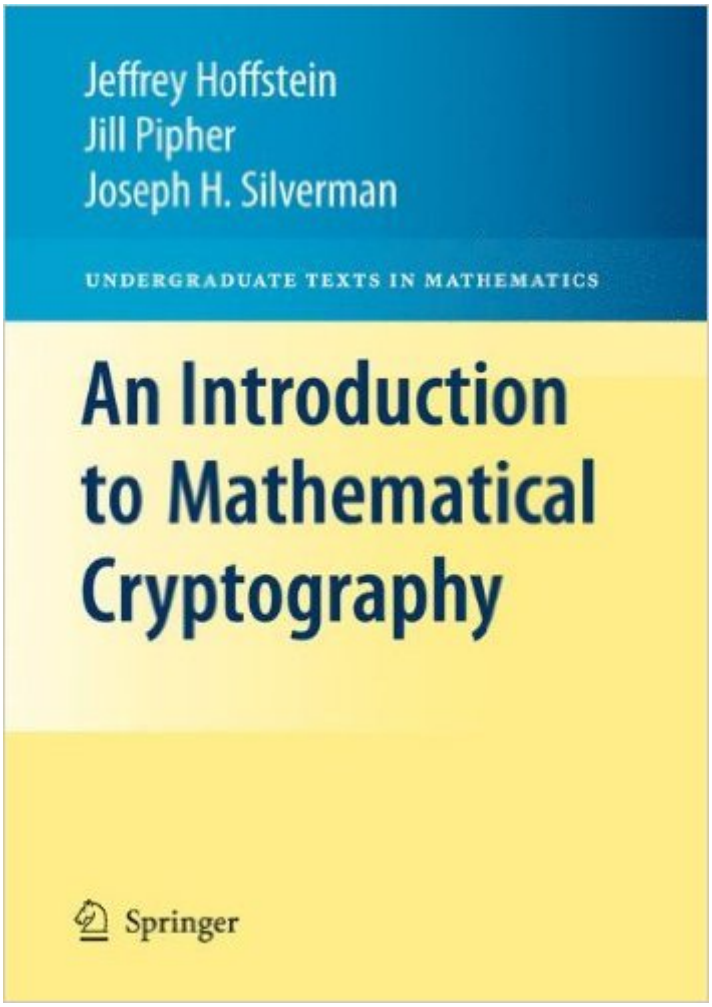
# An Introduction To Mathematical Cryptography (Undergraduate Texts In Mathematics)



## Synopsis

An Introduction to Mathematical Cryptography provides an introduction to public key cryptography and underlying mathematics that is required for the subject. Each of the eight chapters expands on a specific area of mathematical cryptography and provides an extensive list of exercises. It is a suitable text for advanced students in pure and applied mathematics and computer science, or the book may be used as a self-study. This book also provides a self-contained treatment of mathematical cryptography for the reader with limited mathematical background.

## Book Information

Series: Undergraduate Texts in Mathematics

Paperback: 524 pages

Publisher: Springer; Softcover reprint of hardcover 1st ed. 2008 edition (November 23, 2009)

Language: English

ISBN-10: 1441926747

ISBN-13: 978-1441926746

Product Dimensions: 6 x 1.2 x 9 inches

Shipping Weight: 2 pounds (View shipping rates and policies)

Average Customer Review: 4.5 out of 5 starsÂ Â See all reviewsÂ (13 customer reviews)

Best Sellers Rank: #336,001 in Books (See Top 100 in Books) #50 inÂ Books > Science & Math > Mathematics > Pure Mathematics > Algebra > Abstract #60 inÂ Books > Computers & Technology > Programming > Software Design, Testing & Engineering > Structured Design #98 inÂ Books > Science & Math > Mathematics > Pure Mathematics > Number Theory

## Customer Reviews

At least for the chapters that were studied by this reviewer, the authors of this book give an effective introduction to the mathematical theory used in cryptography at a level that can be approached by an undergraduate senior in mathematics. The field of cryptography is vast of course, and a book of this size could not capture it effectively. The topics of primary importance are represented however, and the authors do a fine job of motivating and explaining the needed concepts.The authors give an elementary overview of elliptic curves over the complex numbers, and most importantly over finite fields whose characteristic is greater than 3. The case where the characteristic is equal to 2 is delegated to its own section. In discussing the arithmetic of elliptic curves over finite fields, the authors give a good motivation for Hasse's formula, which gives a bound for the number of points of the elliptic curve (over a finite field), but they do not go into the details of the proof. The Hasse

formula is viewed in some texts as a "Riemann Hypothesis" for elliptic curves over finite fields, and was proven by Hasse in 1934. This reviewer has not studied Hasse's proof, but a contemporary proof relies on the Frobenius map and its separability, two notions that the authors do not apparently want to introduce at this level of book (however they do introduce the Frobenius map when discussing elliptic curves over F2). Separability is viewed in some texts in elliptic curves as more of a technical issue, which can be ignored at an elementary level. It arises when studying endomorphisms of elliptic curves of fields of non-zero characteristic, and involves defining rational functions. The Frobenius map is not separable, and this fact allows one to show that its degree is strictly greater than the number of points in its kernel. Taking the nth power of the Frobenius map and adding to it the endomorphism which simply multiplies elements by -1, one can show that the number of points of the elliptic curve is equal to the degree of this endomorphism. Just a few more arithmetical calculations establishes Hasse's estimate.Some more of the highlights of this part of the book: - The reminder that the fastest known algorithm to solve the elliptic curve discrete logarithm problem takes p^1/2 steps for a finite field Fp (i.e. the algorithms therefore are not really better than "black box" algorithms).- The brief historical discussion on public key cryptography.- The motivational discussion for the Lenstra algorithm using simple calculations that leads to a failed attempt to find the reciprocal of an integer modulo p. This failure is used to explain the workings of the Lenstra elliptic curve factorization algorithm in a way that it is better appreciated by the reader.- The discussion on the Frobenius map in the context of elliptic curves over F2 and its use in finding the number of points of an elliptic curve over a finite field.- The motivational discussion for the use of distortion maps, due to the degeneracy of the Weil pairing. The distortion maps are used to define a modified Weyl pairing, which is proved to be non-degenerate.Some omissions:- Algorithms used to calculate the number of points of an elliptic curve over a finite field that are more efficient than brute-force counting or estimation using Hasse's formula.- The proof that the torsion points of order m can be written as the product of two cyclic groups of order m. The authors apparently do not want to get into the notions of unramified and separable "isogenies" between elliptic curves and Galois extensions, both of which are used in the proof that they reference. Isogenies are mentioned in a footnote to the discussion on distortion maps, since the latter are isogenies.- The proof verifying certain properties of divisors, namely that they are equal if the corresponding rational functions are constant multiples of each other, and that the degree of a divisor is zero if its sum is the zero element of the elliptic curve. The proofs were no doubt omitted due to their dependence on techniques from algebraic geometry.- Quantum cryptography. This is discussed very briefly in the last chapter, but the subject is mature enough to be presented at the undergraduate level.-

Cryptography based on non-Abelian groups. One good example would be cryptography based on the mathematical theory of knots and braids (the braid group is non-Abelian), even though this approach is in its infancy at the present time, and in almost all cases shown to be highly vulnerable to attacks. It could have been included in the last chapter or possibly as a long exercise.- Hyperelliptic curves are discussed very briefly in the last chapter, but a full-fledged presentation could be done in the book without missing the targeted audience. Hyperelliptic curves are also mentioned after the discussion of the MOV algorithm, wherein the authors allude to the use of Weil descent to transfer the elliptic curve discrete logarithm problem to a discrete logarithm problem in a finite field F2^m when m is composite. The authors correctly don't want to elaborate on Weil descent in any more detail, since it requires a solid knowledge of field extensions and theory of algebraic varieties at a level that one obtains in a graduate course in algebraic geometry. Suffice it to say that the strategy of Weil descent involves finding a cover of the elliptic curve by a hyperelliptic curve that is defined over the extension of the ground field. This approach has been shown to be problematic for Koblitz curves, the latter of which are discussed in the book.Note: This review is based on a reading of chapters 5 and 8 of the book.

I'm doing my honor's thesis on theoretical Cryptography as an undergrad at Colby College, and this book has been the perfect resource. It is so clear, and many time teaches by using easy to understand concrete examples. This book is the perfect place to start if you want to learn about Crypto.

Good start to this topic. The only hiccup was that I tried to work through the text example myself and came up with different answers. This is because the text was wrong. There is an extensive errata file that you can get online. May sure you get it before starting to work through text examples and end-of-chapter exercises. I hope that a revised version is issued that corrects these errata.

This is a fantastic book. The writing is simple and clear. Even if I skipped class for a week, I could sit down and read this book, confident I would receive an explanation that was both complete and easy-to-follow. I couldn't recommend it more. Even though we didn't cover elliptic curves in my class, I read the chapter anyway and found that I was able to understand anything in the chapter that I committed to learning.

Good introduction to intermediate level coverage of math-based crypto, however, I found the text

hard to follow because the cross references were hard to look up. E.g. a back reference to proposition x.y is hard to look up bec propositions are somewhat sparse and each chapter x is very large -- so you find yourself thumbing through the chapter trying to find propositions to get your bearing. It really interferes with the reading process. Including a page number would help greatly. (For more purely math books, this isn't as large of an issue bec there are so many propositions and theorems that it's easy to isolate the back reference -- but for this text, it is quite difficult.)

It is for undergrads, but useful at grad level to any student who didn't take the courses as an undergrad (i.e., fresh grad students discovering their love to cryptography)

The text itself is decent and clear. However, I needed the 2nd edition for a class in which I was enrolled, and so rented the kindle version. Unfortunately, the kindle version linked is a reproduction of the first edition and as such is missing some of the exercises I need for the class.Edit (followup):By happy (from my perspective) accident it was the campus bookstore (and therefore the majority of my classmates) who had the wrong edition of the book. This does not alter my rating of the book, since the various formats linked together on a page ought (in my opinion) to be of the same edition of the text.

Examples are Ok, but the book is pretty good in general. I wish the examples were a little more intuitive.

Great Magic Tricks Introduction to Cryptography with Coding Theory Cryptography: A Very Short Introduction The Arithmetic of Dynamical Systems (Graduate Texts in Mathematics) Topics in Banach Space Theory (Graduate Texts in Mathematics) Rarefied Gas Dynamics: From Basic Concepts to Actual Calculations (Cambridge Texts in Applied Mathematics) Transforming Undergraduate Education: Theory that Compels and Practices that Succeed Principles of Colloid and Surface Chemistry, Third Edition, Revised and Expanded (Undergraduate Chemistry: A Series of Textbooks) Before The College Audition: A guide for creating your list of acting and musical theatre undergraduate programs