1.

Record Nr.	UNINA9910624391103321
Autore	Easttom Chuck
Titolo	Modern Cryptography : Applied Mathematics for Encryption and Information Security / / by William Easttom
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2022
ISBN	9783031123047 9783031123030
Edizione	[2nd ed. 2022.]
Descrizione fisica	1 online resource (460 pages)
Collana	Computer Science Series
Disciplina	005.8
Soggetti	Telecommunication Data structures (Computer science) Information theory Number theory Data protection Computational intelligence Statistics Communications Engineering, Networks Data Structures and Information Theory Computational Number Theory Data and Information Security Computational Intelligence Applied Statistics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Chapter 1. History of Cryptography to the 1800s -- Chapter 2. History of Cryptography from the 1800’s -- Chapter 3. Basic Information Theory -- Chapter 4. Essential Number Theory and Discrete Math -- Chapter 5. Essential Algebra -- Chapter 6. Fiestel Networks -- Chapter 7. Substitution-Permutation Networks -- Chapter 8. S-Box Design -- Chapter 9. Cryptographic Hashes -- Chapter 10. Asymmetric Algorithms -- Chapter 11. Elliptic Curve Cryptography -- Chapter 12. Random Number Generators -- Chapter 13.SSL/TLS -- Chapter 14.

Sommario/riassunto

This expanded textbook, now in its second edition, is a practical yet in depth guide to cryptography and its principles and practices. Now featuring a new section on quantum resistant cryptography in addition to expanded and revised content throughout, the book continues to place cryptography in real-world security situations using the hands-on information contained throughout the chapters. Prolific author Dr. Chuck Easttom lays out essential math skills and fully explains how to implement cryptographic algorithms in today's data protection landscape. Readers learn and test out how to use ciphers and hashes, generate random keys, handle VPN and Wi-Fi security, and encrypt VoIP, Email, and Web communications. The book also covers cryptanalysis, steganography, and cryptographic backdoors and includes a description of quantum computing and its impact on cryptography. This book is meant for those without a strong mathematics background with only just enough math to understand the algorithms given. The book contains a slide presentation, questions and answers, and exercises throughout. Presents new and updated coverage of cryptography including new content on quantum resistant cryptography; Covers the basic math needed for cryptography - number theory, discrete math, and algebra (abstract and linear); Includes a full suite of classroom materials including exercises, Q&A, and examples. .