1. Record Nr. UNISA996466067303316

Autore	Pieprzyk Josef
Titolo	Design of Hashing Algorithms [[electronic resource] /] / by Josef Pieprzyk, Babak Sadeghiyan
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1993
ISBN	3-540-48198-2
Edizione	[1st ed. 1993.]
Descrizione fisica	1 online resource (XV, 196 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 756
Disciplina	005.8/2
Soggetti	Data structures (Computer science) Data encryption (Computer science) Coding theory Information theory Combinatorics Algorithms Operating systems (Computers) Data Structures Cryptology Coding and Information Theory Algorithm Analysis and Problem Complexity Operating Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Overview of hash functions -- Methods of attack on hash functions -- Pseudorandomness -- Construction of super-pseudorandom permutations -- A sound structure -- A construction for one way hash functions and pseudorandom bit generators -- How to construct a family of strong one-way permutations -- Conclusions.
Sommario/riassunto	This work presents recent developments in hashing algorithm design. Hashing is the process of creating a short digest (i.e., 64 bits) for a message of arbitrary length, for exam- ple 20 Mbytes. Hashing algorithms were first used for sear- ching records in databases; they are central for digital si- gnature applications and are used for

authentication without secrecy. Covering all practical and theoretical issues related to the design of secure hashing algorithms the book is self contained; it includes an extensive bibliography on the topic.