Cracking Codes Through the Centuries

By William Grimes
Feb. 3, 2015

WASHINGTON — The Sigaba encryption machine squats in the Folger Shakespeare Library here like a thuggish interloper. Used by the American military in the 1940s and 1950s to send coded messages, it looks like an oversize, boxy typewriter with rotors rising above the lid like a mechanical brain. No object could seem less Elizabethan, yet appearances deceive.

"Decoding the Renaissance: 500 Years of Codes and Ciphers," an exhibition that runs through Feb. 26, draws a straight line from the cipher discs devised by the humanist polymath Leon Battista Alberti in the 1460s and Francis Bacon's discovery of bilateral ciphers — a way of writing coded messages with just two letters — to Sigaba, the American answer to the German Enigma machine.

It's a rather fashionable subject at the moment. "The Imitation Game," and Benedict Cumberbatch's performance as Alan Turing, the British mathematician who broke the Enigma code, has transmitted the allure of cryptography to millions of moviegoers. The subject's mystique has drawn unusual visitors to "Decoding the Renaissance," like the F.B.I.'s cryptanalysts, not the typical audience for a library devoted to Shakespeare and his contemporaries.

Together, the Folger Library and the Library of Congress, a major lender to the exhibition, hold one of the world's deepest collections of works on cryptography. This material constitutes the spine of the show, which sets forth the basic principles of code-making, a topic of fevered study during the Renaissance.

"It was a period of cold war, in effect," said Bill Sherman, the head of research at the Victoria & Albert Museum in London and a professor of Renaissance studies at the University of York, who organized the exhibition. The Pan-European tensions between Protestant and Roman Catholic states, the rise of international trading systems and the newfound importance of diplomatic missions demanded spy networks, secrecy and subterfuge — "all the things you get in a John le Carré novel," Mr. Sherman said.

The exhibition includes the earliest printed book on cryptography, "Polygraphiae Libri Sex," written by the Benedictine abbot Johannes Trithemius and published in 1518, as well as a coded letter from Francis Walsingham, Elizabeth I's spymaster. A letter from George Digby, the Second Earl of Bristol, on behalf of Charles I, reports on the progress of rebel forces under Oliver Cromwell using a set of substitutions known as a nomenclator. The number 154, for example, means "danger," and p5 means "with."

One of the rarest books in the exhibition is "A New Method of Cryptography" (1666), written during the English Civil War by Samuel Morland. His proposal for a cyclologic cryptographic machine, illustrated on the book's last page, relies on a series of cipher wheels that make it a close cousin to Sigaba and Enigma.

Not all codes depended on letters and numbers. Steganography — literally "hidden writing" — provided an alternate set of tools for practitioners of the espionage trade. John Wilkins's "Mercury, or the Secret and Swift Messenger," published in 1641, suggests writing with the "juice of glow-worms" to create messages that can be read only in the dark, or "glutinous moisture" — milk or fat — that the recipient can read by scattering dust on the letters. Alphabets could be translated into musical notes or flowers.

A Sigaba encryption machine used by the American military during World War II is also part of the Folger exhibition.
Matt Roth for The New York Times

The road to modern cryptography leads through the stupendous brain of William F. Friedman, chief cryptologist for the American military in both world wars and a primary focus of the exhibition.

Mr. Friedman, whose family emigrated from Kishinev, Russia, as the threat of pogroms mounted, started out as a plant geneticist. That career path was derailed when, in 1915, he joined Riverbank Laboratories, a research institute founded by the eccentric textile magnate George Fabyan.

Mr. Fabyan subscribed to the popular theory that Francis Bacon had written the works attributed to Shakespeare and had embedded coded clues to that effect in the First Folio and other texts. Mr. Fabyan assigned a team to work on the project. Mr. Friedman met and married one of the Bacon researchers, Elizebeth Smith, and quickly became drawn into the world of cryptography, for which he displayed an almost supernatural talent.

The Friedmans gave up on the Bacon theory, which they debunked in 1957 in the book "The Shakespearean Ciphers Examined," but Riverbank's Bacon research made it an ideal cryptographic training center for military personnel during the First World War. The exhibition includes a panoramic photograph of the school's Class of 1918, whose members line up to spell out Bacon's maxim "Knowledge is power" in a code expressed by the way their heads are turned. There were only enough students, however, to spell "Knowledge is pow."

After serving in France as the cryptographer for Gen. John J. Pershing, Mr. Friedman became the chief cryptanalyst for the Army. As the leader of the Signals Intelligence Service, in the 1930s and 1940s, he helped decipher the Japanese cipher machine Purple — he built a replica by analyzing its encrypted messages — and, with his associate Frank Rowlett, developed Sigaba. The machine, which contained 15 encrypting rotors to Enigma's five, was undecodable and remained classified until 2000.

Mr. Friedman took a playful approach to cryptography. The exhibition includes one of his annual encrypted Christmas cards; a coded menu from the "Café Cryptanalytique," presented to dinner guests at his home; and a secret message hidden in sheet music for "My Old Kentucky Home."

He kept one foot in the Renaissance until the end of his life, a connection that explains the centerpiece of the exhibition, the mysterious Voynich manuscript. The document, an illustrated codex written in an unknown language and script in northern Italy in the early 15th century, is named after Wilfrid Voynich, the Polish antiquarian bookseller who acquired it in 1912.

It has never been decoded, though Mr. Friedman spent four decades trying. The illustrations suggest that it might be a scientific treatise, with sections on medicinal herbs, astronomy and other subjects, but no one can be sure. "You could think of it as the ultimate work of outsider art," said Michael Witmore, the Folger's director.

The manuscript was donated to the Beinecke Rare Book & Manuscript Library at Yale in the 1960s. Mr. Friedman did not find the key to the Voynich code but he did have a theory. It was, he thought, an early effort to create an artificial language. He communicated this idea in a Friedman-esque way, concealing it in a 1959 article on Chaucer's anagrams, then putting the solution in an envelope to be opened after his death.

"Decoding the Renaissance: 500 Years of Codes and Ciphers" continues through Feb. 26 at the Folger Shakespeare Library, 201 East Capitol Street SE, Washington; 202-544-4600, folger.edu.

A version of this article appears in print on , Section C, Page 3 of the New York edition with the headline: Cracking Codes Through the Centuries