1. Record Nr. UNINA9910983390903321

Autore	Jajodia Sushil
Titolo	Encyclopedia of Cryptography, Security and Privacy / / edited by Sushil Jajodia, Pierangela Samarati, Moti Yung
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	9783030715229 3030715221
Edizione	[3rd ed. 2025.]
Descrizione fisica	1 online resource (0 pages)
Collana	Computer Science Series
Altri autori (Persone)	SamaratiPierangela YungMoti
Disciplina	652.803
Soggetti	Data structures (Computer science) Information theory Cryptography Data encryption (Computer science) Coding theory Data Structures and Information Theory Cryptology Coding and Information Theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Security Policies and Access Control -- Public key encryption, digital signatures -- Number theory, primality tests, discrete log, factorisation -- Public-key cryptography, hardware, physical attacks -- Implementation aspects of cryptographic algorithms -- Hardware attacks -- Multi-party computation, voting schemes, digital signature schemes -- Web security -- DBMS and Application Security -- Biometrics -- Software Security -- Network Security -- Formal Methods and Assurance -- Sensor and Ad Hoc Networks -- DOS -- Privacy-preserving data mining -- Private information retrieval -- Privacy metrics and data protection -- Wireless Security -- Broadcast channel, secret sharing, threshold schemes, subliminal channels -- Risk management and organizational security and privacy -- Usable/user-centric privacy -- Less-constrained biometrics -- Access and Query

Privacy -- Cryptocurrencies -- Encryption-Based Access Control Based on Public Key Cryptography -- Cyber-physical systems and infrastructure: security andprivacy -- Location privacy and privacy in locations-based applications -- Privacy in emerging scenarios -- Privacy and security in social networks -- Economics of security and privacy -- Key management -- Elliptic curve cryptography -- Sequences, Boolean functions, stream ciphers -- Secure multiparty computations -- Human Aspects in Security and Privacy -- Trustworthy Computing, Physical/Hardware Security -- AI approaches for security and privacy -- Privacy and anonymity in communication networks -- Privacy laws and directives.

Sommario/riassunto

A rich stream of papers and many good books have been written on cryptography, security, and privacy, but most of them assume a scholarly reader who has the time to start at the beginning and work his way through the entire text. The goal of Encyclopedia of Cryptography, Security, and Privacy, Third Edition is to make important notions of cryptography, security, and privacy accessible to readers who have an interest in a particular concept related to these areas, but who lack the time to study one of the many books in these areas. The third edition is intended as a replacement of Encyclopedia of Cryptography and Security, Second Edition that was edited by Henk van Tilborg and Sushil Jajodia and published by Springer in 2011. The goal of the third edition is to enhance on the earlier edition in several important and interesting ways. First, entries in the second edition have been updated when needed to keep pace with the advancement of state of the art. Second, as noticeable already from the title of the encyclopedia, coverage has been expanded with special emphasis to the area of privacy. Third, considering the fast pace at which information and communication technology is evolving and has evolved drastically since the last edition, entries have been expanded to provide comprehensive view and include coverage of several newer topics. .