1. Record Nr. UNINA9910437604503321

Autore	Kocielny Czesaw
Titolo	Modern Cryptography Primer [[electronic resource]] : Theoretical Foundations and Practical Applications / / by Czesaw Kocielny, Mirosaw Kurkowski, Marian Srebrny
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2013
ISBN	3-642-41386-2
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (246 p.)
Disciplina	004 004.6 005.74 005.8
Soggetti	Data structures (Computer science) Computer security E-commerce Computer organization Data Structures and Information Theory Systems and Data Security e-Commerce/e-business Computer Systems Organization and Communication Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di contenuto	Chap. 1 Basic Concepts and Historical Overview -- Chap. 2 Mathematical Foundations of Cryptography -- Chap. 3 Foundations of Symmetric Cryptography -- Chap. 4 Foundations of Asymmetric Cryptography -- Chap. 5 An Electronic Signature and Hash Functions -- Chap. 6 PGP Systems and True Crypt -- Chap. 7 Public Key Infrastructure -- Chap. 8 Cryptographic Protocols -- Chap. 9 Cryptography Application for Data Security -- References -- Index.
Sommario/riassunto	Cryptography has experienced rapid development, with major advances recently in both secret and public key ciphers, cryptographic hash functions, cryptographic algorithms and multiparty protocols, including

their software engineering correctness verification, and various methods of cryptanalysis. This textbook introduces the reader to these areas, offering an understanding of the essential, most important, and most interesting ideas, based on the authors' teaching and research experience. After introducing the basic mathematical and computational complexity concepts, and some historical context, including the story of Enigma, the authors explain symmetric and asymmetric cryptography, electronic signatures and hash functions, PGP systems, public key infrastructures, cryptographic protocols, and applications in network security. In each case the text presents the key technologies, algorithms, and protocols, along with methods of design and analysis, while the content is characterized by a visual style and all algorithms are presented in readable pseudocode or using simple graphics and diagrams. The book is suitable for undergraduate and graduate courses in computer science and engineering, particularly in the area of networking, and it is also a suitable reference text for self-study by practitioners and researchers. The authors assume only basic elementary mathematical experience, the text covers the foundational mathematics and computational complexity theory.