1. Record Nr. UNISA996465732603316

Titolo	Fast software encryption : 6th International Workshop, FSE'99, Rome, Italy, March 1999, proceedings / / edited by Lars Knudsen
Pubbl/distr/stampa	Berlin, Germany ; ; New York, New York : , : Springer, , [1999] Â©1999
ISBN	3-540-48519-8
Edizione	[1st ed. 1999.]
Descrizione fisica	1 online resource (VIII, 324 p.)
Collana	Lecture notes in computer science ; ; Volume 1636
Disciplina	005.82
Soggetti	Computers - Access control - Passwords
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Advanced Encryption Standard -- Improved Analysis of Some Simplified Variants of RC6 -- Linear Cryptanalysis of RC5 and RC6 -- A Revised Version of CRYPTON: CRYPTON V1.0 -- Attack on Six Rounds of CRYPTON -- On the Security of the 128-bit Block Cipher DEAL -- Cryptanalysis of a Reduced Version of the Block Cipher E2 -- On the Decorrelated Fast Cipher (DFC) and Its Theory -- Remotely Keyed Encryption -- Scramble All, Encrypt Small -- Accelerated Remotely Keyed Encryption -- Analysis of Block Ciphers I -- Miss in the Middle Attacks on IDEA and Khufu -- Mod n Cryptanalysis, with Applications against RC5P and M6 -- The Boomerang Attack -- Miscellaneous -- Towards Making Luby-Rackoff Ciphers Optimal and Practical -- A New Characterization of Almost Bent Functions -- Imprimitive Permutation Groups and Trapdoors in Iterated Block Ciphers -- Modes of Operation -- On the Security of Double and 2-Key Triple Modes of Operation -- On the Construction of Variable-Input-Length Ciphers -- Analysis of Block Ciphers II -- Slide Attacks -- On the Security of CS-Cipher -- Interpolation Attacks of the Block Cipher: SNAKE -- Stream Ciphers -- High-Speed Pseudorandom Number Generation with Small Memory -- SOBER Cryptanalysis.