1. Record Nr. UNINA9910792138003321

Autore	McAndrew Alasdair
Titolo	Introduction to cryptography with open-source software / / by Alasdair McAndrew
Pubbl/distr/stampa	Boca Raton, FL : , : CRC Press, an imprint of Taylor and Francis, , 2012
ISBN	0-429-09455-8 1-4398-2570-X
Edizione	[1st edition]
Descrizione fisica	1 online resource (456 p.)
Collana	Discrete Mathematics and Its Applications A Chapman & Hall Book
Disciplina	005.8/2
Soggetti	Computer security Cryptography - Mathematics Data encryption (Computer science) Open source software
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.
Nota di contenuto	Front Cover; Contents; Preface; Chapter 1. Introduction to cryptography; Chapter 2. Basic number theory; Chapter 3. Classical cryptosystems; Chapter 4. Introduction to information theory; Chapter 5. Public-key cryptosystems based on factoring; Chapter 6. Public-key cryptosystems based on logarithms and knapsacks; Chapter 7. Digital signatures; Chapter 8. Block ciphers and the data encryption standard; Chapter 9. Finite fields; Chapter 10. The Advanced Encryption Standard; Chapter 11. Hash functions; Chapter 12. Elliptic curves and cryptosystems; Chapter 13. Random numbers and stream ciphers Chapter 14. Advanced applications and protocolsAppendix A. Introduction to Sage; Appendix B. Advanced computational number theory; Bibliography; Back Cover
Sommario/riassunto	Once the privilege of a secret few, cryptography is now taught at universities around the world. Introduction to Cryptography with Open-Source Software illustrates algorithms and cryptosystems using examples and the open-source computer algebra system of Sage. The author, a noted educator in the field, provides a highly practical learning experience by progressing at a gentle pace, keeping

mathematics at a manageable level, and including numerous end-of-chapter exercises.