Foreword

In the beginning, the only useful works about cryptography were written by David Kahn.

That is not entirely true. There are many historical cryptography texts, and in the early twentieth century there were some books about pencil-and-paper ciphers. Certainly, the NSA and similar agencies had all sorts of information buried in their classified libraries, but when *The Codebreakers* was published in 1967, there was nothing else like it anywhere.

It was a history of cryptography from the beginning of time until the 1960s. I devoured it.

Things started to change in the early 1980s. An academic research community sprang up, and Springer-Verlag started publishing proceedings from the Crypto and Eurocrypt academic conferences. A few books that examined computer cryptography were published: Denning, Konheim, and Meyer and Matyas. The journal *Cryptologia* appeared in 1988—with Kahn as one of the founding editors—publishing both academic and historical papers. More mathematicians wrote books, and cryptography papers began to be regularly presented at both mathematics and engineering conferences.

Still, as a student of cryptography, I found myself returning to Kahn again and again. Cryptographer Whitfield Diffie once compared *The Codebreakers* to the Veda. "In India, if a man loses his cow, he looks

for it in the Veda." Because, of course, everything is in the Veda. For people like Whit and me, *The Codebreakers* was like that.

David Kahn's second book was *Kahn on Codes*. Published in 1983, it is a collection of essays on cryptography from a variety of publications. It, too, was a cornucopia of ideas and stories. Kahn's historical understanding of the role of cryptography is unmatched, and his ability to tell a good historical story is remarkable. *Kahn on Codes* was an invaluable tool as I began to understand cryptography and its role in society.

Now, 30 years later, cryptography research has blossomed, and the use of cryptography on the Internet has exploded. I have nine shelves of books, journals, conference proceedings, and papers on cryptography. But Kahn's writings are no less important today. What you have in your hand is another collection of essays, all previously published but never before collected in a single volume. They appeared in such journals as *Military History Quarterly*, *Cryptologia*, *Foreign Affairs*, and *Intelligence and National Security* over the past two decades. And while it sometimes seems that stories of World War II spying and military codebreaking are worlds apart from the problems of Facebook security, computer viruses, and Internet surveillance, history still has lessons for us today. These essays are timeless. They are worth reading, and they are worth rereading. No matter what cow we have lost or where we have lost it, Kahn's writings contain clues to where it might be found.

Bruce Schneier