1. Record Nr. UNINA9910784136203321

Autore	Oppliger Rolf
Titolo	Contemporary cryptography / / Rolf Oppliger
Pubbl/distr/stampa	Boston : , : Artech House, , ©2005 [Piscataqay, New Jersey] : , : IEEE Xplore, , [2005]
ISBN	1-58053-643-3
Descrizione fisica	1 online resource (529 p.)
Collana	Artech House computer security series
Classificazione	54.62
Disciplina	652/.8
Soggetti	Cryptography Computer security
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; Contents vii; Foreword xv; Preface xix; References xxiii; Acknowledgments; Chapter 1 Introduction 1; Chapter 2 Cryptographic Systems 21; Chapter 3 Discrete Mathematics 47; Chapter 4 Probability Theory 103; Chapter 5 Information Theory 125; Chapter 6 Complexity Theory 141; Chapter 7 One-Way Functions 169; Chapter 8 Cryptographic Hash Functions 195; Chapter 9 Random Bit Generators 219; Chapter 10 Symmetric Encryption Systems 229; Chapter 11 Message Authentication Codes 291; Chapter 12 Pseudorandom Bit Generators 309; Chapter 13 Pseudorandom Functions 321 Chapter 14 Asymmetric Encryption Systems 333Chapter 15 Digital Signature Systems 369; Chapter 16 Key Establishment 405; Chapter 17 Entity Authentication 423; Chapter 18 Secure Multiparty Computation 442; Chapter 19 Key Management 451; Chapter 20 Conclusions 467; Chapter 21 Outlook 473; Appendix A Abbreviations and Acronyms 479; Appendix B Mathematical Notation 485; About the Author 491; Index 493
Sommario/riassunto	This authoritative work brings you a timely, unified analysis of the various satellite navigation technologies, applications, and services in operation or development, and of the challenges that lie ahead in this rapidly evolving field. It describes the segments, signal characteristics, performance, and securities aspects of the GPS system, including the

advances anticipated in the next-generation GPS-III, and brings you up to speed on the developing European GALILEO system and its innovative characteristics, services, and potential. A look at ground-based and satellite-based augmentation systems (GBAS and SBAS) highlights their performance-improving features and how these systems may serve as connection rings between GPS and future networks like GALILEO.