Frank Miller: Inventor of the One-Time Pad

Steven M. Bellovin
http://www.cs.columbia.edu/~smb

Indulging My Hobby…

- I'm interested in old telegraph codebooks
- In January, I had a free day in Washington, so I went to the Library of Congress to look at some – they have many hundreds of them
- Being a security guy, I decided to look at a few that had the word "Secrecy" or some such in the title

TELEGRAPHIC CODE

TO INSURE

PRIVACY AND SECRECY

IN THE

TRANSMISSION OF TELEGRAMS.

BY

FRANK MILLER.

NEW YORK:
CHARLES M. CORNWELL,
247 PEARL STREET.

A Typical Entry in Miller's Codebook

Identity can be established if the party will answer that his or her mother's maiden name is..... **05626 Guineapig**

- Yes, mother's maiden name was used for authentication in 1882…
- Plaintext mapped to code numbers and code words
- In general, though, it wasn't a very good codebook, even by the standards of the time

Confidentiality in that Era

- Could use superencipherment for confidentiality, typically by modular addition of a secret value – the key – to the code number and then selecting the new code word
- Most schemes were pretty bad
- War Department Administrative Code (1899): "When a single key number is used, the number may be alternately added and subtracted. Other methods will readily occur. The use of 50 or 100, while easy to remember, should be avoided."

Miller's Superencipherment

A banker in the West should prepare a list of irregular numbers, to be called "shift-numbers," such as 483, 281, 175, 892, &c.

The differences 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 used again.*

Under said number (which we will call the "serial-number") he will place the first "shift-number" (say 483). He will then add the two numbers and find their sum, which he will write down.

Underneath this new sum, or number, he will write the "cipher-word" which he shall find in the Code standing alongside of said sum.

This is a One-Time Pad!

The one-time pad is believed to have been invented in 1918 by Gilbert Vernam (AT&T, later Bell Labs) and Major Joseph Mauborgne (Head of U.S. Army Signal Corp Research and Engineering)


Copyrighted in 1882, by FRANK MILLER, of Sacramento, California.

1882? Did Vernam or Mauborgne know Miller?

Finding Frank Miller

We know little for sure:

- Book published in Sacramento in 1882
- Miller claims 16 years experience in banking
  - A post-Civil War job?
- There is a quote from an Army colonel about the need for encryption

That's all we know!

Google to the Rescue

- Search for 'bank Sacramento ″Frank Miller″'
- The first page of results had a scanned copy of *History of Sacramento County* – and it listed the name of the bank for *some* Frank Miller
- The book also said there were only three banks in Sacramento then – so I'd probably found the right Frank Miller, just a few hours after I found the codebook
- That also gave me the name of the bank, for future queries

Confirmation

- Old census records are public – and they're online
- In 1880, there were only two Frank Millers in Sacramento; one was a "laboror" and the other worked at the proper bank
- A genealogy book described Miller's Civil War service; he did indeed return to Sacramento after the war and join this bank
- I also learned of a scanned 1896 magazine that had a profile of Miller

Frank Miller

- Born in 1842 in Milwaukee; family moved to Sacramento
- Attended Phillips Academy and Yale; enlisted in the Union Army
- Fought at Antietam, wounded at Bull Run; assigned to Col. Olcott's investigative unit and may have helped investigate Lincoln's assassination
- Returned to Sacramento and became a banker (and later bank president)
- Powerful figure in California; early trustee of Stanford
- Moved to San Francisco after retiring from the bank

Crucial Questions

- How did Miller come up with this idea?
- Did Vernam or Mauborgne have any contact with Miller or his codebook?
  - Probably not Vernam; he wasn't a cryptologist
  - Was Mauborgne in California at the right time?

Parker Hitt

- Parker Hitt, also an Army officer, was a friend and colleague of Mauborgne, and another pioneering cryptologist
- His service record showed that Hitt was stationed in San Francisco 1906-1907
- Mauborgne's service record showed that he wasn't stationed there until well after Miller had died – but it also showed that he sailed to the Philippines in 1913. From San Francisco?
- Might Hitt or Mauborgne have met Miller? Did officers socialize much with civilians?

Social Events

- Searched the San Francisco Chronicle for "22nd Infantry" – Hitt's regiment – to get the phrase "military ball"
- Looking for "military ball" and "Frank Miller" got a hit, in 1907
- Miller and Hitt were both listed as attendees; it was sponsored by the "bachelor officers" (including Hitt), and Miller and his wife were chaperoning their daughter
- His daughter did marry one of Hitt's colleagues just six months later, which strongly suggests that (a) she was looking, and (b) Hitt almost certainly spoke with her father
- (There was also a large military ball while Mauborgne was passing through town, but neither he nor Miller were listed as attendees)

Did Hitt Know?

- I regard it as likely, but not certain, that Miller said something about his book
- However, it was likely a brief, and perhaps not very comprehensible, explanation
- Hitt was the first to realize that for security (for a particular cipher), the key should be as long as the plaintext
- Did Hitt have some subconscious recollection of that conversation? (He was punctilious about assigning credit to others, so it was probably not a conscious memory.)

The Codebook Itself

- Provision for message authenticator (though without a checksum)
- No indicators or other mechanism for synchronizing sender and receiver lists of additives; suggests that it was little-used
- One known holder of Miller's codebook used another codebook with *much* weaker confidentiality
- But – examination of another copy of Miller's codebook suggests that there was a second printing

Miller's Inspiration

- I've found nothing in the documentary record to show how Miller came up with this idea, nor is there any evidence of unusual interest in telegraphy. His Civil War background, perhaps?
- Speculation: it came from discussions with the local Wells Fargo agent; from the (very sketchy) information I have, Wells Fargo used very strong crypto for the time: splitting a message into parts, double transposition, homonyms for codewords, and new codebooks every year.

More on Miller?

- Miller's diaries and papers still existed in 1987 – a grandson had them
- From the data in the genealogy book and assorted online queries, I was able to locate a great-granddaughter
- Unfortunately, I have not been able to get in touch with her
- Several of the other known holders of the codebook were very prominent; their papers may have been preserved. Is there more information there?

Acknowledgments

- I received many pointers and lots of help from many people, especially Betsy Rohaly Smoot of the NSA Center for Cryptologic History
- Other important assistance from David W. Gaddy, Edgar and Rebecca Robbins Raines (U.S. Army Center of Military History), Norman Polmar, David Kahn, and Craig Bauer, among many others
- Full list (and many more details) in the July 2011 *Cryptologia*