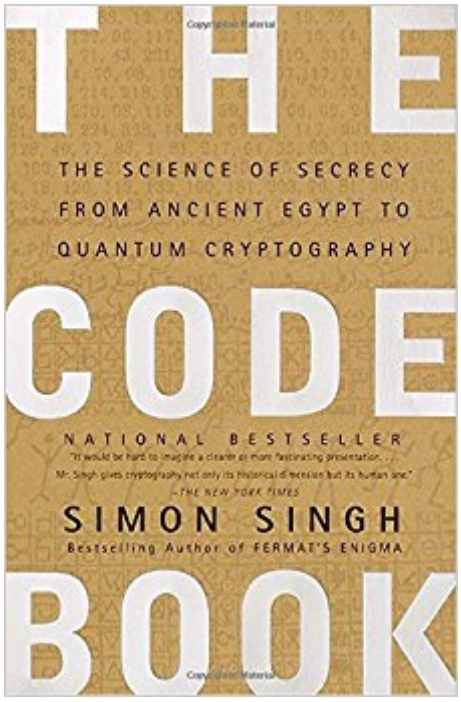
The Code Book: The Science Of Secrecy From Ancient Egypt To Quantum Cryptography



Synopsis

In his first book since the bestselling Fermat’s Enigma, Simon Singh offers the first sweeping history of encryption, tracing its evolution and revealing the dramatic effects codes have had on wars, nations, and individual lives. From Mary, Queen of Scots, trapped by her own code, to the Navajo Code Talkers who helped the Allies win World War II, to the incredible (and incredibly simple) logisitical breakthrough that made Internet commerce secure, The Code Book tells the story of the most powerful intellectual weapon ever known: secrecy.Throughout the text are clear technical and mathematical explanations, and portraits of the remarkable personalities who wrote and broke the world’s most difficult codes. Accessible, compelling, and remarkably far-reaching, this book will forever alter your view of history and what drives it.Â Â It will also make you wonder how private that e-mail you just sent really is.

Book Information

Paperback: 432 pages

Publisher: Anchor; Reprint edition (August 29, 2000)

Language: English

ISBN-10: 0385495323

ISBN-13: 978-0385495325

Product Dimensions: 5.2 x 0.9 x 8 inches

Shipping Weight: 14.4 ounces (View shipping rates and policies)

Average Customer Review: 4.7 out of 5 stars 511 customer reviews

Best Sellers Rank: #11,190 in Books (See Top 100 in Books) #6 inÂ Books > Computers & Technology > Security & Encryption > Encryption #6 inÂ Books > Computers & Technology > Security & Encryption > Cryptography #19 inÂ Books > Engineering & Transportation > Engineering > Reference > History

Customer Reviews

People love secrets. Ever since the first word was written, humans have sent coded messages to each other. In The Code Book, Simon Singh, author of the bestselling Fermat’s Enigma, offers a peek into the world of cryptography and codes, from ancient texts through computer encryption. Singh’s compelling history is woven through with stories of how codes and ciphers have played a vital role in warfare, politics, and royal intrigue. The major theme of The Code Book is what Singh calls "the ongoing evolutionary battle between codemakers and codebreakers," never more clear than in the chapters devoted to World WarÂ II. Cryptography came of age during that conflict, as

secret communications became critical to both sides' success. Confronted with the prospect of defeat, the Allied cryptanalysts had worked night and day to penetrate German ciphers. It would appear that fear was the main driving force, and that adversity is one of the foundations of successful codebreaking. In the information age, the fear that drives cryptographic improvements is both capitalistic and libertarian--corporations need encryption to ensure that their secrets don't fall into the hands of competitors and regulators, and ordinary people need encryption to keep their everyday communications private in a free society. Similarly, the battles for greater decryption power come from said competitors and governments wary of insurrection. The Code Book is an excellent primer for those wishing to understand how the human need for privacy has manifested itself through cryptography. Singh's accessible style and clear explanations of complex algorithms cut through the arcane mathematical details without oversimplifying. --Therese Littleton

In an enthralling tour de force of popular explication, Singh, author of the bestselling Fermat's Enigma, explores the impact of cryptographyAthe creation and cracking of coded messagesAon history and society. Some of his examples are familiar, notably the Allies' decryption of the Nazis' Enigma machine during WWII; less well-known is the crucial role of Queen Elizabeth's code breakers in deciphering Mary, Queen of Scots' incriminating missives to her fellow conspirators plotting to assassinate Elizabeth, which led to Mary's beheading in 1587. Singh celebrates a group of unsung heroes of WWII, the Navajo "code talkers," Native American Marine radio operators who, using a coded version of their native language, played a vital role in defeating the Japanese in the Pacific. He also elucidates the intimate links between codes or ciphers and the development of the telegraph, radio, computers and the Internet. As he ranges from Julius Caesar's secret military writing to coded diplomatic messages in feuding Renaissance Italy city-states, from the decipherment of the Rosetta Stone to the ingenuity of modern security experts battling cyber-criminals and cyber-terrorists, Singh clarifies the techniques and tricks of code makers and code breakers alike. He lightens the sometimes technical load with photos, political cartoons, charts, code grids and reproductions of historic documents. He closes with a fascinating look at cryptanalysts' planned and futuristic tools, including the "one-time pad," a seemingly unbreakable form of encryption. In Singh's expert hands, cryptography decodes as an awe-inspiring and mind-expanding story of scientific breakthrough and high drama. Agent, Patrick Walsh. (Oct.) FYI: The book includes a "Cipher Challenge," offering a $15,000 reward to the first person to crack that code.

Like all narrative non-fictional works that, eventually in this case, deal with technical subjects whose details are beyond the scope of the non-specialist reader, this book attempts to strike a balance between two extremes, between a book so chock-full of technical detail that it reads like a textbook and a book that skimps so completely on the heart of the matter at hand that it can only be described as fluff. Singh has done a remarkable job in balancing the two here, it seems to me, and the book is worth any reader's time whose interest is piqued by cryptography.Singh is singularly aided by his subject matter here. This book was recommended to me by a fellow poster on a crossword puzzle blog which I frequent, as a daily solver of the New York Times crossword. The discussions on the blog vary from the whimsical to the technical with all manner of things mooted. So goes Singh's book as well. But what makes this possible is that cryptography and cryptanalysis, for most of human history, has been no more complex, au fond, than a very difficult crossword puzzle. And one is not surprised to see a crossword used during WWII by the British to test potential candidates for work at top secret Bletchley Park, which was responsible for cracking Germany's "Enigma" code. The crossword is provided in the book and was jolly fun to solve.It seems to me that up to the VigenÃ¨re polyalphabetic coding, known for centuries as "le chiffre indÃ©chifferable", anyone with an interest in this book could understand and create such a cipher and write an encrypted message in it. Indeed, it's in deciphering such messages without the "keyword" that the technical going gets somewhat involved and perhaps beyond the ken of some readers not familiar with basic statistical analysis, and, not coincidentally, this decipherment of such encryptions is where maths starts to predominate. But it's certainly not difficult to understand the concept of how these encryptions are deciphered, it's merely very tedious and painstaking to do it as Charles Babbage finally did in the 19th Century.Up to this point, for this reader in any event, no trade-off was necessary and Singh is free to fill his tale of codes and ciphers with histories which hinge upon them, starting with the life and death of Mary, Queen of Scots. Also, he makes an elegant segue in the tale of how the Linear B tablets were finally translated, and the toing and froing of certain egotistical archaeologists etc. - It should be noted here the final decipherment and translation of Linear B was the cumulative work of men (and one woman) of genius who were linguistic prodigies. - Again, pass the 19th century and the non-specialist becomes more than a tad lost in the, literally and figuratively, nuts and bolts of Enigma machines and multi-lingual scholarship and fluency.Thus, it's no surprise that the ending of the book was the weakest part for me. Though it must be said that Singh goes out of his way to use "Alice, Bob, Eve" analogies to make the concepts clearer most effectively, being able to do what the main players in the tale are doing is far beyond the amateur's grasp. Also, the book is thirteen years old and the final sections dealing with computer encryption

seem a bit dated already.In sum though, a very pleasing, well-written book about the perennial human need to keep matters secret.

I really enjoyed the historical perspective of encryption and codes. Simon Singh does a great job of showing how both cryptography techniques were created and broken through history. As someone involved in the computer industry, however, the more "modern" sections are showing their age. This is a fast moving area. It would be great to see the book updated with more context of state actors and the revelations that have surfaced over the last ~10 years.

I read the condensed version a decade ago and loved it, so decided to get the full book now. To be honest, I think the condensed version is better and more appealing to non-geeks, but I have enough geek in me to not be bored by the TL;DR version.What's great is that encryption still hasn't moved on much since the book was written so it is still very relevant. The discussion about quantum computers and quantum encryption is great introduction to stuff that is becoming a reality today.

Great book! Let me tell you that those who may not have a fascination with cryptography will surely find this book at least interesting. The science of secrecy is every bit as important in its contributions to human progress as with the other sciences. Prepare to be both surprised and mesmerized at how cryptography is a necessary part of human survival.

My husband's all-time favorite book. He'd read me passages, and even I found them interesting. He called it highly intriguing and he couldn't put it down. So, if you love engineering and cryptology, you'll love this.

I've been developing an interest in physics as well as cryptography. I was turned on to Singh's The Code Book simply because it mentioned quantum physics in the title, a happy intersection between my two new hobby subjects. Soon after cracking it open, I realized that I'd picked up one of my favorite books in the past few years.Singh does a great job of laying out the history of cryptography (code writing) and cryptanalysis (code breaking, essentially) as well as explaining the logic behind each of the codes he discusses. It's a fascinating history that builds and builds upon itself, making it clear to the reader how the cryptography readily available to him/her now was born. All the while, Singh's explanation of the thought behind the codes is clear enough for a non-math major to quickly grasp (i.e. myself).I admit that the subject matter was right up my alley and this might not be the

case for everyone, but I feel Singh's ability to weave a narrative into a convoluted subject (as it would be) is excellent and warrants a pick up. The history is sturdy enough to support just about any reader and the analysis of the logic is clear and simple to latch on to, even as it delves into some deeper details.In all, this was a great read and I'd highly recommend picking it up.

This was a very easy reading book-- in spite of the level of sophistication of some of the ideas. It is also very good how the author reviews just enough math for what you will need to know in order to understand some of the ideas in codebreaking.There are also lots of nuggets of knowledge for people who like trivia-- such as the contribution of the Navajo to the war effort by the use of their language, or the Poles to codebreaking technology because of their being in between two hostile neighbors. It is also often not understood the level of aggression of the Germans during WWII and how much thought went into the military strategies of the various nations.The prose is clear and concise. This is defnitely worth a second read.As a final testatment to how absorbing this book was: I read most of it on a train traveling through China while seated in a car that held about 150 other people (in spite of being designed for 105), and that was so crowded that it was not possible to move down the aisles. This book kept me busy for almost the whole train ride.

(International Code Council Series) Alexander: The Great Leader and Hero of Macedonia and Ancient Greece (European History, Ancient History, Ancient Rome, Ancient Greece, Egyptian History, Roman Empire, Roman History) Ancient Egypt: A History From Beginning to End (Ancient Civilizations Book 2) Lucifer's Banker: The Untold Story of How I Destroyed Swiss Bank Secrecy Bank Secrecy Act/ Anti-Money Laundering Examination Manual (AML) :Examination Procedures: Narrative Guidance and Background Information Power Wars: The Relentless Rise of Presidential Authority and Secrecy Rule by Secrecy: The Hidden History That Connects the Trilateral Commission, the Freemasons, and the Great Pyramids