Introduction to modern cryptography

Katz, Jonathan, 1974-, author

Abstrak

ryptography is ubiquitous and plays a key role in ensuring data secrecy and integrity as well as in securing computer systems more broadly. Introduction to Modern Cryptography provides a rigorous yet accessible treatment of this fascinating subject. The authors introduce the core principles of modern cryptography, with an emphasis on formal definitions, clear assumptions, and rigorous proofs of security. The book begins by focusing on private-key cryptography, including an extensive treatment of private-key encryption, message authentication codes, and hash functions. The authors also present design principles for widely used stream ciphers and block ciphers including RC4, DES, and AES, plus provide provable constructions of stream ciphers and block ciphers from lower-level primitives. The second half of the book covers public-key cryptography, beginning with a self-contained introduction to the number theory needed to understand the RSA, Diffie-Hellman, and El Gamal cryptosystems (and others), followed by a thorough treatment of several standardized public-key encryption and digital signature schemes. Integrating a more practical perspective without sacrificing rigor, this widely anticipated Second Edition offers improved treatment of:Stream ciphers and block ciphers, including modes of operation and design principlesAuthenticated encryption and secure communication sessionsHash functions, including hash-function applications and design principles Attacks on poorly implemented cryptography, including attacks on chained-CBC encryption, padding-oracle attacks, and timing attacksThe random-oracle model and its application to several standardized, widely used public-key encryption and signature schemesElliptic-curve cryptography and associated standards such as DSA/ECDSA and DHIES/ECIESContaining updated exercises and worked examples, Introduction to Modern Cryptography, Second Edition can serve as a textbook for undergraduate- or graduate-level courses in cryptography, a valuable reference for researchers and practitioners, or a general introduction suitable for self-study.