1. Record Nr. UNINA9910788023603321

Autore	Gonzalez Vasco Maria Isabel
Titolo	Group theoretic cryptography / / Maria Isabel Gonzalez Vasco, Universidad Rey Juan Carlos, Madrid, Spain, Rainer Steinwandt, Florida Atlantic University, Boca Raton, FL
Pubbl/distr/stampa	Boca Raton, Florida : , : CRC Press, , [2015] ©2015
ISBN	0-429-13660-9 1-4665-2723-4
Descrizione fisica	1 online resource (244 p.)
Collana	Chapman and Hall/CRC Cryptography and Network Security
Disciplina	005.82
Soggetti	Cryptography Data encryption (Computer science) Computer networks - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	A Chapman and Hall book--Title page.
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Cover; Dedication; Contents; List of Figures; Symbol Description; Preface; Part I: Preliminaries; Chapter 1: Mathematical background; Chapter 2: Basics on complexity; Chapter 3: Cryptology: An introduction; Part II: Public-Key Encryption; Chapter 4: Provable security guarantees; Chapter 5: Public-key encryption in the standard model; Chapter 6: Public-key encryption using infinite groups; Part III: Secret-Key Encryption; Chapter 7: Block ciphers; Chapter 8: Cryptographic hash functions and message authentication codes; Part IV: Other Cryptographic Constructions Chapter 9: Key establishment protocolsChapter 10: Signature and identification schemes; Part V: Appendix; Appendix A: Solutions to selected exercises; References
Sommario/riassunto	Group theoretic problems appear to be the most promising source of hard computational problems for deploying new cryptographic constructions. This reference focuses on the specifics of using nonabelian groups in the field of cryptography. It provides an introduction to cryptography (mostly asymmetric) with a focus on group theoretic constructions, making it the first book to use this

approach. The authors include all of the needed cryptographic and group theoretic concepts. They supply exercises at the end of each chapter, selected solutions in the back of the book, and suggestions for student