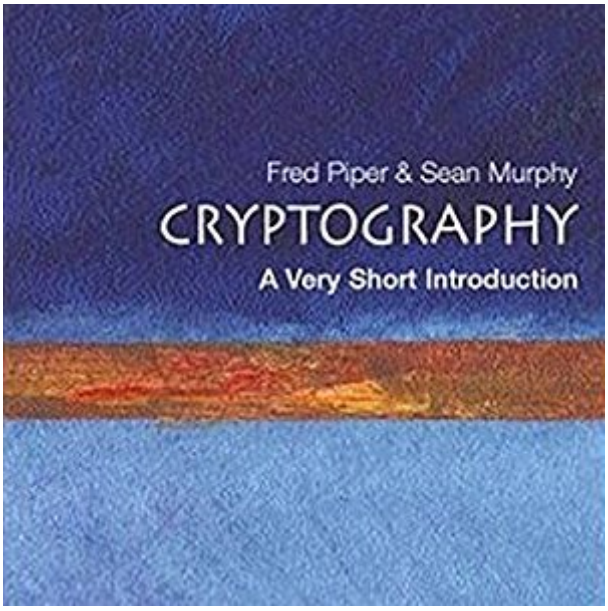
Cryptography: A Very Short Introduction



Synopsis

This book is a clear and informative introduction to cryptography and data protection - subjects of considerable social and political importance. It explains what algorithms do, how they are used, the risks associated with using them, and why governments should be concerned. Important areas are highlighted, such as Stream Ciphers, block ciphers, public key algorithms, digital signatures, and applications such as e-commerce. This book highlights the explosive impact of cryptography on modern society, with, for example, the evolution of the Internet and the introduction of more sophisticated banking methods.

Book Information

Audible Audio Edition
Listening Length: 4 hoursÂ andÂ 26 minutes
Program Type: Audiobook
Version: Unabridged
Publisher: Audible Studios
Audible.com Release Date: April 13, 2010
Whispersync for Voice: Ready
Language: English
ASIN: B003H2O91Y
Best Sellers Rank: #50 inÂ Books > Audible Audiobooks > Science > Mathematics #93 inÂ Books > Computers & Technology > Security & Encryption > Encryption #99 inÂ Books > Computers & Technology > Security & Encryption > Cryptography

Customer Reviews

this book is exactly what it says it is and is excellent at that task. i highly recommend this book to a sys-admin that wants to understand the basics of encryption without being an expert, anyone interested in cryptograms, or anyone with just a casual interest in the history, and concepts of cryptography.this book is not designed for mathematicians or security experts looking deep inner workings of algorithms.the book is easy to follow without the need for a technical or mathematics background and gives occasional problems for the reader to solve which will be of interest to anyone who enjoys cryptograms.as a network engineer, i found this an enjoyable pleasure read which shed some light on the encryption protocols employed on some of the gear i manage.

The book is good as befits its subtitle. Indeed, a very short introduction, with only a minimal

evocation of maths background. But there is enough qualitative explanation so that you can understand the broad historical development. From the Caesar Cipher to a Simple Substitution Cipher to a Vigenere Square Cipher. Then, the text goes into modern ideas, all of which involve using computers to encrypt and decrypt. Notably the invention of the public key system. Truly quite different from all that preceded it.There is also a brief foray into quantum computing. Here, it is mostly conceptual; discussing the possible potential, since current implementations are very rudimentary. The text has no mention of man in the middle attacks and how to guard against these. Pity. Because while this is a very hard attack to perform, if it can done, then it is very hard to defend against. One of the promises of quantum computing is that it inherently offers a simple detection, based on quantum interference by the attacker.

I was surprised that the booklet goes into the history of cryptography, but it’s relatively thorough. Great resource if you need a quick, accurate, and complete review of the subject for people who aren’t cryptologists or cryptographers.

Be aware that there are multiple errors on page 30, so don’t get flustered and give up. It’s a practice exercise, and a fun one, but if you get stumped, just use some ingenuity and keep moving through. I did a quick skim afterward for an answer key and a "surprise, we threw in some errors!", but didn’t find it. So, if you think you’re solving it and then a wrench gets thrown into the gears, just keep going and assume that it’s one of the errors. With Kryptos, there are both intentional and accidental errors, so I just assumed each one was an error after I checked my own deduction, and kept going. Sure enough, things made sense, but there are "typos", so don’t let that stop you. I was doing it in my head, so I got very frustrated having to second-guess myself, thinking that I made a mistake, because I DID make one letter mistake which I caught when it made its second appearance, before any of the errors were against me. Not having anything on paper, realizing a mistake that I made, and then coming across more mistakes which I couldn’t blame on myself and correct was very frustrating and confusing. Do it on paper and laugh at the sloppy mistakes, or do it in your head and know that you don’t have to quadruple-check that it’s not your own fault. Check once, know that they messed up, and don’t let it ruin the fun...it almost ruined my fun. ...And that’s how I spent my Thursday night without a girlfriend anymore.I’m not new to the idea of encryption since my background is in IT, but I wanted to do some serious learning and start from the ground floor to better understand the algorithms in practice. This book is the first of three I’m reading to correct any misunderstandings I may have had, and it’s an easy and good read so far. I haven’t finished it yet (I

often get bored and skim, then move to a new book), but I may as well warn others of page 30 in the event I don't update my review. Good starter book. I'm glad I got it.

This book is exactly as described: A straight-forward, quick summary of Cryptography concepts. It doesn't provide much detail at the level of Mathematical Theory or computer-programming on any one of them, but it clearly explains the value and downfalls of various types of encryption, including most of the more common modern standards.It speaks in terms of how each can be broken, and why some are extremely difficult to break (although certainly not impossible). It talks about various attack vectors and how to mitigate them. It includes straight-forward descriptions of how these encryption standards work in web-based E-commerce.It also addresses some security concerns not strictly tied to or limited to encryption. For example, you have a secure channel, but how do you know whether the person at the other end of that channel is whom you think it is?It's generally well-written, and its illustrations pretty easy to follow.

It is hard to find a crypto book that achieves a good balance between math, theory and practice. This book scores a bullseye in balancing all three. I recommend it for newbies learning about crypto and also for security practitioners who want more perspective on the crypto aspects of their field. The only people it would not be suitable for are crypto specialists. In 133 pages of text, this book provides insight into history, algorithms, mathematical foundations and practical applications. It is also an enjoyable read!

Very Short Introduction (Very Short Introductions) Gandhi: A Very Short Introduction (Very Short Introductions) Judaism: A Very Short Introduction (Very Short Introductions) Coral Reefs: A Very Short Introduction (Very Short Introductions)