

1. Record Nr.	UNISALENT0991003611739707536
Autore	Katz, Jonathan
Titolo	Introduction to modern cryptography / Jonathan Katz, University of Maryland, College Park, MD, USA, Yehuda Lindell, Bar-Ilan University, Ramat Gan, Israel
ISBN	9781466570269 (hardback)
Edizione	[Second edition]
Descrizione fisica	xx, 583 pages : illustrations ; 25 cm
Collana	Chapman & Hall/CRC cryptography and network security series
Classificazione	AMS 94A60 AMS 94-01 LC QA76.9.A25K36
Altri autori (Persone)	Lindell, Yehuda
Disciplina	005.82
Soggetti	Computer security Cryptography
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index
Sommario/riassunto	"Cryptography 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 principles
Authenticated encryption and secure communication sessions
Hash functions, including hash-function applications and design principles
Attacks on poorly implemented cryptography, including attacks on chained-CBC encryption, padding-oracle attacks, and timing attacks
The random-oracle model and its application to several standardized, widely used public-key encryption and signature schemes
Elliptic-curve cryptography and associated standards such as DSA/ECDSA and DHIES/ECIES
Containing 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. "--

2. Record Nr.

Titolo

UNISA996625572503316

Intonation, accent and rhythm : studies in discourse phonology / edited by Dafydd Gibbon and Helmut Richter

Pubbl/distr/stampa

Berlin ; New York, : De Gruyter, 1984

ISBN

3-11-009832-6

Descrizione fisica

IX, 350 p. ; 24 cm

Collana

Research in text theory = Untersuchungen zur Texttheorie ; 8

Disciplina

414

Soggetti

Fonologia

Collocazione

IV.2. 1082 (IL t II 30)

Lingua di pubblicazione

Inglese

Formato

Materiale a stampa

Livello bibliografico

Monografia