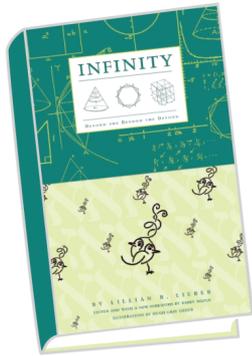




BOOKSHELF

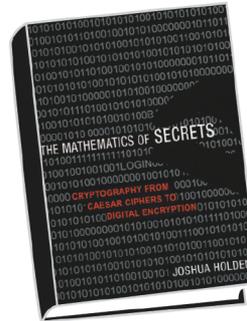
New and Noteworthy Titles on Our Bookshelf August 2017



Infinity: Beyond the Beyond the Beyond, by Lillian R. Lieber, with illustrations by Hugh Gray Lieber (Paul Dry Books, November 2007).

In the May 2017 installment of the BookShelf, we noted the paucity of women authors of popular math books in the twentieth century—as compared to the fairly large number today—and asked readers to let us know of any popular math books by women published before around 1990. One

reader kindly wrote in to let us know about Lillian Lieber (1886–1986), who wrote several outstanding books that attempt to explain modern mathematics to the general public. The books are deftly illustrated with whimsical drawings by her husband, Hugh Gray Lieber (1896–1961). Both Liebers were mathematicians—Lillian received a PhD and Hugh a master's degree in the subject—and both taught math at Long Island University. The book highlighted here was originally published in 1953 and reissued in abridged form in 2007. The abridgements were made by Barry Mazur of Harvard University, who in the book's foreword writes, “the *joy of thinking* the Liebers radiate is timeless.” He goes on to say, “The Liebers sometimes appear to me to be discerning shoppers in the platonic fruit-stall of mathematics. Never content to just think a concept, they also have to test it, squeeze it, pinch it, sniff it, take a few bites, and muse about their own reactions to it before buying it. And then to thoroughly enjoy it.” Paul Dry Books has also reissued two other Lieber classics, *The Education of T. C. Mits: What Modern Mathematics Means to You* (also with a foreword by Mazur) and *The Einstein Theory of Relativity: A Trip to the Fourth Dimension* (edited by David Derbes and Robert Jantzen, who also wrote the foreword). This latter book was praised by Einstein himself and later by his biographer Walter Isaacson, who called it “the clearest explanation of relativity available—and the most fun.”



The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption, by Joshua Holden (Princeton University Press, February 2017).

Related to this month's Opinion column by Jintai Ding and Daniel Smith-Tone, who address the topic of post-quantum cryptography, is this new book by Joshua Holden, a mathematician at Rose-Hulman Institute of Technology. In the book's preface, Holden quotes

Cambridge mathematician Ian Cassels, who was a cryptanalyst during World War II: “cryptography is a mixture of mathematics and muddle, and without the muddle the mathematics can be used against you.” Holden decided that in his book he would set aside the muddle and concentrate on the mathematics. He also takes great care to keep the mathematics very simple—readers need background only up to the level of high school algebra to understand the exposition. The book is organized according to the historical development of cryptography, starting with Julius Caesar's use of ciphers, and throughout the book the historical background provides context and color to the story. But the emphasis is on the development of the underlying mathematical ideas. The book covers polyalphabetic substitution ciphers, connections between ciphers and computer encryption, ciphers involving exponentiation, and public-key ciphers. The book ends with a look to the future, including the effects quantum computers could have on cryptography. One section deals with post-quantum cryptography, including lattice-based cryptographic systems.

The BookShelf is prepared monthly by Allyn Jackson. Suggestions for the BookShelf can be sent to notices-booklist@ams.org.

We try to feature items of broad interest. Appearance of a book in the *Notices* BookShelf does not represent an endorsement by the *Notices* or by the AMS. For more, visit the AMS Reviews webpage www.ams.org/news/math-in-the-media/reviews.