

<<密码导论及编码原理>>

图书基本信息

书名：<<密码导论及编码原理>>

13位ISBN编号：9787030124708

10位ISBN编号：7030124707

出版时间：2004-1

出版时间：科学出版社

作者：Wade Trappe

页数：490

字数：504000

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>

<<密码导论及编码原理>>

内容概要

本书的一个重要特色——它覆盖的范围相当广泛。

本书前8章涵盖了密码学的主要领域：经典密码理论、基础数论、RSA算法与数字签名等。

本书后9章讲述了密钥共享方案、游戏理论、信息论、电子商务、数字钞票与“零知识”技术等等。

在附录部分，作者给出了分别用Mathematica、Maple和MATLAB实现算法的事例。

本书可作为高年级本科生和研究生的有关密码学与网络安全及相关专业的教材。

<<密码导论及编码原理>>

书籍目录

Preface1 Overview 1.1 Secure Communications 1.2 Cryptographic Applications2 Classical Cryptosystems 2.1 Shift Ciphers 2.2 Affine Ciphers 2.3 The Vigenere Cipher 2.4 Substitution Ciphers 2.5 Sherlock Holmes 2.6 The Playfair and ADFGX Ciphers 2.7 Block Ciphers 2.8 Binary Numbers and ASCII 2.9 One-Time Pads 2.10 Pseudo-random Bit Generation 2.11 Linear Feedback Shift Register Sequences 2.12 Enigma 2.13 Exercise 2.14 Computer Problems3 Basic Number Theory 3.1 Basic Notions 3.2 Solving $ax+by=d$ 3.3 Congruences 3.4 The Chinese Remainder Theorem 3.5 Modular Exponentiation 3.6 Fermat and Euler 3.7 Primitive Roots 3.8 Inverting Matrices Mod n 3.9 Square Roots Mod n 3.10 Finite Fields 3.11 Exercises 3.12 Computer Problems4 The Data Encryption Standard 4.1 Introduction 4.2 A Simplified DES-Type Algorithm 4.3 Differential Cryptanalysis 4.4 DES 4.5 Modes of Operation 4.6 Breaking DES 4.7 Password Security 4.8 Exercises5 AES:Rijndael 5.1 The Basic Algorithm 5.2 The Layers 5.3 Decryption 5.4 Design Considerations6 The RBA Algorithm 6.1 The RSA Algorithm 6.2 Attacks on RSA 6.3 Primality Testing 6.4 Factoring 6.5 The RSA Challenge 6.6 An Application to Treaty Verification 6.7 The Public Key Concept 6.8 Exercises 6.9 Computer Problems7 Discrete Logarithms 7.1 Discrete Logarithms 7.2 Computing Discrete Logs 7.3 Bit Commitment 7.4 The ElGamal Public Key Cryptosystem 7.5 Exercises 7.6 Computer Problems8 Digital Signatures 8.1 RSA Signatures 8.2 The ElGamal Signature Scheme 8.3 Hash Functions 8.4 Birthday Attacks 8.5 The Digital Signature Algorithm 8.6 Exercises 8.7 Computer Problems9 E-Commerce and Digital Cash10 Secret Sharing Schemes11 Games12 Zero-Knowledge Techniques13 Key Establishment Protocols14 Information Theory15 Elliptic Curves16 Error Correcting Codes17 Quantum CryptographyA MathematicaB Maple ExamplesC MATLAB ExamplesD Further Reading BibliographyIndex

<<密码导论及编码原理>>

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>