Introduction to Cryptography : Principles and Applications /

Delfs, Hans

Springer Berlin Heidelberg,
2002

Electronic books

Monografía

Due to the rapid growth of digital communication and electronic data exchange, information security has become a crucial issue in industry, business, and administration. Modern cryptography provides essential techniques for securing information and protecting data. In the first part, this book covers the key concepts of cryptography on an undergraduate level, from encryption and digital signatures to cryptographic protocols. Essential techniques are demonstrated in protocols for key exchange, user identification, electronic elections and digital cash. In the second part, more advanced topics are addressed, such as the bit security of one-way functions and computationally perfect pseudorandom bit generators. The security of cryptographic schemes is a central topic. Typical examples of provably secure encryption and signature schemes and their security proofs are given. Though particular attention is given to the mathematical foundations, no special background in mathematics is presumed. The necessary algebra, number theory and probability theory are included in the appendix. Each chapter closes with a collection of exercises. The second edition contains corrections, revisions and new material, including a complete description of the AES, an extended section on cryptographic hash functions, a new section on random oracle proofs, and a new section on public-key encryption schemes that are provably secure against adaptively-chosen-ciphertext attacks

Título: Introduction to Cryptography Principles and Applications by Hans Delfs, Helmut Knebl

Editorial: Berlin, Heidelberg Springer Berlin Heidelberg 2002

Descripción física: 1 online resource (xiv, 310 pages)

Mención de serie: Information Security and Cryptography, Texts and Monographs 1619-7100

Bibliografía: Includes bibliographical references (pages 297-304) and index

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 -- 7.1 Bit Security of the Exp Family -- 7.2 Bit Security of the RSA Family -- 7.3 Bit Security of the Square Family -- 8. One-Way Functions and Pseudorandomness -- 8.1 Computationally Perfect Pseudorandom Bit Generators -- 8.2 Yao's Theorem -- 9. Provably Secure Encryption -- 9.1 Classical Information-Theoretic Security -- 9.2 Perfect Secrecy and Probabilistic Attacks -- 9.3 Public-Key One-Time Pads -- 9.4 Computationally Secret Encryption Schemes -- 9.5 Unconditional Security of Cryptosystems -- 10. Provably Secure Digital Signatures -- 10.1 Attacks and Levels of Security -- 10.2 Claw-Free Pairs and Collision-Resistant Hash Functions -- 10.3 Authentication-Tree-Based Signatures -- 10.4 A State-Free Signature Scheme -- A. Algebra and Number Theory -- A.1 The Integers -- A.2 Residues -- A.3 The Chinese Remainder Theorem -- A.4 Primitive Roots and the Discrete Logarithm -- A.5 Quadratic Residues -- A.6 Modular Square Roots -- A.7 Primes and Primality Tests -- B. Probabilities and Information Theory -- B.1 Finite Probability Spaces and Random Variables -- B.2 The Weak Law of Large Numbers -- B.3 Distance Measures -- B.4 Basic Concepts of Information Theory -- References

Copyright/Depósito Legal: 934994329 936316928 1202737704

ISBN: 9783642871269 electronic bk.) 3642871267 electronic bk.) 9783642871283 3642871283 9781441990037 electronic bk.) 1441990038 electronic bk.) 3540422781 9783540422785

Materia: Computer science Data encryption (Computer science) Coding theory Coding theory Computer science Data encryption (Computer science) Systèmes informatiques- Sécurité- Mesures Cryptographie Chiffrement (Informatique) Geheimschrift Kommunikationsprotokoll Kryptologie Public-Key-Kryptosystem

Autores: Knebl, Helmut

Enlace a formato físico adicional: Print version 9783642871283

Punto acceso adicional serie-Título: Information Security and Cryptography, Texts and Monographs

---