Frank Miller: Inventor of the One-Time Pad*

Steven M. Bellovin
Department of Computer Science
Columbia University
http://www.cs.columbia.edu/~smb

CUCS-009-11

Abstract

The invention of the one-time pad is generally credited to Gilbert S. Vernam and Joseph O. Mauborgne. We show that it was invented about 35 years earlier by a Sacramento banker named Frank Miller. We provide a tentative identification of which Frank Miller it was, and speculate on whether or not Mauborgne might have known of Miller's work, especially via his colleague Parker Hitt.

1 Introduction

One-time pads are in theory the strongest possible algorithmic cipher: if the key is used properly, they *cannot* be broken, even in theory. The invention of the one-time pad is generally credited to Gilbert S. Vernam of Bell Telephone Laboratories and Joseph O. Mauborgne of the U.S. Army Signal Corps [29, 60]. Vernam invented a device that would exclusive-OR keystream bits from a paper tape with the Baudot code generated by letters typed on a keyboard; he and Mauborgne realized that if the keystream tape characters were (a) perfectly random, and (b) never reused, "the messages are rendered entirely secret, and are impossible to analyze without the key" [60]. (To be sure, others have made similar assertions about their ciphers; Vernam and Mauborgne's claim has the advantages of being both correct and mathematically provable.)

In fact, they were anticipated by about 35 years. In 1882, a California banker named Frank Miller published *Telegraphic Code to Insure Privacy and Secrecy in the Transmission of Telegrams*. In it, he describes the first one-time pad system, as a superencipherment mechanism for his telegraph code [42]. If used properly, it would have had the same property of absolute security.

Although in theory Miller can claim priority, reality is more complex. As will be explained below, it is quite unlikely that either he or anyone else ever used his system for real messages; in fact, it is unclear if anyone other than he and his friends and family ever knew of its existence. That said, there are some possible links to Mauborgne. It thus remains unclear who should be credited with *effectively* inventing the one-time pad.

We start by describing and analyzing Miller's codebook. We then explain our tentative identification of the author, and speculate on possible linkages to Mauborgne.

2 The State of 19th Century Cryptography

It is worth discussing common 19th century cryptography, to better understand Miller's starting point. The state of the art, at least in the United States, was very poor [14, Lecture V]. Broadly speaking, two principle systems were in use, straight-forward ciphers and superenciphered codes. Both were rather simple. (For further background, also see [62] and [63].)

*Note: this is a preprint copy of a paper that has been submitted for publication. The final form may vary significantly.

During the Civil War, the Confederacy primarily used a Vignère cipher (which they often called a "court" or "diplomatic" cipher) [49], via manual tables [14, Lecture IV]. A Vignère square was also used by John Wilkes Booth and others in their plot against Lincoln. The Confederacy often used meaningful phrases as high-level keys; in February 1865 they switched to "Come Retribution" from "Complete Victory" [59].

The Union employed a cipher disk to implement an easy-to-change monoalphabetic substitution. The key — that is, the rotation — could be changed in mid-message, or by switching disks. It also employed Stager's route transposition cipher [29, 49, 63], which combined a codebook for (many) proper names with a word-based transposition. (An advantage of transposing words, rather than characters, is that it allowed telegraph operators to correct many transmission errors.)

Codebooks were certainly not new. In some form, they go back to the optical telegraphs of the 18th century [57]; superencipherment goes back to the very first telegraph codebook, compiled by Smith in 1845 [54]. His codebook represented each word as a letter/number pair. He described using an additive to provide confidentiality, and even described using different additives for different codewords:

> For instances, instead of confining the pre-agreements of the parties, to the deduction or addition of one number only, let one number be agreed on, for every alternate word sent in figures, and another number for every other word; or, by the same rule, let several numbers be used for addition or deduction, in any order that may be agreed on.

In addition, he suggested the use of a monoalphabetic substitution of the code letter.

Few late-19th century codebooks were much better at superencryption. The 1899 U.S. War Department code [25], though intended primarily for administrative use, did provide for superencipherment; it was less sophisticated than Smith's. It suggested adding or subtracting a "key number or series of key numbers", and gave as examples the sequence "25, 50, 75, 100". It did, however, note that "the use of 50 or 100, while easy to remember, should be avoided".

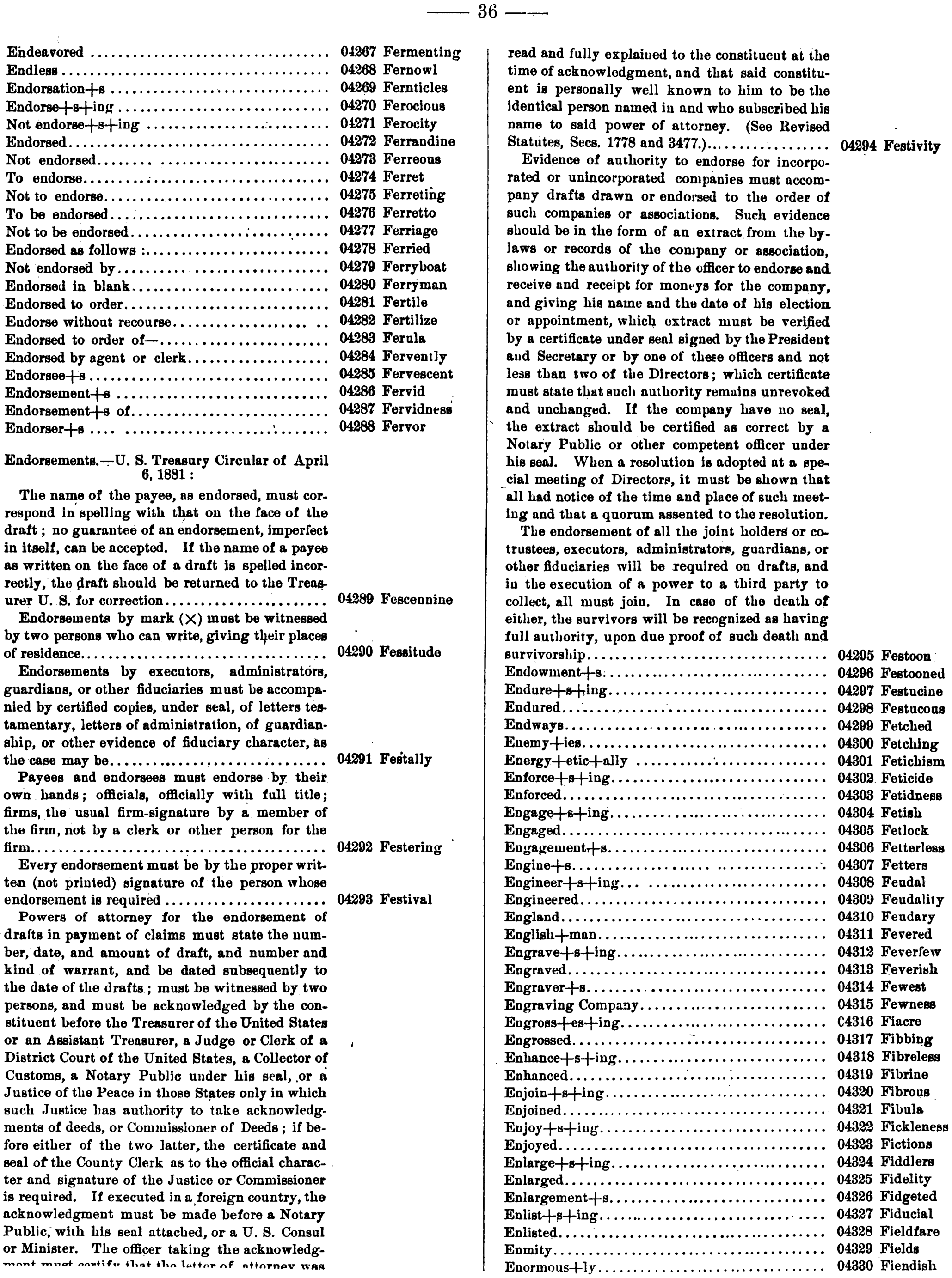
One well-known codebook stood out. Slater's *Telegraphic Code, to Ensure Secresy in the Transmission of Telegrams* [sic] [52] talked about simple additives, but he also described a variety of more complex transforms. For example, he suggested transposing digits in code numbers, or regrouping the 5-digit code numbers into 4-digit ones. In addition, he suggested using combinations of these methods. Despite its limitations, Slater's codebook became the basis of a War Department code [14, 63]. (Curiously, Friedman's discussion of Slater's superencipherment focuses only on the use of additives, and misses the more complex transformations [14, p. 96].)

None of these schemes were that sophisticated. Friedman conjectures that European cryptanalysts were able to read American State Department correspondence with little trouble.

3 Miller's Codebook

Miller's codebook has two independent components, a conventional telegraph code intended for message compression and a superencipherment system. The telegraph code is conventional for its time: it mapped phrases into both English words and 5-digit code groups. While an 1882 codebook cannot be rated against the very sophisticated works produced in the 1920s and 1930s, it does not appear to be a particularly good compression system even when ranked against its peers. Contrast a page from Miller's book (Figure 1) with one from Bloomer's 1874 codebook (Figure 2), another one intended to provide confidentiality [19]; in general, Miller maps a single plaintext word into a single codeword, though there are glaring exceptions such as the entire paragraphs that are represented by FESTIVAL or FESTIVITY, while most of Bloomer's code words represented phrases. (Bloomer also understood security better than most. Although he did not carry out the work himself, he apparently recognized the virtue of two-part codes; the book provides instructions on how to generate one and blank columns in which to write alternate code numbers.)

One of Miller's codewords, GUINEAPIG, is interesting both because it shows the limitations of the code but also for what it says about authentication over the years:



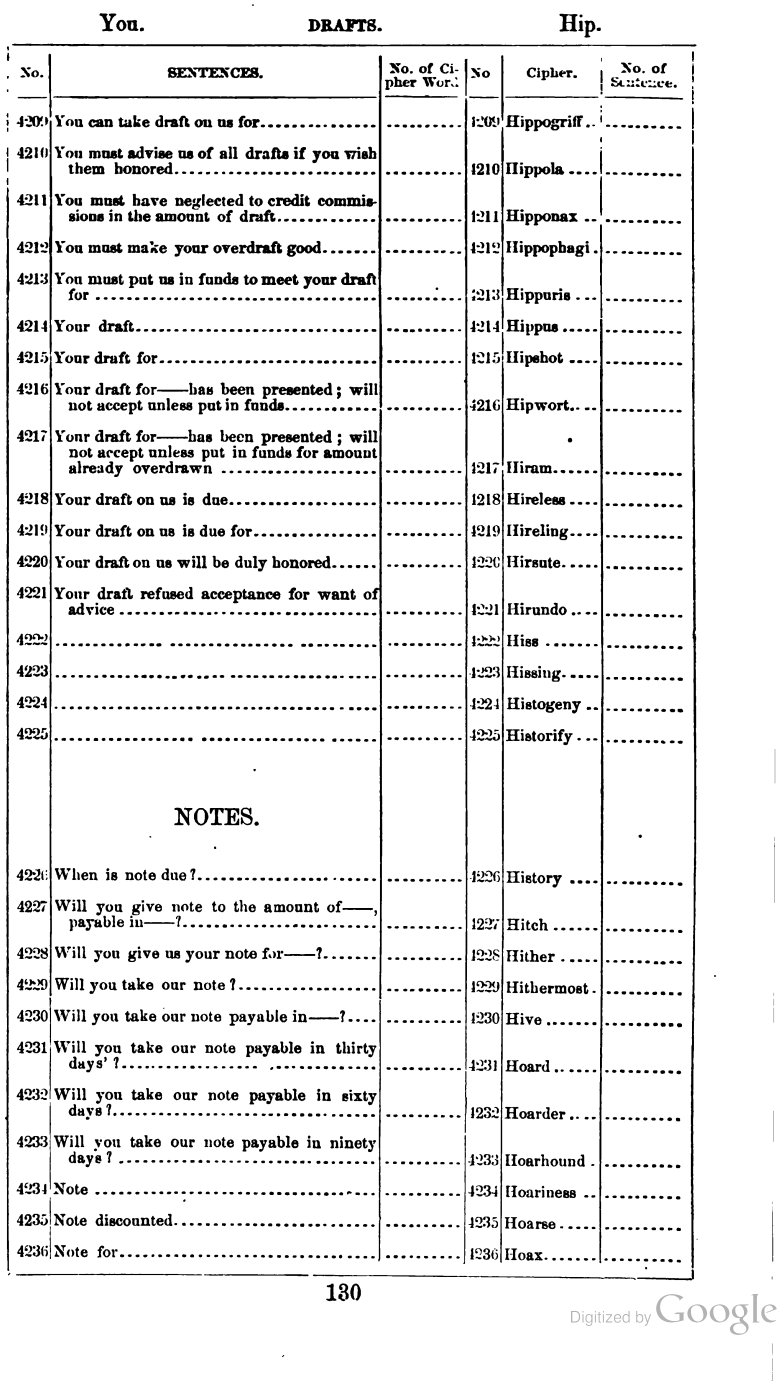
—— 36 ——

Endeavored	04267	Fermenting
Endless	04268	Fernowl
Endorsation+s	04269	Fernticles
Endorse+s+ing	04270	Ferocious
Not endorse+s+ing	04271	Ferocity
Endorsed	04272	Ferrandine
Not endorsed	04273	Ferreous
To endorse	04274	Ferret
Not to endorse	04275	Ferreting
To be endorsed	04276	Ferretto
Not to be endorsed	04277	Ferriage
Endorsed as follows :	04278	Ferried
Not endorsed by	04279	Ferryboat
Endorsed in blank	04280	Ferryman
Endorsed to order	04281	Fertile
Endorse without recourse	04282	Fertilize
Endorsed to order of—	04283	Ferula
Endorsed by agent or clerk	04284	Fervently
Endorsee+s	04285	Fervescent
Endorsement+s	04286	Fervid
Endorsement+s of	04287	Fervidness
Endorser+s	04288	Fervor

Endorsements.—U. S. Treasury Circular of April 6, 1881 :

The name of the payee, as endorsed, must correspond in spelling with that on the face of the draft ; no guarantee of an endorsement, imperfect in itself, can be accepted. If the name of a payee as written on the face of a draft is spelled incorrectly, the draft should be returned to the Treasurer U. S. for correction	04289	Fescennine
Endorsements by mark (X) must be witnessed by two persons who can write, giving their places of residence	04290	Fessitude
Endorsements by executors, administrators, guardians, or other fiduciaries must be accompanied by certified copies, under seal, of letters testamentary, letters of administration, of guardianship, or other evidence of fiduciary character, as the case may be	04291	Festally
Payees and endorsees must endorse by their own hands ; officials, officially with full title; firms, the usual firm-signature by a member of the firm, not by a clerk or other person for the firm	04292	Festering
Every endorsement must be by the proper written (not printed) signature of the person whose endorsement is required	04293	Festival
Powers of attorney for the endorsement of drafts in payment of claims must state the number, date, and amount of draft, and number and kind of warrant, and be dated subsequently to the date of the drafts ; must be witnessed by two persons, and must be acknowledged by the constituent before the Treasurer of the United States or an Assistant Treasurer, a Judge or Clerk of a District Court of the United States, a Collector of Customs, a Notary Public under his seal, or a Justice of the Peace in those States only in which such Justice has authority to take acknowledgments of deeds, or Commissioner of Deeds ; if before either of the two latter, the certificate and seal of the County Clerk as to the official character and signature of the Justice or Commissioner is required. If executed in a foreign country, the acknowledgment must be made before a Notary Public, with his seal attached, or a U. S. Consul or Minister. The officer taking the acknowledgment must certify that the letter of attorney was read and fully explained to the constituent at the time of acknowledgment, and that said constituent is personally well known to him to be the identical person named in and who subscribed his name to said power of attorney. (See Revised Statutes, Secs. 1778 and 3477.)	04294	Festivity
Evidence of authority to endorse for incorporated or unincorporated companies must accompany drafts drawn or endorsed to the order of such companies or associations. Such evidence should be in the form of an extract from the by-laws or records of the company or association, showing the authority of the officer to endorse and receive and receipt for moneys for the company, and giving his name and the date of his election or appointment, which extract must be verified by a certificate under seal signed by the President and Secretary or by one of these officers and not less than two of the Directors ; which certificate must state that such authority remains unrevoked and unchanged. If the company have no seal, the extract should be certified as correct by a Notary Public or other competent officer under his seal. When a resolution is adopted at a special meeting of Directors, it must be shown that all had notice of the time and place of such meeting and that a quorum assented to the resolution. The endorsement of all the joint holders or co-trustees, executors, administrators, guardians, or other fiduciaries will be required on drafts, and in the execution of a power to a third party to collect, all must join. In case of the death of either, the survivors will be recognized as having full authority, upon due proof of such death and survivorship	04295	Festoon
Endowment+s	04296	Festooned
Endure+s+ing	04297	Festucine
Endured	04298	Festucous
Endways	04299	Fetched
Enemy+ies	04300	Fetching
Energy+etic+ally	04301	Fetichism
Enforce+s+ing	04302	Feticide
Enforced	04303	Fetidness
Engage+s+ing	04304	Fetish
Engaged	04305	Fetlock
Engagement+s	04306	Fetterless
Engine+s	04307	Fetters
Engineer+s+ing	04308	Feudal
Engineered	04309	Feudality
England	04310	Feudary
English+man	04311	Fevered
Engrave+s+ing	04312	Feverfew
Engraved	04313	Feverish
Engraver+s	04314	Fewest
Engraving Company	04315	Fewness
Engross+es+ing	C4316	Fiacre
Engrossed	04317	Fibbing
Enhance+s+ing	04318	Fibreless
Enhanced	04319	Fibrine
Enjoin+s+ing	04320	Fibrous
Enjoined	04321	Fibula
Enjoy+s+ing	04322	Fickleness
Enjoyed	04323	Fictions
Enlarge+s+ing	04324	Fiddlers
Enlarged	04325	Fidelity
Enlargement+s	04326	Fidgeted
Enlist+s+ing	04327	Fiducial
Enlisted	04328	Fieldfare
Enmity	04329	Fields
Enormous+ly	04330	Fiendish

Figure 1: A sample page from Miller's codebook. Note the general lack of compression; most codewords, with a few exceptions and a few glaring exceptions, represent a single plaintext word rather than a phrase.

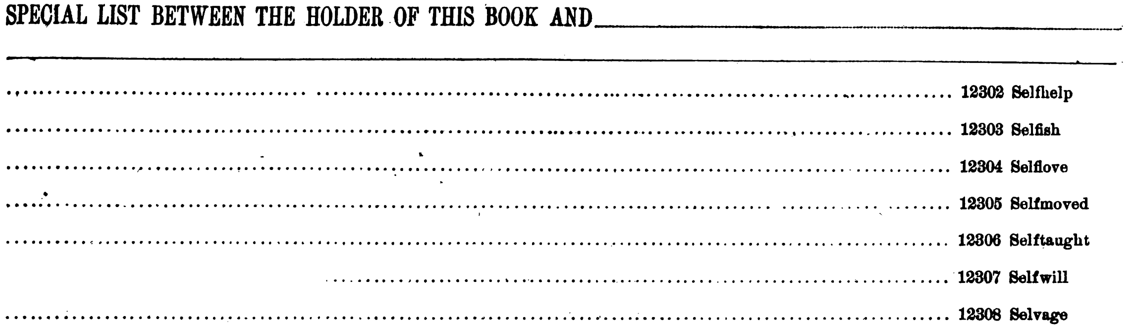


You. DRAFTS. Hip.

No.	SENTENCES.	No. of Cipher Word.	No	Cipher.	No. of Sentence.
4209	You can take draft on us for	....	4209	Hippogriff	....
4210	You must advise us of all drafts if you wish them honored	....	4210	Hippola	....
4211	You must have neglected to credit commissions in the amount of draft	....	4211	Hipponax	....
4212	You must make your overdraft good	....	4212	Hippophagi	....
4213	You must put us in funds to meet your draft for	....	4213	Hippuris	....
4214	Your draft	....	4214	Hippus	....
4215	Your draft for	....	4215	Hipshot	....
4216	Your draft for——has been presented; will not accept unless put in funds	....	4216	Hipwort	....
4217	Your draft for——has been presented; will not accept unless put in funds for amount already overdrawn	....	4217	Hiram	....
4218	Your draft on us is due	....	4218	Hireless	....
4219	Your draft on us is due for	....	4219	Hireling	....
4220	Your draft on us will be duly honored	....	4220	Hirsute	....
4221	Your draft refused acceptance for want of advice	....	4221	Hirundo	....
4222	....	....	4222	Hiss	....
4223	....	....	4223	Hissing	....
4224	....	....	4224	Histogeny	....
4225	....	....	4225	Historify	....
	NOTES.				
4226	When is note due?	....	4226	History	....
4227	Will you give note to the amount of——, payable in——?	....	4227	Hitch	....
4228	Will you give us your note for——?	....	4228	Hither	....
4229	Will you take our note?	....	4229	Hithermost	....
4230	Will you take our note payable in——?	....	4230	Hive	....
4231	Will you take our note payable in thirty days'?	....	4231	Hoard	....
4232	Will you take our note payable in sixty days?	....	4232	Hoarder	....
4233	Will you take our note payable in ninety days?	....	4233	Hoarhound	....
4234	Note	....	4234	Hoariness	....
4235	Note discounted	....	4235	Hoarse	....
4236	Note for	....	4236	Hoax	....

130

Figure 2: A sample page from Bloomer's codebook. The blank columns permit conversion into a two-part code.



SPECIAL LIST BETWEEN THE HOLDER OF THIS BOOK AND ____________

.... 12302 Selfhelp

.... 12303 Selfish

.... 12304 Selflove

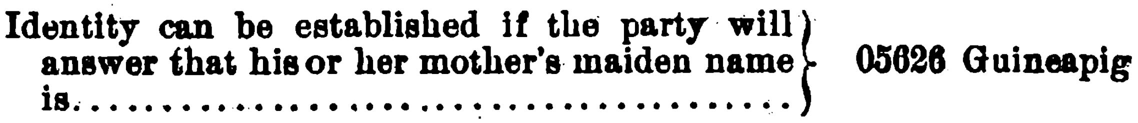
.... 12305 Selfmoved

.... 12306 Selftaught

.... 12307 Selfwill

.... 12308 Selvage

Figure 3: Blank codewords, for use with a particular correspondent.



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

Mother's maiden name, that old standby "secret", was used that way at least as early as 1882.

Note, though, that there is a crucial security failure here: that codeword, suitably shifted, is to be followed by the secret, and the secret almost certainly has to be in plaintext: there won't be a codeword for most family names. The appearance of something that looks like a family name and is a word not in the codebook would quite likely be of interest to any eavesdropper. The alternative is using codewords to spell out the name, but that will result in a large expansion of the message and hence an increase in cost. This, of course, is a failure mode of all codebooks, not just Miller's, but it does show the limitations of Miller's code for one of its intended purposes. (We note that the 1899 *Preliminary War Department Telegraphic Code* [25] included codewords for all officers then in the Army, to avoid precisely this problem.)

Miller's codebook was not as easy to use as some. It mostly lacked subject divisions; encoders would have had to find each phrase alphabetically, and perhaps guess at precisely which word the phrase was indexed under. A clerk who is experienced with a given codebook would be less inconvenienced; this, however, creates a bias in favor of sticking with more familiar works. (Familiarity can help. Lord Nelson's famous signal "England expects that every man will do his duty" originally started "England *confides* that...". However, his signal officer pointed out that "confides" was not in the codebook, and hence would be slower to send, whereas "expects" was. Nelson agreed to the change [24].)

Given the poor compression and usability, and given that telegraph codebooks are subject to a network effect — a codebook owned by many recipients is more valuable to a sender than one owned by just a few — we suspect that it was little-used in practice. The problem was likely exacerbated by a lack of marketing: Miller had a full-time job as a banker, and probably couldn't spend his time persuading other banks to use his code book. As in so many other fields, marketing is extremely important when selling codebooks [29, 30].

One unusual feature of the codebook does warrant further attention. As with virtually all codebooks, this one has blank positions for user-supplied plaintext; see, for example, the middle section of Figure 2. Miller, by contrast, provided about 20 pages of pair-wise lists of extra words; each such page was intended for correspondence with a different individual (Figure 3). This clearly shows his orientation towards point-to-point communication, rather than one-to-many or many-to-many. Any realistic use of one-time pads would indeed require point-to-point messaging. A broadcast scenario, where one party sent to multiple others, would require everyone to have a receive-only list; Miller does not describe any such thing. Given the lack of broadcast transmission media then, this is not surprising.

Miller's superencipherment, by means of additives and modular arithmetic, is much more interesting. As noted earlier, additives were well-known. Miller, however, identified the essence of the one-time pad: randomness and non-repetition [emphasis in the original]:

> 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*.
>
> A copy of the list is to be sent to the New York Banker, who prepares a *different list* and sends copy thereof to the Western Banker.

It seems clear that Miller understood the threat he was countering: "Any system which allows a cipher word to be used twice with the same signification is open to detection. A little talk with a telegraph operator will convince one of this fact." One can, of course, question how deep his understanding was of the cryptanalytic threat, but it's hard to be clearer than that in a single sentence.

Is this a true one-time pad? Kahn defines such a system as one consisting of "a random key used once, and only once" [29, p. 398]. That Miller understood the "once, and only once" part is clear. But is "the differences ... *must not be regular*" equivalent to "random"? We submit that it is. He stressed the phrase, showing that he thought patterns were a serious, exploitable flaw. It would have been nice, though, if he had explained techniques for generating the additives, and if his samples had not all been 3-digit numbers. (According to Kahn, Vernam and his colleagues used "characters drawn from a hat" for keying material.)

Miller also thought about the threat model. He suggested that messages that could be sent verbally by a messenger need not be encrypted, though he also noted that as a practical matter not many people in a town would possess the codebook. Even then, however, he realized that messages needed to be authenticated, even if not encrypted. To this end, he provided a list of 100 "test words"; a sender would take the next available shift-number modulo 100 and use that to select the appropriate test word. The receiver would verify the test word against his list of shift-numbers; both parties, of course, would cancel that value. Miller does not seem to have considered that a telegraph operator could substitute a different message to one protected by a simple authenticator, nor does he mention that receivers must be properly trained to insist that all messages be authenticated. By contrast, Slater's authentication codebook recognizes both problems [51, pp. 4-5]:

> In very many cases, however, and it is surprising in how many, the receivers of messages purporting to come from some well-known correspondent, take it for granted that every telegram which so reaches their hand must be genuine, and, without further consideration of the consequences, act upon it.
>
> ...
>
> There still remains, however, the possibility of a fraud being committed, as it were, over the blank signature of the sender, by a dishonest servant who may be entrusted to carry to the telegraph office the message it is intended to transmit, inasmuch as he would have it in his power to substitute another message drawn up in his own interests and certified by his master's test, or to interpolate some additional words of his own.

and

> Nothing then is easier for a dishonest cable operator than the commission of a fraud of gigantic extent.

The concept of the test word as a message authenticator appears to have been relatively new to telegraphy at the time. "Test word" itself appears to have been a reasonably-common 19th century phrase for actions or writing designed to prove something or someone authentic or genuine. The Freemasons are claimed have employed a secret test word [18, p. 86], as did the Templars [21, p. 122] and the Ku Klux Klan [15, p. 24]. (Though [18] and [15] are works by outsiders attacking the Freemasons and the Klan, that does not affect our point: both works use the phrase "test word" without further explication, buttressing our assertion that readers were familiar with the concept.) The earliest use we have found in telegraphy was just six years before Miller, by Slater [51]; in essence, he suggests use of a book code to authenticate messages. He also gives a number of variants to protect the date, word count, etc. Interestingly, he suggests using sentences; this way, a missing word can indicate that a particular message was never received. Miller put the phrase "test word" in quotes, as if his audience might not be familiar with it in this context. It is unclear if Miller was familiar with Slater's book (which was much less well known than his secrecy code [52]). While we do not know if Miller was a member of any quasi-secret fraternal organization, he was an officer of the Grand Army of the Republic [47], a Civil War veterans' association which is said to have used Masonic rituals [33] and certainly kept them secret [17].

Use of test words in telegrams did become commonplace later on. Lieber [41] references the phrase, though without explanation. [22, p. 155] describes how Wells Fargo used test words on internal telegrams. By the time of World War I, test words were sufficiently common that there were special provisions in the censorship regulations to accept such words that were not in the standard codebooks [13, p. 40]. A banking textbook [40, p. 170] gives a detailed explanation of how test words are added and verified by a special department in the bank.

Checksums appear to date from the same period as Miller's book. For example, during an 1881 meeting of the Royal Astronomy Society, Lord Crawford said [48, p. 170]

> Mr. Ritchie opened a communication with me a short time ago, with a view of introducing a method, which he and Mr. Chandler had contrived, for the despatch of astronomical information of interest. By this method the elements and the ephemeris, which are comprised in twelve lines of printing, were transmitted in sixteen words on a cipher telegram. We cannot go wrong in the telegram, because one test-word checks the whole message.

The full scheme was published a few years later by Chandler and Ritchie [20].

For all its cryptographic sophistication, we doubt that Miller's superencipherment system was ever used in practice: there are some serious operational deficiencies. The most important is the lack of any indicators to show where in the shift-number list the sender started; the scheme as described assumes that all messages are delivered, received, and decrypted in order. This is not a realistic assumption; a high-priority telegram composed late in the day would arrive before a "night letter" composed earlier. Real-world one-time pads generally use something like a page number/additive number pair to show where to start decrypting. There is one nod in that direction — the codeword PECCADILLO means "For this and all other dispatches from us we beg that you will use 'shift-numbers' from our list commencing next below Number ___" — but that is rather clumsier than using indicators routinely.

There are also two codewords to deal with a shortage known to one side but the other. PEBBLES means "send more shift numbers"; PECANA means "No shift numbers here available, so use the 'plain cipher' [the codebook without superencryption] or English". However, the sender's list has to be in synchrony with the receiver's; one side can't run out without the other knowing it [61]. Possibly, the intent was to deal with exception cases, such as loss or compromise of an additive list; if so, one would expect special codegroups to indicate the problem, and most like coupled with the "send more" message.

4 Who Was Frank Miller?

It is difficult, at this remove in time, to be certain just which Frank Miller developed the one-time pad system. (To avoid confusion, in this section we will refer to the author of [42] as the "compiler", and reserve the proper name "Frank Miller" for a particular historical figure.) That said, there are enough clues that — aided by happenstance — we have come to a strong, albeit not certain, conclusion. We believe that the compiler is the Frank Miller who later became the president of the National Bank of D.O. Mills & Co. in Sacramento, as well as one of the founding trustees of Stanford University.

The codebook itself offers a few concrete details. The copyright page identifies the compiler as living in Sacramento. In the preface, he describes himself as having "sixteen years' banking experience". Sixteen years before the publication date was 1866, immediately after the U.S. Civil War ended; this would be a logical time for a young man leaving the army to have started a permanent job. It also seems likely that the compiler had at least some acquaintance with cryptanalysis.

The population of Sacramento was not large at the time, probably around 35,000–36,000 given the 1880 and 1890 census figures.[1] There were 14,526 males over 21 years old in 1880, reducing the set still further. (That figure was not collected in 1890.)

[1] Data retrieved from the University of Virginia Library *Historical Census Browser*, `http://mapserver.lib.virginia.edu/`.

We know that there were not many banks in Sacramento then [16, 64]. Conceivably, of course, someone could have worked at other banks before moving to Sacramento; that said, a Frank Miller who did start at a Sacramento bank in 1866 would very likely be the person we are looking for. Assorted Internet searches turned up a published genealogical history [50] that describes a person with precisely those characteristics; except as otherwise indicated, the biographical information in the remainder of this chapter is taken from it. (The other valuable source was a brief 1896 biography of Miller in *Overland Monthly* [47]. To modern eyes, that one starts strangely, addressing him as "Comrade Frank Miller" and describing him as coming from "good old revolutionary stock", phrases we would regard as more apt for a descendant of a veteran of Mao's Long March than for a California banker.) Additionally, census record searches via `www.familysearch.org` show just two Frank Millers in Sacramento in 1880; one worked at the D.O. Mills bank and the other was a "laboror" [sic].[2]

Frank (or Franklin) Miller was born in Milwaukee on 18 January, 1842, the son of Henry and Nancy Robinson Miller. His family moved to Sacramento in 1856 [50] or 1857 [47] (though [1], an obituary for his father from the Sacramento Record-Union, says 1850). He attended Phillips Academy in Exeter, New Hampshire, enrolled at Yale in 1861, and enlisted in the Second Wisconsin Volunteer Infantry regiment in 1862. He fought at Antietam and was wounded at the Second Battle of Bull Run.

Figure 4: Frank Miller in 1896. (Picture taken from [47], from an electronic copy held by the University of Michigan Digital Library.)

In 1863, Miller, by then a sergeant, was transferred to clerical duties in the Inspector General's office. The following year he was "promoted to a civil clerkship" in New York [47] working for Colonel Henry Steel Olcott, a prominent investigator of fraud and corruption during the Civil War [43, 58].[3] Olcott offered to assist in investigating Lincoln's assassination; Secretary of War Stanton replied, "come and bring your force of detectives" [23, 43]. He was apparently effective, being described as "the most conscientious member of the investigative team" [32]. Miller apparently came with that "force of detectives", though we do not know what his role was. We suspect that it was during the 1863-1865 period, investigating various crimes and peculations, that Miller became acquainted with encryption and perhaps cryptanalysis.

Miller's father was the founding vice president of the D.O. Mills bank; Frank Miller was the "cashier". On his father's death in 1878 he became vice president; he became president in 1893 when Edgar Mills, the founding president, died. Miller retired as president in 1904 [3]. After that, he was no longer resided full-time in Sacramento; he and his wife traveled a great deal and resided in a number of different places before settling down in Berkeley in 1910 or 1911. He and his wife moved to the Pendleton Hotel in San Francisco in 1905 [34] after spending a year or so in Europe; they moved to Sausalito for the summer of 1906 [35] and ended up staying there [37], probably because

[2] The census record for the banker Frank Mills at `https://www.familysearch.org/s/recordDetails/show?uri=http://pilot.familysearch.org/records/trk:/fsrs/rr_206956290/p_334654861&hash=HloWXpZgU9zB10k5M56iYku8TUc%253D` shows a birth year of 1850, which is inconsistent with other sources and difficult to reconcile with Civil War service. The other data listed agree so well with [50] that we suspect an error in the record or in its digitization.

[3] Olcott himself had a very colorful career. After the war, he became a lawyer. He grew interested in spiritualism, converted to Buddhism, and was one of the founders of the American Theosophical Society. Most of the published information on him concentrates on his religious career.

of the 1906 earthquake and fire. Fortuitously, that move took place a few days before the quake [36]. He did plan to return frequently to San Francisco; he was one of the guests of honor at a banquet scheduled for 20 April 1906 [5], and he and his wife had purchased opera tickets for the forthcoming season [8]. They also returned to Sacramento often [4, 6, 7, 36], as well as traveling to Oregon where Miller had significant business interests [3].

We know little of Miller as a person. Examination of his correspondence to and from the president and trustees of Stanford University [2, 9] suggests that he was a forthright, blunt, almost brusque individual; he concluded more than one letter with "do not bother to answer this" or similar words. Another letter, evaluating a proposed personnel policy, concluded with "He is not so competent, nor is any other man." He resigned as a trustee in 1916 — a post that, from his resignation letter, he valued highly — because of ill health [9] and failing eyesight [50]. His relations with one of his sons was strained, apparently over financial issues but with the sense that he thought this son was rather irresponsible.

At some point, the compiler acquired an interest in communications. The codebook's preface quotes a "Colonel Myers" [sic] on the value of cryptography; this is Albert J. Myer, the father of the U.S. Army Signal Corps, and the quote is slightly paraphrased from from Myer's classic work "A Manual of Signals" [45]. (Myer is also considered the father of the Weather Bureau; as a result, he was sometimes known as "Old Probabilities" [63].) It is worth noting that the passage does not appear in the 1864 version of the Manual [44], the only one Miller might have seen while in the service; it does appear in the 1866 and later editions. It is unclear whether an ordinary soldier would have known of or remembered Myer, or been familiar with that book; someone who had worked in intelligence or cryptanalysis almost certainly would. Myer was reasonably prominent after the war, though; it is conceivable that the 1879 edition [46] — the first to be issued by the Government Printing Office — or Myer's death in 1880 stimulated the creation of the codebook.

We suspect that the compiler did not have hands-on experience as a code or communications clerk or as a cryptanalyst; such a person would have been more familiar with indicators, message serial numbers, telegrams being sent out of order, etc. On the other hand, the preface does discuss common transmission errors on telegraph systems (e.g., confusing some Morse symbols with others). It was comparatively unusual to see such discussions in codebooks of that era; this may indicate more than usual familiarity with telegraphy.

It is fortunate indeed for our research that Frank Miller was a prominent person. He was sufficiently important that he was one of the original trustees of Stanford University and left a considerable paper trail, including coverage on the Society pages of the *San Francisco Chronicle*. Even more important, his descendants preserved information about him and someone compiled it all [50].

5 Linkages

The compiler of this codebook — we are certain that it was this Frank Miller — clearly developed the one-time pad; his influence on history, however, is much less clear. It is much like the old philosophical conundrum of a tree falling in a forest with no one around: does it make a sound? Did Vernam or Mauborgne ever learn of Miller's work? Again, there are no firm answers; the best we can do is to speculate.

We can almost certainly rule out contact with Vernam [31]. Vernam was an electrical engineer whose specialty was the encryption hardware; he was not a cryptologist. Kahn concluded long ago that Mauborgne, not Vernam, had the essential cryptologic insight on non-reuse of keys; see the endnote discussion about the development of the non-repeating key for a Vernam machine in [29].

There was not much more chance of direct contact between Miller and Mauborgne. Mauborgne was not stationed in San Francisco until 1932 [55], well after the period of interest. He did pass through the port of San Francisco en route to the Philippines [11], but any encounter with Miller would have been pure coincidence. There does, though, appear to have been one possible opportunity. Mauborgne's ship was scheduled to sail on November 5, 1913; there was a large ball to open the Portola Festival on October 23, and officers were invited [12]. However, we have not found any evidence that either he or Miller attended it. Neither is in the attendee list given in [10], though that article lists people who were "*among* the invited guests" [emphasis added]. Furthermore, a quick scan of the Society columns of the San Francisco Chronicle shows very few mentions of Miller after 1910.

A more intriguing possibility is contact between Miller and Parker Hitt. Hitt, an expert cryptologist and the author of *Manual for the Solution of Military Ciphers* [27], was Mauborgne's mentor and colleague. In 1914, he took a major step towards development of the one-time pad when he wrote "No message is safe in the Larrabee cipher unless the key phrase is comparable in length with the message itself" [29]; his first observations along that line were presented a few years earlier at an Army Signal School Technical Conference [28].[4] (The text makes it clear that he was worried about Kasicki superimpositions in what was essentially a Vignère cipher, rather than any more general principle. The text also notes that multiple encryption with keys of different lengths is not that strong, either; this was later relearned by Vernam and Mauborgne.) Kahn has conjectured that this observation resulted from joint work with Mauborgne; again, see the endnote discussion mentioned above. It is quite clear that if Hitt knew of Miller's system, he would have shared the information with Mauborgne when they were together at the Army Signal School in Fort Leavenworth.

Crucially, it is virtually certain that Miller and Hitt did meet, and under circumstances where the codebook could very easily have come up in conversation. Hitt was stationed at the Presidio in San Francisco February–July 1906; according to his diary, he did attend a number of social functions during that time [26], though we do not know if Miller was at any of them. More importantly, Hitt and Miller both attended "the most brilliant military ball which San Franciscans remember to have seen in many years" [38]. This party was hosted by "the bachelor officers of the Twenty-Second Infantry", including Hitt. The hosts "received the guests at the entrance to the hall, then escorting them to the ladies of the receiving party". Given that this was a party by "bachelor officers", and given that Miller and his wife were accompanied by their daughter Edith, it is hard to imagine that Hitt and Miller did not talk. Edith would have been regarded as highly eligible; she was 25, single, an "unusually attractive, charming girl" [39] (also see her picture at [50, p. 445]), a former Stanford student, and from a prominent, well-to-do family. She may herself have been looking; marriages to officers of that regiment were regarded as quite desirable [39]. Indeed, six months later she married another officer listed as a host, Lieutenant Matthew H. Thomlinson [37].

Given this, we are convinced that Miller and Hitt at least exchanged greetings and probably chatted more. Furthermore, given that the ball was partly to celebrate the first anniversary of the regiment's return from the Philippines, we assume that Miller asked Hitt about his activities there. As it turns out, among other activities Hitt had set up communications lines. He was also very interested in telecommunications [56]. Had this come up at all in conversation, it strikes us as highly probable that Miller — a man who was interested in the subject, and knew of and quoted Myer's book — would have recounted his own efforts in the field. But Miller was brusque; it is also easy to imagine that his manner in speaking could have put off Hitt, who could easily have treated this as an amateur giving advice on telecommunications to someone who had done it in the real world.

Speculation can only take us so far. Simply mentioning authorship of a codebook, or even a codebook and superencipherment system, is very different from trying to explain shift-numbers at a party. Based on the evidence available thus far, we cannot quite conclude that Hitt knew enough about Miller's system to have been influenced by it. Conversely, of course, we also cannot conclude that he was ignorant of it. Perhaps one aspect — keying material as long as the plaintext — stayed with him and influenced his comments about the Larrabee system.

Our overall verdict is "not proven". For effective transmission to have happened, Miller would have had to tell Hitt of his idea in some detail. Hitt would have had to retain enough memory of it to use in in formulating his maxim about key length, but not enough to actually credit Miller. Thus, though Miller's idea may have lived on, if so it it was via a subconscious channel, and almost certainly through Hitt. (We also note that Mauborgne told Kahn that he came up with the idea himself while working with Vernam [29].)

Drawing any further conclusions will be difficult unless more documentation is unearthed. Hitt's papers have been scrutinized by many historians; they are unlikely to hold any surprises, unless there are cryptic references to Miller that would have been meaningless without the context supplied here. Miller's papers and diary may hold clues; they existed at least as late as 1987 [50], but we have been unable to locate them. (Neither of the two obvious repositories, Stanford University and the California State Library, has them.) We leave these matters to other historians who are more diligent, or who have access to resources that we do not.

[4] Kahn had speculated that Hitt formulated this precept before 1914. Research by Craig Bauer and Drew Wicke of York College of Pennsylvania and John W. Dawson, Jr., retired from Penn State University at York, has confirmed this. However, the note is by Hitt and Lieutenant Karl Truesdell, rather than with Mauborgne. Truesdell compiled the first set of multilingual frequency for the U.S. Army [29].

6 Conclusions

It is clear that Miller invented the one-time pad: res ipsa loquitur. His work was remarkable, not just because he invented a secure encryption scheme 35 years before it was reinvented, but also because it came out of the blue. Vernam and Mauborgne were working in the field; Vernam was trying to build a secure communications system and Mauborgne was the head of research and engineering for the U.S. Army Signal Corp. They were the sort of people one would expect to invent such a thing. Miller, on the other hand, was a banker, whose only first-hand experience with cryptology (if any) was likely 16 years earlier. Still, he was not the first amateur to make a significant contribution to the field. Indeed, Kahn has a chapter entitled "The Contribution of the Dilettantes". The most remarkable tale in that chapter is that of Thomas Jefferson, who invented a wheel cipher in the 1790s, an invention that was promptly forgotten and not rediscovered in his papers until 1922. Ironically enough, Jefferson's cipher was reinvented a few years before that by French cryptologist Étienne Bazeries; it was brought to the U.S. and refined by none other than Parker Hitt and Joseph Mauborgne.[5]

One can also speculate on the risks of tying a bad system — the conventional codebook Miller authored — to a good one. Had Miller published — and marketed — his superencipherment independently from his codebook, it might have succeeded. Robert Slater's codebook [52], intended only for confidentiality, was even worse than Miller's for compression (though it had 25,000 words, compared with Miller's 12,800); despite that, the work went through nine editions, the last published in 1938 [53], and even was the basis for a U.S. government codebook [14, 63]. The difference was likely marketing — Slater was secretary of the French Atlantic Telegraph Company —but regardless, Slater's work survived and was influential; Miller's work has been forgotten.

It is tempting to speculate on how history may have been different had people paid attention. Almost certainly, one-time pads would never have been employed for most military communications; the operational difficulties, then as now, would have been prohibitive. But what of high-level diplomatic correspondence? Kahn tells many tales of cryptanalysis of such messages between 1882 and 1918; might things have been different? Might the German Foreign Ministry been able to protect Zimmernan's fateful telegram with a one-time pad if they had known of Miller's work? And if so, would the U.S. have entered World War I when it did? History might not have been changed — years later, the Japanese used their PURPLE machine for diplomatic messages, rather than a Vernam machine — but perhaps it might have been.

Finally, it takes nothing away from Vernam or Mauborgne's own creativity to acknowledge that Miller had the same idea. If nothing else, their system — an online, automated mechanism that operated on the 0s and 1s of Baudot code — was far more usable and was the precursor to today's computerized stream ciphers.

Acknowledgments

As always when we are doing historical research, we must first thank the generations of librarians and archivists who have collected, indexed, and preserved crucial documents over the decades. At least as important, they help me find obscure materials. We are especially indebted to the staffs of the Library of Congress (where we first found Miller's book), the Columbia University Library Network, the Stanford University Library, and the California State Library. Google Books also deserves a mention for its role in making many rare works easily available.

William Shurtleff's genealogy book was an extremely valuable resource; his private comments were also helpful.

I had limited time to travel; I was aided in "remote research" by Roy Frostig of Stanford University.

Craig Bauer and Drew Wicke of York College of Pennsylvania and John W. Dawson, Jr., retired from Penn State University at York found Hitt's paper at the Army Signal School Technical Conference, confirming Kahn's opinion on when the observation on key length was made, but also showing the context of that opinion.

We have received a lot of useful information and guidance from many historians, most especially Betsy Rohaly Smoot of the NSA Center for Cryptologic History, David W. Gaddy, and Dr. Edgar F. Raines, Jr. and Rebecca Robbins Raines of the U.S. Army Center of Military History. Norman Polmar of the U.S. Naval Institute and David Kahn also provided very important advice and pointers. Errors, of course, are all ours.

[5] One should not draw the conclusion that Hitt was a habitual plagiarist who stole from both Miller and Bazeries. Kahn quotes Hitt's memo as explicitly crediting Bazeries for the wheel cipher.

References

[1] Obituary of Henry Miller. Milwaukee County Online Genealogy and Family History Library, 1878. Reprint of obituary from the *Sacramento Record-Union*. Retrieved Jan 13, 2011. Available from: http://www.linkstothepast.com/milwaukee/obitsM.php.

[2] Papers of D.S. Jordan. Department of Special Collections and University Archives, Stanford University Libraries, 1891–1909. Folder/pages: 15/2, 63/7, 214/22, 342/35, 452/45, 476/47, 478/48, 617/64.

[3] President of D.O. Mills' Sacramento Bank resigns. In *San Francisco Chronicle*, page 20, February 7, 1904.

[4] Society. In *San Francisco Chronicle*, page 7, June 13, 1905.

[5] Banquet in honor of Stanford trustees: Alumni, students, and faculty will pay respects to governing body. In *San Francisco Chronicle*, page 3, April 16, 1906.

[6] Club notes. In *San Francisco Chronicle*, page 33, March 25, 1906.

[7] Society events of the week. In *San Francisco Chronicle*, page 29, July 15, 1906.

[8] These are names of the ticket holders. In *San Francisco Chronicle*, page 9, April 17, 1906.

[9] Board of Trustees supporting documents. Department of Special Collections and University Archives, Stanford University Libraries, 1906–1916. Folder/pages: 4/1, 13/1, 18/11, 19/11, 1/12.

[10] Ball is the first Portola society event: Army and Navy represented at dance. In *San Francisco Chronicle*, page 11, October 23, 1913.

[11] Presidio troops on hike tomorrow. In *San Francisco Chronicle*, page 42, October 26, 1913.

[12] Society preparing for Portola season. In *San Francisco Chronicle*, page 1, October 13, 1913.

[13] *Exporters' Review*. 1917. Available from: http://books.google.com/books?id=ROXmAAAAMAAJ.

[14] *The Friedman Legacy: A Tribute to William and Elizabeth Friedman*. Number 3 in Sources in Cryptologic History. Center for Cryptologic History, National Security Agency, 2006. Available from: http://www.nsa.gov/about/_files/cryptologic_heritage/publications/prewii/friedman_legacy.pdf.

[15] Anonymous. *The Nations Peril. Twelve Years Experience in the South. Then and Now. The Ku Klux Klan, a Complete Exposition of the Order: Its Purpose, Plans, Operations, Social and Political Significance; the Nations Salvation*, volume 2. Friends of the Compiler, New York, 1872. Identified in the Library of Congress as Republican campaign literature. Available from: http://www.archive.org/details/nationsperiltwel02newy.

[16] Le Roy Armstrong and J.O. Denny. *Financial California: An Historical Review of the Beginnings and Progress of Banking in the State*. Coast Banker Publishing Company, San Francisco, 1916. Google Books ebook. Available from: http://books.google.com/books?id=p7llDshxfHEC.

[17] Robert B. Beath. *History of the Grand Army of the Republic*. Bryan, Taylor, & Co., New York, 1889.

[18] D. Bernard. *Light on Masonry: A Collection of All the Most Important Documents on the Subject of Speculative Free Masonry: Embracing the Reports of the Western Committees in Relation to the Abduction of William Morgan . . . with All the Degrees of the Order conferred in a Master's Lodge ...* W. Williams, printer, 1829. Available from: http://books.google.com/books?id=QlIZAAAAYAAJ.

[19] J. G. Bloomer. *Bloomer's Commercial Cryptograph: A Telegraph Code and Double Index—Holocryptic Cipher*. A. Roman & Co., 1874. Available from: http://books.google.com/books?id=90UKAAAAIAAJ.

[20] Seth Carlo Chandler and John Ritchie, Jr. *Science Observer Code*. Boston Scientific Society, 1888. Available from: `http://books.google.com/books?id=pktGAAAAYAAJ`.

[21] Simeon B. Chase. *A Digest of the Laws, Decisions, Rules and Usages, of the Independent Order of Good Templars: With a Brief Treatise on Parliamentary Practice*. W. J. Moses' publishing house, 1867. Available from: `http://books.google.com/books?id=9bAVAAAAYAAJ`.

[22] P.L. Fradkin. *Stagecoach: Wells Fargo and the American West*. Simon & Schuster, 2002. Available from: `http://books.google.com/books?id=QILdMe7lYXgC`.

[23] David W. Gaddy. Private communication, January 21, 2011.

[24] Great Britain Admiralty. *Nelson's Signals: The Evolution of the Signal Flags*. Printed for His Majesty's Stationery Office by Eyre and Spottiswoode, London, 1908. Naval Intelligence Division Historical, No. 1.

[25] Adolphus W. Greely. *Preliminary War Department Telegraphic Code, Supplemental to and to be Inserted as an Appendix to Western Union Telegraphic Code*. Government Printing Office, Washington, DC, 1899. War Department Document Number 93.

[26] Parker Hitt. Personal diary, 1906. Reviewed by E.R. Smoot, January 2011.

[27] Parker Hitt. *Manual for the Solution of Military Ciphers*. Press of the Army Service Schools, 1916. Available from: `http://books.google.com/books?id=2MVBAAAAIAAJ`.

[28] Parker Hitt and Karl Truesdell. Comments on paper of Captain Muirhead's "military cryptography". In *Army Signal School Technical Conference 1911–1912*, 1912. Conference 14.

[29] David Kahn. *The Codebreakers*. Macmillan, New York, 1967.

[30] David Kahn. Private communication, October 2009.

[31] David Kahn. Private communication, January 13, 2011.

[32] Michael W. Kaufman. *American Brutus: John Wilkes Booth and the Lincoln Conspiracies*. Random House, New York, 2004.

[33] Glenn B. Knight. Brief history of the Grand Army of the Republic, February 1997. Note: date shown is the earliest known to `http://www.archive.org`; it includes the information used here. Available from: `http://suvcw.org/gar.htm`.

[34] Lady Teazle. Society. In *San Francisco Chronicle*, page 9, April 25, 1905.

[35] Lady Teazle. Society. In *San Francisco Chronicle*, page 9, April 14, 1906.

[36] Lady Teazle. Society. In *San Francisco Chronicle*, page 6, June 18, 1906.

[37] Lady Teazle. Society. In *San Francisco Chronicle*, page 5, August 24, 1907.

[38] Lady Teazle. Society. In *San Francisco Chronicle*, page 7, February 13, 1907.

[39] Lady Teazle. Society. In *San Francisco Chronicle*, page 5, July 10, 1907.

[40] L.H. Langston and First National City Bank of New York. *Practical Bank Operation*, volume 1, pts. 1-13 of *Practical Bank Operation*. The Ronald Press Company, 1921. Available from: `http://books.google.com/books?id=pkIOAAAAYAAJ`.

[41] Benjamin Franklin Lieber. *Lieber's Standard Telegraphic Code*. Lieber Pub. Co., 1896. Available from: `http://books.google.com/books?id=jesOAAAAYAAJ`.

[42] Frank Miller. *Telegraphic code to Insure Privacy and Secrecy in the Transmission of Telegrams*. Charles M. Cornwell, New York, 1882. Available from: http://books.google.com/books?id=jNf2GwAACAAJ.

[43] H. Murphet. *Hammer on the Mountain: Life of Henry Steel Olcott (1832-1907)*. Theosophical Publishing House, 1972. Note: this is a biography of the founder of a religious movement, issued by the movement's own publishing house. Its objectivity is thus perhaps open to question.

[44] A.J. Myer. *A Manual of Signals: For the Use of Signal Officers in the Field*. 1864.

[45] A.J. Myer and United States Army Signal Corps. *A Manual of Signals: For the Use of Signal Officers in the Field, and For Military and Naval Students, Military Schools, etc.* D. Van Nostrand, 1866. Available from: http://books.google.com/books?id=Pf9BAAAAYAAJ.

[46] A.J. Myer and United States Army Signal Corps. *A Manual of Signals: For the Use of Signal Officers in the Field, and For Military and Naval Students, Military Schools, etc.* Governmentt Printing Office, 1879. Available from: http://books.google.com/books?id=t11CAAAAYAAJ.

[47] Frank Elliott Myers. Defenders of the Union. *Overland Monthly and Out West magazine*, 27(160):434–462, April 1896. Note: Miller's profile is on pp. 459-461. Available from: http://quod.lib.umich.edu/cgi/t/text/pageviewer-idx?c=moajrnl;cc=moajrnl;rgn=full%20text;idno=ahj1472.2-27.160;didno=ahj1472.2-27.160;view=image;seq=0440;node=ahj1472.2-27.160%3A13.

[48] NASA Astrophysics Data System Abstract Service. *The Observatory*, volume 4. Editors of the Observatory, 1881. Available from: http://books.google.com/books?id=Qfg3AAAAMAAJ.

[49] W.R. Plum. *The Military Telegraph During the Civil War in the United States: With an Exposition of Ancient and Modern Means of Communication, and of the Federal and Confederate Cipher Systems; Also a Running Account of the War Between the States*. Number v. 1. Jansen, McClurg & Company, 1882. Available from: http://books.google.com/books?id=trpBAAAAIAAJ.

[50] William Roy Shurtleff. *The Miller and Simmons Families: Geneaology and History Documents*, volume II. Pine Hill Press, Lafayette, California, second edition, 1993. Available from: http://books.google.com/books?id=Gq0nIm8B22EC.

[51] R. Slater. *Banking Telegraphy: Combining Authenticity, Economy, and Secrecy, a Code for the Use of Bankers and Merchants*. W.R. Gray, 1876. Available from: http://books.google.com/books?id=6A4EAAAAQAAJ.

[52] Robert Slater. *Telegraphic Code, to Ensure Secresy in the Transmission of Telegrams*. W.R. Gray, London, first edition, 1870. Available from: http://books.google.com/books?id=MJYBAAAAQAAJ.

[53] Robert Slater. *Telegraphic Code, to Ensure Secrecy in the Transmission of Telegrams*. Simpkin Marshall, Ltd., London, ninth edition, 1938.

[54] Francis O.J. Smith. *The Secret Corresponding Vocabulary, Adapted for use to Morse's Electro-Magnetic Telegraph: and Also in Conducting Written Correspondence, Transmitted by the Mails, or Otherwise*. Thurston, Ilsley & Co., Portland, ME, 1845. Available from: http://books.google.com/books?id=Z45clCxsF7EC.

[55] Betsy Rohaly Smoot. Private communication, January 19, 2011.

[56] Betsy Rohaly Smoot. Private communication, February 2, 2011.

[57] Tom Standage. *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-line Pioneers*. Walker and Co., New York, 1998.

[58] Edward Steers, Jr. *The Lincoln Assassination Encyclopedia*. Harper Perennial, New York, 2010.

[59] W.A. Tidwell, J.O. Hall, and D.W. Gaddy. *Come Retribution: The Confederate Secret Service and the Assassination of Lincoln*. University Press of Mississippi, 1988. Available from: `http://books.google.com/books?id=MDNdbLv8eRMC`.

[60] Gilbert S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Journal of the American Institute of Electrical Engineers*, XLV:109–115, February 1926. Available from: `http://www.cs.columbia.edu/~smb/vernam.pdf`.

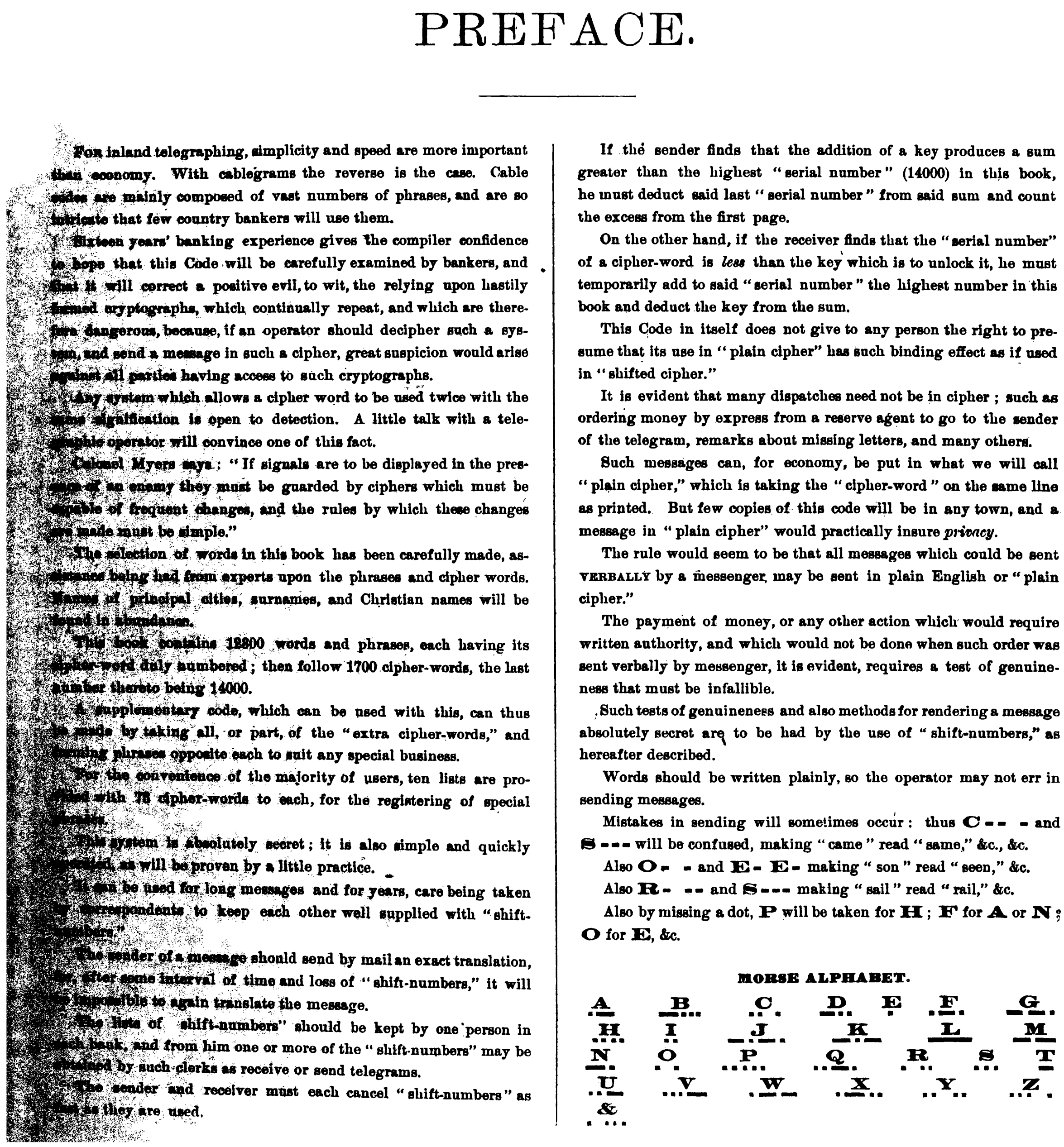
[61] David A. Wagner. Private communication, January 14, 2011.

[62] Ralph E. Weber. *United States Diplomatic Codes and Ciphers, 1775–1938*. Precedent Publishing, Chicago, 1979.

[63] Ralph E. Weber. *Masked Dispatches: Cryptograms and Cryptology in American History, 1775–1900*, volume 1 of *United States Cryptologic History, Series 1: Pre-World War I*. Center for Cryptologic History, National Security Agency, second edition, 2002. Available from: `http://www.nsa.gov/about/_files/cryptologic_heritage/publications/prewii/masked_dispatches.pdf`.

[64] William Ladd Willis. *History of Sacramento County, California*. Historic Record Company, Los Angeles, 1913. Available from: `http://www.archive.org/details/historyofsacrame01will`.

The Preface to Miller's Codebook



PREFACE.

For inland telegraphing, simplicity and speed are more important than economy. With cablegrams the reverse is the case. Cable codes are mainly composed of vast numbers of phrases, and are so intricate that few country bankers will use them.

Sixteen years' banking experience gives the compiler confidence to hope that this Code will be carefully examined by bankers, and that it will correct a positive evil, to wit, the relying upon hastily formed cryptographs, which continually repeat, and which are therefore dangerous, because, if an operator should decipher such a system, and send a message in such a cipher, great suspicion would arise against all parties having access to such cryptographs.

Any system which allows a cipher word to be used twice with the same signification is open to detection. A little talk with a telegraphic operator will convince one of this fact.

Colonel Myers says: "If signals are to be displayed in the presence of an enemy they must be guarded by ciphers which must be capable of frequent changes, and the rules by which these changes are made must be simple."

The selection of words in this book has been carefully made, assistance being had from experts upon the phrases and cipher words. Names of principal cities, surnames, and Christian names will be found in abundance.

This book contains 12300 words and phrases, each having its cipher-word duly numbered; then follow 1700 cipher-words, the last number thereto being 14000.

A supplementary code, which can be used with this, can thus be made by taking all, or part, of the "extra cipher-words," and forming phrases opposite each to suit any special business.

For the convenience of the majority of users, ten lists are provided with 78 cipher-words to each, for the registering of special phrases.

This system is absolutely secret; it is also simple and quickly operated, as will be proven by a little practice.

It can be used for long messages and for years, care being taken by correspondents to keep each other well supplied with "shift-numbers."

The sender of a message should send by mail an exact translation, for, after some interval of time and loss of "shift-numbers," it will be impossible to again translate the message.

The lists of "shift-numbers" should be kept by one person in each bank, and from him one or more of the "shift-numbers" may be obtained by such clerks as receive or send telegrams.

The sender and receiver must each cancel "shift-numbers" as fast as they are used.

If the sender finds that the addition of a key produces a sum greater than the highest "serial number" (14000) in this book, he must deduct said last "serial number" from said sum and count the excess from the first page.

On the other hand, if the receiver finds that the "serial number" of a cipher-word is *less* than the key which is to unlock it, he must temporarily add to said "serial number" the highest number in this book and deduct the key from the sum.

This Code in itself does not give to any person the right to presume that its use in "plain cipher" has such binding effect as if used in "shifted cipher."

It is evident that many dispatches need not be in cipher; such as ordering money by express from a reserve agent to go to the sender of the telegram, remarks about missing letters, and many others.

Such messages can, for economy, be put in what we will call "plain cipher," which is taking the "cipher-word" on the same line as printed. But few copies of this code will be in any town, and a message in "plain cipher" would practically insure *privacy*.

The rule would seem to be that all messages which could be sent VERBALLY by a messenger may be sent in plain English or "plain cipher."

The payment of money, or any other action which would require written authority, and which would not be done when such order was sent verbally by messenger, it is evident, requires a test of genuineness that must be infallible.

Such tests of genuineness and also methods for rendering a message absolutely secret are to be had by the use of "shift-numbers," as hereafter described.

Words should be written plainly, so the operator may not err in sending messages.

Mistakes in sending will sometimes occur: thus **C** ·· · and **S** ··· will be confused, making "came" read "same," &c., &c.

Also **O** · · and **E** · **E** · making "son" read "seen," &c.

Also **R** · ·· and **S** ··· making "sail" read "rail," &c.

Also by missing a dot, **P** will be taken for **H**; **F** for **A** or **N**; **O** for **E**, &c.

MORSE ALPHABET.

A	B	C	D	E	F	G
·—	—···	·· ·	—··	·	·—·	——·
H	I	J	K	L	M	
····	··	—·—·	—·—	⸺	——	
N	O	P	Q	R	S	T
—·	· ·	·····	··—·	· ··	···	—
U	V	W	X	Y	Z	
··—	···—	·——	·—··	·· ··	··· ·	
&						
· ···						

A copy of this Code has been sent to, and will remain with, each bank in New York City, whose address and "cipher-word" follows hereafter.

A copy has likewise been sent to each bank which is a member (in 1822) of the Clearing House in Chicago, St. Louis, New Orleans, and San Francisco.

This Code is stereotyped and no changes will be made at any time.

SHIFT-NUMBERS.

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.*

A copy of the list is to be sent to the New York Banker, who prepares a *different list* and sends copy thereof to the Western Banker.

Each party should enter his own list in black ink in a book, and copy his correspondent's list in red ink upon the opposite page; thus the black figures will denote his "sending numbers," and the red figures will denote his "receiving numbers."

Having occasion to telegraph an order requiring the payment of money, and knowing that an English dispatch would receive no attention, the Western banker will write his dispatch on a sheet of paper, leaving a few lines blank between the written lines.

He will then find his first word in this Code, and copy upon the sheet of paper its number, placing the number under the word.

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.

Thus he gets the first cipher-word for his telegram.

To the appropriate "serial number" of the second word he will add the second "shift-number" (say 281), and, finding their sum, he will take the cipher-word which is found opposite said sum.

He will follow the same plan with the remaining words.

EXAMPLE.

Extended	for	eight	days
4651	4942	226	3271
483	281	175	892
5134	5223	401	4163
Gentleness	Glaired	Allegro	Fantasia

The receiver will reverse the operation, writing down the first cipher-word of the telegram; under it placing its "serial number," and from that deducting the first "shiit number" (say 483), thus finding the "serial number" of the first English word transmitted.

From the serial number of the second cipher-word in the telegram he will deduct the second "shift-number" (say 281), thus finding the serial number of the second English word transmitted.

EXAMPLE.

Gentleness	Glaired	Allegro	Fantasia
5134	5223	401	4163
483	281	175	892
4651	4942	226	3271
Extended	for	eight	days

For many telegrams it will suffice that the common English words be used with a "test word" that shall indicate that the dispatch was genuine *as sent.* Economy and much safety can also be secured by using a "test word" and placing the rest of the message in "plain cipher"—that is, using the Code as printed without any "shifting."

The sender will, in such cases, take the two right-hand figures of his first "shift-number," and use the test word indicated by such two figures; thus he will use the test word "Abstruse" if his first key is 483, and place the rest of the message in English or in "plain cipher."

The receiver will note that a "test word" is used, and that its number is the same as the two right-hand figures of the key (or "shift-number"), which is then available.

Said "shift-number" must, of course, be then erased by both sender and receiver, for it is void for further use.

EXAMPLE.

Abstruse Foredated Furuncle Admirers Disgusted

Abstruse: Extended for eight days.