

Book Review: Modern Cryptanalysis Review

Title: Modern Cryptanalysis

Author: Christopher Swenson

ISBN: 9780470135938

Publisher: 2008, Wiley Publishing

Review by Don Franke

I do not have a mathematics background, but I wanted to get a deeper understanding of cryptography in general, as well as a little more detail on the different kinds of encryption solutions out there, with the option of digging deeper into the actual math and mechanics behind them. This book allow me to do this. Overall, it provides three things:

- Background and history of cryptography
- Overview of the important cryptographic solutions currently being used (S-boxes, Feistel structures, DES, etc.)
- Details on mathematics of how encryption algorithms work, to the point of understanding their exploitable vulnerabilities, not just their well-publicized strengths

Each chapter is also concluded with a summary and exercises, to help you better understand and learn by doing. The following are three chapters I thought that really stood out.

Simple Ciphers

This chapter provides an excellent introduction to the beginnings of cryptography (ROT13, even Klingon!) This chapter dovetails nicely into coincidence and how to start performing cryptanalysis, studying algorithmic flaws. As an aside, the discussion on the Vigenere Tableau goes well with the more detailed chapter on the same topic in *The Code Book* by Simon Singh.

Number Theoretical Ciphers

What I liked about this chapter is that it contained sections like Probability, which begins with what every Stats course begins with: the coin flip. But subtly the chapter gets more complicated, evolving to permutations, dependence, then breaks with the section Fun With Poker. After this is the Birthday Paradox, an important demonstration of probability, then moves on to cryptographic hashes. This is an example of how the chapters work: they start out with the basics, then lead you into more and more detail.

The section Number Theory Refresher Course in this chapter was the reason I got the book, and I wasn't disappointed. It gets the reader ready for the involved math that is to follow in the rest of the book.

Block Ciphers

This chapters covers all the different forms of modern block ciphers. It begins with an overview of binary arithmetic, then moves on to the S-box, P-box, and shift registers. FEAL, DES, and Fiestel Structures are covered, including some demonstrative Python code. All of the other important ciphers are also included: Blowfish, AES, MD5, each with it's own quick history section. Random Number Generators earns its own section, importantly, because it's the generation of predictable numbers that often is the flaw in cryptographic implementations.

Summary

I got what I wanted out of the book: a good background on fundamental concepts of cryptography, a good introduction on how cryptanalysis can be performed on what seems to be unbreakable ciphers, and enough math to keep me busy for a long time. There's also some Python code snippets to help explain how how some pieces of encryption solutions work. Also at the end of each chapter is a list of references, providing ample reading material to continue your learning.

If you are interested in cryptography beyond just to how to implement prepackaged solutions, this book is a great primer. This would also serve as a great textbook for any cryptography class.