1. Record Nr. UNISA996465806003316

Titolo	Cryptography : proceedings of the Workshop on Cryptography, Burg Feuerstein, Germany, March 29-April 2, 1982 / / edited by Thomas Beth
Pubbl/distr/stampa	Berlin ; ; Heidelberg ; ; New York : , : Springer-Verlag, , 1983
ISBN	3-540-39466-4
Edizione	[1st ed. 1983.]
Descrizione fisica	1 online resource (VIII, 402 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 149
Disciplina	001.5436
Soggetti	Cryptography
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Classical Cryptography -- Cryptology - Methods and Maxims -- Mechanical Cryptographic Devices -- Cryptanalysis of a Kryha Machine -- Enigma Variations -- Mathematical Foundations -- Encrypting by Random Rotations -- Analogue Scrambling Schemes -- Analogue Speech Security Systems -- A Voice Scrambling System for Testing and Demonstration -- The Rating of Understanding in Secure Voice Communications Systems -- Analysis of Multiple Access Channel Using Multiple Level FSK -- Analog Scrambling by the General Fast Fourier Transform -- Stream Ciphers -- Stream Ciphers -- Multiplexed Sequences: Some Properties of the Minimum Polynomial -- On Using Prime Polynomials in Crypto Generators -- Cryptography in Large communication Systems -- Communication Security in Remote Controlled Computer Systems -- Privacy and Data Protection in Medicine -- The Data Encryption Standard -- Cryptanalysis of the Data Encryption Standard by the Method of Formal Coding -- Are Big S-Boxes Best? -- The Average Cycle Size of The Key Stream in Output Feedback Encipherment -- Authentication Systems -- Authentication Procedures -- Fast Authentication in a Trapdoor-Knapsack Public Key Cryptosystem -- The Merkle — Hellman — Scheme -- A New Algorithm for the Solution of the Knapsack Problem -- Trapdoors in Knapsack Kryptosystems -- The Rivest - Shamir - Adleman - Scheme -- Is the RSA - Scheme safe? (Abstract) -- Ein Effizienzvergleich der Faktorisierungsverfahren von Morrison-Brillhart und Schroeppel

(Extended Abstract) -- Finite Semigroups and The RSA-Cryptosystem -- How to Share a Secret.