

《Introduction to cryp》

图书基本信息

书名：《Introduction to cryptography对密码学的介绍》

13位ISBN编号：9780387207568

10位ISBN编号：0387207562

出版时间：2004-7

出版社：Springer Verlag

作者：Johannes Buchmann

页数：335

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《Introduction to cryp》

内容概要

Cryptography is a key technology in electronic key systems. It is used to keep data secret, digitally sign documents, access control, and so forth. Users therefore should not only know how its techniques work, but they must also be able to estimate their efficiency and security. Based on courses taught by the author, this book explains the basic methods of modern cryptography. It is written for readers with only basic mathematical knowledge who are interested in modern cryptographic algorithms and their mathematical foundation. Several exercises are included following each chapter. This revised and extended edition includes new material on the AES encryption algorithm, the SHA-1 Hash algorithm, on secret sharing, as well as updates in the chapters on factoring and discrete logarithms. Johannes A. Buchmann is Professor of Computer Science and Mathematics at the Technical University of Darmstadt, and an Associate Editor of the Journal of Cryptology. In 1985, he received a Feodor Lynen Fellowship of the Alexander von Humboldt Foundation. He has also received the most prestigious award in science in Germany, the Leibniz Award of the German Science Foundation (Deutsche Forschungsgemeinschaft).

《Introduction to cryp》

书籍目录

Preface for the Second Edition Preface
1 Integers 1.1 Basics 1.2 Divisibility 1.3 Representation of Integers 1.4
O- and \mathbb{Z} -Notation 1.5 Cost of Addition, Multiplication, and Division with Remainder 1.6 Polynomial Time 1.7
Greatest Common Divisor 1.8 Euclidean Algorithm 1.9 Extended Euclidean Algorithm 1.10 Analysis of the
Extended Euclidean Algorithm 1.11 Factoring into Primes 1.12 Exercises
2 Congruences and Residue Class Rings 2.1 Congruences 2.2 Semigroups 2.3 Groups 2.4 Residue Class Ring 2.5 Fields 2.6 Division in the Residue Class
Ring 2.7 Analysis of the Operations in the Residue Class Ring 2.8 Multiplicative Group of Residues mod m 2.9
Order of Group Elements 2.10 Subgroups 2.11 Fermat's Little Theorem 2.12 Fast Exponentiation 2.13 Fast
Evaluation of Power Products 2.14 Computation of Element Orders 2.15 The Chinese Remainder Theorem 2.16
Decomposition of the Residue Class Ring 2.17 A Formula for the Euler ϕ -Function 2.18 Polynomials 2.19
Polynomials over Fields 2.20 Construction of Finite Fields 2.21 The Structure of the Unit Group of Finite Fields
2.22 Structure of the Multiplicative Group of Residues Modulo a Prime Number 2.23 Exercises
3 Encryption 3.1 Encryption Schemes 3.2 Symmetric and Asymmetric Cryptosystems 3.3 Cryptanalysis 3.4 Alphabets and Words
3.5 Permutations 3.6 Block Ciphers 3.7 Multiple Encryption 3.8 The Use of Block Ciphers 3.9 Stream Ciphers
3.10 The Affine Cipher 3.11 Matrices and Linear Maps 3.12 Affine Linear Block Ciphers 3.13 Vigenere, Hill, and
Permutation Ciphers
4 Probability and Perfect Secrecy
5 DES
6 AES
7 Prime Number Generation
8 Public-key Encryption
9 Factoring
10 Discrete Logarithms
11 Cryptographic Hash Functions
12 Digital Signatures
13 Other Systems
14 Identification
15 Secret Sharing
16 Public-key Infrastructures
Solutions of the exercises
References
Index

《Introduction to cryp》

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:www.tushu000.com