1. Record Nr. UNINA9910695294003321

Autore	Dworkin Morris
Titolo	Recommendation for block cipher modes of operation [[electronic resource]] : the CCM mode for authentication and confidentiality / / Morris Dworkin
Pubbl/distr/stampa	Gaithersburg, MD : , : U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, , [2004]
Descrizione fisica	iv, 21 pages : digital, PDF file
Collana	NIST special publication ; ; 800-38 C. Computer security
Altri autori (Persone)	DworkinM. J
Soggetti	Computer security - Standards - United States Authentication - Standards Data encryption (Computer science)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Title from title screen (viewed on July 19, 2006). "May 2004."
Nota di bibliografia	Includes bibliographical references.
Sommario/riassunto	This Recommendation defines a mode of operation, called Counter with Cipher Block Chaining-Message Authentication Code (CCM), for a symmetric key block cipher algorithm. CCM may be used to provide assurance of the confidentiality and the authenticity of computer data by combining the techniques of the Counter (CTR) mode and the Cipher Block Chaining-Message Authentication Code (CBC-MAC) algorithm.