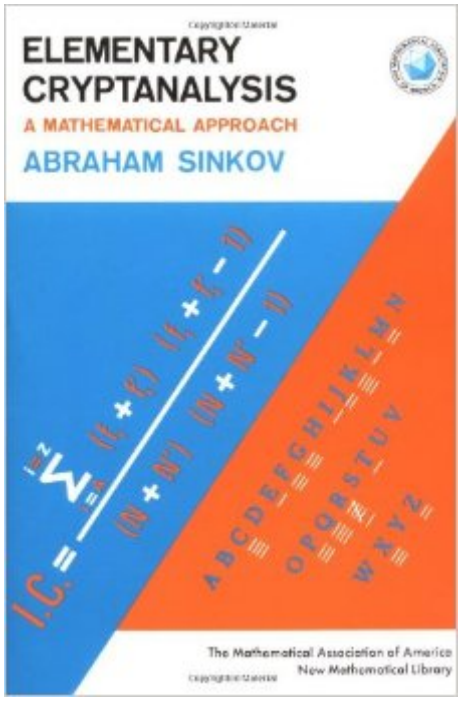
Elementary Cryptanalysis: A Mathematical Approach (Mathematical Association Of America Textbooks)



Synopsis

Most people, acquainted with cryptology either through sensational cloak and dagger stories or through newspaper cryptograms, are not aware that many aspects of this art may be treated systematically, by means of some elementary mathematical concepts and methods. In this introduction, Professor Sinkov explains some of the fundamental techniques at the basis of cryptanalytic endeavor from which much more sophisticated techniques have evolved, especially since the advent of computers. The mathematical topics relevant in these discussions include modular arithmetic, a little number theory, some linear algebra of two dimensions with matrices, some combinatorics, and a little statistics. Also included are programs in BASIC developed by Paul Irwin for use in his course based on this book.

Book Information

Series: Mathematical Association of America Textbooks (Book 22)

Paperback: 232 pages

Publisher: The Mathematical Association of America (August 1998)

Language: English

ISBN-10: 0883856220

ISBN-13: 978-0883856222

Product Dimensions: 6 x 0.7 x 9 inches

Shipping Weight: 10.4 ounces

Average Customer Review: 4.4 out of 5 starsÂ Â See all reviewsÂ (9 customer reviews)

Best Sellers Rank: #1,138,577 in Books (See Top 100 in Books) #203 inÂ Books > Science & Math > Mathematics > Pure Mathematics > Combinatorics #245 inÂ Books > Computers & Technology > Security & Encryption > Encryption #255 inÂ Books > Computers & Technology > Security & Encryption > Cryptography

Customer Reviews

Dr. Sinkov has been-there, done-that. He was in the first group of three mathematicians hired by William Friedman of the Army’s Signal Intelligence Service (SIS) back in 1930. After two name changes, the agency became the NSA, and Sinkov became the Chief of Communications Security, and later, Deputy Director for Production.Using only high school math, the good doctor takes us on a tour of cryptanalysis that is remarkable for it’s clarity and completeness. If you don’t start with Sinkov’s book, you’re doing it the hard way.

This, along with the book by Helen Gaines, is one of the best introductions to classical cryptology, but if you want to go further into contemporary cryptology, you'll need a more recent book. I like Applied Cryptology by Bruce Schneier.For by far the best book on background but not for mathematics, try The Codebreakers by David Kahn.All four belong on any crypto bookshelf.

Sinkov presents the basics of simple cryptanalysis in clear, easy to understand language. His examples and sample exercises that accompany each chapter provide the reader with hands-on practice of the concepts introduced. Whether you are new to the study of cryptography and cryptanalysis or you are well familiar with the basics of the field, Sinkov's presentation will have something to interest you. A mathematical approach to cryptanalysis that is well thought out and easy to understand.

Messages can be enciphered by replacing the letters of its words by other letters or symbols, or by mixing them up (transposing them) as in an anagram. This book treats these processes on the basis of the mathematics of these transformations. It covers single alphabet substitutions, substitutions using multiple alphabets, two letter substitutions and transposition type ciphers. These ciphers are studied using modular arithmetic, probability mathematics, series mathematics and matrix algebra. The book contains numerous example problems as well as exercises and their answers.This is much more of a book on deciphering messages than one on mathematics, and only the basics of these various types of mathematics are utilized in deciphering. While the math discussed is not treated in depth, I think you have to be interested in math to like this book. If you do crosswords or other puzzles by intuition instead of by a mathematical analysis this book may not be for you, but then again you may find the mathematical insights to be interesting and very helpful.While I was quite familiar with most of the math covered in the book, I was never exposed to modular arithmetic and found this part of the book challenging. In fact, I found the few pages allotted to the math, as opposed to their use in deciphering, to be insufficient to fully grasp what I needed to. Fortunately the applications were basic enough that I was able to learn what I needed from the Internet, primarily from the excellent Khan Academy tutorial on codes.I learned a lot from the book, but you have to want to or need to study ciphers to like the book, and you have to be interested in the mathematical aspects of the subject.

This is simply the best book in elementary cryptanalysis. Every concept is clarified and explained through the examples. There are questions and practice exercises at the end of every chapter.

Elementary Cryptanalysis: A Mathematical Approach (Mathematical Association of America Textbooks) A Course in Mathematical Modeling (Mathematical Association of America Textbooks) Non-Euclidean Geometry (Mathematical Association of America Textbooks) Math Through the Ages: A Gentle History for Teachers and Others, Expanded Edition (Mathematical Association of America Textbooks) Elementary Algebraic Geometry (Student Mathematical Library, Vol. 20) (Student Mathematical Library, V. 20) Chaos: An Introduction to Dynamical Systems (Textbooks in Mathematical Sciences) Understanding Nonlinear Dynamics (Textbooks in Mathematical Sciences) Set Theory: A First Course (Cambridge Mathematical Textbooks) Spanish Reader for Beginners-Elementary 2-Short Paragraphs in Spanish: Spanish to English Translation (Spanish Reader for Beginners-Elementary 1, 2 & 3) (Spanish Edition) Subtraction Facts Math Practice Worksheet Arithmetic Workbook With Answers: Daily Practice guide for elementary students and other kids (Elementary Subtraction Series) (Volume 1) The American Heart Association Low-Salt Cookbook: A Complete Guide to Reducing Sodium and Fat in Your Diet (AHA, American Heart Association Low-Salt Cookbook) American Diabetes Association Complete Guide to Diabetes: The Ultimate Home Reference from the Diabetes Experts (American Diabetes Association Comlete Guide to Diabetes) American Heart Association Low-Salt Cookbook, 4th Edition: A Complete Guide to Reducing Sodium and Fat in Your Diet (AHA, American Heart Association Low-Salt Cookbook) American Heart Association Low-Salt Cookbook, 3rd Edition: A Complete Guide to Reducing Sodium and Fat in Your Diet (AHA, American Heart Association Low-Salt Cookbook) American Medical Association Complete Medical Encyclopedia (American Medical Association (Ama) Complete Medical Encyclopedia) American Bar Association Family Legal Guide (third edition): Everything your family needs to know about the law and real estate, consumer protection, ... Association Complete Personal Legal Guide) The Homeowners Association Manual (Homeowners Association Manual)(5th Edition) Publication Manual of the American Psychological Association (Publication Manual of the American Psychological Association (Spiral) 6th (sixth) edition Applied Abstract Algebra with MapleTM and MATLABÂ®, Third Edition: A Maple and MATLAB Approach, Third Edition (Textbooks in Mathematics) Elementary Molecular Quantum Mechanics: Mathematical Methods and Applications