cryptography3.1 The Concept of Public-Key Cryptography3.2 Modular Arithmetic3.2.1 The Integers3.2.2 The Integers Modulo  $n$ 3.3 RSA3.3.1 Key Generation and Encryption3.3.2 Digital Signatures3.3.3 Attacks Against RSA3.3.4 The Secure Application of RSA Encryption3.4 Hash Functions3.4.1 Merkle's Meta Method3.4.2 Construction of Hash Functions3.4.3 Probabilistic Signatures3.5 The Discrete Logarithm3.5.1 ElGamal's Encryption3.5.2 ElGamal's Signature Scheme3.5.3 Digital Signature Algorithm3.6 Modular Squaring3.6.1 Rabin's Encryption3.6.2 Rabin's Signature Scheme4. Cryptographic Protocols4.1 Key Exchange and Entity Authentication4.1.1 Kerberos4.1.2 Diffie-Hellman Key Agreement4.1.3 Key Exchange and Mutual Authentication4.1.4 Station-to-Station Protocol4.1.5 Public-Key Management Techniques4.2 Identification Schemes4.2.1 Interactive Proof Systems4.2.2 Simplified Fiat-Shamir Identification Scheme4.2.3 Zero-Knowledge4.2.4 Fiat-Shamir Identification Scheme4.2.5 Fiat-Shamir Signature Scheme4.3 Commitment Schemes4.3.1 A Commitment Scheme Based on Quadratic Residues4.3.2 A Commitment Scheme Based on Discrete Logarithms4.3.3 Homomorphic Commitments4.4 Electronic Elections4.4.1 Secret Sharing4.4.2 A Multi-Authority Election Scheme4.4.3 Proofs of Knowledge4.4.4 Non-Interactive Proofs of Knowledge4.4.5 Extension to Multi-Way Elections4.4.6 Eliminating the Trusted Center4.5 Digital Cash4.5.1 Blindly Issued Proofs4.5.2 A Fair Electronic Cash System4.5.3 Underlying Problems5. Probabilistic Algorithms5.1 Coin-Tossing Algorithms5.2 Monte Carlo and Las Vegas Algorithms6. One-Way Functions and the Basic Assumptions6.1 A Notation for Probabilities6.2 Discrete Exponential Function6.3 Uniform Sampling Algorithms6.4 Modular Powers6.5 Modular Squaring6.6 Quadratic Residuosity Property6.7 Formal Definition of One-Way Functions6.8 Hard-Core Predicates7. Bit Security of One-Way Functions8. One-Way Functions and Pseudorandomness9. Provably Secure Encryption10. Provably Secure Digital SignaturesA. Algebra and Number TheoryB. Probabilities and Information TheoryReferencesIndex

<<密码学导引>>

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>