THE LAWYER'S BOOKSHELF

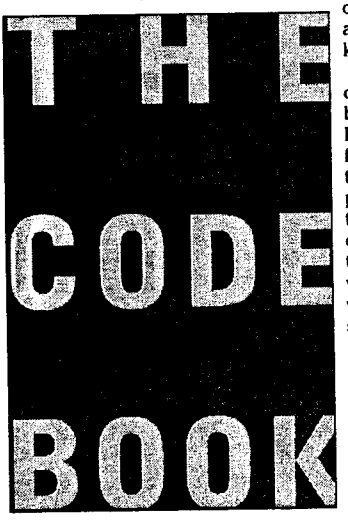
REVIEWED BY PAUL M. SCHWARTZ

The Code Book: The Evolution of Secrecy From Mary, Queen of Scots to Quantum Cryptography

By Simon Singh. Doubleday, New York, N.Y. $24.95

In the Information Age, encryption is of the highest social importance. Because information is now the most valuable commodity, encryption, which provides today's digital locks and keys, has become a critical area. Simon Singh's fascinating *The Code Book* traces the history of the science of secrecy. The book is an illuminating and entertaining account of a subject of relevance for all attorneys who practice information law.

From the first page, Singh shows his knack both for explaining complex areas of science and telling rip-roaring stories. Chapter 1 begins with the trial of Mary Queen of Scots in 1586 before an English court in Fotheringhay Castle. The challenge for Queen Elizabeth's Principal Secretary, Sir Francis Walsingham, was to convince the English Queen that her cousin Mary had authorized a deadly plot against her. Mary had made sure, however, that her correspondence with the conspirators was written in cipher. Although Walsingham had intercepted her letters, he still needed to break their code.



At this dramatic point, Singh pauses to explain the history of secret writing up to 1586. This tale includes Julius Caesar; cryptanalysis among Arab scholars in the 10th century; and the monk Roger Bacon's work in 13th-century England. Singh then returns to Mary Queen of Scots to continue her tragic tale. He explains the desperate straits that led her to join the conspirators in 1586 and the process of smuggling messages to her by hiding them inside a hollow bung used to seal barrels of beer.

As Singh points out, the code used by Mary and the conspirators was a cipher alphabet mixed with code words. This kind of encoding is easily broken through frequency analysis, a technique that entails comparison of the frequency of characters in a scrambled message with their occurrence in the language likely used in the plaintext. Mary's code was broken by Elizabeth's experts, the Scottish Queen was found guilty, and her execution followed on Feb. 9, 1587.

The first chapter could not more clearly establish the importance of its subject: encryption is sometimes a matter of life and death. In the following chapters, the author finds no shortage of science to explain and great stories to tell. Among the individuals and topics discussed en route to contemporary cryptography are: the Man in the Iron Mask; Charles Babbage; the start of World War I and the Zimmermann Telegram; English codebreakers, including Alan Turning, at Bletchley Park during World War II; and the Navajo speakers, called "code talkers," employed by the U.S. Navy in the Pacific during World War II.

Singh reaches the Information Age in his last three chapters. With the exchange of digital data now an integral part of our society, "[e]ncryption can be seen as providing the locks and keys of the Information Age." Cryptography is now more vital than ever — not just for political leaders, like Mary Queen of Scots, but for anyone who purchases products on the Internet or uses digital signatures to prove his identity.

The Code Book offers crystal clear explanations of the two essential breakthroughs of cryptography in our time, which are asymmetric ciphers and public key cryptography. Asymmetric ciphers are codes that do not encode and decode in the same fashion, as a result of which encryption and decryption keys are no longer identical. This approach permits the use of public keys. Anyone who wants to receive a secret message can publish a public key, available to the world, and still be the only person to open the padlock around the data by using the private key.

Asymmetric ciphers and public key cryptography provide the science behind Phil Zimmerman's free software PGP, or Pretty Good Privacy. PGP is the freeware that brought strong encryption to the Internet masses and the product that the U.S. government long tried to stop as a munition. Singh explains how the U.S. government has tried to include encryption software within its definition of munitions, along with missiles and mortars, and make it subject to licensing restrictions. He carries out an evenly balanced portrayal of these developments and other government attempts to restrict encryption, such as its proposals for the clipper chip and key escrow.

In Singh's summation, "The success of the Information Age depends on the ability to protect information as it flows around the world, and this relies on the power of cryptography." As ordinary people begin to depend on cryptography in order to protect their privacy, government has tried to limit strong cryptography.

But one twist on this story took place too recently to be included in *The Code Book*. This fall, a panel of the Ninth Circuit extended First Amendment protection to publication of encryption expressed in source code, which is the high-level programming language that machines translate into the object code that the computer actually executes. This decision, *Bernstein v. U.S.*, is now awaiting a rehearing by the entire Ninth Circuit and may be headed for the Supreme Court. If encryption receives strong constitutional protection under the First Amendment, the government's ability to restrict it will be seriously curtailed. In the Information Age, code books may also be free speech.

Paul M. Schwartz *is a professor of law at Brooklyn Law School and co-author of* Data Privacy Law *(1996).*