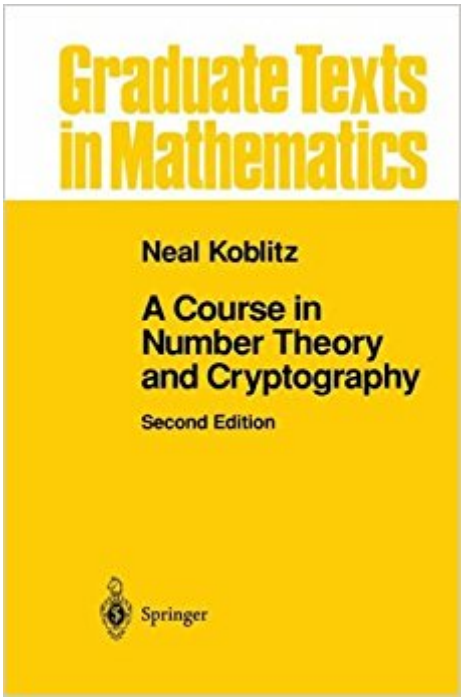
A Course In Number Theory And Cryptography (Graduate Texts In Mathematics)



Synopsis

This is a substantially revised and updated introduction to arithmetic topics, both ancient and modern, that have been at the centre of interest in applications of number theory, particularly in cryptography. As such, no background in algebra or number theory is assumed, and the book begins with a discussion of the basic number theory that is needed. The approach taken is algorithmic, emphasising estimates of the efficiency of the techniques that arise from the theory, and one special feature is the inclusion of recent applications of the theory of elliptic curves. Extensive exercises and careful answers are an integral part all of the chapters.

Book Information

Series: Graduate Texts in Mathematics (Book 114)
Hardcover: 235 pages
Publisher: Springer; 2nd edition (September 2, 1994)
Language: English
ISBN-10: 0387942939
ISBN-13: 978-0387942933
Product Dimensions: 6.1 x 0.6 x 9.2 inches
Shipping Weight: 12.8 ounces (View shipping rates and policies)
Average Customer Review: 4.7 out of 5 stars 19 customer reviews
Best Sellers Rank: #402,166 in Books (See Top 100 in Books) #114 inÂ Books > Science & Math > Mathematics > Pure Mathematics > Number Theory #4901 inÂ Books > Textbooks > Science & Mathematics > Mathematics

Customer Reviews

The purpose of this book is to introduce the reader to arithmetic topics, both ancient and modern, that have been at the center of interest in applications of number theory, particularly in cryptography. No background in algebra or number theory is assumed, and the book begins with a discussion of the basic number theory that is needed. The approach taken is algorithmic, emphasizing estimates of the efficiency of the techniques that arise from the theory. A special feature is the inclusion of recent application of the theory of elliptic curves. Extensive exercises and careful answers have been included in all of the chapters. Because number theory and cryptography are fast-moving fields, this new edition contains substantial revisions and updated references.

I won’t be sharing too many textbooks but this one needs attention. Written by Neal Koblitz, one of my favorite mathematicians and the inventor of elliptic curve cryptography. I love two of his books. This is one of them. I’ll keep the other book secret until the next part of the series. I love Neal’s book because he gets straight to the point and uses a smaller font in his books to pack more information on one page.This is one of the first books I ever read on mathematical foundations of cryptography. It says graduate on the cover but don’t listen to that. It’s really an undergraduate level book. All you need to know is a bit of algebra. Book starts with a review of several key number theory topics, moves to finite fields, then to the public key cryptography, RSA, zero-knowledge proofs, then primality testing, factoring and finally elliptic curves.This book follows definition-theorem-proof-example style that I like and it has many exercises with answers. If you like math but don’t have experience with fundamentals of cryptography then this is the book to get to quickly get yourself up to speed. Fundamentals don’t change and once you master what’s in this book (shouldn’t take more than a week or two if you’re smart and dedicated), you’ll be able to read any crypto text.I’ve placed this book #17 in my Top 100 Programming, Computer and Science books list:[...](If this link gets removed, google for >>catonmat top 100 programming computer science books

I was a little leery of this book as I’m certainly no William Friedman or Alan Turing. But I was surprised to find the topic not as daunting as I thought although people who lock up when they see formulas may be intimidated at first glance. This book deals with number theory, dealing with some fundamental properties of numbers with application to cryptographic uses. Each section takes you slowly through the theory and provides exercises at the end of each chapter you can work through. (The answers are in the back of the book.) This is a particularly useful book if you are conversant in programming and want to play with certain aspects of number theory and cryptography to ’see how it really works.’ It’s like a course in tumblers and pins for someone who is fascinated by locks.

This is a great read on the topic from a mathematical perspective. Still, if you believe that cryptography is the only point of this book, you’re doing it wrong.

The item is in great conditions!

This book is an outstanding introduction to cryptographic techniques and algorithms Although it’s labelled as a "graduate text in mathematics", most of it should be accessible to anyone who knows

a little linear algebra. For readers just interested in the how-to of the algorithms, not even that is needed. Koblitz does a thorough job of leading up to each algorithm and proving its formal properties. He also presents the algorithms themselves, unencumbered by denser material of interest to mathematicians.The book covers a variety of topics - public-key encryption, primality testing, factoring, and cryptographic protocols. It introduces zero-knowledge proofs and blind transfer, techniques that offer real hope of personal privacy in a world where data transfer is mandatory. I was a little disappointed by the chapters on elliptic cryptography, however. I hoped that Koblitz would bring is explanatory powers to bear on the algorithms. Somehow, I never quite connected with his descriptions of elliptic curves - perhaps I'm just thick, or perhaps a bit more introductory material would have helped.The rest of the book is a very fine example of clear, readable math writing. Its clarity its range of topics earn it a place with anyone interested in cryptography, factoring, and prime numbers.

Two areas of this book deserve special mention. The first chapter develops a careful treatment of the _exact_ bit complexity of operations on numbers, such as +,-,*,/, modular powering, and gcd. While other books give crude estimates, or leave out such details entirely, Koblitz invests a good deal of time not only in giving the number of operations, but in teaching the reader how to make his own estimates. *Highly* useful.Second, the book contains a concise introduction to modern factoring algorithms. After a discussion of primality testing, it goes on to develop the notion of a "B-smooth" number and then show how this leads to algorithms which use factor bases. Examples are given in the text, and the reasons behind that funny-looking time estimate O(e^(c*sqrt(log n log log n)) are provided. Seriously good stuff.The exercises are also first rate - fun, intriguing, and serve to teach new ideas (not just test knowledge of the chapter).In parts it shows its age (1994); for example, the Chor-Rivest knapsack described on p.115 has been broken by Serge Vaudenay. Much more discussion of randomized cryptography would also have been nice (though perhaps much in an intro book?). The most glaring deficiency is the lack of any real discussion of chosen ciphertext attacks, signature forgery, or padding schemes. You can't use this by itself to develop a new real-world project.Instead, it's more like a "cryptographer's toolbox," which gives you a thorough introduction to the primitives involved, giving you the understanding necessary to start thinking intelligently about how they are used.

Financial Cryptography and Security (Chapman & Hall/CRC Cryptography and Network Security Series) Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) Representation Theory: A First Course (Graduate Texts in Mathematics) A Course in the Theory of Groups (Graduate Texts in Mathematics, Vol. 80) Aprender InglÃªs: N.o 3: Textos Paralelos, FÃ¡cil de ouvir, FÃ¡cil de ler : [Learn English: Number 3, Parallel Texts, Easy to Hear, Easy to Read]: Curso de Ã•udio de InglÃªs, N.o 3 [English Audio Course, Number 3] Aprender AlemÃ£o, N.o 2: Textos Paralelos, FÃ¡cil de ouvir, FÃ¡cil de ler [Learn German, Number 2: Parallel Texts, Easy to Hear, Easy to Read]: Curso de Ã•udio de AlemÃ£o, N.o 2 [German Audio Course, Number 2] An Introduction to Number Theory with Cryptography An Introduction to Mathematical Cryptography (Undergraduate Texts in Mathematics) Algebraic Geometry: A First Course (Graduate Texts in Mathematics) (v. 133) Cryptography: Theory and Practice, Third Edition (Discrete Mathematics and Its Applications) Matrices: Theory and Applications (Graduate Texts in Mathematics) Introduction to Lie Algebras and Representation Theory (Graduate Texts in Mathematics) (v. 9) Graph Theory (Graduate Texts in Mathematics) Algebraic Graph Theory (Graduate Texts in Mathematics) Matroid Theory (Oxford Graduate Texts in Mathematics) Deformation Theory (Graduate Texts in Mathematics) An Introduction to Ergodic Theory (Graduate Texts in Mathematics) Quantum Theory for Mathematicians (Graduate Texts in Mathematics)