Frank Miller's Codebook

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

TELEGRAPHIC CODE

TO INSURE

PRIVACY AND SECRECY

IN THE

TRANSMISSION OF TELEGRAMS.

BY

FRANK MILLER.

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

Miller's Superencipherment – What is This?

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 n·t 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 (Bell Telephone Laboratories) and 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?

Desperately Seeking the *right* Frank Miller

- In the preface, the author claims 16 years of banking experience in 1882 – sounds like a post-(U.S.) Civil War career
- Look for 19th century Sacramento bankers named "Frank Miller" (not many banks there then), especially those who served in the Civil War
- Lots of Google and Google books searches; lots of searching digitized newspaper archives; lots of email with military historians
- Check census records – only two people named "Frank Miller" in Sacramento in 1880; one was a banker; the second a "laboror". The other data on the banker fit very, very well – and a relative compiled a genealogy book in 1987 and sent it to Google Books

Who Was Frank Miller?

(From U. Mich Library)

- A prominent Sacramento banker and founding trustee of Stanford
- During the Civil War era, worked as a clerk on anti-fraud and Lincoln's assassination investigations
- He never met Vernam; he probably didn't meet Mauborgne
- He almost certainly met Parker Hitt in 1907, under circumstances that made a discussion of codebooks quite plausible
- Hitt was Mauborgne's mentor and colleague – and was the first to say that for security, a key should be as long as the plaintext (1914)…

But – no proof that Hitt heard about this cipher from Miller

Conclusion and Open Issues

Miller clearly invented the one-time pad 35 years before Vernam and Mauborgne. But did his work have any lasting effect?

- Do I have the right Frank Miller? I have no smoking guns.
- What in his background led him to create that cipher?
- Did he explain his idea to Hitt; if so, did Hitt have a (vague, subconscious?) memory of it in 1912 when he formulated his maxim?
- Does the evidence exist for any of this?

Thanks to: many librarians; also Roy Frostig, David Kahn, David Gaddy, Norman Polmar, Edgar Raines, Rebecca Raines, Betsy Rohaly Smoot, Bill Shurtleff. Errors from: me.

For More Information

CS Department Technical Report CUCS-009-11

Frank Miller: Inventor of the One-Time Pad

http://mice.cs.columbia.edu/getTechreport.php?techreportID=1460