1. Record Nr. UNINA9910465192303321

Autore	Oppliger Rolf
Titolo	Contemporary Cryptography
Pubbl/distr/stampa	Norwood : , : Artech House, , 2011 [Piscataqay, New Jersey] : , : IEEE Xplore, , [2011]
ISBN	1-60807-146-4
Edizione	[Second edition.]
Descrizione fisica	1 online resource (598 p.)
Collana	Artech House information security and privacy series
Disciplina	005.82
Soggetti	Cryptography Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Contemporary Cryptography Second Edition; Contents; Foreword; Preface; Acknowledgments; Chapter 1 Introduction; 1.1 CRYPTOLOGY; 1.2 CRYPTOGRAPHIC SYSTEMS; 1.2.1 Classes of Cryptographic Systems; 1.2.2 Secure Cryptographic Systems; 1.2.3 Real Security of Secure Cryptosystems; 1.3 HISTORICAL BACKGROUND INFORMATION; 1.4 OUTLINE OF THE BOOK; References; Chapter 2 Cryptographic Systems; 2.1 UNKEYED CRYPTOSYSTEMS; 2.1.1 One-Way Functions; 2.1.2 Cryptographic Hash Functions; 2.1.3 Random Bit Generators; 2.2 SECRET KEY CRYPTOSYSTEMS; 2.2.1 Symmetric Encryption Systems. 2.2.2 Message Authentication Codes2.2.3 PRBGs; 2.2.4 PRFs; 2.3 PUBLIC KEY CRYPTOSYSTEMS; 2.3.1 Asymmetric Encryption Systems; 2.3.2 DSSs; 2.3.3 Key Agreement; 2.3.4 Entity Authentication; 2.3.5 Secure Multiparty Computation; 2.4 FINAL REMARKS; References; Part I UNKEYED CRYPTOSYSTEMS; Chapter 3 One-Way Functions; 3.1 INTRODUCTION; 3.2 CANDIDATE ONE-WAY FUN.
Sommario/riassunto	Whether you're new to the field or looking to broaden your knowledge of contemporary cryptography, this newly revised edition of an Artech House classic puts all aspects of this important topic into perspective. Delivering an accurate introduction to the current state-of-the-art in modern cryptography, the book offers you an in-depth understanding of essential tools and applications to help you with your daily work. The second edition has been reorganized and expanded, providing

mathematical fundamentals and important cryptography principles in the appropriate appendixes, rather than summarized at the beginning of the book. Now you find all the details you need to fully master the material in the relevant sections. This allows you to quickly delve into the practical information you need for your projects. Covering unkeyed, secret key, and public key cryptosystems, this authoritative reference gives you solid working knowledge of the latest and most critical concepts, techniques, and systems in contemporary cryptography. Additionally, the book is supported with over 720 equations, more than 60 illustrations, and numerous time-saving URLs that connect you to websites with related information.