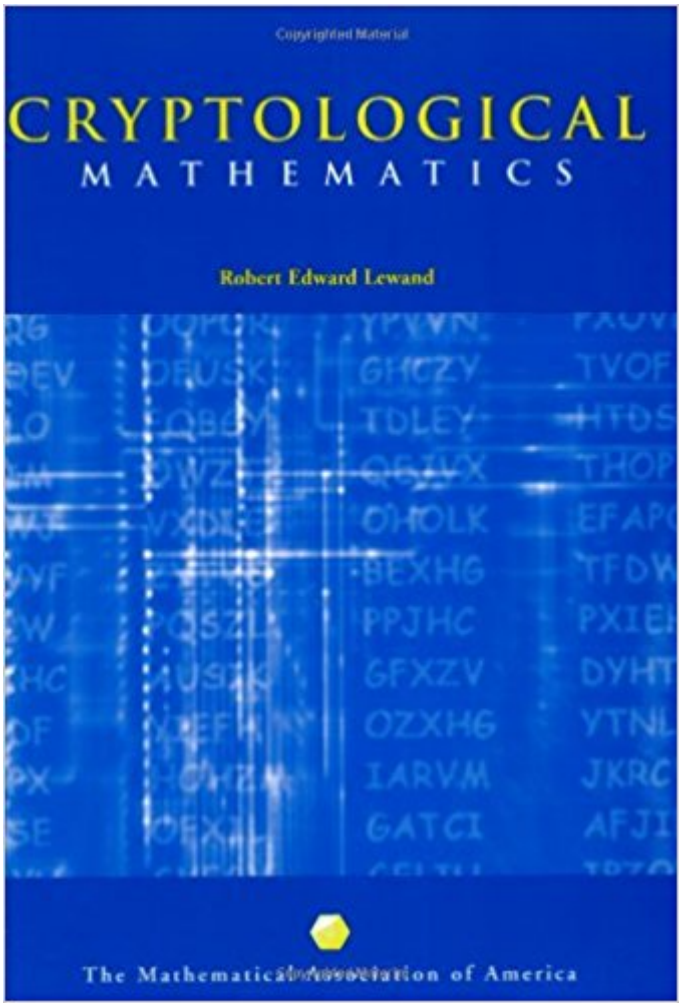
Cryptological Mathematics (Mathematical Association Of America Textbooks)



Synopsis

This is an introduction to the mathematics involved in the intriguing field of cryptology, the science of writing and reading secret messages which are designed to be read only by their intended recipients. It is written at an elementary level, suitable for beginning undergraduates, with careful explanations of all the concepts used. The basic branches of mathematics required, including number theory, abstract algebra and probability, are used to show how to encipher and decipher messages, and why this works, giving a practical as well as theoretical basis to the subject. Challenging computer programming exercises are also included. The book is written in an engaging style which will appeal to all, and also includes historical background on some of the founders of the subject. It will be of interest both to students wishing to learn cryptology per se, and also to those searching for practical applications of seemingly abstract mathematics.

Book Information

Series: Mathematical Association of America Textbooks
Paperback: 211 pages
Publisher: The Mathematical Association of America; UK ed. edition (November 2000)
Language: English
ISBN-10: 0883857197
ISBN-13: 978-0883857199
Product Dimensions: 6 x 0.9 x 9 inches
Shipping Weight: 11.2 ounces (View shipping rates and policies)
Average Customer Review: 4.7 out of 5 stars 6 customer reviews
Best Sellers Rank: #413,601 in Books (See Top 100 in Books) #108 inÃ Â Books > Science & Math > Physics > System Theory #168 inÃ Â Books > Science & Math > Mathematics > Pure Mathematics > Discrete Mathematics #368 inÃ Â Books > Science & Math > Mathematics > History

Customer Reviews

An elementary introduction to the mathematics involved in cryptology, the science of reading and writing secret messages. The book has an engaging style, and all concepts used are carefully explained. It will be suitable for all students interested in cryptology and those looking for practical applications of seemingly abstract mathematics.

Robert Edward Lewand received his PhD in mathematics from the University of Virginia. He is the

co-author of two books: Expert System Development, and Intelligent Systems Design. He has delivered numerous talks and published extensively in professional journals largely in the areas of expert systems and artificial intelligence. He has been the recipient of several awards: Outstanding Teacher in the Faculty of Science (from Goucher College, 1980), Fulbright Faculty Exchange Award (Great Britain, 1987), Outstanding Scholarship Award (Groucher College, 1989), and the Caroline Doebler Bruckerl Award for the Outstanding Faculty Member (Groucher College, 1999).

This book is a delightful as an exposition to fundamental concepts beyond Algebra I with excellent examples for immediate application. The overview is insightful on the concerns raised in the recent presidential election with regard to communication.

Good :)

Good bargain.

As I do not work for M.I.6, the N.S.A. or some other `Secret Service' a computer program as Wolfram's ` Mathematical Explorer' [at for $75, or so] which can encrypt a message by R.S.A [heavy duty crypto] is `really' all I need.I have a number of books on all kinds of cryptography ... `classical' crypto, `Codes' [different from cyphers], number theory and so on.While there are `better' books on specific parts of cryptology this book is by far the best overall introduction.The title of this book scared me a bit. I have never been that `comfortable' with some sorts of maths and this book `sounded' brutal, and while it is a `math' book it is really not impossible to `figure out' [although some spots I must have read twenty times but thats the topic].`REQUIRED BACKGROUND'You can `do' with less but it helps to know basic algebra and understand variables. The vocabulary and nomenclature of areas as Set Theory and Probability [which I had to `study up' on] would be `nice' but you can `slide' without them,Reading level: age 14 through senility :-) [ but a challenge for those `dead and encrypted'.`Classical', pen and paper, cryptology: B+Clear Writing: A-The `History' of cryptology: C+Physical [binding and paper, type, type size ...] BAlso covered in detail is "public key' cryptography which as I wrote I do by `pre - written' computer program.

I *loved* this book.It covers the essential number theory required to understand various encryption schemes, and while it is a thin book, it doesn't omit any steps between various mathematical steps (" ... and then magic happens ..."). You end up with the satisfying feeling of being able to derive the

proof for RSA, starting from high-school math.Highly recommended.

Book was in excellent condition, and arrived just a matter of days after I placed my order. I would definite suggest and will order from them again.

Cryptological Mathematics (Mathematical Association of America Textbooks) Number Theory Through Inquiry (Maa Textbooks) (Mathematical Association of America Textbooks) Mathematical Interest Theory (Mathematical Association of America Textbooks) A Course in Mathematical Modeling (Mathematical Association of America Textbooks) Non-Euclidean Geometry (Mathematical Association of America Textbooks) Thinking Geometrically: A Survey of Geometries (Mathematical Association of America Textbooks) Knot Theory (Mathematical Association of America Textbooks) Real Infinite Series (Classroom Resource Material) (Mathematical Association of America Textbooks) Fourier Series (Mathematical Association of America Textbooks) Chance, Strategy, and Choice: An Introduction to the Mathematics of Games and Elections (Cambridge Mathematical Textbooks) Exploring Mathematics: An Engaging Introduction to Proof (Cambridge Mathematical Textbooks) Introduction to Mathematical Proofs: A Transition (Textbooks in Mathematics) Elements of Advanced Mathematics, Third Edition (Textbooks in Mathematics) Discrete Mathematics and Applications, Second Edition (Textbooks in Mathematics) Handbook of Mathematical Functions: with Formulas, Graphs, and Mathematical Tables (Dover Books on Mathematics) Bayesian Filtering and Smoothing (Institute of Mathematical Statistics Textbooks) Chaos: An Introduction to Dynamical Systems (Textbooks in Mathematical Sciences) Chaotic Dynamics: Fractals, Tilings, and Substitutions (Cambridge Mathematical Textbooks) Understanding Nonlinear Dynamics (Textbooks in Mathematical Sciences) An Introduction to Hilbert Space (Cambridge Mathematical Textbooks)