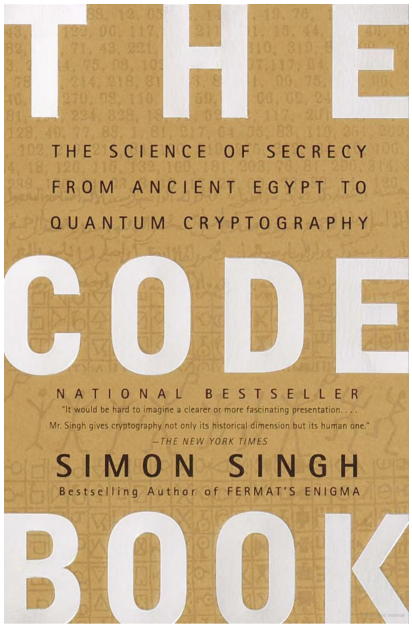

THE CODE BOOK

Simon Singh

Review Written by John Lensmire

OVERVIEW

- Simon Singh
- The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography
- Anchor Books
  A Division of Random House, Inc.
  New York
- 1999
- Buy on Amazon
- Author's Website

WHAT IS A SECRET CODE OR CIPHER?

It all starts with a message, called *plaintext* which you want to send secretly.

Then there is a method, called an *algorithm*, to *encrypt* the message, turning it into what's referred to as the *ciphertext*. The ciphertext is meant to be unreadable to anyone intercepting it.

Lastly, the the receiver uses another algorithm to *decrypt* the message, recovering the plaintext.

A simple example would be swapping A with Z, B with Y, C with X, etc. This gives:

Plaintext: HELLO Ciphertext: SVOOL

This cipher is often referred to as the Atbash Cipher, Mirror Cipher, or the Backwards Alphabet.

REVIEW

The Code Book by Simon Singh tells the history of secret codes, ciphers, and encryption throughout history. On the surface, the book is a historical description of different ways to communicate secretly. Make no mistake, the book is a fun read for this alone, but those who wish to dive deeper will also learn some of the mathematics and engineering behind the methods of sending encrypted messages. For me, the mixing of the history, math, and engineering is what makes the book such a great read.

The book opens with a description of basic substitution ciphers, where each letter is swapped to another in an encrypted message. The simplest and most famous, the Caesar Cipher, shifts the letters up or down in the alphabet. Singh describes how Julius Caesar would shift each letter in a message down three places. For example, 'CODE' becomes 'FRGH'. Of course this message would be easy to decrypt, especially with a long message. Singh goes on to describe how any basic substitution cipher is insecure due to statistics and how often different letters appear in the alphabet.

One of my favorite chapters, "Cracking the Enigma", provides a great example of how Singh weaves history, mathematics, and engineering to tell a compelling story. The Enigma machine was used by Nazi Germany in World War II for secret communication. The Polish, French, and English were all instrumental in cracking the code. Many will recognize the name Alan Turing as one of the codebreakers working for the English at Bletchley Park. There is, however, much more to the story. Singh describes the back and forth: progress is made on breaking the Enigma code, but then improvements to the Enigma code are made, more progress breaking is made, etc. For example, one improvement was adding additional 'scramblers' to the machine, and Singh masterfully explains how this added mechanical depth makes the codes more mathematically complicated (more permutations to consider) and thus harder to break. And if this sounds too dense, remember the historical backdrop and real world consequences. Even after the code was cracked, the English did not want to make the Germans suspicious, so they would sometimes ignore intelligence and let certain submarines escape, deciding a minor loss might be more beneficial in the long run. The fact that even after the mathematical and engineering problems were solved there were real-world complications to consider has stuck with me ever since I first read the book in high school.

In the second half of the book, Singh goes on to describe how the introduction of computers and later the internet lead (and continues to lead) to new developments in codes and encryption. Here, the mechanical machines like Enigma are replaced by computer programs, and the math gets more complicated. However, Singh still strikes a balance of giving readers the idea and flavor of the algorithms used without getting too technical. Interested readers can then delve more into the mathematics if they want while others can move on and continue to enjoy the history and explanations of real world consequences.

Overall, I highly recommend *The Code Book* to aspiring STEM high school students and their families. Whether you just want to focus on the history or delve deeper into the math, Singh provides an enjoyable reading experience for all.