1.

Record Nr.	UNIORUON00433356
Autore	RAABE, Wilhelm
Titolo	Briefe / Wilhelm Raabe ; [bearbeitet von Karl Hoppe ; unter Mitarbeit von Hans-Werner Peter]
Pubbl/distr/stampa	Göttingen, : Vandenhoeck & Ruprecht, 1975
ISBN	35-252-0156-7
Descrizione fisica	553 p. ; 19 cm.
Disciplina	830.8
Lingua di pubblicazione	Tedesco
Formato	Materiale a stampa
Livello bibliografico	Monografia

2.

Record Nr.	UNINA9910437569303321
Autore	Buchmann Johannes A
Titolo	Introduction to Public Key Infrastructures / / by Johannes A. Buchmann, Evangelos Karatsiolis, Alexander Wiesmaier
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2013
ISBN	3-642-40657-2
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (XV, 194 p. 146 illus.)
Disciplina	005.74
Soggetti	Data structures (Computer science) Computer security Electronic commerce System safety Data Structures and Information Theory Systems and Data Security e-Commerce/e-business Security Science and Technology
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 and index.

Nota di contenuto

Sommario/riassunto

The introduction of public key cryptography (PKC) was a critical advance in IT security. In contrast to symmetric key cryptography, it enables confidential communication between entities in open networks, in particular the Internet, without prior contact. Beyond this PKC also enables protection techniques that have no analogue in traditional cryptography, most importantly digital signatures which for example support Internet security by authenticating software downloads and updates. Although PKC does not require the confidential exchange of secret keys, proper management of the private and public keys used in PKC is still of vital importance: the private keys must remain private, and the public keys must be verifiably authentic. So understanding so-called public key infrastructures (PKIs) that manage key pairs is at least as important as studying the ingenious mathematical ideas underlying PKC. In this book the authors explain the most important concepts underlying PKIs and discuss relevant standards, implementations, and applications. The book is structured into chapters on the motivation for PKI, certificates, trust models, private keys, revocation, validity models, certification service providers, certificate policies, certification paths, and practical aspects of PKI. This is a suitable textbook for advanced undergraduate and graduate courses in computer science, mathematics, engineering, and related disciplines, complementing introductory courses on cryptography. The authors assume only basic computer science prerequisites, and they include exercises in all chapters and solutions in an appendix. They also include detailed pointers to relevant standards and implementation guidelines, so the book is also appropriate for self-study and reference by industrial and academic researchers and practitioners.