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

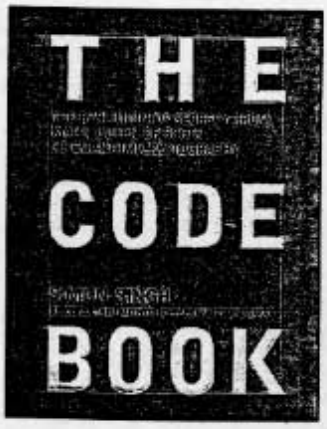
Reviewed by Jim Reeds

The Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography
Simon Singh
Doubleday Books, 1999
ISBN 0-385-49531-5
402 pages, $24.95

It is hard to write a good book about the history of cryptography. The subject is technical enough to be a turnoff for many readers. The evidence a historian of cryptography works from is often suspect. Because much of the practice and research in the field was carried out in secret, any particular document or interview must be viewed with suspicion: did the author or interviewee know the full truth? Healthy suspicion about the competency of sources is of course appropriate in all branches of historical research, but in the history of cryptography the proportion of misinformed or deceptive sources is probably greater than generally found in the history of science or of technology. The historian's standard technique of precise and thorough citation of documentary evidence is therefore especially important in the history of cryptography. Unfortunately, for popular works this technique can mean death to readability.

In cryptography technical developments often came in reaction to events and activities which were at the time secret or, conversely, had ceased to be secret. If we do not understand the "who knew what when" details correctly, our reconstructed timetables for technical progress seem to show puzzling fits and starts, apparently unconnected with contemporary

Jim Reeds is at AT&T Labs, Florham Park, NJ. His e-mail address is reeds@research.att.com.



events. This makes coherent exposition difficult. Almost every war, however, has notable instances where some cipher message solution foils a plot or wins a battle. Here it is easy to connect the cryptographic or cryptanalytic technicalities with particular historical events, but a book that relies too much on such instances becomes in effect no more than an adventure story anthology.

So it is no surprise that there are few general surveys of the history of cryptography and fewer good ones. The rule of thumb seems to be one new book every thirty years.

In 1902 and 1906 Alois Meister published his immensely scholarly *Die Anfänge der Modernen Diplomatischen Geheimschrift* and *Die Geheimschrift im Dienste der Päpstlichen Kurie*, reproducing and summarizing texts relevant to cryptography in the late medieval and early modern periods. The readership cannot have been large.

At the opposite extreme of readability was the 1939 *Secret and Urgent: The Story of Codes and Ciphers* by the journalist and naval affairs commentator Fletcher Pratt. The book presented a breezy series of thrilling anecdotal historical episodes involving ciphers and code-breaking exploits. Each episode came complete with Sunday supplement-style character sketches and just the

right amount of technical information about the cipher or cryptanalysis in question. The technical discussions were not always tightly bound to the factual historical setting: although they were always illustrative of the type of ciphers involved in this or that historical episode, they were not necessarily verbatim transcripts of documents in archives. Pratt thus managed to make the technicalities—always clearly explained—seem important and managed to teach a bit of history in the nonrigorous way a historical movie or novel might teach a bit of history. Like many others, I was inspired by this book when I read it in my early teens. It was only much later that I came to realize that its lack of bibliography and detailed footnotes made it useless as a serious history of cryptography.

In 1967, about thirty years after Pratt's book, a much more serious book appeared, *The Codebreakers*, by David Kahn, also a journalist, but one with a far sterner approach to standards of documentation. Where Pratt had two pages of notes and no literature references, Kahn gave 163 pages. Kahn's method (which he pursued over many years with great energy) seems to have been simply this: to read everything about cryptography in all the world's libraries and archives, to interview all cryptographers, and to write it all down as sensibly, as accurately, and with as much detail as possible; his book has 1,180 pages. This is the book I read when I was in college. By then I had grown up enough to appreciate Kahn's comment in his preface that although his love for cryptography had also been sparked by Pratt's book, he was disappointed in the book. Kahn bemoaned Pratt's "errors and omissions, his false generalizations based on no evidence, and his unfortunate predilection for inventing facts."

Unfortunately, Kahn's book was published a short time before the facts about the Polish and British success in breaking the German Enigma cipher of World War II became publicly known and also a short while before the amazing invention of the new number-theoretical "public key cryptography" techniques now pervasive in computers and the Internet. As a result, these interesting and important topics received no treatment.

Now, thirty years after Kahn's book, a new history of cryptography has appeared, again by a journalist: Simon Singh's *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography*, a bestseller in England in its first months of publication. Singh states in his preface that "In writing *The Code Book*, I have had two main objectives. The first is to chart the evolution of codes...the book's second objective is to demonstrate how the subject is more relevant today than ever before."

Singh's first five chapters cover the history of cryptography up through the end of the Second World War, summarizing material found in earlier books and journal articles, presented by the episodic snapshot method. His remaining three chapters are based mostly on personal interviews with leading participants. Chapter 6 describes the invention and early development of public key cryptography by W. Diffie, M. Hellman, R. Merkle, R. Rivest, A. Shamir, and L. Adleman in the U.S., and independently, but in secret, by J. Ellis, C. Cocks, and M. Williamson in the U.K. Chapter 7 describes the current controversy about the proper role of cryptography in a free society: personal freedom versus the interests of the state, privacy versus wiretapping, key escrow, export of strong cryptography, and so on. The final chapter describes quantum cryptography, the new system of communications made untappable by exploiting the fact that the polarization of a photon is altered when it is measured.

The good news is that Singh's book has all the good qualities of Pratt's. Unfortunately, Kahn's criticism of Pratt's book also applies to Singh's book. Almost every page has small errors of fact. In many places it is clear that Singh does not really understand the material he copies from his sources. Many of these errors are of little consequence when taken individually, but their cumulative effect is to destroy a knowledgeable reader's confidence in the author's standards of accuracy.

Here are just a few examples:

- On page 128 Singh describes the wired code wheels of the Enigma cipher machine (the "rotors", which he oddly calls "scramblers"): "The scrambler, a thick rubber disc riddled with wires..." But the Enigma's rotors were *not* made of rubber but of aluminum, brass, and Bakelite. Singh may have misunderstood a sentence on page 411 of Kahn's book: "The body of a rotor consists of a thick disk of insulating material, such as Bakelite or hard rubber...", accurately describing the rotors, not of an Enigma machine, but of a different cipher machine.
- On page 168 Singh states that A. M. Turing (in his 1937 paper "On computable numbers, with an application to the Entscheidungsproblem") called "this hypothetical device a *universal Turing machine* [Singh's italics]." But of course the terms "Turing machine" and "universal Turing machine" were *not* used by Turing himself; a glance at his paper shows he used "computing machines" and "universal machines".
- On pages 187–8, Singh states that the British WWII code-breaking organization, the "Government Code and Cypher School", was disbanded after the war and then replaced by another, the "Government Communications Headquarters", or GCHQ. In fact, the change occurred in 1942 and was one in name only.
- On page 191 Singh claims the American breaking of the Japanese "Purple" cipher enabled the naval victory at Midway and the assassination

of Admiral Yamamoto. In fact, these were due to the breaking of the "JN-25" code. "Purple" was a machine cipher, roughly equivalent to the German Enigma, whereas "JN-25" was a hand system relying on code books and random number tables.

Singh's unfamiliarity with the technical vocabulary used by his sources seems to have led him into a more serious mistake in the first two chapters. To explain this, I must first summarize material in Kahn's chapters 3 to 6.

From before 1400 until about 1750 only one kind of encryption method was widely used (although others were discussed in books). This method used what were called at the time "ciphers" or "keys". A cipher was a collection of arbitrary symbols or numbers that substituted for letters, syllables (or other letter sequences), names, and common words and phrases found in plain text. By 1700 ciphers with as many as 1,000 or 2,000 substitutions were common, and even larger ones with as many as 10,000 or 50,000 substitutions were in use later on. Although the general trend was towards greater size and complexity, throughout this period ciphers of widely varying size and complexity were used. Modern scholars have used a variety of terms—more or less interchangeably—for this cryptographic genre, including "homophonic cipher", "nomenclator", "code", "code chart", and so on, as the original terms "cipher" and "key" are no longer precise enough to distinguish these methods from more modern ones.

At the same time a theory for another kind of cryptography was being developed, discussed, and elaborated in successive printed cryptography books all through the 1500s and into the 1600s. The set-piece example of this new kind of cryptography, the "Vigenère" cipher, also known as *chiffre indéchiffrable*, was more algebraic in nature, based on Latin squares and what we now know as modular arithmetic. This kind of cryptography was slow to gain acceptance: although available for use in 1575, it was not actually used until the mid-1600s, and then only sparingly. Even at the end of the 1700s Thomas Jefferson's adoption of the Vigenère cipher by the U.S. State Department was an innovation, and when he left office, the department reverted to the older nomenclator technology. Only in the nineteenth century did the Vigenère cipher come into common use and serve as a basis for further technical developments.

Singh, however, seeing one author use the term "nomenclator" to describe a cipher in use in 1586 and another author using the term "homophonic cipher" to describe one in use in 1700, supposes the two ciphers to be different kinds of things. And he invents a theory explaining why the latter kind was devised: he says on page 52 that the "homophonic cipher" was invented in Louis XIV's reign to serve as a more practical alternative to the *chiffre indéchiffrable*. But Kahn (whose book appears in Singh's list of references), on page 107, shows an example of a homophonic cipher, labelled as such, from 1401, about three centuries before Singh's invented invention.

A different kind of misunderstanding occurs in the discussion of the attack on the German Enigma machine in the early 1930s. The mathematical basis for the initial Polish success was the well-known fact that the cycle type of a permutation is invariant under conjugation: when one writes the permutations τ and $\sigma\tau\sigma^{-1}$ as the products of disjoint cycles, the same lengths appear with the same multiplicities. On pages 148–54 Singh explains very clearly how Marian Rejewski applied this fact to the problem of recovering German Enigma keys. If ever there was a real-world story problem handed to mathematics teachers on a silver platter, this would be it.

The sample permutation Singh uses to illustrate the Enigma application decomposes into cycles of length 3, 9, 7, and 7. (Here, of course, the permutation is a permutation of the 26-letter alphabet: $3 + 9 + 7 + 7 = 26$.) But here is the kicker. The permutations τ which actually occur in the Enigma application are of the form $\tau = \alpha\beta$, where α and β are each the products of 13 disjoint 2-cycles. This forces τ to have even cycle length multiplicities, which Singh's example does not have. That is, Singh presents an imitation example, not an example of an actual Enigma τ permutation he has worked out. This is perfectly adequate for illustrating the mathematical fact of the invariance of cycle type under conjugation, but will not do for illustrating the historical facts of Rejewski's solution of the Enigma cipher.

This is as if a historian of trigonometry, describing some early work, wrote: "In a right triangle with sides of lengths 2, 3, and 4, the angle opposite the side of length 2 was found by taking the inverse sine of the ratio of the opposite side to the hypotenuse, in this case $\arcsin(2/4) = 30°$." The formula is correctly stated and worked out, but applied in an impossible context. Which is the worse fault: Singh not bothering to use an actual historical—or even realistic—example, or not knowing that his example is unrealistic?

Singh does better in the remaining chapters, where the story line and technical explanations derive from interviews. His interviewees' personalities are clearly visible, and the technical explanations are usually comprehensible.[1]

Chapter 6, about the invention of public key cryptography, repeats the stories which have been told in public lectures by Diffie, Hellman, and Shamir about their discovery of the basic ideas of

[1] *Whitfield Diffie, however, has complained in a book review (*Times Higher Education Supplement, *10 September 1999) that not everything he told Singh was accurately reported.*

one-way functions and public key cryptography, as well as their discovery of the number-theoretic examples based on modular exponentiation and the difficulty of factoring. More interesting is Singh's description of the secret and somewhat earlier independent discovery of these ideas by Ellis, Cocks, and Williamson at the GCHQ, the secret British government cryptography organization. GCHQ has recently "gone public" in this matter, making Cocks a media celebrity by GCHQ standards. (The chronology of this matter is somewhat hard to assess because not all the relevant GCHQ files have been made available. One result, the Diffie–Hellman exponential key exchange, seems *not* to have been first discovered by GCHQ.)

In this chapter Singh spends many pages discussing the matter of priority of scientific discovery, exulting in the recent declassification of the earlier GCHQ work as if an injustice had been righted. This vision of the abstract reward of "credit", based on strict chronological priority, distracts Singh from looking at the historically more interesting questions of influence of ideas. These include: how were the initial GCHQ discoveries understood by the discoverers' colleagues at the time, how were these ideas developed, and how were they used? The available evidence is scanty, but it seems likely that they were regarded within GCHQ as impractical curiosities and ignored until the rediscoveries on the outside alerted GCHQ to their importance.

The historiographic issue is neatly illustrated in an example at the end of the chapter, referring back to an episode in Chapter 2, which Singh takes as a parallel foreshadowing. One of the techniques for breaking the Vigenère *chiffre indéchiffrable* was first published in 1863 by F. Kasiski, but apparently sometime in the 1850s Charles Babbage had worked out the same method in private. Singh claims (on no evidence whatsoever) that Babbage did not publish his results because of the interests of military secrecy during the Crimean War of 1854. But now Babbage's injustice is also righted: he gets the credit in the end. Regardless of the reasons for Babbage's failure to publish, the following seems clear: Babbage's discovery, since it was unpublished, had no influence on the further development of cryptography. That he made this discovery tells us something about Babbage's mental capabilities; that it was independently rediscovered tells us something (but not much) about its intrinsic level of difficulty. Babbage might have been first, but (in this matter) he was historically unimportant. Society uses credit and priority as a reward to encourage the dissemination of new ideas, and it is not at all clear that a researcher who fails to publish a new idea—whether out of diffidence, patriotism, or employment at a secret research laboratory—is done an injustice when not awarded credit. Righting such imagined wrongs is not what history is about.

Chapter 7, based on interviews with the PGP (Pretty Good Privacy) programmer Philip R. Zimmermann, concentrates on the currently unsettled matter of the proper role of cryptography in a free society. Zimmermann represents the libertarian side: the people should use—must use, if they do not trust their government—the strongest kind of cryptography they can. Governments, however, remembering the invaluable results of cryptanalysis during the Second World War (and presumably since then) would wish to somehow keep the strongest forms of cryptography out of the hands of potential enemies. As the target of a grand jury investigation, Zimmermann suffered from the American government's embarrassingly inept way of trying to make up its mind on this public policy issue.

The final chapter returns to the purely technological, with a discussion of quantum cryptography. Here again, interviewees (D. Deutsch and C. Bennett) carry the story along. The description of the basics of quantum mechanics is painfully incoherent, that of quantum computing is superficial and vague, but the explanation of how polarized photons can carry untappable information is fairly clear.

In the preface—justifying his rejection of a pedantically more accurate title for his book—Singh states "I have, however, forsaken accuracy for snappiness." With hindsight this is ominous. His carelessness with facts will not harm those readers who pick up the book, skim it, and find the subject not to their taste. Nor will it harm the enthusiasts (like myself), who will seek out other, more reliable books.[2] But most, I suspect, will fall in the middle ground: interested readers who will rely on this book alone for their information about cryptography. This group, which will mine Singh's book for years, if not decades, for term-paper and lecture material, and possibly material for other books, will be disserved by the author's lax standards of accuracy.

[2] *My favorites: Instead of Singh's Chapters 1–3, people should read D. Kahn,* The Codebreakers: The Story of Secret Writing *(Macmillan, 1967) and F. Bauer,* Decrypted Secrets : Methods and Maxims of Cryptology *(Springer, 1997). Instead of Singh's Chapter 4, read F. H. Hinsley and A. Stripp,* Codebreakers: The Inside Story of Bletchley Park *(Oxford, 1993) and G. Welchman,* The Hut Six Story *(McGraw-Hill, 1982). Instead of Chapter 7, read W. Diffie and S. Landau,* Privacy on the Line: The Politics of Wiretapping and Encryption *(MIT, 1998). All but one of these books are in Singh's "Further Reading" list, pages 388–393.*