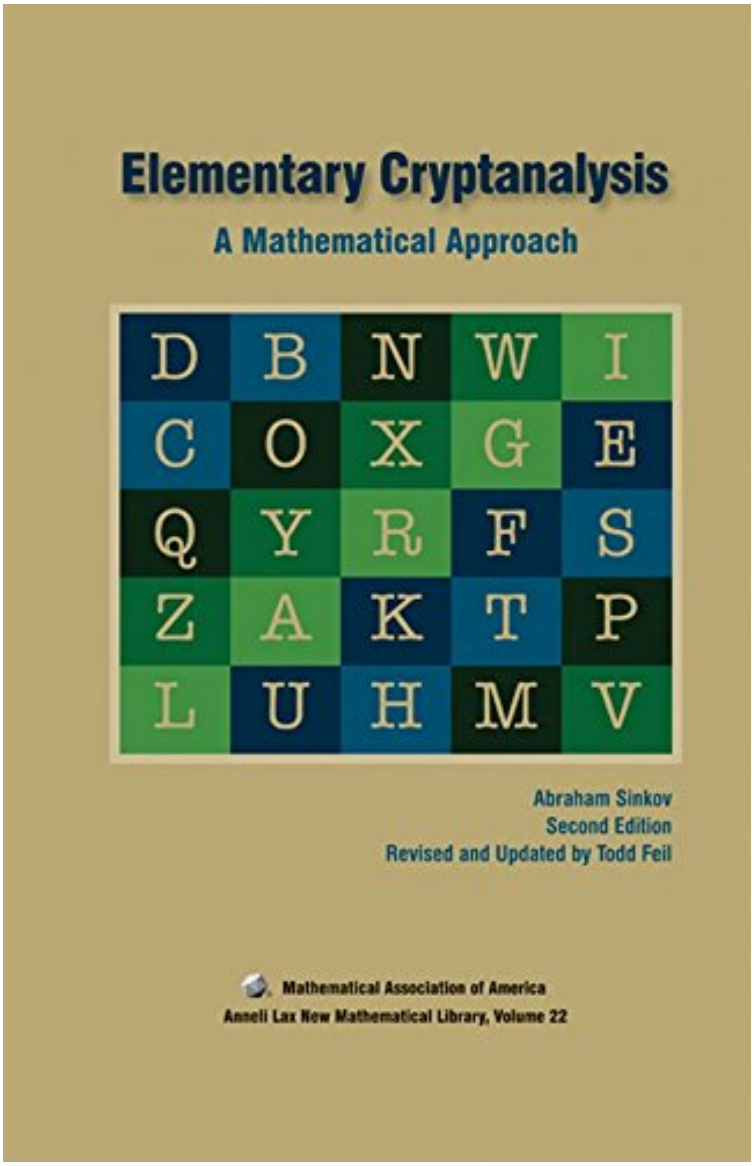
(Download pdf ebook) Elementary Cryptanalysis 2nd edition (Anneli Lax New Mathematical Library)

Elementary Cryptanalysis 2nd edition (Anneli Lax New Mathematical Library)

Abraham Sinkov
*ePub | *DOC | audiobook | ebooks | Download PDF*



Donwload Read Online

#936541 in Books Mathematical Association of America 2009-07-16Original language:EnglishPDF # 1 8.98 x .63 x 5.98l, .0 #File Name: 0883856476212 pages | File size: 76.Mb

Abraham Sinkov : Elementary Cryptanalysis 2nd edition (Anneli Lax New Mathematical Library) before purchasing it in order to gage whether or not it would be worth my time, and all praised Elementary Cryptanalysis 2nd edition (Anneli Lax New Mathematical Library):

2 of 3 people found the following review helpful. A Truly Remarkable Book ...By Richard T. LeitnerThis is absolutely

a classic of basic cryptanalysis. Like Gaines' book (originally called "Elementary Cryptanalysis" but also known by its Dover Book title "Cryptanalysis: A Study of Ciphers and Their Solution"), it covers only "classic" ciphers, those which can be used with pencil and paper for example, and it covers only a subset of those. Still, for beginners in the black art, it is indispensable for learning the techniques for breaking these ciphers. It has an advantage over Gaines text in that if the reader is willing to indulge in some mathematics, it provides a systematic, straightforward method of breaking the ciphers it covers. Those mathematics include basic linear algebra (which virtually everyone gets these days by the time of high school graduation), probability (which I believe very FEW get by high school graduation) and some elementary number theory (which I believe virtually no one gets in high school and most don't get in college). But neither the probability nor the number theory is too difficult for the average student and good basic texts are available for those that want to make the effort but lack the mathematical background. If you're truly interested in cryptanalysis as a hobby, GET THIS BOOK and make an effort to understand the methods it teaches and you will be rewarded with a profound understanding of basic cryptanalytic technique. Note: I own both the paperback version ("Mathematical Association of America Textbooks") and the 2nd Edition hardcover (Anneli Lax New Mathematical Library). The newer text includes 2 additional chapters (on RSA and One Time Pads) but leaves out some computer programs from older text that were written by Paul Irwin in BASIC for analyzing text. That's too bad because even though BASIC is somewhat dated, the algorithms are still valid and could easily be translated over to Perl, Java, C or any other modern language. In fact, they could be probably be copied with a little massaging into a Linux/Unix BASH shell script. Nonetheless, I highly recommend either version.

Originally published in the New Mathematical Library almost half a century ago, this charming book explains how to solve cryptograms based on elementary mathematical principles, starting with the Caesar cipher and building up to progressively more sophisticated substitution methods. Todd Feil has updated the book for the technological age by adding two new chapters covering RSA public-key cryptography, one-time pads, and pseudo-random-number generators.Exercises are given throughout the text that will help the reader understand the concepts and practice the techniques presented. Software to ease the drudgery of making the necessary calculations is made available. The book assumes minimal mathematical prerequisites and therefore explains from scratch such concepts as summation notation, matrix multiplication, and modular arithmetic. Even the mathematically sophisticated reader, however, will find some of the exercises challenging. (Answers to the exercises appear in an appendix.)

As a young mathematician, I learned how to make and break simple codes from Sinkov's beguiling introduction to cryptanalysis. In the intervening forty years there has been a revolution in cryptography, and it is fitting that for a modern edition of Sinkov's classic, Todd Feil has indicated the nature of this revolution by adding a lucid introduction to RSA public-key encryption and the number theory which underlies it. If you know a young code breaker who might become a young mathematician, buy her or him this book! Or buy it for yourself and try decoding those messages. --Phil Straffin, Professor Emeritus of Mathematics and Computer Science at Beloit CollegeSinkov's Elementary Cryptanalysis is an eminently readable classic that introduces the reader to both the techniques and the spirit of cryptanalysis -- the art and science of reading secret messages. Todd Feil has done a fine job of modernizing the language of the original. His chapters on RSA encryption and one-time pads give added value to the original, especially the very nice treatment of RSA that assumes almost no prior knowledge of number theory. --Ezra Brown, Virginia Tech UniversityAs a young mathematician, I learned how to make and break simple codes from Sinkov's beguiling introduction to cryptanalysis. In the intervening forty years there has been a revolution in cryptography, and it is fitting that for a modern edition of Sinkov's classic, Todd Feil has indicated the nature of this revolution by adding a lucid introduction to RSA public-key encryption and the number theory which underlies it. If you know a young code breaker who might become a young mathematician, buy her or him this book! Or buy it for yourself and try decoding those messages. --Phil Straffin, Professor Emeritus of Mathematics and Computer Science at Beloit College