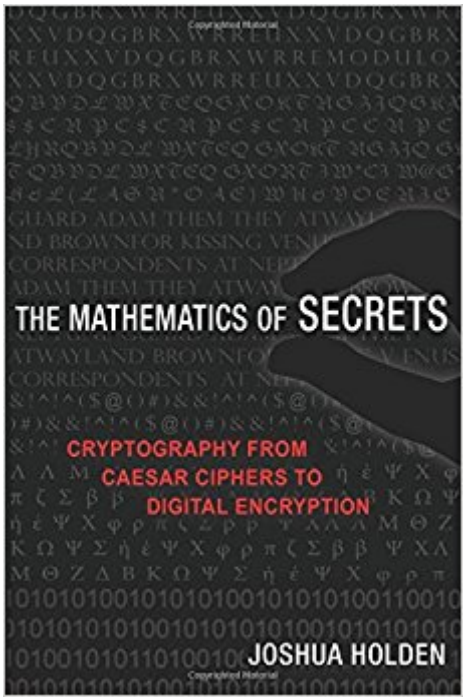
The Mathematics Of Secrets: Cryptography From Caesar Ciphers To Digital Encryption



Synopsis

The Mathematics of Secrets takes readers on a fascinating tour of the mathematics behind cryptographyÃ¢â ¬â ¢the science of sending secret messages. Most books about cryptography are organized historically, or around how codes and ciphers have been used, such as in government and military intelligence or bank transactions. Joshua Holden instead shows how mathematical principles underpin the ways that different codes and ciphers operate. Holden focuses on both code making and code breaking and he discusses the majority of ancient and modern ciphers currently known.Holden begins by looking at substitution ciphers, built by substituting one letter or block of letters for another. Explaining one of the simplest and historically well-known ciphers, the Caesar cipher, Holden establishes the key mathematical idea behind the cipher and discusses how to introduce flexibility and additional notation. Holden goes on to explore polyalphabetic substitution ciphers, transposition ciphers, including one developed by the Spartans, connections between ciphers and computer encryption, stream ciphers, and ciphers involving exponentiation. He also examines public-key ciphers, where the methods used to encrypt messages are public knowledge, and yet, intended recipients are still the only ones who are able to read the message. He concludes with a look at the future of ciphers and where cryptography might be headed. Only basic mathematics up to high school algebra is needed to understand and enjoy the book.With a plethora of historical anecdotes and real-world examples, The Mathematics of Secrets reveals the mathematics working stealthily in the science of coded messages.

Book Information

Hardcover: 392 pages
Publisher: Princeton University Press (February 14, 2017)
Language: English
ISBN-10: 0691141754
ISBN-13: 978-0691141756
Product Dimensions: 6.5 x 1.2 x 9.3 inches
Shipping Weight: 3.1 pounds (View shipping rates and policies)
Average Customer Review: 4.7 out of 5 stars 4 customer reviews
Best Sellers Rank: #96,135 in Books (See Top 100 in Books) #37 inÃ Â Books > Computers & Technology > Security & Encryption > Encryption #38 inÃ Â Books > Computers & Technology > Security & Encryption > Cryptography #74 inÃ Â Books > Science & Math > Mathematics > History

Customer Reviews

"A fascinating tour of the mathematics behind cryptography, showing how its principles underpin the ways that different codes and ciphers operate. . . . While itÃ¢â ¬â„¢s all about maths, [The Mathematics of Secrets] is accessibleÃ¢â ¬â ¢basic high school algebra is all thatÃ¢â ¬â„¢s needed to understand and enjoy it."--Cosmos Magazine"For anyone with an interest in cryptography."--Noel-Ann Bradshaw, Times Higher Education"Any book on cryptography written for a more-or-less lay audience must inevitably face comparisons to The Code Book . . . by Simon Singh. . . . The Mathematics of Secrets is tilted (and indeed titled) more towards a fuller explanation of the mathematical techniques underlying the various ciphers. . . . [F]or anyone who wants to go a bit deeper than Simon Singh took them."--Paul Taylor, Aperiodical

"Suitable for anyone with a basic understanding of high school math, The Mathematics of Secrets presents the theoretical principles of cryptography, from Julius Caesar’s primitive cipher to the intricacies of the modern digital signature. This terrific book is a testament to the almost supernatural power of mathematics."--Paul J. Nahin, author of In Praise of Simple Physics

I have read until know just the half of the book but I just wanted to say that. The writer has made the subject of cryptography very interesting, One thing that was a little annoying that in the end of the book. For every chapter he wrote some notes and it was annoying to go each time to the end of the book and read that but overall good book look forward for ending it!

The book is described in a way that makes it sound on the level of other popular survey of history books.It really contains a lot of ’meat’ and describes in detail how mathematical tools can be used--and is very clear in doing so.Top notch book. Colleges and public libraries should have this book.

2017 has produced an excellent book on cryptography. Clear, simple explanations of the concepts. A historical depth that builds an interesting storyline and some remarkable facts. I was amazed that non-carrying binary addition (XOR) was used in 1917. Many concepts are introduced in a historical context where technology was much simpler. Some people will still find the math a bit challenging. But this is a great introduction.

Thanks, interesting book.

The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption ISO/IEC 18033-2:2006, Information technology - Security techniques - Encryption algorithms - Part 2: Asymmetric ciphers Uncracked Codes and Ciphers (Cryptography: Code Making and Code Breaking) Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) Handbook of Financial Cryptography and Security (Chapman & Hall/CRC Cryptography and Network Security Series) Caesar's Legion: The Epic Saga of Julius Caesar's Elite Tenth Legion and the Armies of Rome A Caesar Reader: Selections from Bellum Gallicum and Bellum Civile, and from Caesar's Letters, Speeches, and Poetry (Latin Edition) (Latin Readers) (Latin and English Edition) Photography: DSLR Photography Secrets and Tips to Taking Beautiful Digital Pictures (Photography, DSLR, cameras, digital photography, digital pictures, portrait photography, landscape photography) Cryptography: Theory and Practice, Third Edition (Discrete Mathematics and Its Applications) A Course in Number Theory and Cryptography (Graduate Texts in Mathematics) An Introduction to Mathematical Cryptography (Undergraduate Texts in Mathematics) Privacy on the Line: The Politics of Wiretapping and Encryption (MIT Press) Approaches to Solve Big Data Security Issues and Comparative Study of Cryptographic Algorithms for Data Encryption Mastering Algorithms with C: Useful Techniques from Sorting to Encryption Bitcoin Basics: Cryptocurrency, Blockchain And The New Digital Economy (Digital currency, Cryptocurrency, Blockchain, Digital Economy) Photography: Complete Guide to Taking Stunning,Beautiful Digital Pictures (photography, stunning digital, great pictures, digital photography, portrait ... landscape photography, good pictures) Top Secret: A Handbook of Codes, Ciphers and Secret Writing Codes and Ciphers (Spy Files) The Ciphers of Muirwood: Covenant of Muirwood, Book 2 Unsolved!: The History and Mystery of the World's Greatest Ciphers from Ancient Egypt to Online Secret Societies