

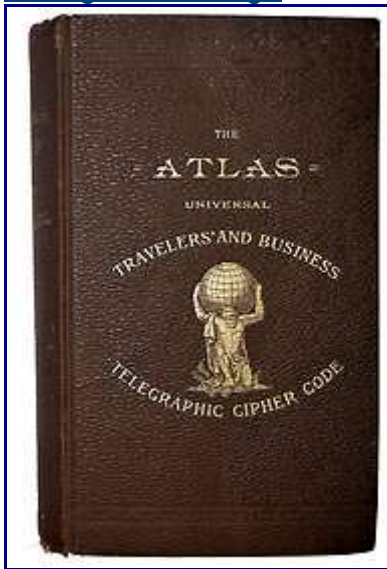
Codebook Shows an Encryption Form Dates Back to Telegraphs

By [JOHN MARKOFF](#)

Published: July 25, 2011

If not for a computer scientist's hobby of collecting old telegraph codebooks, a crucial chapter in modern cryptography might have been lost to history.

[Enlarge This Image](#)



Steven Bellovin

KEY Codebooks like this one from 1896 cut the cost of telegrams, which were charged by the word.

The collector is Steven M. Bellovin, a professor of computer science at the Columbia University School of Engineering and a former computer security researcher at AT&T Bell Laboratories. On a recent trip to Washington he found himself with a free afternoon and decided to spend it at the Library of Congress, looking for codebooks that weren't in his collection.

In the 19th century codebooks were used not so much for secrecy as for compression, to bring down the prohibitive cost of telegraph communication. (The first trans-Atlantic cables cost \$5 a word.) Designers devised lists of words to replace phrases and even sentences.

But when Dr. Bellovin hunted through the card catalog, his interest was piqued by an 1882 codebook whose title included the word "secrecy."

"I thought, 'O.K., let me go see how they did it,'" he recalled. "When I read the two-page preface, my jaw dropped."

He could plainly see that the document described a technique called the one-time pad fully 35

years before its supposed invention during World War I by Gilbert Vernam, an AT&T engineer, and Joseph Mauborgne, later chief of the Army Signal Corps.

Although not widely used today because it is relatively difficult to work with, the one-time pad is still viewed as one of the strongest ways to encrypt a communication. The technique is distinguished by the use of a random key, shared by both parties, to encode the message and decode it; the key must be used only once and then securely disposed of.

It was the Soviet Union's misuse of the technique — code clerks were occasionally reusing the one-time pads instead of discarding them — that led to the Venona project, the collaboration between the United States and British intelligence services that yielded code-cracking coups during World War II and the cold war.

The 1882 monograph that Dr. Bellovin stumbled across in the Library of Congress was “Telegraphic Code to Insure Privacy and Secrecy in the Transmission of Telegrams,” by Frank Miller, a successful banker in Sacramento who later became a trustee of Stanford University. In Miller's preface, the key points jumped off the page:

“A banker in the West should prepare a list of irregular numbers to be called ‘shift numbers,’ ” he wrote. “The difference between such numbers must not be regular. When a shift-number has been applied, or used, it must be erased from the list and not be used again.”

That sent the astonished Dr. Bellovin to the Internet to try to find out whether Mr. Miller's innovation was known to the later inventors.

The [results of his largely online detective work](#) can be found in the July issue of the journal *Cryptologia*. Born in Milwaukee in 1842, Mr. Miller attended Yale and then joined the Union Army, where he fought at Antietam and was wounded at the Second Battle of Bull Run.

He was transferred to the Army inspector general's office, where he became a member of a squad of detectives investigating Lincoln's assassination — perhaps his first contact with cryptanalysis, Dr. Bellovin speculates. He seems to have kept a diary that still belongs to his descendants, but Dr. Bellovin was unable to obtain it.

According to several independent specialists in cryptography, Mr. Miller was undoubtedly the first to propose the concept of the one-time pad.

“Miller probably invented the one-time pad, but without knowing why it was perfectly secure or even that it was,” said David Kahn, the author of the definitive 1967 book “The Codebreakers.” “Moreover, unlike Mauborgne's conscious invention, or the Germans' conscious adoption of the one-time pad to superencipher their Foreign Office codes, it had no echo, no use in cryptology. It sank without a trace — until Steve found it by accident.”

Dr. Bellovin found no evidence that either Mr. Vernam or Mr. Mauborgne ever met Mr. Miller, but he did uncover one more tantalizing clue — in the society pages of *The San Francisco Chronicle*, of all places. At a military ball at the Presidio in 1907, Mr. Miller met Parker Hitt, a cryptographer who was a student and colleague of Mr. Mauborgne's.

“It is quite certain that if Hitt knew of Miller's system,” Dr. Bellovin writes, “he would have shared that knowledge with Mauborgne when they were together at the Army Signal School in Fort Leavenworth.” But as he acknowledges, that is still a big “if.”