1. Record Nr. UNISA996465592203316

Titolo	Information Security and Privacy [[electronic resource]] : First Australasian Conference, ACISP '96, Wollongong, NSW, Australia, June 24 - 26, 1996, Proceedings / / edited by Josef Pieprzyk, Jennifer Seberry
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1996
ISBN	3-540-49583-5
Edizione	[1st ed. 1996.]
Descrizione fisica	1 online resource (XI, 341 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1172
Disciplina	005.8
Soggetti	Computer security Data encryption (Computer science) Computer communication systems Computers and civilization Management information systems Computer science Combinatorics Systems and Data Security Cryptology Computer Communication Networks Computers and Society Management of Computing and Information Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	The changing face of information technology security -- Replicating the Kuperee authentication server for increased security and reliability -- Non-repudiation without public-key -- Investigation of non-repudiation protocols -- A dynamic secret sharing scheme with cheater detection -- A nonlinear secret sharing scheme -- The access structure of some secret-sharing schemes -- On construction of resilient functions -- Another approach to software key escrow encryption -- Cryptography based on transcendental numbers -- Breakthroughs in

standardisation of IT security criteria -- Tailoring authentication protocols to match underlying mechanisms -- On the design of security protocols for mobile communications -- A framework for design of key establishment protocols -- On period of multiplexed sequences -- Edit distance correlation attacks on clock-controlled combiners with memory -- A faster cryptanalysis of the self-shrinking generator -- Modeling a multi-level secure object-oriented database using views -- Support for joint action based security policies -- Access control: The neglected frontier -- On the quantitative assessment of behavioural security -- On the modelling of preventive security based on a PC network intrusion experiment -- Evidential reasoning in network intrusion detection systems -- A group-oriented (t, n) undeniable signature scheme without trusted center -- Cryptosystems for hierarchical groups -- On selectable collisionful hash functions -- On password-based authenticated key exchange using collisionful hash functions -- A new universal test for bit strings -- An alternative model of quantum key agreement via photon coupling.

Sommario/riassunto

This book constitutes the thoroughly refereed post-conference proceedings of the First Australiasian Conference on Information Security and Privacy, ACISP '96, held in Wollongong, NSW, Australia, in June 1996. The volume includes revised full versions of the 26 refereed papers accepted for presentation at the conference; also included are three invited contributions. The papers are organized in topical sections on authentication, secret sharing, encryption and cryptographic functions, authentication protocols, stream ciphers, access control, security models and intrusion detection, threshold cryptography, and hashing.