1.	Record Nr.	UNINA9910790280403321
	Autore	Galbraith Steven D.
	Titolo	Mathematics of public key cryptography / / Steven D. Galbraith (University of Auckland)
	Pubbl/distr/stampa	Cambridge : , : Cambridge University Press, , 2012
	ISBN	9781139012843 1-107-22971-5 1-280-39333-5 1-139-22286-4 9786613571250 1-139-01284-3 1-139-21806-9 1-139-21497-7 1-139-22458-1 1-139-22114-0
	Descrizione fisica	1 online resource (xiv, 615 pages) : digital, PDF file(s)
	Classificazione	MAT008000
	Disciplina	003/.54
	Soggetti	Codificació, Teoria de la Criptografia - Matemàtica Coding theory Cryptography - Mathematics Criptografia Teoria de la codificació Llibres electrònics
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Title from publisher's bibliographic system (viewed on 05 Oct 2015).
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	1. Introduction -- Part I. Background -- 2. Basic algorithmic number theory -- 3. Hash functions and MACs -- Part II. Algebraic Groups -- 4. Preliminary remarks on algebraic groups -- 5. Varieties -- 6. Tori, LUC and XTR -- 7. Curves and divisor class groups -- 8. Rational maps on curves and divisors -- 9. Elliptic curves --10. Hyperelliptic curves -- Part III. Exponentiation, Factoring and Discrete Logarithms -- 11. Basic

algorithms for algebraic groups -- 12. Primality testing and integer factorisation using algebraic groups --13. Basic discrete logarithm algorithms -- 14. Factoring and discrete logarithms using pseudorandom walks -- 15. Factoring and discrete logarithms in subexponential algorithms -- Part IV. Lattices -- 16. Lattices -- 17. Lattice basis reduction -- 18. Algorithms for the closest and shortest vector problems -- 19. Coppersmith's method and related applications -- Part V. Cryptography Related to Discrete Logarithms -- 20. The Diffie-Hellman problem and cryptographic applications -- 21. The Diffie-Hellman problem -- 22. Digital signatures based on discrete logarithms -- 23. Public key encryption based on discrete logarithms -- Part VI. Cryptography Related to Integer Factorisation -- 24. The RSA and Rabin cryptosystems -- Part VII. Advanced Topics in Elliptic and Hyperelliptic Curves -- 25. Isogenies of elliptic curves -- 26. Pairings on elliptic curves.

Sommario/riassunto

Public key cryptography is a major interdisciplinary subject with many real-world applications, such as digital signatures. A strong background in the mathematics underlying public key cryptography is essential for a deep understanding of the subject, and this book provides exactly that for students and researchers in mathematics, computer science and electrical engineering. Carefully written to communicate the major ideas and techniques of public key cryptography to a wide readership, this text is enlivened throughout with historical remarks and insightful perspectives on the development of the subject. Numerous examples, proofs and exercises make it suitable as a textbook for an advanced course, as well as for self-study. For more experienced researchers it serves as a convenient reference for many important topics: the Pollard algorithms, Maurer reduction, isogenies, algebraic tori, hyperelliptic curves and many more.