

SRH#001

D4/SRE

COPY 1

HISTORICAL BACKGROUND
OF THE
SIGNAL SECURITY AGENCY

VOLUME ONE

CODES AND CIPHERS

PRIOR TO WORLD WAR I

ARMY SECURITY AGENCY

WASHINGTON, D.C.

12 APRIL 1946

DECLASSIFIED per Sec. 5, E. O. 11652
by Director, NSA/Chief, CSS

WRG

Date: 14 MAR. 77



ARMY SECURITY AGENCY

Washington, D. C.

HISTORICAL BACKGROUND OF THE SIGNAL SECURITY AGENCY

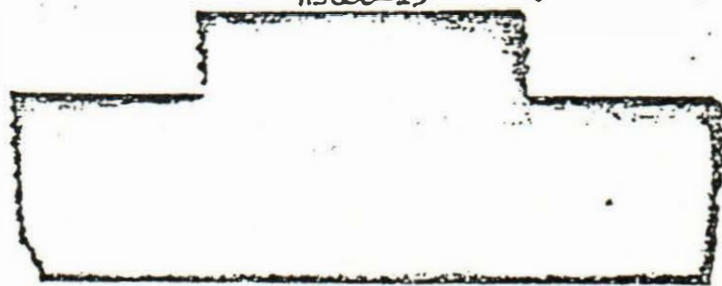
VOLUME ONE

CODES AND CIPHERS PRIOR TO WORLD WAR I

Prepared under the Direction of the
ASSISTANT CHIEF OF STAFF, G-2

12 April 1946

WDGSS-13



000 001

~~SECRET~~
7402166

HISTORICAL NOTE

When, in October 1944, plans were first made for the preparation of a comprehensive History of the Signal Security Agency, it was intended to include therein an account of the historical background of the Agency beginning with the earliest record of the use of cryptography by the United States Army. As the material was gathered together, however, it became increasingly clear that to do this would result in expanding the bulk of the History to such proportions as to discourage many readers. For this reason, the historical background has been prepared as a separate work in three volumes, as follows:

- Volume One: Codes and Ciphers prior to World War I 1776 - 1917
- Volume Two: World War I 1917 - 1919
- Volume Three: The Peace 1919 - 1939

Volumes One and Two of this series are provided with indexes covering the content of each respectively. The index in Volume Three, however, covers the text and footnotes of the entire series of three volumes.

It was not planned in the beginning to include any tab material in the Historical Background of the Signal Security Agency. After the work was finished, however, a number of documents were found which seemed worthy of note, and these were simply listed and added as an appendix to volume Three.

HISTORIAN, ASA
20 April 1948

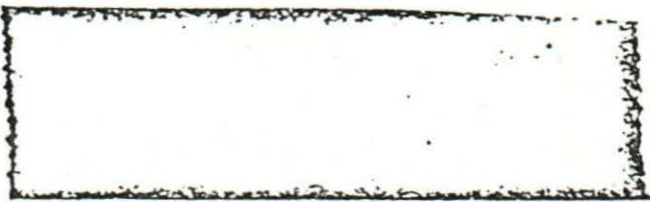
0 0.002



HISTORICAL BACKGROUND OF THE SIGNAL SECURITY AGENCY

Contents

<u>Chapter</u>	<u>Page</u>
Volume One: Codes and Ciphers prior to World War I	
I. The American Systems in the Revolutionary Period	
a. Monoalphabetic substitutions	1
b. Thomas Jefferson's cipher device	4
c. The dictionary codes	5
d. Codes	6
e. Secret ink	11
II. The British Systems in the Revolution	
a. The Clinton Papers	13
b. Monoalphabetic substitutions	14
c. "The decypher of Mr. L."	14
d. The grille	16
e. The dictionary codes	17
f. Codes	17
g. Secret ink	18
h. The Arnold-Andre treason	18
III. The Federal Systems in the Civil War	
a. The sources	21
b. The Military Telegraph Corps	26
c. The Signal Corps	34
d. Monoalphabetic substitutions	35
e. The cipher disk	39
f. Polyalphabetic substitutions	42
g. Hawley's cipher device	44
h. Anton's cipher device	44
i. The Navy cipher disk	45
j. Route transpositions	46
k. Other transpositions	67
l. Civil War terminology	71
m. An appraisal of Federal cryptography	72



IV. The Confederate Systems in the Civil War

- a. The Vigenère table 75
- b. The cipher cylinder 85
- c. The running key 86
- d. Confederate espionage systems 87
- e. An appraisal of Confederate cryptography .. 93

V. A Diplomatic System in the Civil War Period 96

VI. Cryptographic Progress 1865-1917

- a. The Telegraphic Code 1895 99
- b. The Spanish-American War 100
- c. The War Department Telegraphic Code 1899 . 103
- d. The Cipher of the War Department 1902 107
- e. The War Department Telegraphic Code 1906 . 108
- f. The War Department Telegraph Code 1915 ... 110
- g. Suggestions from Inventors 114
- h. The eve of the conflict 115

Index 119





HISTORICAL BACKGROUND OF THE SIGNAL SECURITY AGENCY

VOLUME ONE: PRIOR TO WORLD WAR I

CHAPTER I. THE AMERICAN SYSTEMS IN THE REVOLUTIONARY PERIOD¹

A. Monoalphabetic Substitutions

The simplest form of substitution cipher is, of course, the monoalphabetic, so it is not surprising to find that ciphers of this type were used by Americans in the Revolutionary period. Such a cipher appears in the letters of William Lee² and another was used by John Jay in a letter to Robert Morris dated 19 November 1780 in which Jay also suggests "the use of Entick's dictionary paged backwards, to be supplemented by the use of a transposed alphabet."³

-
1. This chapter and the one following present a summary of what is now known concerning the cryptographic systems in use during the Revolutionary Period. The sources are in every case secondary in character: no attempt has been made to examine the original documents in the Library of Congress and the National Archives. Nor has any exhaustive attempt been made to exploit the voluminous literature on the period for incidental references to cryptography.
 2. Edmund C. Burnett, "Ciphers of the Revolutionary Period," The American Historical Review, vol. XIII (1916-1917), 330, citing Ford's edition of the Letters of William Lee, vol. II, 417, 666.
 3. Burnett, 330. Jay is referring to a dictionary code (see Sec.C). A "transposed alphabet" is apparently a substitution system in which the cipher alphabet is a reversed standard alphabet.

Another type of cipher, essentially monoalphabetic in character if not in origin, was used by several persons in this period. This employs a sentence or paragraph—all that is necessary is a passage long enough to contain each of the twenty-six letters at least once—in which the letters are numbered in order. Then each plain letter is replaced by the number of that letter. The effect is to produce a cipher alphabet which is a completely mixed sequence. Moreover, variants are provided for the more frequent letters in direct proportion to their respective frequencies in the passage chosen as the key. This type of substitution is said to be found in the papers of Benjamin Franklin in the American Philosophical Society.⁴ The key there used was taken from a long passage in French, containing 682 letters numbered consecutively, which resulted in providing many variants for the more frequent letters.

Another form of monoalphabetic substitution was employed by James Lovell, when he was a member of the Committee on Foreign Affairs, in letters to John Adams, Abigail Adams, and others. In this case the plain alphabet was mixed by writing a key word first and then adding the remaining letters, including the ampersand (&) as a letter after 2. The cipher alphabet was apparently a series of numbers, probably

4. Burnett, 331, citing vol. L(i), p. 24 of the Franklin Papers.

see "History of the Army
Strip Cipher Device" for
true account of M-94.

Invented independently by
Major J. O. Mauborgne in
1917. E. Corder

in numerical order. Burnett (331) describes one example of his use of this alphabet as follows:

Letters in which it is used are found in the Adams manuscripts, June to December, 1781. The key, as suggested by Lovell, was "the first sixth part of that family name where you and I spent our last Evening with your Lady before we sat (sic) out on our Journey hither." The key turns out to be "C R". The name was probably Cranch. A letter from Lovell to General Gates, March 1, 1779 (N. Y. Hist. Soc., Gates Papers), uses the key-word "James."

Robert Livingston used this cipher in his first correspondence with John Adams, who apparently did not understand it.⁵ Thomas Jefferson had also used a cipher of the same type at an earlier period in writing to William Short, the key word then being "Nicholas."⁶ James Madison wrote to Edmund Randolph during the summer and the autumn of 1782 what proved to be the most noteworthy series of letters in this cipher. Errors made by Madison in writing the cipher texts prevented Randolph from deciphering them, but the alphabet was reconstructed on the assumption that certain cipher letters stood for the word "commission," as proved to be true. This is probably the first example of the use of the probably word method in America. Madison's footnote⁷ giving the key word was later found: it was probably, according to Burnett,

5. So Burnett, 331, citing Wharton.

6. Burnett, 331, citing Southern Bivouac, new series, II, 425-427.

7. Burnett (332) does not state where the footnote was found but it seems probable that the key was concealed somewhere in the letter itself.



ms. [unclear]
[unclear]
[unclear]
7

"Cupid," the name of a slave who used to serve Madison.⁸

B. Thomas Jefferson's Cipher Device

In the papers of Thomas Jefferson now in the Library of Congress there has been found a description of a cipher device designed by him at some unknown date.⁹ The device, which anticipated the basic features of another invented independently in the late nineteenth century by Commandant Bazeries, the eminent French cryptographer, and a third invented, also independently, in ¹⁹¹³ 1917 by Parker Hitt, now Colonel, Signal Corps, United States Army, retired, was designed to encipher plain text by providing twenty-five different cipher variants for the single plain sequence. Essentially, the device was a series of ² twenty disks, on the periphery of which mixed cipher alphabets were lettered. The disks could be arranged on central shaft in any agreed upon order, generally according to a key. Then, by revolving each disk, the plain sequence could be formed. Following this, any one of the twenty-five cipher sequences found on the other lines could be set down for transmission. This device was of so high a security that, in the form designed

8. On this point Burnett cites a letter of Randolph to Madison, 5 July 1782, Library of Congress, Ac. 1081.

9. Jefferson Papers, vol. CCXXCII, item 42575, reproduced in a photograph in Articles on Cryptography and Cryptanalysis, reprinted from The Signal Corps Bulletin (Washington, 1942), pp. 190-191, transcribed, ibid. pp. 161-162.

by Colonel Hitt, it was adopted for use by the United States Army as Cipher Device M-94 which became obsolete at only a recent date. Though both Bazeries and Hitt worked without knowledge of the Jefferson paper, the resemblance between the three designs is striking, and to Jefferson must be attributed great credit for designing a device far ahead of its time.

C. The Dictionary Code

Another well-known cryptographic system, the dictionary code, was extensively used during the Revolutionary period. The dictionary code differs from the ordinary code in one respect only: instead of preparing a list of plain equivalents and equating them with a series of arbitrary code groups, a published dictionary is used, the location of the desired word being indicated by the number of the page, column and line desired, a method used by some governments as recently as the First World War.

That such a system be used was proposed by Arthur Lee in a letter dated 3 June 1776 addressed to the Committee of Secret Correspondence¹⁰

miss (reiter)

10. Burnett, 330, citing Force, American Archives, 4th series, vol. VI, p. 625; Wharton, Revolutionary Diplomatic Correspondence, vol. II, 95; Papers of the Continental Congress, No. 83, vol. I, p. 21.



One form of the dictionary code used an arabic numeral for the page symbol, the letters a or b for the column, and a roman numeral for the line. A system of this kind was employed in the correspondence of the brothers, Arthur, Richard Henry, and William Lee, in the years 1777-1779, the base chosen being the 1777 edition of John Entick's New Spelling Dictionary,¹¹ a dictionary suggested for this purpose also by John Jay.¹²

Instead of using a dictionary in this way, other published works could be used, but there is no evidence of any American using such a work except in espionage activity (see Chapter II).

D. Codes

No example of the true code has been found prior to the autumn of 1781 when Robert Livingston became Secretary for Foreign Affairs under the government of the Continental Congress. At that time Livingston had

11. See the letter of Arthur Lee to Richard Henry Lee, 25 November 1777, in the Life of Arthur Lee, vol. II, p. 117. In this work the letter b of the cipher text is usually printed as 6 through error in reading the handwriting. An editorial note in the Letters of William Lee, vol. II, p. 417, deals with this and other ciphers used by William Lee (so Burnett, 330).

12. See above sec. A.

had some forms printed, on one side of which were the numbers from 1 to 1700, and on the other, the alphabetical list of words and syllables. Correspondents then prepared two identical copies of their code, using these convenient blank forms for the purpose.¹³ The Virginia delegates to Congress in 1762 wrote officially to their governor in such a numerical code,¹⁴ the code groups being the numbers 1-846. A great deal of the private correspondence between James Madison and John Randolph during the year 1762 was transmitted in this code.¹⁵ A dictionary code was used by Jefferson and Madison during January and February 1783, but from April 1783 to May 1785, a numerical code was employed, "the key to which has not been found."¹⁶ A code was reconstructed, Burnett does not say by whom, from Madison's decipherments of some of the letters between Jefferson and Madison and this aided in the decipherments of other letters.

In the Writings of Jefferson (ed. Ford) some attempts toward decipherment have been made, but with indifferent success. Not to speak of erroneous renderings of ciphers, some mistaken editorial interpretations call for correction. A foot-note to Jefferson's

-
13. Burnett (332): "A good many ciphered passages in the diplomatic correspondence of the period remain undeciphered. In particular may be mentioned the letters of Livingston to Jay from November 1, 1779 to April 16, 1782."
14. Burnett (332): "The code is found among the Executive Papers in Richmond."
15. Burnett (332).
16. Burnett (332-33).

letter to Madison, March 18, 1785 (Writings, IV.35), suggests that the paragraph relates to Patrick Henry. Jefferson is actually speaking of Lafayette. In his letter of August 11, 1793 (VI. 367), he says: "Just as I had finished so far, 812.15 called on me." A foot-note says: "Edmund Randolph." The cipher means "the President," that is, Washington. In the letter of April 25, 1784 (III. 470) several wrong renderings give quite erroneous suggestions.

During the same period Monroe employed a numerical code of limited extent in a series of letters to Madison. Burnett (333) states that "the interpretation of most of these ciphers was found in the text of the letters," but what this statement means is not clear. It probably means that the plain text of the letters was written under the cipher text in the extant originals. No key has been found, however, for the letters written by Madison and Monroe between May 1785 and May 1786, but even in these cases it was possible to decipher the texts by reconstructing the code from extant decipherments. The codes by which Jefferson and Monroe corresponded between May 1784 and March 1785 are still in existence¹⁷ and permit the reading of letters otherwise undeciphered. Using the printed forms which Robert Livingston es-

17. Burnett (333): "In the Jefferson Papers, 2nd ser., vol. LVII., fol. 172, are three codes, one marked "1st cypher," another "2d cypher," and a third endorsed: "Cypher sent in Col. Monroe's lre (sic) of April 12, 1785." In fact, the latter is a copy of a cipher sent to Jefferson by Monroe July 20, 1784. At the same place is found the alphabetical part of the "2d cipher." The "alphabetical part" is, of course, the encode.

established in 1781, Jefferson constructed a new and more extensive code in the spring of 1785, which was then used in correspondence with Madison and Monroe.¹⁸

"The Culpers", two American patriots whose identity was concealed under this designation engaged in espionage for Washington and used a numerical code in which the group 729 stood for Setauket, Long Island.¹⁹

Shortly after the government of the United States had been set up under the Constitution in 1789, an elaborate code, called a cipher after the terminology then current, was made for official diplomatic use. There is no record of the person or persons who made this code, but as it was said to be based on the "Rossignol cipher,"²⁰ there is some probability that French experts lent their assistance.

The American code contained nearly 1600 digit code groups providing every possible English syllable, several variants for each letter, punctuation marks, and a considerable number for words. Though small, this code at first rendered good service, and was used by the few

18. Burnett (333): "One copy of this code is in the Jefferson papers, 5th ser., vol. XI., fol. 35, and another in the Monroe Papers, vol. XIII., fol. 2926. See Jefferson to Monroe, March 18, 1785, and to Madison, May 11. Jefferson was still using this cipher with Madison in 1793."

19. John C. Fitzpatrick, The Diaries of George Washington 1748-1799. (Boston 1925), vol. II, pp. 208, 214-215.

20. Antoine Rossignol, a sixteenth century cryptographer. See Fletcher Pratt, Secret and Urgent (Garden City, 1942), pp. 127-128.



ministers our government then sent to foreign countries. These men understood the cryptographic processes and knew the value of security but with the close of the Napoleonic Wars, diplomatic matters lost their wartime urgency. When dispatches were sent during peace time, the ordinary diplomatic mails could carry them in comparative safety, as ships were no longer held up by the navies of warring powers with the consequent seizure of all dispatches. On account of this changed situation, the American diplomatic code fell into disuse from 1815 on, to be revived for a short time in 1866.²¹

A good illustration of the lack of interest in cryptographic matters in this period is to be found in a letter of George Washington to the Reverend William Gordon, dated Mount Vernon, 23 December 1788:

As it is really so long since I have had any occasion to make use of a cypher or key to communicate my sentiments to my Correspondents; and as it was so little probable that I should ever have any occasion to express them by such modes in future, I have absolutely mislaid or entirely lost yours, with others. Besides, I have not a single idea to communicate to any person while in Europe; the knowledge of which could give any advantage to those who should be curious enough, or mean enough, to inspect my letters.²²

-
21. Ibid., 128-129, 189-190; John H. Haswell, "Secret writing: the ciphers of the ancients and some of those in modern use," The Century Illustrated Monthly Magazine, vol. LXXXV (1912), p. 88. The source of this information is unknown.
22. John C. Fitzpatrick, The Writings of George Washington (United States Government Printing Office, Washington, 1931-1944), vol. XX, P. 169.




Here is a curious anticipation of the common idea, prevalent in the first decade after the First World War, that the desire to read diplomatic correspondence exhibited traits of a low character.

B. Secret Ink

Prior to the sailing of Silas Deane for France in June 1776, John Jay furnished him with a supply of invisible ink which Jay's elder brother, Sir James Jay, an English physician, had invented. Later, Sir James wrote to Thomas Jefferson, stating that although work in sympathetic inks was not unknown, it still was highly necessary that a new invisible ink be invented before the actual outbreak of hostilities which were then clearly foreseen. He felt that "a fluid might possibly be discovered for invisible writing, which would elude the generally known means of detection, and yet could be rendered visible by a suitable counterpart."²³

Sir James not only furnished supplies of his invisible ink and a chemical preparation for making it legible to his brother John, who gave them to Silas Deane for his French mission, but he also supplied General Washington with this ink. From England, Sir James conveyed

23. Victor Hugo Paltsits, "The Use of Invisible Ink for Secret Writing during the American Revolution," New York Public Library Bulletin, vol. XXIX (1935), p. 362; Haswell, p. 87-88.




in invisible ink "the first authentic account which Congress received, of the determination of the British Ministry to reduce the Colonies to unconditional submission.²⁴ By the same means, Franklin and Deane were informed by mail from London to Paris that Burgoyne was planning to head an expedition from Canada down the Hudson River.

All of the first letters were addressed to "John Jay, Esq., Attorney at Law," as he was the only one who knew the secret. After a time, Sir James was afraid suspicion would be aroused if he wrote only to his brother, John, so letters were written to other members of the family as well. Three or four lines written in black ink would constitute the visible letter. The remaining blank parts of the sheet of paper would be filled with invisible writing, containing intelligence and matters useful to the American cause.

Deane's secret messages were at first boldly addressed to the Committee of Correspondence but later Deane was advised that he had better send the letters to individual members. In the end, he even wrote to fictitious persons. All of these letters were then sent to John Jay who had the developing fluid and would forward the letters to the committee.

"The Culpers" also used a secret ink which required a chemical reagent to produce the secret writing.

24. Paltsits, 362.





CHAPTER II. THE BRITISH SYSTEMS DURING THE REVOLUTION

A. The Clinton Papers

Information concerning types of secret writing used by the British during the Revolution is available in the papers of Sir Henry Clinton, now preserved in the William L. Clements Library, Ann Arbor, Michigan. A short article on these ciphers written by Howard H. Peckham, then a member of the staff of the library, appeared under the title, "British Secret Writing in the Revolution," in the Michigan Alumnus Quarterly Review, " issue of the winter of 1938 (9 November 1938), a reprint of which is available in the Pamphlet Exchange Collection, Library of Congress. Peckham's specialty was not cryptography: his article would have been improved had he been a cryptographer, since in some instances it is difficult to classify the system he is describing from the scanty details given. On the other hand, for most of the British systems Peckham's paper is the only available source. So far as can be determined, the British used during the Revolution the following types of secret writing:

- a. Monoalphabetic substitution;
- b. An unidentified type (possibly a modified Vigenère table);
- c. Grilles;
- d. The dictionary code;
- e. Codes;
- f. Secret ink.

B. Monoalphabetic Substitution

An example of monoalphabetic substitution found in the Clinton

Papers is the following:

plain: A B C D E F G H I K L M N O P Q R S T U
 cipher: 51 52 53 54 55 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74

plain: V W X Y Z
 cipher: 75 76 77 75 78

Note the absence of J and the repetition of 75 as the cipher equivalent of both V and Y. The following message as deciphered exhibits the same type of system but the key is not quite the same:

cipher text: 75 62 55 57 77 68 74 69 71 68 69 68 72 55 54 73 62 55
 plain text: W h e n-y o u-p r o p o s e d-t h e

cipher text: 66 51 73 73 55 71 73 68 66 55 63 73 62 68 74 61 62 73
 plain text: m a t t e r-t o-m e-I-t h o u g h t-

cipher text: 63 62 51 54 60 74 65 65 77 55 76 69 65 51 63 67 55 54
 plain text: I-h a d-f u l l y-e x p l a i n e d-

cipher text: 66 77 72 55 65 60
 plain text: m y s e l f

C. "The Decypher of Mr. L."

Peckham quotes a manuscript note found in the Clinton Papers as follows:

The Decypher of Mr. L

Reversing the alphabet, using the last as the first letter, in the first line, in the second line, using the last but one as the first continuing to drop a letter each line in that manner to o inclusive, then beginning again as at first.

The description is far from clear but it seems possible that the idea was to use a kind of Vigenère table containing a reversed standard.



alphabet instead of a direct alphabet and to use only twenty-four alphabets, the following twelve repeated:

ZYXWVUTSRQPONMLKJINGFEDCBA
 YXWVUTSRQPONMLKJINGFEDCBAZ
 XWVUTSRQPONMLKJINGFEDCBAZY
 WVUTSRQPONMLKJINGFEDCBAZYX
 VUTSRQPONMLKJINGFEDCBAZYXW
 UTSRQPONMLKJINGFEDCBAZYXWV
 TSRQPONMLKJINGFEDCBAZYXWVU
 SRQPONMLKJINGFEDCBAZYXWVUT
 RQPONMLKJINGFEDCBAZYXWVUTS
 QPONMLKJINGFEDCBAZYXWVUTSR
 PONMLKJINGFEDCBAZYXWVUTSRQ
 ONMLKJINGFEDCBAZYXWVUTSRQP

If this is the correct explanation, a key would be necessary but no key is mentioned. Moreover, if only twelve alphabets are used, the keys can be composed of only the letters O to Z inclusive; if so, why there should be a need for a repetition of the square is not clear. Finally, Peckham calls this a transposition. It is therefore impossible to classify the cipher.

Peckham suggests that the "Mr. L." may have been either a British agent named Lawrence, or William Lee, an American agent abroad, of whom mention has already been made in paragraph 1, above, or even James Lovell, the member of the Committee on Foreign Affairs whom Peckham credits with deciphering "nearly all, if not all, of the British code messages intercepted by the Americans." As Peckham suggests, this paper may have been an American document captured by the British. If so, it does not seem to bear any relation to Lovell's monoalphabetic



substitution. The problem needs considerably more investigation of the primary documents.

D. The Grille

The grille was not used by the Americans but was employed by General Clinton to inform Burgoyne that he had sailed to Philadelphia, and that Burgoyne would have to fight his way to Albany and south of that city without the promised reinforcements. Like many other grilles, the letter was prepared so as to involve also the use of open code. The grille was placed on the paper and the secret message written in the openings. Then the grille was removed and the remainder of the paper filled with innocent writing. In this case the grille was an hour glass figure, a particularly weak arrangement, since fairly long fragments of the secret text would remain continuous.

That the British also used a grille cipher of a different sort is clear from evidence in the Clinton Papers, so Peckham says. In this case the grille was the form of the message which was transmitted. A newspaper or book known to be in the possession of the addressee was marked in such a way as to make the cipher text. Then a grille would be cut so as to reveal only the cipher text when it was placed on the page. The difficulty of cutting such a grille would seem to make the idea impracticable. If no book or paper was known to be in the possession of the addressee, the grille and the printed text would have both to be sent to him, perhaps by different messengers and routes.

E. The Dictionary Code

Like the Americans, the British also employed a dictionary code and actually used the very same dictionary for this purpose, John Entick's New Spelling Dictionary in the edition of 1777. Doubtless, this was the most common dictionary available to both sides.

F. Codes

Peckham (127-8) also mentions a small dictionary containing approximately 700 words, including personal and geographical names, arbitrarily arranged so as to have some one-part and some two-part characteristics. The sample he gives is as follows:

above	50
about	51
abound	52
abroad	53

The arrangement continued to be approximately one-part until the number 200 was reached, when the code looked like the following:

destroy	199
detach	200
discourage	1
determine	2
dispatch	3

Security would have been increased by introducing thoroughly two-part characteristics. If the code were used by spies, then it would have the disadvantage of being in danger of capture, and, of course, it was so small as to limit the vocabulary which would be transmitted, since it apparently had no spelling groups.

G. Secret Ink

Though Sir James Jay's secret ink was actually prepared for the Americans in England, the British themselves seem not to have had much success with such ink. The state of chemistry at the time was by no means advanced, and consequently, it was necessary to use the greatest care in handling the secret documents. A letter dated 31 May 1779 from Jonathan Odell to Major John André, of whom more in the next paragraph illustrates the result of neglect and bad handling of secret ink messages:

I assay'd it (the secret ink letter) by the Fire, when to my inexpressible vexation, I found that the paper, having by some accident got damp on the way, had spread the Solution in such manner as to make the writing all one indistinguishable blott (sic), out of which not the half of any line can be made legible. I shall use every diligence to forward a letter to him (the writer), and to instruct him how to guard against the like accident in the future, and hope it will not be long before I shall receive a return.²⁵

H. The Arnold-André treason

The history of the relations of General Benedict Arnold with Major John André are too well known to require repeating in this connection. The reader is referred to an excellent work by Carl Van Doren, The Secret History of the American Revolution (New York, 1941), which is largely based on the papers of Sir Henry Clinton already mentioned as preserved in the William L. Clements Library, Ann Arbor, Michigan. Many

25. Peckham, 127; Carl Van Doren, The Secret History of the American Revolution (New York, 1941), 203.



of these papers contain messages in code and cipher, and some in secret ink.²⁶

André, while still a captain, had corresponded in cipher with "a mild, pliant man" named Joseph Stansbury, who kept a glass and china shop on Front Street in Philadelphia, and Stansbury was selected as one of the intermediaries between Arnold and André. The key was chosen from the fifth Oxford edition of Blackstone's Commentaries on the Laws of England, in four volumes, or from some other equally long book. The method was that already described as a dictionary code, except that the operation of encoding involved a search through the book until the desired word was found, whereas, if a dictionary, alphabetically arranged, had been used, the search would have been much faster. In some instances, invisible ink was also used and in these cases the letter F (for fire) was marked at the top of the letter to indicate that heat was to be applied, or the letter A, to indicate acid. Later, Nathan Bailey's English Dictionary, in the twenty-first, twenty-third or twenty-fifth editions, was also used to supplement Blackstone's Commentaries.

Another intermediary was the Reverend Jonathan Odell, a graduate of the College of New Jersey (now Princeton) and a grandson of its first president. On 26 May 1780 Stansbury wrote Odell that the cipher

26. See also Peckham, op. cit.; Oscar Sherman, Ciphers used by () as told in "Benedict Arnold" (New York, 1931); The American Historical Record (Philadelphia, 1872), vol. 1; John C. Fitzpatrick, The Diaries of George Washington, 1743-1799 (Boston, 1925, vol. II (1771-1785)).

of two letters, now missing, which he had sent, was based on the twenty-fifth edition of Bailey's Dictionary. On 9 June, Odell replied: "Stick to your Oxford Interpreter," in other words Blackstone's Commentaries. Stansbury wrote from Moorestown that same day, telling Odell that Blackstone had its disadvantages and that Bailey was to be preferred.²⁷

These correspondents devised a small code to conceal the names of prominent persons and places. The following appeared in the list:

<u>Plain</u>	<u>Code</u>
Philadelphia	Jerusalem
Detroit	Alexandria
Pittsburgh	Gomorrah
Susquehanna	Jordan
General Washington	St. James
General Sullivan	St. Matthew
General Gates	St. Andrew
General Bird	Judas Iscariot ²⁸
Indians	Pharisees
Congress	Synagogue
Delaware	Red Sea

27. Peckham (131) makes the undocumented statement that the German Foreign Office in 1918 used Clifton's Nouveau Dictionnaire Francais in the same way when sending the famous Zimmermann message to the German ambassador in Mexico. This statement is completely false.

28. An inappropriate name for a man "relatively harmless and innocent." See Peckham (178); Sherwin (278).



CHAPTER III. THE FEDERAL SYSTEMS IN THE CIVIL WAR

A. The Sources

The sources for the present chapter and the next are for the most part the work of eyewitnesses and are, in those instances of primary value. Though they are long since out of print and difficult to obtain, no serious attempt has hitherto been made to assess their value in terms of modern cryptography. They are as follows:

a. Myer's Manual of Signals.—General Albert James Myer (1827-1880) the first Chief Signal Officer of the Army and the man for whom Fort Myer was named, served during the war as signal officer with the Army of the Potomac and also as Signal Officer of the Army, the latter position being roughly comparable in scope to that of the present Chief Signal Officer. Myer's earlier career had been as assistant surgeon, but in the years immediately preceding the war he had been experimenting with signals, aided, among others, by two young officers who later served with considerable distinction in Lee's Army, E. Porter Alexander, signal officer under Beauregard at the first battle of Manassas, later Chief of Artillery of Longstreet's First Corps, Army of Northern Virginia, and J. E. B. Stuart, the famous Confederate cavalry commander. Myer's career as Signal Officer of the Army was stormy; he was relieved on 10 November 1863 and did not regain the position until much later. The story is interestingly told in considerable detail by J. Willard Brown (see below).



Relieved from active duty, Colonel Myer, as he then was, apparently decided to utilize the time for the preparation of a field manual on signals, a subject on which he was undoubtedly the leading authority then living on this continent. In any case, there soon appeared, with a prefatory note dated January 1864, a pamphlet of 148 pages, of which a copy now exists in the Rare Book Collection of the Library of Congress. The title page reads as follows: "A Manual of Signals: for the use of Signal Officers in the field. By Col. Albert J. Myer, Signal Officer of the Army. Washington, D. C. 1864."

The prefatory note already mentioned is printed on a slip attached to the cover and states that a comprehensive work on signals was then in preparation but that the urgency of the war had made it imperative that a part of it be printed in advance for the use of Signal officers in the field. Even so, there was a space to include a good deal of theoretical information on signals but the section on cryptography (pages 114-118) is relatively small and is, for the most part, limited to a description of the cipher disk. The author found space, however, to reprint an article on "Modes and Curiosities of Cipher" which had originally appeared in Harper's Weekly, 19 December 1863 (the article was also included in the second edition of the Manual, pages 302-317). This pamphlet was, then, the first edition of the Manual; only the second has been used in the preparation of this paper, since it is much larger than the first and is identical on every essential point.

The second edition appeared in 1866 and was published by D. Van Nostrand, New York, with the following title: A Manual of Signals, for the use of Signal Officers in the field, and for Military and Naval Students, Military Schools, etc. Subsequent editions, of which there were several, need not concern us here.¹ It is interesting to note that in the library of the Office of the Chief Signal Officer (then Colonel Myer himself) there was in 1872 no copy of the first edition (see Catalogue of the Library, Office Chief Signal-Officer, United States Army, Washington, June 30, 1872: Washington, Government Printing Office, 1872). The material on cryptography in the second edition appears on pages 256-317 and includes two plates of illustrations. It should be pointed out that the plan of the work excluded the historical point of view: Myer was interested only in methods, not in historic events.

b. Plum's history.—In 1882 W. R. Plum, a former captain in the Military Telegraph Corps, published a two-volume work entitled The Military Telegraph during the Civil War in the United States, with an exposition of ancient and modern means of communication, and of the

-
1. In 1868 two editions, one in 1871, one in 1872 and one in 1874, all published by Van Nostrand; an edition appeared in Washington in 1870, and two were printed by the Government Printing Office (1877 and 1879).

Federal and Confederate cipher systems; also a running account of the War between the States (Chicago: Jansen, McClurg & Co., 1882).

Plum's primary interest was, of course, the telegraph, but since the telegraph operators had, during the war, assumed the function of cipher clerks, he gives a good deal of information concerning cryptography. His style, however, leaves much to be desired and the material is not well organized. Specialists in American History regard him as highly inaccurate. The chief passages dealing with cryptography are the second chapter (33-61) and the appendix (370-377), both in the first volume.

c. Brown's history.—J. Willard Brown, who began the war as a private in the Signal Corps but ultimately rose to the rank of lieutenant, was the author of a one-volume record (916 pages quarto) of his experiences, together with much historical material, entitled The Signal Corps, U.S.A., in the War of the Rebellion, with numerous illustrations and maps (Boston: U. S. Veteran Signal Corps Association, 1896). Like Plum, Brown was primarily interested in preparing a volume of reminiscences for the Union veterans, but since he was in the Signal Corps, rather than in the Military Telegraph Corps, his work supplements rather than duplicates Plum's two volumes. Neither Brown nor Plum were historians; their work is a rich source for historical research, rather than history itself.



d. Bates' reminiscences.—David Homer Bates (died 1926) had been from 1861 to 1866 a telegrapher and cipher clerk in the telegraph office maintained in various rooms in the old War Department Building, located on the site of the present State Department. He there came into daily contact with President Lincoln and was an eyewitness of many important events in the course of the war. In 1898 he published a short article in Harper's Weekly (pages 105-109) entitled "A Rebel Cipher Despatch", which has some information on Confederate cryptography. Later he published his reminiscences in a book called Lincoln in the Telegraph Office (New York, Century, 1907)¹.

e. Haswell's article.—John H. Haswell, for many years a State Department employee, published in the Century Magazine, volume LXXIV (1912-1913), pages 83-92, an article entitled "The Ciphers of the Ancients, and some of those in modern use." Haswell is a primary source; he compiled an unpublished history of State Department Communications of which the article is probably an abridgement.

f. Pratt's book.—Fletcher Pratt, the author of numerous articles and books on military subjects, published in 1939 a work called Secret and Urgent (reprinted, Garden City, 1942). This book is entertainingly written and Pratt followed the laudable practice of checking statements found in his sources, even to the extent of making certain that the

1. Parts of this book had already appeared in a series of articles in the Century Magazine, volume LXXIV (New series vol. LII), May to October, 1907. Lincoln in the Telegraph Office was attractively reprinted in 1939 by D. Appleton-Century.

cryptograms used as illustrations are deciphered correctly: his text is frequently more correct than those he has followed, but Pratt possessed no information concerning official cryptographic systems not available in the published books or articles already cited, except that he was much better informed on the history of cryptography than any of the others.

B. The Military Telegraph Corps

When the Civil War began, the electric telegraph had been in use for less than a quarter century (the date of Morse's patent was 1837). In the Crimean War of the preceding decade telegraphy had been used for military purposes for the first time in history: it was now to be given its first thorough trial in combat operations on a large scale. With the development of the military telegraph the present paper is not concerned: the reader is referred to the works of W. R. Plum and David Homer Bates cited in the foreword. Nevertheless, since the personnel of the Military Telegraph Corps served also as cipher clerks and on occasion even as compilers and cryptanalysts, it will be well to give a short account of the founding of the corps.²

2. Apparently, the word "corps" was adopted by the members without authorization: see Plum, vol. I, page vi.

When the war broke out, David Homer Bates was employed as a telegrapher by the Pennsylvania Railroad at Altoona, Pennsylvania. About 22 April 1861 he received a message from Andrew Carnegie, the Superintendent of the Pittsburg Division of the railroad, then temporarily in Washington with Colonel Thomas A. Scott, Assistant Secretary of War and General Manager of Military Railroads and Telegraphs. Carnegie and Scott were organizing governmental control of railroads and telegraphs, and ordered Bates to proceed to Washington with David Strouse, Samuel M. Brown, and Richard O'Brien, also operators for the railroad, to enter the military telegraph service. These four men reported at once to Colonel Scott and were followed by additional operators in May and June.³

These four operators formed on 27 April 1861 the nucleus of the United States Military Telegraph Corps, which had a maximum strength of over 1,500 members, and rendered much important service to the Federal Government during the Civil War. The first superintendent was David Strouse, one of the original four operators, who held that post until October 1861, shortly before his death which was caused, apparently, by tuberculosis, complicated, so Bates implies, by overwork. Strouse was

3. See Bates, Century, 123-125, and his article, "A Rebel Cipher Despatch, one which did not reach Judah P. Benjamin," in Harper's Weekly, June 1898, 105.

succeeded for a short period by James R. Gilmore, and he in turn by Thomas T. Eckert, who remained in charge from 1861 to 1866. Eckert, first a captain, was promoted to major and ultimately to Brevet Brigadier General before the war was over; he took a large part in the apprehension of the persons charged with the Lincoln assassination plot. After the war he became president and later chairman of the board of the Western Union Telegraph Company and was still living at an advanced age in 1907. Brown and O'Brien were soon sent elsewhere as operators but Bates remained in the War Department Telegraph office until 1866. He had thus an unusual opportunity to observe President Lincoln and to gain a first-hand knowledge of the cryptographic systems used for enciphering Lincoln's dispatches. He was aided also by Charles A. Tinker and Albert B. Chandler, who after the war long occupied influential positions in the commercial telegraph companies,⁴ as did Bates himself.

These men continued to serve as operators of the telegraph throughout the war, but they did not participate in the field activities of their comrades in the corps: they laid no wires and were not subject to the dangers of battle. Instead, they mastered the technique of enciphering and deciphering cryptographed dispatches and at times succeeded in solving Confederate ciphers. Bates alone of the four War Department operators has left any memoirs.

4. Bates, *Century*, 127, 132; *Harper's* 105; *Plum*, I, 66-68, 79.

At this point it would be well to point out that the friction which on both sides so frequently interfered with the efficient prosecution of the war did not fail to infect even the Military Telegraph Corps. Plum (I, 59) goes so far as to express in detail his opinion that the telegraph operators were more competent to serve as cipher clerks than staff officers. Surprisingly enough, he suggests that staff officers had during lulls in campaigns very little to do, and therefore attempted to usurp the functions which Plum, rightly or wrongly, believed the privilege of the telegraph operators.⁵ Certainly it can be said at this late date, with the advantage of the experience of two World Wars, that assignment of technical functions, such as cipher work, to personnel not required to do anything else makes for greater efficiency.

Commanding generals themselves undertook on occasion to handle cipher matters with unfortunate results. General Grant, for example, when at La Grange, Tennessee, sent a message in cipher to General Hamilton at the front.⁶ Hamilton was unable to read the message and asked for a repetition. Grant then insisted that the encipherment he had made

5. See the letter of Colonel Anson Stager to General Halleck, 21 January 1864 (Plum II, 171-172) which confirms Plum's feeling. Stager signs the letter as superintendent of the Military Telegraph Corps, a post which was held, according to Bates and Plum, by Major Eckert. Stager seems to have served in a confidential capacity, not clearly defined.

6. Plum, I, 59-60.

was correct but handed over the message to his operator. At another time, Grant went to Knoxville from Nashville and left his operator, S. H. Beckwith, at headquarters in Nashville. Meanwhile, several cipher telegrams arrived at Knoxville, and Grant, unable to read them, gave orders to his operator to give the cipher key to Lieutenant Colonel Cyrus B. Comstock of his staff, so that all future messages could be read. At this juncture, the operator, Beckwith, refused to turn over the key to Comstock.

stating that his orders from the War Department were not to give it to anybody—the commanding general or any one else. I told him I would see whether he would or not. He said that if he did he would be punished. I told him if he did not he most certainly would be punished. Finally, seeing that punishment was certain if he refused longer to obey my order, and being somewhat remote (even if he was not protected altogether from the consequences of his disobedience to his orders) from the War Department, he yielded. When I returned from Knoxville I found quite a commotion. The operator had been reprimanded very severely and ordered to be relieved. I informed the Secretary of War, or his assistant secretary in charge of the telegraph, Stager, that the man could not be relieved, for he had only obeyed my orders. It was absolutely necessary for me to have the cipher, and the man would most certainly have been punished if he had not delivered it; that they would have to punish me if they punished anybody, or words to that effect.⁷

The operator, Beckwith, was unfortunate enough to be in a position where two jurisdictions conflicted. General Grant was, surprisingly enough, unacquainted with the following admirable order:

7. U. S. Grant, Personal Memoirs (New York, 1866), II, 103-105. Grant's memory was then faulty: he calls Comstock a captain.

WAR DEPARTMENT
Washington City, January 1st, 1864.

ORDERED:

That the cipher books issued by the Superintendent of Military Telegraphs be entrusted only to the care of telegraph experts, selected for the duty by the Superintendent of Telegraphs, and approved and appointed by the Secretary of War for duty at the respective headquarters of the Military Departments, and to accompany the armies in the field. The ciphers furnished for this purpose are not to be imparted to anyone, but will be kept by the operator to whom they are entrusted, in strict confidence, and he will be held responsible for their privacy and proper use. They will neither be copied nor used by any other person, without special permission from the Secretary of War. Generals commanding will report to the War Department any default of duty by the cipher operator, but will not allow any staff or other officer to interfere with the operators in the discharge of their duties.

By order of the Secretary of War.
Official: T. S. Bowers, A. A. G.

E. D. Townsend.
A. A. G.

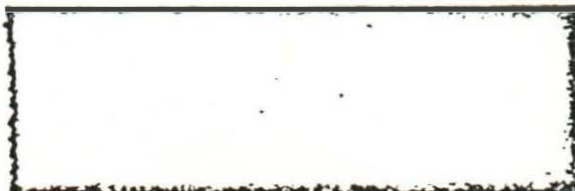
Had Captain Beckwith presented this order to General Grant, the friction would have been avoided; why Grant himself had not already seen it is not clear. In any case, General Halleck's letter to Grant is a masterpiece of exposition:

Head-quarters of the Army.
Washington, January 22, 1864.

Major General Grant, Chattanooga:

I enclose herewith a copy of a note from Colonel Stager, in regard to his instruction to Mr. Beckwith respecting the new cipher. Your telegrams in regard to Lieutenant Colonel Comstock's orders to Mr. Beckwith⁸ have been submitted to the Secretary of War. It was known that the contents of telegrams communicated by means of exist-

8. Just when Beckwith was made a captain is not known.



012 335

ing ciphers, had been made public without authority. As these ciphers had been communicated to a number of persons, the Department was unable to discover the delinquent individual. To obviate this difficulty, a new and very complicated cipher was prepared for communications between you and the War Department, which, by the direction of the Secretary of War, was to be communicated to only two individuals—one at your head-quarters, and one in the War Department. It was to be communicated to no one else—not even to me or any member of my staff. Mr. Beckwith, who was sent to your head-quarters, was directed by the Secretary of War to communicate the cipher to no one. In obeying Colonel Comstock's orders, he disobeyed the Secretary, and has been dismissed. He should have gone to prison, if Colonel Comstock had seen fit to put him there. Instead of forcing the cipher from him in violation of the orders of the War Department, Colonel Comstock should have reported the facts of the case here, for the information of the Secretary of War, who takes the personal supervision and direction of the Military Telegraphs. On account of this cipher having been communicated to Colonel Comstock, the Secretary has directed another to be prepared in its place, which is to be communicated to no one, no matter what his rank, without his special authority. The Secretary does not perceive the necessity for communicating a special cipher, intended only for telegrams to the War Department, to members of your staff, any more than to members of my staff, or to the staff officers of other Generals commanding geographical departments. All your communications with others were conducted through the ordinary cipher. It was intended that Mr. Beckwith should accompany you wherever you required him—transportation being furnished for that purpose. If by any casualty he should be separated from you, communications would be kept up by the ordinary cipher until the vacancy could be supplied. It is to be regretted that Colonel Comstock interfered with the orders of the War Department in this case. As stated in former instructions, if any telegraphic employee should not give satisfaction, he should be reported, and if there be a pressing necessity, he may be suspended; but as the Corps of Telegraphic Operators receive their instructions directly from the Secretary of War, their instructions should not be interfered with, except under very extraordinary circumstances, which should be immediately reported.

Very respectfully, etc.,

H. W. Halleck,
General-in-Chief.

010 336

P. S. Colonel Stager is the confidential agent of the Secretary of War, and directs all telegraphic matters under his orders.

H. W. H.

Grant's reply, likewise, is of great interest:

Head-quarters Military Division of the Mississippi,
Nashville, Tenn., February 4, 1864.

Major General H. W. Halleck,
General-in-Chief, Washington, D. C.:

Your letter of the twenty-second, enclosing a copy of Colonel Stager's, of the twenty-first, to you, is received. I have also circular, or order, dated January 1, 1864, post-marked Washington, January 23, and received on the twenty-ninth. I will state that Beckwith is one of the best of men. He is competent and industrious. In the matter for which he has been dismissed, he only obeyed my orders, and could not have done otherwise than he did and remained. Beckwith has always been employed at head-quarters, as an operator, and I have never thought of taking him with me, except when head-quarters were moved. On the occasion of my going to Knoxville, I received Washington despatches which I could not read until my return to this place. To remedy this for the future, I directed Colonel Comstock to acquaint himself with this cipher. Beckwith desired to telegraph Colonel Stager on the subject before complying with my directions. Not knowing of any order defining who and who alone could be entrusted with the Washington cipher, I then ordered Beckwith to give it to Colonel Comstock, and to inform Colonel Stager of the fact that he had done so. I had no thought in this matter of violating any order, or even wish, of the Secretary of War. I could see no reason why I was not as capable of selecting a proper person to entrust with this secret as Colonel Stager; in fact, thought nothing further of the matter than that Colonel Stager had his operators under such discipline that they were afraid to obey orders from any one but himself, without knowing first his pleasure. Beckwith has been dismissed for obeying my orders. A better man can not be selected for the position. I respectfully ask that Beckwith be restored. When Colonel Stager's directions were received here, the cipher had already been communicated. The order was signed by himself and not by direction of the Secretary of War. It is not necessary for me to state that I am

no stickler for form but will obey any order or wish from any of my superiors, no matter how conveyed, if I know or only think it comes from them. In this instance, I supposed Colonel Stager was acting for himself, and without the knowledge of any one else.

I am, General, very respectfully, your obedient servant,

U. S. Grant, Maj. Gen.

C. The Signal Corps

The work of the Signal Corps, as organized and directed by Major (later Colonel) Albert J. Myer, has been already described in other publications to which the reader is referred for full accounts.⁹ It is sufficient here to point out that there was a sharp cleavage between the assignment of the Signal Corps and that of the Military Telegraph Corps, the former organization confining itself to providing signals by means of flags, lights, and even electrical means for the use of units in the field, while the latter concerned itself primarily with telegraphic communication between less mobile stations. That there was rivalry, at times ill-natured, between the two corps, appears occasionally in the narratives of Plum and Brown.

Myer's great achievement was not, of course, in the field of cryptography:¹⁰ rather is he to be credited with developing in only a few

9. See Historical Sketch of the Signal Corps (1850-1941), Eastern Signal Corps Schools Pamphlet No. 52, Fort Monmouth, New Jersey, 1942, pp. 1-17, and J. Willard Brown, The Signal Corps, U.S.A., 1851-1865 (Boston: U.S. Veterans Signal Corps Association, 1896).

10. Brown (24) says that Myer discussed methods of decipherment with Horace Porter at West Point in 1860 but he gives no details.

years time the science of signals, and with organizing an efficient Signal Corps. His Manual is concerned primarily with visual signals; when he speaks of encipherment, he does so only incidentally because messages to be transmitted often need to be enciphered. He apparently did not realize the fact that the problem of enciphering plain text, whether the message was to be sent by telegraph, by visual signal, or by courier, was largely the same. Had he remembered this simple fact, his description of cryptographic devices would have been much easier to follow. As it is, in illustrating his methods he often converts letters to signals and then reconverts signals to letters before encipherment, finally reconverts enciphered letters once more to signals.

Our knowledge of Federal systems not based on transposition is confined to Myer's Manual: this is because the Military Telegraph Corps uniformly used transpositions. A description of the Federal systems becomes therefore, except for the sections on transpositions, largely a summary of the pertinent paragraphs in Myer's Manual.

D. Monoalphabetic substitutions

The term which heads this paragraph was, of course, unknown to Myer's contemporaries but the section of his book entitled "Cryptograms" (pages 256-266) contains no cipher not included in the term. A word must be said of Myer's type of signal code, the best example of which, for illustrative purposes, is his "Code of Two Elements" (page 80) which

is fundamentally not dissimilar from the Morse Code. Each letter is indicated by a symbol composed of two elements, in this case, the digits 1 and 2. Thus, A = 11, B = 1221, C = 212, etc., and in this way the letters can be converted to a flag movement, a colored light, or any other medium, including the electric telegraph, which the signal officer might choose. But in illustrating his cryptographic systems, Myer selected an eight-element code in which the digits 1 to 8 form dinomes, one for each letter of the alphabet, i.e. A = 12, M = 52, etc. At this point Myer digresses for the moment from the visual signal to one written on paper and carried by hand. He suggests that the arrowhead may be used as a symbol: two sizes of arrowheads may be employed to represent the two-element symbols, and by changing the direction of the arrowheads, symbols for the eight-element code may be provided.¹¹ In enciphering, the process begins first with the conversion of the plain text to the eight-element code, that is, to a series of dinomes, and then converting the dinomes to a sequence of arrowheads. He points out, however, that if a two-element code be used, then the large arrowheads could represent one element, the small ones the other, and the direction could then be varied at will to provide for confusing the enemy. Instead of the arrowheads, a succession of straight and curved

11. This idea seems to have been derived from the cuneiform inscriptions of Babylonia and Assyria which, owing to the fact that they had only recently become known in America, were enjoying a great vogue.

lines may be used, or the message may even be sent in a bouquet of flowers, certain types having been agreed upon in advance or by using different size nails in the shoes of the messenger.¹² He also gives an illustration of the use of his "General Service Homographic Code" (Manual, pages 130-149) to send a message disguised as a commissary memorandum (page 261) as follows:

OFFICE OF THE A.A.C.S.

Memorandum of stores issued.

Pork (bbls.)	2251
Beef (rations)	33,531651
Salt (sacks)	1154
Rations - Coffee	33,421143
Rations - Hard-bread	42,223254

The digits at the right when paired off in twos can be deciphered from the Homographic Code as WE MOVE AT MIDNIGHT.

Still another means of transmitting a message on paper is to draw a series of dancing men, after the manner of the cryptogram in Sir Arthur Conan Doyle's Story of the Dancing Men (see the illustration on page 262). It is possible that Doyle got his idea from Myer's Manual.

That the use of variants increased the security of a message was well understood by Myer who suggests that a cipher based on a two-element

12. Were such methods actually used during the War?



code but using several symbols, either letters or digits, as variants would be preferable. He gives an illustration of a five-element code (Manual, pages 101-111) using letters as variants. This worked as follows (pages 264-5):

element 1: A F K P U V
 element 2: B G L Q W
 element 3: C H M R X
 element 4: D I N S Y
 element 5: E J O T Z

Note the progression in the columns and the position of V. The letter F, which in the five-element code has the value of 12, may be enciphered by any letter in the first line followed by any letter in the second. Thus, there are 30 permutations of a digraph for a single letter. When the first element is not involved, then the permutations are only 25.

To illustrate:

plain text:	F	L	E	E	T
five-element:	12	23	51	51	54
one variant:	FB	QL	TA	ZP	EY
another: ¹³	KW	LR	OF	JR	TI

and so on.

The final monoalphabetic substitution is mentioned by Nyer not because he regarded it as worth recommending but because "it may sometime be encountered". The alphabet is written as follows:

-
13. Thus, the word FLEET might have been enciphered by 4,687,500 different ten-letter combinations without a repetition identical in all ten letters. The fact that E is repeated reduces this figure from 117,187,500.

A B C	D E F	G H I
1 2 3	1 2 3	1 2 3
J K L	M N O	P Q R
1 2 3	1 2 3	1 2 3
S T U	V W X	Y Z
1 2 3	1 2 3	1 2

Each letter was indicated by its number inserted in lines indicating the proper angle, e.g. A = 1, N = 2, etc.¹⁴

E. The Cicher Disk

Myer's section on the cipher disk is entitled "Signalling in Cipher" (Manual, pages 266, 278,¹⁵ plates V¹⁶ and W¹⁷) and the description is as follows:

Description of Signal Disk.—On a small disk of cardboard, or other material (Pl. V, Fig. 1), are written or printed the letters of the alphabet in irregular sequence and arranged around the circumference of the disk. These letters are so placed that when the disk is properly held, all the letters are upright. On this small disk are also printed those combinations of letters which frequently occur in words, as "tion", "ing", "ous", etc., and a sign to mark "the end of a word". On a larger disk are written or printed arranged around its circumference in the same manner, either the letters of the alphabet or the symbolic numbers of signals which are to be used.

The disks are fastened concentrically together in such a manner that one may revolve upon the other, and that they may be clamped in any position. They are of such sizes that, when so fastened, the letters, etc. upon the inner disk, will each appear close to and directly opposite one of the signal combinations upon the outer disk. (See Plate V, Fig. 1).

14. This type of cipher is called the "Rosicrucian or pig-pen cipher" by Fletcher Pratt, Secret and Urgent (Garden City, 1942), 142.

15. Reprinted, without acknowledgment, by Brown, 99-101.

16. See Figure 1.

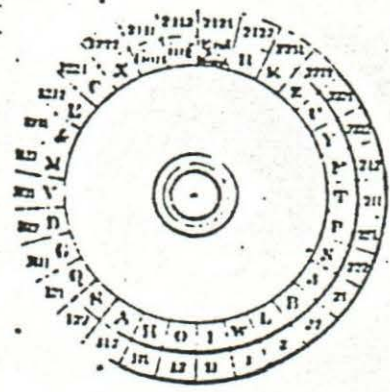
17. See Figure 2





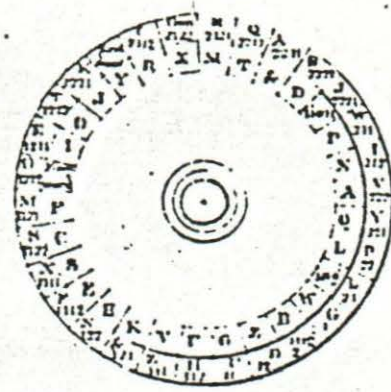
PLATE V.

Figure 1



Two Discs.

Figure 2

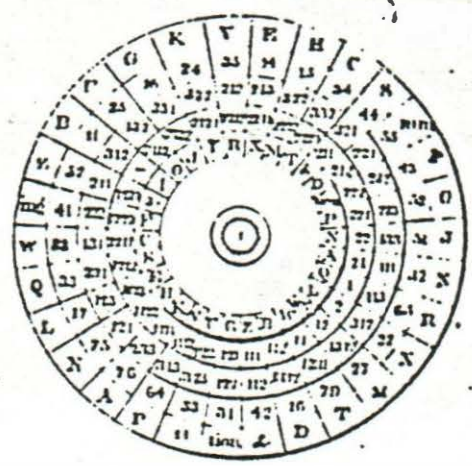


Two Discs.

Vertical Section
Figure 3



Figure 4



Plan for Service Discs.

Vertical section exhibiting plan for four Discs

Figure 5.

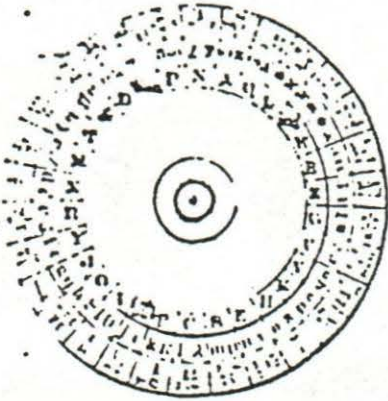


Figure 1. Myer's Manual, Plate V



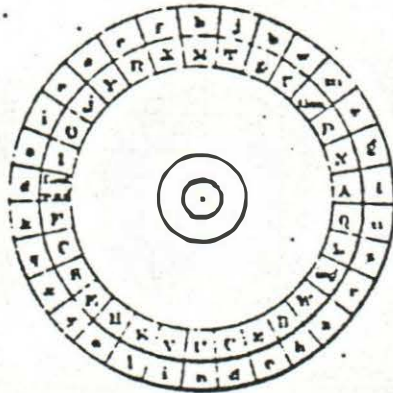
PLATE W.

Fig. 1.



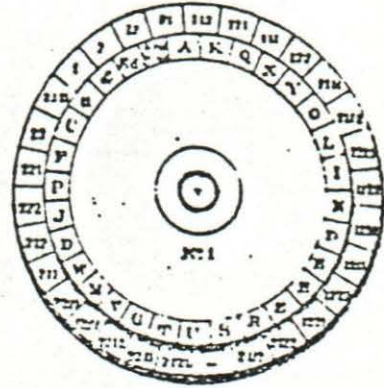
Discs for Cryptographic writing.

Fig. 2.



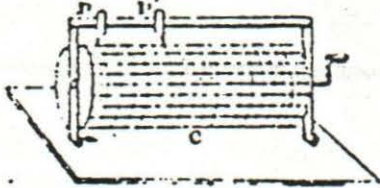
Discs cut from writing paper.

Fig. 3.



Seven large & seven small discs joined.

Fig. 4.



Cylinder Reel.

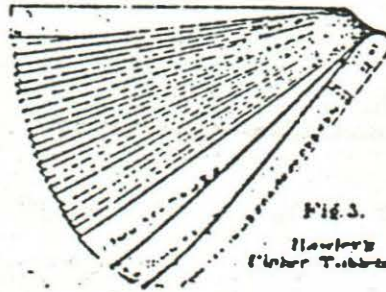


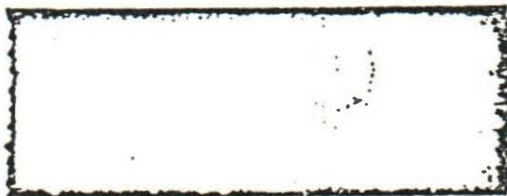
Fig. 5.

Hawley's
Cipher Tablets

Vertical Section
Fig. 6.



Figure 2. Myer's Manual, Plate W



The figures "1" and "6" are sometimes used instead of the figures "1" and "2", to symbolize the elements "one" and "two" because the figure "6" is upright in most positions on the disks.

Having a disk arranged and clamped as at Fig. 1, Plate V, it will be clearly understood by any signalist that so provided he has before him an alphabetic code with every letter opposite its signal symbols. And he will comprehend that, by referring to the disk, he can transmit it in secret signals or cipher by moving the disks upon each other, and so make changes in the code.¹⁸

The use of such a disk requires, of course, that both the sender and the recipient know the key. The most secure way of effecting this would be to have the keys determined by a central bureau and made known to the signal officers by some publication. This possibility was not overlooked by Myer but, surprisingly enough, he seems to have intended the keys to be chosen at will and the key indicated to the recipient at the beginning of the transmission of a message! Under the conditions of field signalling during the Civil War, it would often happen that an enemy signal officer might easily intercept such a message, key and all. That the Confederates were unaware of the general character of Myer's systems of signalling is impossible. The Confederate signal service was organized at the outbreak of the war by Captain (later General)

18. Rules for the use of the disk are given in the Manual, 269-273. More complicated disks than the one described are discussed: they all utilize the same basic principles. J. Wyatt Reid (Manual, 287) had prepared a brass disk in which the letters were detachable for changing the alphabetic sequences.

E. Porter Alexander, who had been associated with Major Myer in the old Army while the latter was devising his signals.¹⁹ Moreover, it seems improbable that at no time the Confederates captured one of the cipher disks. If Myer knew of this, then his confidence in the security of the disk after the war shows how little the possibility of cryptanalysis was understood at the time.

One of the weaknesses of the disk was, of course, the abnormally high frequency of the signal standing for "end of word". Sergeant Francis M. Metcalf²⁰ realized this and called attention to it in 1864. To obviate the difficulty, one had only to eliminate the signal, running the words together, but this seems not to have occurred to Metcalf, who, instead, invented a four-disk device,²¹ the first and second having the letters (an alphabet plus &, "tion", "ing" and "end of word"), fifteen on each disk, and the third and fourth the signals; but before completing his experiments with the disk, he discovered that it would be better to place all the letters on the inner disk and the signals on the three outer disks, ten on each. In forwarding Metcalf's cipher to Washington, Captain L. B. Norton emphasized the weakness of the "end of word" signal and his suggestion that it be omitted was apparently adopted.

19. See Brown, 213.

20. See Brown, 118-119.

21. This may have been similar to the five-disk device shown in Myer's Manual, plate V, fig. 5, which has a second alphabet on the outermost disk.



070 247

F. Polyalphabetic substitutions

Yet the vulnerability of monoalphabetic substitutions such as would be produced by the cipher disk was to some extent realized—Poe's story, The Gold Bug, probably was sufficient demonstration, for L'yer (pages 273-277) advises the user of the disk to change key in the middle of the message, and specifically, at the end of each word.²² This would produce a kind of polyalphabetic substitution, and would delay a cryptanalyst to some extent. An alternative way of changing the key would be to use a key word—L'yer calls this a "countersign word"—such as BALTIMORE, GERMANIC HOSTS, and the like. In this way, each letter of the key would determine the setting of the disk for a single word or for two consecutive words. Care should be taken to choose keys in which letters were not repeated.²³ L'yer advises that the sentence be reversed before enciphering, or that at least the clauses be reversed. He appears never to have reached the point where he realized that the observance of the word lengths was a weakness. The following is his illustration of the cipher disk used with the key word MOHICAN:

Key	M	O	H	I	C	A	N
Plain text:	The	enemy	have	crossed	the	river.	Send a

22. Much to the surprise of the modern reader, L'yer (page 278) actually mentions as a permitted practice the inclusion of plain text in a cipher message!

23. Confederate keys (see Par. 13) overlooked this point.

Key: C A N
 Plain text: cavalry force to his rear.

When the cipher disk is set at N = 11, the following is the cipher text:

FIV GVEVNH GRPINGZUSERRINGK NINGK QIFOCEZFC. UDR & QNJDJITDRPTNZ
 INGIJTION..Q IQFL

Note the repetitions of ING and the combination TION which result from the fact that the outer ring of the disk, having the two-element code written on it, has been used as the plain alphabet, and the inner ring, which has the combinations TION and ING, as a cipher alphabet. The four examples of cipher ING stand for different plain letters in each case.

Another way of producing this kind of polyalphabetic substitution involves the signal on the disk called "end of word" which Myer calls "the front signal" from the notion of the flag indicating it. In the preceding examples, the "end of word" signal would have its obvious plain value, but it could also be used as the cipher equivalent of whatever letter happens to be opposite it, and some other combination be agreed upon as the signal for "end of word", and also as a switch group.

The possibility of making rings for special purposes is mentioned and also of using Greek and Hebrew letters in place of the Roman. (Presumably, the chaplains would be called upon to assist signal officers!) Moreover, it is suggested that rings can be made to be used according to the days of the week, or the disk may be provided with variants.

G. Hawley's Cipher Device

Sergeant Edwin H. Hawley, of the Signal Corps, devised a "very ingenious and valuable plan of cipher".

The apparatus consists of twenty-six long and narrow tablets fastened together at one end, arranged as the tablets or strips of some kinds of wooden fans. On each tablet is inscribed an alphabet and the numeral signals for its letters, and the combination of letters generally used. The alphabets are so arranged that the alphabet on the first strip commences with the letter A and its signal at the top of the strip; the letter B and its signal are at the top of the second strip, and so on. In enciphering a message, a key-word being given, the alphabets and signals upon these tablets are used, each being taken in such sequence as are indicated by the letters of the key-words.

The device produced, of course, no other effect than that of polyalphabetic substitution using different sliding alphabets based on a key word.²⁴

H. Anton's Cipher Device

Private John C. Anton, of the Signal Corps, was the inventor of a cipher table²⁵ which he intended to be marked on tin or leather, or some other durable material. The table is nothing more than a series of direct standard alphabets to which the polygraphs tion, ing, and, and a dash have been added. These are placed as follows:

- | | | | | | | |
|-----|-----------------------|------|-----|-----|---|----------------|
| I. | FCHIJKLMNOPQRSTUVWXYZ | tion | ing | and | — | ABCDE |
| II | JKLMNOPQRSTUVWXYZ | tion | ing | and | — | ABCDEFCHI |
| III | STUVWXYZ | tion | ing | and | — | ABCDEFGHIJKLMN |
| IV | OPQRSTUVWXYZ | tion | ing | and | — | ABCDEFGHIJKLM |
| V | UVWXYZ | tion | ing | and | — | ABCDEFGHIJKLMN |

24. Manual, 267-8; Brown, 118.

25. Manual, 286-291.

Above these five alphabets is a row containing the signals, e.g. 1, 8, 11, 18, etc., and below them a row contains numerals, e.g. 10, 20, 30, etc.; 1, 2, 3, etc.; 200, 300, 400, etc.; up to 20,000. A final row contains signals for "Are you ready?" and the like. The transmitter establishes communication and first signals the number of the initial alphabet, or it has been agreed that alphabet "I" will be used to start every message. Then the first letter of the plain text is found in alphabet "I" and the signal taken from the top row of that column. The second plain letter is found and the signal likewise taken from the top row of that column. Before and after numerals or abbreviations, the signals are, respectively, 11811 and 82183. This cipher table will have the same effect as that produced by Hawley's device, but is inferior to it in that only five cipher alphabets are used, whereas in Hawley's device there are twenty-five which can be chosen according to a key word, permitting a large variety of polyalphabetic substitutions.

I. The Navy Cipher Disk

Haswell²⁶ states, without citing his authority that during the Civil War and until the eighties the United States Navy used a cipher disk. The description shows that this was identical with the simpler disks

26. Century LXXXIV (1912), 90.

described by Myer and produced only monoalphabetic substitution. It was supplanted by a digit code.

J. Route Transposition

Of all the ciphers suggested by Myer, route transpositions are ostensibly, at least, the weakest, since the units transposed are not letters but whole words. Basically, the method was this: by preconcerted arrangement it has been decided that a rectangle four columns wide is to be used; and the number of rows is determined, of course, by the length of the message which it is desired to send. In addition, the route has been agreed upon and is, for this illustration, down the first column, up the fourth, down the second, and up the third. Every fifth word is to be a null ("blind word") inserted to cause confusion. Myer's example is as follows:

Plain text inscribed

The	night.	Smith	the
enemy	Deserters	retreating	during
has	say	is	position
changed	that	he	his

Inscription is according to the route agreed upon, transcription is normal.

The cipher text, with the nulls inserted, as as follows in Myer's version:

The night. Smith the attacking enemy Deserters retreating
during summer has say is position unchanged changed that he his him.

The words "attacking," "summer", "unchanged" and "him" are nulls, but Myer has inadvertently transposed "changed" with "unchanged". The use of capital-



ization and punctuation is, of course, very vulnerable. The capital letters of "The" and of "Deserters" show that these words begin sentences, the period after "night" shows that this word is final. Even without these telltale hints, the ingenious reader could easily proceed with the analysis and soon reach solution.

In spite of the criticism which can be justly made of the weak security in this type of transposition, the Federal cipher operators constantly made use of only slightly more complicated forms of the system and with great success, as they claimed, since they never knew of any solutions made by Confederate agents. The system was first devised by Anson Stager,²⁷ a telegrapher who was later commissioned and rose to be a General Officer. In 1861 Governor Dennison of Ohio had asked Stager to arrange telegraphic facilities and to prepare a cipher so that the governors of Ohio, Indiana, and Illinois, could conduct secret communications one with another. All that is known of this cipher—Plum and Bates apparently never saw it—is that it was "doubtless the first telegraphic cipher used for war purposes".²⁸

Stager was a little later asked by General McClellan to prepare a cipher for his use during the campaign in West Virginia, prior to the general's coming to Washington in the summer of 1861. It is known that Stager based this McClellan cipher, which was afterwards adopted as the

27. Plum, I, 44; Bates, Century, 290.

28. Evidently, cipher had not been used by telegraphers in the Crimean War.

official cipher of the War Department, on his earlier work made at the instance of Governor Dennison.²⁹ From the description, it is clear that basically the new cipher was similar to modern columnar transposition except that it was a transposition of words, not of letters, and it used nulls. One of the first copies was given to the famous detective, Allan C. Pinkerton, for use in Kentucky.³⁰

Judged by the standards of its own day, this cipher was adequate: it was not too complex to be practicable, and yet it delayed solution for a sufficient time. Though Myer's illustration of the system involves nothing but word transposition with the insertion of nulls, the system as actually used during the war added to this the element of code, though that word was not used at the time. A list of code words, in the modern sense, called by contemporary writers, "arbitraries," was prepared, and the users of the cipher assigned to these code words values made from lists of place names, personal names, and, on occasion, frequent common nouns and phrases. Stager's system, then, was really a combination of code and route transposition cipher. The user was given a printed card, about three by five inches in size, on which were printed the code words and the keys. The keys were known as "commencement words", a term which also included the "check words" which was the designation of what are now called nulls. The first column

29. See Plum, I, 44; John H. Haswell, "Secret Writing", The Century Illustrated Monthly Magazine, LXXXV (1912). p. 91.

30. Plum, I, 44-45; Pratt, Secret and Urgent 178.



contained the key words indicating the number of lines in the message, the second column the nulls, while the remaining columns contained the code words which, incidentally, included in some cases variants for words of such frequent occurrence as the names of the President, cabinet officers, important generals, and the like. The heading of the message was regularly subjected to encipherment as well as to the text. In addition, the route of the transposition was indicated on the card. Why it was thought necessary to indicate the number of lines in the message is not clear; since the number of columns was in each message the same (six), the dimensions of the rectangle, which was always filled by the addition of the necessary number of nulls at the end, could be determined without an indicator of the number of lines. If, for example, a message of 54 words were received, it was a foregone conclusion, even without an indicator for the number of lines, that there would be nine lines in all.³¹ Had the compiler intended the user to construct rectangles of varying width, as was certainly done in later writing, then the indicator would be necessary, but in that case additional information as to route must also be agreed upon.

Plum (page 44) makes the definite statement in regard to the cipher devised by Stager for McClellan that in this case the route, number of columns, and names of the holders did not appear on the card, being orally

31. Bates (Century, 290) shows clearly that he understood the essentially rectangular nature of the transposition and he also realized that the system was crude. He wrote, however, over forty years after the war, and as he was then a telegraph official, he was in a position in 1907 to know something of the advances made in cryptography during the interim. He regarded Plum's work as adequate and therefore confined himself to giving such details as bore directly on his subject, Abraham Lincoln.

communicated, but Bates (Century, page 292) prints a facsimile of another of these cards used as early as 1861 which does have indication of the route and instructions as to use. It is probable that Stager at first omitted such significant details because they could be orally arranged: when this type of system was produced in quantity, then the necessary details were added.

Colonel J. J. S. Wilson, one of the officers of the Military Telegraph Corps, carried the small card which was used not only during McClellan's campaign in West Virginia, but also in Anderson's early operations in Kentucky, and in Fremont's campaign farther west. It seems certain that this card was identical with Stager's cipher prepared for McClellan. The following is an exact copy (see Plum, I, 44-45).

COLLECEMENT WORDS.

ARBITRARY WORDS.

Cipher Words.					
1 Mail.	Check..	Scott.	55 Bagdad.	6 Dennison.	London.
2 May.	Charge.	McClellan.	Mecca.	Curtin.	Vienna.
3 August.	Change.	Steedman.	Bremen.	Private.	Star.
4 March.	Cheap.	Kelly.	Berlin.	Bird's Pt.	Uncle.
5 June.	Church.	Yates.	Dublin.	Columbus, Ky.	Danube.
6 April.	Caps.	Bates.	Turin.	Memphis.	Darien.
7 July.	Show.	Morris.	Venice.	Paducah.	Darby.
8 Telegraph.	Sharp.	Cox.	Brussels.	Mound City.	Geneva.
9 Marine.	Shave.	Washington.	Ninrod.	Navy Yard.	Mexico.
10 Board.	Shut.	Parkersburg.	Cain.	Pillow.	Brazil.
11 Account.	Ship.	Cornwallis.	Abel.	Ben. M'Cullough	Grenada.
12 Director.	Shields.	Smithton.	Kane.	Fremont.	Paris.
13 President.	Poles.	Clarksburg.	Noah.	Hunter.	Moscow.
14 Central.	Tools.	Grafton.	Lot.	Grant.	Arabia.
15 January.	Glass.	Cumberland.	Jonah.	Gen. Smith.	Baltic.
16 Buffalo.	Pet.	Wheeling.	Peter.	Gen. Payne.	Britain.
17 Pittsburg.	Vile.	Fairmount.	Paul.	Gen. McCellan.	Egypt.
18 Cleveland.	Base.	Horner's Ferry.	Judas.	Gen. Allen.	Negro.
19 Rochester.	Miscreant.	Cumberland.	Job.		
20 Audit.	Scoundrel.	Martinsburg.	Joe.		
21 Company.	Scamp.	Richmond.	Frank.		
22 Station.	Thief.	Cairo.	Sam.		
23 Report.	Puppy.	St. Louis.	Ham.		
24 December.	Gentleman.	Marietta.	Shen.		
25 Boston.	Nobleman.	Prentiss.	Mary.		
26 Balance.	Just.	Lyon.	France.		
27 Refund.		Blair.	Rome.		
28 Debtor.		Pope.	Niagara.		
29 Creditor.		Morton.	Peru.		
30 Abstract.					
31 United.					
32 Annual.					
33 Duplicate.					

No. lines.³²

32. That is, the words above are the indicators of the number of lines. Certain traces of one-part arrangement may be seen in the second column. This is probably accidental. It is possible that the second column of "cipher words" was meant to be used as nulls, rather than as variants of the indicators for number of lines. The use of "check" as the first word suggests this.

002 057

The following is an example (Plum, I, 45-46) of a message enciphered by this system:

Text as received by addressee

To Maj. Gen. G. W. McClellan,³³ Parkersburg, Va., June 1, 1861.
Cincinnati, Ohio:

Telegraph the have be not I hands profane right hired held
must start my cowardly to an responsible Crittenden to at polite
ascertain engine for Colonel desiring demands curse the to success
by not reputation nasty state go of superseded Crittenden past kind
of up this being Colonel my just the road division since advance
sir kill.

(Signed) F. W. Lander.³⁴

The recipient proceeded to the decipherment by noting from his card the indicator of the number of lines: Telegraph = eight lines. A rectangle of six columns and eight lines was then constructed, and a seventh column was added to provide for the nulls which were every seventh word. Then the cipher text was written in the rectangle in normal order as follows:

<u>1</u>	<u>2</u>	<u>3</u>	<u>4</u>	<u>5</u>	<u>6</u>	<u>nulls</u>
the	have	be	not	I	hands	profane
right	hired	held	must	start	my	cowardly
to	an	responsible	Crittenden	to	at	polite
ascertain	engine	for	Colonel	desiring	demands	curse
the	to	success	by	not	reputation	nasty
state	go	of	superseded	Crittenden	past	kind
of	up	this	being	Colonel	my	just
the	road	division	since	advance	sir	kill

The message was now read by columns: up the sixth, down the first, up the

33. Note that McClellan's middle initial is incorrect.

34. See Plum, I, 45-46.

fifth, down the second, up the fourth, and down the third.³⁵

The cipher text then becomes in plain language the following:

Sir:

My past reputation demands at my hands the right to ascertain the state of the advance. Colonel Crittenden not desiring to start, I have hired an engine to go up road. Since being superseded by Colonel Crittenden, must not be held responsible for success of this division.

In this example, no word has been intentionally misspelled, but as the cipher operators developed maturity, the device of nonstandard spelling was frequently used to increase the confusion, e.g. meet becomes meat or even flesh, wood is used in place of would.

Stager, the originator of the system, appears to have continued to compile new editions of his route-transposition cipher as necessary, aided by the practical experience of men like Major Eckert, Bates, Chandler, and Tinker, and also by operators in the field, like Beckwith. Successive editions embodied constant improvements, including ever-increasing lists of code words, longer lists of nulls, and variations of the routes. Non-standard spellings were probably used at the discretion of the cipher clerks since the interpretation of such a spelling would be comparatively easy, once the route was known. As the ciphers increased in complexity, the old form of a card was abandoned and a pamphlet substituted for it. Twelve pocket-sized editions were printed, the first containing sixteen, the last of the series 48 printed pages.

35. Plum states that this "was the only route used in this cipher." He means, of course, the only route used with this particular card. The facsimile already referred to (Bates, Century, page 292) employs a route quite different: up the third, down the fourth, up the sixth, down the first, up the fifth, and down the second.

The earliest were designated Ciphers Nos. 6 and 7,³⁶ and were introduced in 1861. They were patterned closely after the first cipher devised by Stager, and were used for General Buell's early operations in Kentucky and Tennessee, and also for General Halleck's operations prior to the occupation of Corinth, Mississippi. Cipher No. 6 was a simple elaboration of the original cipher, the column routes and the general arrangement being left the same. The indicators, however, no longer represented the numbers of lines but the number of words in the message, e.g. mail meant six; May, twelve; August, eighteen words in the message; in modern parlance, they were a group count. This change probably reflects realization of the fact that when the number of columns did not vary, there was no real need for an indicator; the compilers were apparently not yet ready to abandon their indicator system, so they used it for a group count.

Cipher No. 7 was very similar to Cipher No. 6 but the indicators once more were used to represent the number of lines and there were indicators for as many as twenty lines: evidently dispatches were getting longer. Both of these ciphers were discarded in 1862 when one of the operators was captured with the ciphers on his person.³⁷

36. Plum, I, 47-48.

37. This was Brooks, captured by General John H. Morgan at Gallatin, Tennessee, in August 1862 (see Plum, I, 47).

An example (Plum, I, 47-48) of a message enciphered by Cipher No. 7 is as follows:

Text as received by addressee

Colonel Anson Stager, Washington:³⁸

Austria await I in over to requiring orders olden rapture blissful for your instant command turned and instructions and rough looking further shall further the Camden me of ocean September poker twenty I the to I command obedience repair orders quickly pretty Indianapolis your him accordingly my fourth received 1862 wounded nine have twenty turn have to to to alvord hasty.

William H. Drake.³⁹

The word Austria was the indicator of a message in nine lines, with the route up the first, down the sixth, up the second, down the third, up the fifth, and down the fourth column. When the text as received had been inscribed normally, transcription of the plain text was by the route indicated. The plain text is as follows:

Louisville, Ky., September 29, 1862.

Maj.-Gen. Halleck, General in Chief:

I have received your orders of the 24th inst., requiring me to turn over my command to Maj.-Gen. G. H. Thomas. I have accordingly turned over the command to him, and in further obedience to your instructions, I shall repair to Indianapolis and await further orders.

D. C. Buell,
Major-General.⁴⁰

38. For some time all telegrams sent to officers in Washington were addressed to Colonel Stager. They were then deciphered by the clerks and the text forwarded to the addressee whose name had been enciphered.

39. The name of the cipher clerk who prepared the message.

40. Plum, 48.

Q.2 081

Cipher No. 12⁴¹ adopted in 1862, marked a great improvement over its predecessors and remained in force until August 1864. It contained code words for each hour and each half-hour of the day; for the names of all prominent Federal and Confederate civil, military, and naval officials; for the names of all the States; and even for words and phrases in common use in messages. Stephen L. Robinson, a cipher clerk with General Smith, was captured in July 1864 by guerillas (see Plum, I, 49) and Cipher No. 12 was thus compromised and abandoned. In addition to abundant provision for indicators of the number of lines, there was a page of indicators to be used with a transposition not based on routes of the type already discussed but a somewhat different route to be described below.

The following is an example of a message enciphered by Cipher No. 12 using a route of the more conventional type:

Text as received by addressee

To George C. Kaynard, Washington

Regulars ordered of my to public out suspending received
1862 spoiled thirty I dispatch command (sic) of continue of
best otherwise worst Arabia my command discharge duty of my
last for Lincoln September period your from sense shall duties
the until Seward ability to the I a removal evening Adam herald
tribune.

Philip Bruner,⁴²

When deciphered by the route and rectangle prescribed by the indicator

"Regulars" this message becomes:

41. See Plum, I, 48-52.

42. Plum, I, 49-50.

Louisville, Ky., September 30, 1862.

General Halleck:

I received last evening your dispatch suspending my removal from command. Out of a sense of public duty, I shall continue to discharge the duties of my command to the best of my ability until otherwise ordered.

D. C. Buell,
Major General.

Note that in the case of this message the encipherer inscribed the plain text normally and transcribed it according to the route: up the fourth, down the third, up the fifth, down the second, and up the first columns. The nulls were placed at the end of each column. Moreover, this message in Cipher No. 12 was sent only one day after Buell's message of 29 September 1862 which was enciphered by No. 7. Perhaps the two were used simultaneously at Buell's headquarters.

In January 1863 it was considered advisable for security reasons to substitute for Cipher No. 12 a new system, but distribution of the replacement was apparently confined to the Western Department. Cipher No. 9⁴³ was therefore compiled and delivered, but No. 12 was left in general use, No. 9 being used only in the Western Department.⁴⁴ The code words for intervals of time in No. 9 were girls' names, and there was provision for the names of all Federal governors. A wide variety of different routes was provided.

43. This cipher is printed in full in the appendix to Plum's first volume (370-377). See also I, 52 for Plum's description.

44. No. 10 followed a few months later.

One of these was devised by Stager, so Plum (I, 50-51) says, as the result of a conversation he had with a reformed gambler. The gambler had told him of a card trick by which he was able to identify cards through the use of a key sequence which was as follows:

13-8-4-2-12-7-9-5-11-3-6-1-10

Apparently the gambler had used this key sequence to effect a transposition of a simpler type:

Key: 13 8 4 2 12 7 9

Plain text: I am going home on today's express.

Key: 5 11 3 6 1 10

Plain text: Please meet me on arrival there.

Transposing words, the cipher text becomes:

			1	2	3	4	5	6	7	
Jack	(indicator)	arrival	home	me	going	please	on	today's		
8	9	10	11	12	13					
am	express	there	meet	on	I.					

Stager developed this simple idea much further and inserted the device into ciphers nos. 12, 9, and 10 in the following manner:

MESSAGE OR PART OF MESSAGE⁴⁵
 Six column route
 Indicators: Stanton
 McClellan
 McDowell

45. Plum, I, 51.

x			x	x	x
6	17	27	36	26	16
7	5	28	35	25	15
8	18	4	34	24	14
9	19	29	3	23	13
10	20	30	33	2	12
11	21	31	32	22	1
x	x	x			

The letter x marks the location of nulls. Note the diagonal across the rectangle. The route then followed the progression of the numbers. The following is an example of this cipher:

Text as received by addressee

Washington, July 15, 1863.

To W. G. Fuller, Memphis, Tenn.:

Clara McClellan applause query spare safe occupied for present sufficiently your forces prentiss if the world valley the render have caught bear line you to he hard chorus to all to zebras run if the can operate wafers lean towards on send wiley blubber up.

T. T. Eckert.⁴⁶

In this message, the word "Clara" meant 10:30 A.M. and "McClellan" was the indicator. The decipherment becomes therefore:

Washington, 10:30 A.M., July 15, 1863.

For Genl S. A. Hurlbut, Memphis:

If Gen. W. T. Sherman's movements have sufficiently occupied the enemy to render your line safe, send ll the forces you can spare to Brig.-Gen. Prentiss to operate on Price's rear if he advances toward Missouri.

H. W. Halleck
Maj.-Gen'l.



Captain S. H. Beckwith, cipher operator for General Grant, while at Memphis made a single key book to contain all three ciphers, using black ink for No. 12, blue ink for No. 9, and red ink for No. 10. Since the key indicators and the code words were identical in all three ciphers, all that was necessary to change from one key to the next was to use the writing in a different color. Bates (Century, 293) reproduces as an illustration two pages of Beckwith's copy of the last cipher used. At the bottom of the page are two phrases with digits as follows:

Page IX

4	2	6		8			
K	I	S	S	A	L	A	D
	1			9	5		7
							3

Page X

2	6			4	10	8	
T	I	E	H	E	R	S	H
		9	5	1			7
							3

This is probably only an ingenious method of indicating the route. He also was able to suggest many plain equivalents for future editions.

Cipher No. 9 was supplanted by Cipher No. 1⁴⁷ in which were sent, so Plum states, more important telegrams than in any other cipher. Compiled in 1862, it did not come into general use until February 1864.

47. Plum, I, 52-55. Apparently No. 10 was not abandoned simultaneously with No. 9.

The pamphlet in which it was printed contained twenty-five pages. One page was devoted to code words for time intervals; six contained indicators, and there were variants for each indicator, and nearly 900 code words, of which the following are a few:

Adam	Maine
Animal	Fort Monroe
Apple	Fort Sumter
Arno	Arkansas
Attica	Potomac
Berlin	Red River
Bologna (and seven variants)	President Lincoln
Bruno (and five variants)	Secretary of War

There were also code words for arms, brigadier general, by way of, cavalry, defeat-ed-ing, movement, surprise, regiment, troops, encountered the enemy in strong force, etc. This code had clearly passed the rudimentary stage. Cipher No. 2, not so widely distributed as No. 1, was identical in code words and indicators but the values were assigned differently.

An interesting message enciphered by No. 2 is as follows:

New Orleans, June 19, 1864

To Albert B. Chandler, War Department, Washington:

McDowell unsound returned vessel period was pine squad also store this nay of Russell hot ginger revenue for leave to brocade this each revenue at wonderful feat your tulip flower Baker violet side date houses at of by former he cant audit bale they in possibly quack about sun bale mason Saint Luke f burning shreve byrne and party place F shreve Fremont Dayton law cipher Austin black at picked proposes a happy marriage Cupid made fork French etc. and or in about the same port T yardstick wilby Honduras and port the T Morgan sailed for Peru spit with boats fraction Arnold male like is volunteers resist surprise sometimes good Stephen of a on Ben freckled or clear Downing swallow recently Stephen little nose hand deal they feel hot poplar spits inside the above scars atop slim George Clarke phased has probably and sulphur of a close call Windham all thum head are

073 257

spit as swallow swallow Jonah inches Browne cut side behind and
 spit while ware rooms awful in he on at head leave tash slender
 girl built mouse two topoph also also yacht wilby mastiff flower
 pistils conversing the four the and so hare high flyer.

S. P. Kimber.⁴⁸

The first word "McDowell" indicated a rectangle of ten columns; the second "unsound" that it had two lines and the third "returned," that it had eight, making ten in all. (By inadvertence Plum's text omitted the word "returned.") The route used was up the fifth, down the first, up the tenth, down the sixth, up the fourth, down the second, up the ninth, down the eighth, up the third, and down the seventh. This rectangle was, however, not large enough for the whole message, even when the nulls at the end of each column were discarded, but at the point when the rectangle has been completely filled occur the three words volunteers resist surprise, which are a new set of indicators: volunteers indicates a nine-column rectangle, resist and surprise add to nine lines. Therefore, the remainder of the message was enciphered by a square of nine columns and nine lines, and transcription followed a different route from the first: up the second, down the third, up the ninth, down the first, up the sixth, down the fourth, up the eighth, down the seventh, and up the fifth.

When these directions are followed, the plain text becomes:

48. Plum, I, 53-54.

New Orleans, La., June 19, 1864.

To Gen. Halleck, Washington, D. C.

Lieut. T. F. Beal, of rebel secret service, made a lieutenant for burning the "Sunny Side" near Memphis, proposes to leave Shreveport about this date with ten picked assistants to burn and destroy storehouses, boats, etc., at Louisville, Cincinnati, and St. Louis; possibly also at Memphis and Cairo. This party will be in squads of two or three at each place. They correspond by mail in cipher. Lieut. T. F. Beal was formerly a lawyer at Shreveport, La. He is about five feet six or seven inches high, light built, slender, slim faced, freckled, light brown hair, light mustache. Has been recently cut so as to leave scars, probably on left side and near top of head, above and a little behind the ear; also at the junction of nose and forehead; also on inside of left hand near the thumb. He spits a good deal while conversing. All will be in citizen's clothes; sometimes they wear pistols.

E. R. S. Canby
Major-General

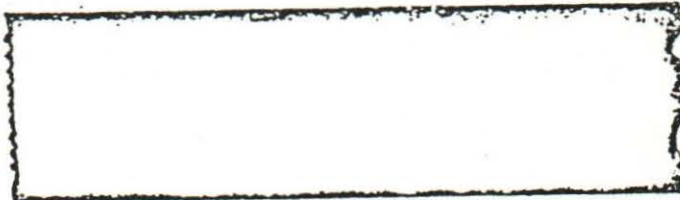
The first of a new series of three ciphers, No. 3, was introduced 25 December 1864 for use at headquarters of Generals Grant, Sherman, Thomas, Sheridan, and Canby.⁴⁹ Although intended for western stations as well, it is believed that it never reached the West. In fact, after No. 4 was adopted on 23 March 1865, No. 3 was little used. Plum says that No. 4 was the last cipher used in the war. Upon its adoption it was sent to Captain W. G. Fuller at Headquarters, Military Department west of the Mississippi; to Captain S. H. Beckwith at Grant's Headquarters; to C. G. Eddy at Sherman's Headquarters; to Captain W. R. Plum at Thomas's Head-

49. One of the more interesting features of the compilation was an attempt to choose code words in such a way as to reduce telegraphic garbles to a minimum. (see Plum, I, 55).

quarters, and one copy was kept at the War Department. Apparently, it had been prepared some time before and was available in the War Department. It had been used by the War Department operators in 1863 to encipher a famous message from Lincoln to Simon Cameron, temporarily at Meade's Headquarters shortly after the Battle of Gettysburg. The message referred to is described by Bates (Century, 291) as in cipher No. 12, which, however, had an entirely different route. In any case, whatever the explanation of the inconsistency, the message is highly interesting both from the point of view of historical significance and as an example of unusual cryptography.

The following illustration of the message is a combination of the versions given by Bates (Century, 291) and Plum (I, 58), which differ in minor details. The plain text was first written by the operator in a rectangle seven columns by eleven lines, using nonstandard spelling, as follows:

<u>1</u>	<u>2</u>	<u>3</u>	<u>4</u>	<u>5</u>	<u>6</u>	<u>7</u>
Washington	July	15	18	60	3	for
Sigh	man	Cammer	on	period	I	wood
give	much	Toby	relieved	of the	impression	that
Meade	comma	Couch	comma	Smith	and	and
comma	since	the	battle	of	Get	ties
burg	Comma	have	striven	only	to	get :
the enemy	over	the river	without	another	fight	period
please	tell	Es	if	you	know	who
was	the	one	corps	commander	who	was
for	fighting	comma	in the	counsel	of	war
on	Sunday	night	signature	A. Lincoln	Bless	him



Note the introduction of punctuation, which has a modern appearance, and the position of the postscript.

The clerk then substituted code words for such ideas as appeared in the code, producing the following text which is merely a mixture of plain text and code words, still in normal order, the code words being underlined:

<u>Incubus</u>	<u>Stewart</u>	<u>Brown</u>	<u>Morris</u>	<u>Knox</u>	<u>Madison</u>	<u>for</u>
sigh	man	Canner	on	flea	I	wood
give	much	Toby	<u>tranneled</u>	<u>serenade</u>	impression	that
<u>Bunyan</u>	<u>bear</u>	<u>ax</u>	<u>cat</u>	<u>children</u>	and	awl
<u>bat</u>	since	the	<u>knit</u>	of	get	ties
<u>large</u>	<u>ass</u>	have	striven	only	to	get
<u>Village</u>	<u>skeleton</u>	<u>turnip</u>	without	another	<u>optic</u>	<u>hound</u>
Please	tell	me	if	you	<u>no</u>	who
was	the	<u>Harry</u>	<u>Madrid</u>	<u>locust</u>	who	was
for	<u>oppressing</u>	<u>bitch</u>	<u>quail</u>	<u>counsel</u>	of	war
on	<u>Tyler</u>	<u>Rustle</u>	<u>upright</u>	<u>Adrian</u>	Bless	him

The next step was to transcribe the text according to the route prescribed, prefixing the indicator of the route ("Blonde") to the beginning:

Washington, D. C.

To A. Harper Caldwell,

Cipher Operator, Army of the Potomac:

Blonde bless of who no optic to get and impression I Madison
 Square⁵⁰ Brown canner Toby ax the have turnip me Harry bitch rustle
 silk Adrian counsel locust you another only of children serenade flea
 Knox County⁵¹ for wood that awl ties get hound who was war him suicide
 on for was please village large bat Bunyan give sigh incubus heavy
Morris on tranneled cat knit striven without if Madrid quail upright
 martyr Stewart man much bear since ass skeleton tell the oppressing
 Tyler monkey.

D. Homer Bates.

50. The word "square" apparently stood in the code after "Madison" but was omitted in inscription.

51. The word "Knox" was probably followed in the code by "County" which does not appear in the rectangle.



As was seen from the text of the message of 15 July 1863, Cipher No. 4⁵² had code words for a few phrases, the total number of code words being 1608, exclusive of the indicators and nulls. The indicators occupied twelve pages. The book was devoid of instructions: if captured it was hoped that the lack of directions would prove completely confusing to the Confederates. Page 7, for example, appeared as follows:

		3		7		4		2		
8			10		14			12		
		13		11			9			
6			5		1					

Bedroom.	1.	Lazy.	Blonde.	11.	Liniment.
Bedstead.	2.	League.	Bloody.	12.	Lion.
Beverage.	3.	Leather.	Bosom.	13.	Liquid.
Beyond.	4.	Legacy.	Boy.	14.	Loafer
Eig.	5.	Lemon.	Bread.	15.	Log.
Bill.	6.	Lesson.	Eride	16.	Lomax.
Billiards.	7.	Let.	Brush.	17.	Long.
Bilious.	8.	Library.	Bulk.	18.	Lucky
Blanket.	9.	Life.	Bushel.	19.	Luscious
Bliss.	10.	Linen.	Buxom.	20.	Luxury. ⁵³

52. Cipher No. 4 was abandoned on 20 June 1865, when all existing ciphers were discarded by the Federal Government and supplanted by No. 5 which was then sent to over 19 operators.

53. This is copied from Plum, I, 57.

According to Plum, the square at the top of page 7 of the cipher book indicates the route: the route to be followed in this case was up the column marked 6, down that marked 3, up that marked 5, down that marked 7, up that marked 1, down that marked 4 and down that marked 2. The blank columns were inserted to confuse the enemy, as were the figures placed in the second and third rows. Only the digits on the top and bottom lines were significant. The highest figure in the top or bottom line indicated the number of columns to be used.

On occasion, need would arise for special ciphers not to be given wide distribution and a cipher would be compiled for a single department of the Army. The Department of Missouri used these so-called "Departmental Ciphers", which were basically similar to the earlier ciphers devised by Stager, more than any other department.

K. Other Transpositions

The following passage describes a transposition cipher of a somewhat different type which was devised for a special purpose:⁵⁴

During Burnside's Fredericksburg campaign in 1862, the War Department operators discovered indication of an interloper⁵⁵ on the wire leading to his headquarters at Acquia Creek. These indications consisted of an occasional irregular opening and closing of the circuit and once in a while strange signals, which were evidently not made by any of our own operators. It is proper to

54. Bates, Century, 292-296.

55. This is certainly one of the earliest instances of an attempt at interception by electrical means.

note that the characteristics of each Morse operator's sending are just as pronounced and as easily recognized as are the characteristics of ordinary handwriting, so that when a message is being transmitted over a wire, the identity of the sender may readily be known to any other operator within hearing who has ever worked with the sender of such signals. A somewhat similar means of personal identification occurs every day in the use of the telephone.

At the time referred to, therefore, we were certain that our wire had been tapped at an unguarded point. In some way or other the Confederate learned that we suspected his presence on the wire, and he then disclosed to us the fact that he was from Lee's army and had been on our wire for several days, and that, having learned all that he wanted to know, he was then about to cut and run. We gossiped with him for a while and then ceased to hear his signals and knew, or believed, that he had gone.

Meanwhile, we had taken measures to discover his whereabouts by sending out linemen to patrol the line; but his tracks were well concealed, and it was only after the intruder had left that we found the place where our wire had been tapped. He had made the secret connection by means of fine silk-covered magnet wire, so-called, in such a manner as to conceal the joint almost entirely. Meantime, Burnside's operator was temporarily absent from his post,⁵⁶ and we were obliged to have recourse to a crude plan for concealing the text of telegrams to the Army of the Potomac, which we had followed on other somewhat similar occasions when we believed the addressee or operator at the distant point (not provided with the cipher-key) was particularly keen and alert. This plan consisted primarily of sending the message backward, the individual words being misspelled and otherwise garbled. We had practised on one or two despatches to Burnside before the Confederate operator was discovered to be on the wire, and we were pleased to get his prompt answers, couched also in the same outlandish language, which was, however, intelligible to us after a short study of the text in each case. The general and ourselves soon became quite expert in this home-made cipher game, as we all strove hard to clothe the despatches in strange, uncouth garb.

56. Replacement pools were evidently unknown at this date.

In order to deceive the Confederate operator, however, we sent to General Burnside a number of cipher-messages, easy of translation, and which contained all sorts of bogus information for the purpose of misleading the enemy. General Burnside or his operator at once surmised our purpose, and the general thereupon sent up in reply a lot of "balderdash," also calculated to deceive the uninitiated.

It was about this time that the following specially important despatch from Lincoln was filed for transmission:

November 25, 1862.

MAJOR-GENERAL BURNSIDE, Acquia Creek, Va.: If I should be in boat off Acquia Creek at dark to-morrow (Wednesday) evening, could you, without inconvenience, meet me and pass an hour or two with me.—A. Lincoln.

Although the Confederate operator had said good-by several days before the date of this message, we were not sure that he had actually left. We undertook therefore to put Lincoln's telegram in our home-made cipher, so that if the foreign operator were still on our wire, the message might not be readily made out by the enemy. At the same time extra precautions were taken by the Washington authorities to guard against any accident to the President while on the visit to General Burnside. No record is now found of the actual text of this cipher-despatch, as finally prepared for transmission, but going back over it word for word, I believe the following is so nearly like it as to be called a true copy:

Washington, D. C.

November 25, 1862.

BURNSIDE, Acquia Creek: Can Inn Ale me withe 2 oar our Ann pas Ann me flesh ends N. V. Corn Inn out with U cud Inn heaven day nest Wed roe Moore Tom darkey hat Greek Wny Hawk of abbott Inn B chewed I if.—Bates.

By reading the above backward, observing the phonetics, and bearing in mind that flesh is the equivalent of meat, the real meaning is easily found. It cannot be said that this specimen exhibits especially clever work on the part of the War Department staff; nor is it likely that the Confederate operator, if he overheard its transmission, had much trouble in unraveling its meaning. As to this we can only conjecture.

Burnside readily translated this cryptogram, if it may be dignified with so high-sounding name, and replied in similar gibberish that he would meet Lincoln at the place and time specified. At that meeting on the steamer Baltimore was discussed the plan of a movement against Lee's intrenchments which was made three weeks later, and which resulted in our army being repulsed with the loss of many thousands of lives.⁵⁷

Another special transposition of this type was used in 1865 when Lincoln was staying at City Point and Richmond. After 6 April the route transposition ciphers were no longer used for presidential dispatches. The reason for this abandonment of cipher is not clear: the operators may have felt that now that the war was believed practically over—Lee surrendered three days later—cipher communication was less imperative. In any case, telegrams were sent in plain text thereafter.

For an important message sent by Lincoln on 3 April a special type of cipher was used, closely resembling that to Burnside. The reason for the unusual encipherment was a desire to conceal the news from cipher operators who might happen to see it while relaying it to Washington. The ruse resorted to was surprisingly simple: the order of the words was merely reversed and nonstandard spelling adopted! The text is as follows:

57. The battle of Fredericksburg, 13 December 1862.

City Point, Va., 8:30 A.M., April 3, 1865.

Tinker, War Department: A. Lincoln its in fume a in hymn to start
I army treating there possible if of cut too forward pushing
is He is so all Richmond aunt confide is Andy evacuated Peters-
burg reports Grant morning this Washington Secretary War. Beck-
with.⁵⁸

L. Civil War Terminology

During the Civil War certain terms were used in senses different from those in use at the present time; likewise, technical terms denoted ideas now designated by different names. The following is a glossary of such terms:

Civil War term

modern equivalent

adjustment letter

letter indicating key position

arbitrary

code word or code group

bulled

gerbled

check word

null

cipher

both code and cipher in the

modern sense

code

in general, a signalling code,

not used in the modern sense

of cryptographic system

commencement word

key indicator

countersign word

key word in polyalphabetic

substitution

to put up

to encipher a message

translation

decipherment

58. Bates, Century, 296; Plum, I, 35. The latter actually seems to attribute the encipherment to President Lincoln himself! A photograph of the message in plain text is printed by Bates (Century, 295) so it seems clear that Plum is wrong about this.

M. An Appraisal of Federal Cryptography

Modern cryptographers will be impressed by the insecurity of all the systems in general use by the Federal forces during the Civil War. These systems include monoalphabetic substitutions, polyalphabetic substitutions, and route transpositions. The way in which polyalphabetic substitutions are mentioned suggests that these were not in much use; indeed, they may not have been used by the Federals at all. If so, Myer mentions them simply because the Confederates used them, and they were solved by Federal experts with comparative ease. In any case, no Federal system would long have resisted attack by competent cryptanalysts possessed of a sufficient body of traffic. Though not inherently more secure than the substitutions, the transpositions proved to be in actual practice adequate against the very inexperienced Confederate cryptanalysts. Both Plum and Bates make the statement that no Federal message was ever solved by a Confederate expert:⁵⁹ indeed they claim that the Confederates actually published intercepted messages in the newspapers in the hope that some one would come forward with a solution. It must be remembered that Plum and Bates were Northerners, interested very naturally, in making the achievement of the union operators seem more notable. Yet it must be presumed that if the Confederates had succeeded in reading intercepted traffic, they would have recorded this fact to their own credit. So

59. Brown (213) quotes Lieutenant Frank Markoe, Confederate Signal Officer at Charleston, as saying that he had read many Federal messages, but the context clearly shows that these were unenciphered signals.

careful a historian of the Confederacy as D. S. Freeman says nothing of any solution in his seven volumes on the campaigns of Lee and his lieutenants. This failure of the Confederates is the more surprising when one learns that they were aware of the relatively advanced system known as the Vigenère cipher square. Perhaps the real reason why the Confederates failed was that they never intercepted sufficient traffic to develop a competent cryptographic bureau.

The route transposition, as outlined by Myer in his Manual, seems now, at any rate, a childish system, but it must be remembered that the illustration given by him was selected for training purposes only: in actual practice the true meaning of the messages appeared much less obvious. Compare, for example, the cipher text of the famous message from Lincoln to Cameron dated 15 July 1863 (see page 33 above). Without sufficient coverage and modern methods, how would any one guess that "Adrian" stood for Abraham Lincoln and that "incubus" was Washington? And who would have supposed that President Lincoln would have used the word "bless" in a telegram?

The Federal code, called by its users a "list of arbitraries" was the most secure feature of Federal cryptography. It had been developed from a rudimentary form in Stager's earliest compilations to the point where later editions were including such code words as quail = in the.

Had the war lasted longer and the demand for greater security been increased, it is probable that before long the Federals would have been using much larger, and therefore much better codes than these, and with the continued use of the route transposition the Federal system would for all intents and purposes have reached the stage of enciphered code, one not achieved during the First World War by most governments, and not even in the Second by all.

Q13 273

CHAPTER IV. THE CONFEDERATE SYSTEMS IN THE CIVIL WAR

A. The Vigenère Table

The most widely used Confederate cipher was that known to modern cryptographers by the name of Vigenère cipher square and was thus a form of polyalphabetic substitution controlled by a key word or phrase. No Confederate or Federal writer¹ actually calls the cipher by Vigenère's name: probably none of them knew that it was first published by Blaise de Vigenère in his Traicté des chiffres ou secrets manières d'escrire (Paris 1586). That a copy of Vigenère's book was still extant during the war in some Southern library is possible, but it is not likely that it was consciously used by Colonel J. H. Alexander who devised the first Confederate cipher in the spring of 1862. Alexander was the brother of General E. Porter Alexander, already mentioned as an associate of Myer in the old Army before the war. In the spring of that year he was assigned the task of preparing a manual for Confederate signal officers, which included "a table for compiling cipher dispatches."² This sounds very much like the Vigenère table which the Confederates were known to be using in messages successfully solved by Federal cipher clerks.

The earliest dated Confederate cipher, however, is a message sent by

-
1. Myer, Manual, 298; Plum, I, 38; Brown 211; Bates, Century, 296.
 2. Brown (206-207) prints a letter from Alexander dated 6 June 1888 in which the writer given no further details.



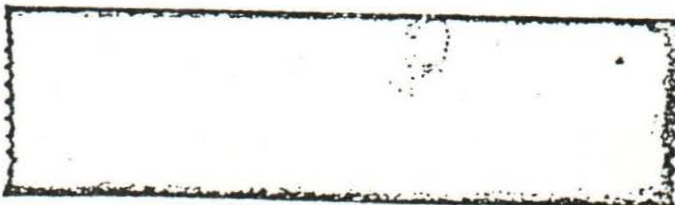
Beauregard after the Battle of Shiloh (8 April 1862), giving the number and condition of his forces at Corinth.³ The text had been enciphered "by merely putting the last half of the alphabet first, that is, substituting M for A, N for B, O for C, etc." The message first reached Richmond in a northern newspaper, for it was intercepted by Federals. From Brown's description it seems clear that the method was monoalphabetic substitution with the cipher alphabet a reversed standard alphabet, thus:

Plain: ABCDEFGHIJKLMN OPQRSTUVWXYZ
 Cipher: ZYXWVUTSRQPONMLKJIHG FEDCBA

This Beauregard message thus probably antedates the appearance of Alexander's manual, which accounts for the abrupt change in type of system. The Federals prepared cryptographic systems in 1861, whereas not until 1862 did the Confederates make any systematic attempt to prepare comprehensive systems. This is surprising in view of the widely held view that the Confederate Armies included a larger percentage of abler officers of the old Federal Army than did their Northern opponents. Brown says, however, that all Confederate signal officers were instructed in cipher and intrusted with the key word.⁴

3. Brown, 212.

4. Brown, 209.



Only four keys are known to have been used by the Confederates; others may have been used in traffic not solved. Three of the four appear to have been constructed by the same compiler:

COME RETRIBUTION
COMPLETE VICTORY
MANCHESTER BLUFF

Note that they all contain fifteen letters, and that there are repeated letters, at least two in each key, and in the first, several letters (E, I, O, R, and T). This was a defect which was recognized by Northern cryptographers—see Myer's Manual, page 273. The fourth key was IN GOD WE TRUST, and shows no affinity with the others: it does not have fifteen letters. Brown (page 211) calls this "the Court cipher" and says that it has been much used in diplomatic correspondence. It therefore seems probable that some one found it in an earlier work on cryptography and adopted it for Confederate use.

Myer's illustration of the Vigenère table (pages 298-299) is based on the first key and is as follows:

Plain text: THE ARMY WILL MOVE TONIGHT.⁵
Key: COM PLET EVIC TORY COMPLET.
Cipher text: VVQ PCQR ADTN FCMC VCZXRLL.

Note that the word lengths are retained, a vulnerable feature. What is more, the Confederates enciphered only parts of their messages, leaving the remainder in plain text, a fact which led to successful solution.

5. This is Myer's favorite text; he uses it in most of his illustrations.

Had the cipher disks been less clumsy, it is probable that their messages would have successfully resisted solution, for it is doubtful if any Federal cryptanalyst was aware that polyalphabetic substitutions can be solved by factoring the interval between repetitions of polygraphs.

The following example will illustrate the Confederate methods:

Jackson, May 25th, 1863

Lieut. Genl. Pemberton: My XAPV. USLX was VVUFLSJP by the BRCYA
 (1) J 200 000 VEGT. SUAJ. NERP. ZIFM It will be GFCECSZO (Q) D
 as they NTYLSX. Bragg LUTPHINZG a QR (K) CKEESE when it D23JXI will
 YOIG. AS. QHY. NITFM do you YTIAM the IIKL. VFVEY. How and where
 is the JSCMLGUSFTVE. HEFY is your ROEEL.

J. E. Johnston.

This message was intercepted by Grant and forwarded to Washington on the day it was sent by Johnston. Grant revealed in his accompanying letter that eight men had been captured while attempting to get through the Federal lines and that they had 200,000 percussion caps on them.

The message was assigned at once to the cipher operators in the War Department who soon solved it, but Bates, who must have participated in the work, fails to record the steps. It should be obvious, however, that one of the points for attack was the word VEGT, following 200 000, which immediately suggested the plain text CAPS. Bates' description of the method of encipherment used in this message is incorrect: he states that the key was MANCHESTER BLUFF, as indeed it was, but he then goes on to say that the letters of the key were found on the top line of the square, the plain letters in the column headed by the key letter, and the cipher letters at either end of the line in which the plain occurred. This is probably only a confusion, in the mind of Bates, of the operation of re-

covering a key when both plain and cipher are known, with the operation of encipherment: Johnston actually found the plain letter at the top of the square, the key letter at the left, and the cipher letter at the intersection. Note that the key was not written over the entire message but only over those letters which were to be enciphered. By using this method, the following plain text was reached:

Jackson, May 25th, 1863.

Lieut. Genl. Pemberton, Vicksburg:

My last note was returned by the bearer. 200,000 caps have been sent. It will be increased as they arrive. Bragg is sending a division. When it comes I will move to you. What do you think the best route? How and where is the enemy encamped? What is your force?

J. E. Johnston.

Three other Confederate messages were received in the autumn of 1869 by the cipher department at New Orleans, of which Captain W. R. Plum was then officer in charge. The first was an old telegram partly in cipher, not hitherto seen by the Federals, which had been sent on 26 December 1862 by Pemberton at Vicksburg to Johnston at Jackson, and had been intercepted about the time it was sent. The second telegram in plain text was, according to a note attached, found among Confederate papers after the fall of Vicksburg in July 1863, and it was suggested in the note that it was the plain text of the first telegram, inasmuch as the two messages were identical in date, correspondents, phraseology, and letter count. Plum, who

knew the essential features of the Vigenère table, did not take long to prove that this assumption was right. The following will illustrate:

Message No. 1: I prefer OAAVVR, it has reference to XHVAJ CCHFF IBPZE
 Message No. 2: I prefer Canton. It has reference to forti ficat ionsa

LREQP ZRNK to prevent PNUZE YXSWS TFWJ at that point. ROEL PSQHV ELVTZ
 tYazo oCity to prevent passa goefr iver at that point. Force lande dabou

FIUTL ILASL TLHIF NOIGT SLLF GCCAJ D.⁶
 tthre ethou sanda bovev outho frive r.

By searching for the plain letter at the top of the Vigenère table, and running down the column to the cipher letter, the key letter would be found at the left hand column. Thus, it was shown that the key used was MANCHESTER BLUFF.

An attempt to read the third message by using the key MANCHESTER BLUFF was a failure: it had not been enciphered with that key. The text was as follows:

Montgomery, 30th (September 1864.)

To Gen'l E. K. Smith,
 Shreveport, La., via Wi.

What are you doing to execute the instructions sent you, to HCDLLVW-YLWIG-KK-GOEI-DMWI-JN-VAS-IGUGUHDITD.-If success will be more certain, you can substitute-EJTEKPG-OPGHEVT-KCFARKF-TAG-HEEPZZN-BEWYPHDN-CHOMKOG-By which you may effect C-TPQGEXYK-above that part HJ-OPG-KRLCT-patrolled by the ZGRK-GLUL-C-EBNDLYL.

Jeffn. Davis.

The cryptanalysts were assisted by two facts: (1) the plain text suggested probable values for the cipher; and (2) the word lengths had been indicated by the dashes. The sequence O TPGEXYK following, as it does, "you may effect," suggested the plain text A CROSSING; likewise, the cipher text

"above that part HJ-CPG-KVMCT" suggested CF THE RIVER. Having attempted to recover the key used with the first passage, Plum found ...TE VICTORY C...: from the other passage, the result was ...ORI COMPLE... By joining the two fragments, the entire key was recovered: COMPLETE VICTORY.

The Complete decipherment with the key and plain text is as follows:⁷

Cipher text: What are you doing to execute the instructions sent you,
Key:

Plain: What are you doing to execute the instructions sent you,

Cipher text: to HCDLLWV YKMGIG KH GOEI DMVI JN VAS DGUGUHDMLTD.

Key: COMPLET EVICTO RY COMF LETE VI CTO RYCOMPLETEV

Plain: to FORWARD TROOPS TO EAST SIDE OF THE MISSISSIPPI.

Cipher text: If success will be more certain, you can substitute

Key:

Plain: If success will be more certain, you can substitute

Cipher text: EJTFKZPG OPGREVT KOFARKF TAG HEEPLEN BEMYPHDN QMOLNQQG

Key: ICTORYCO MPLETEV ICTORYC OLP LETEVIC TORYCCLP LETEVICT

Plain: WHARTONS CAVALRY COMMAND FOR WALLERS INFANTRY DIVISION

Cipher text: by which you may effect O TPOGEMK above that part HJ OPG

Key: O RYCOMPLE TE VIC

Plain: by which you may effect A CROSSING above that part OF THE

Cipher text: KVMCT patrolled by the ZMGRK GGIUL CF EMBNDLXL.

Key: TORYC COMPLET EVICT OR YCOMPLET

Plain: RIVER patrolled by the LARGER CLASS OF GUNBOATS.

Plum gives another message sent to Smith, this time by Lee, which was also enciphered by the key COMPLETE VICTORY:

7. Where the key is not written, no encipherment took place.

Head-quarters, C. S. Armies, March 24, 1865.

Gen. E. Kirby Smith, comdg. Trans-Miss. Dept., Gen.:--VVV
 ECILMREPM RVCCG UI LHOMNIDES KFCH KDF VASPTF US TFCFSTO ABXC
 BJK AZJMLNGJSEIDIVECER CB NDEL UEISU HT KFG AUMD EGH OPCM LFS
 UVAJWH XRYECCCI YU DDNTIPT IU ICJCKPXT ES VVJAU LVER THTC
 ABXC IU EOLEG O RDCGX EN UCR PV NTIPTVTEC ROVARIYB RGGZ RSPZ
 RRSJCPH PTAX RSP EKEE RAECDSREPT LEMSEB ACGG NSFOVVF MC KFG
 SMGE FTRF WH MWV KNGE PYH FEEM CKFLISITVEL EJ JTBX RQ HTAD
 WBHZ ANVV FD ACGG AVKREVV YCIAG OE NZY FET LGXA SCUH.

I am most respectfully your obt. servt.

R. E. Lee.

In this message, Lee's cipher operator, enciphered the entire message, except for the salutation and relatively meaningless complimentary close, though he kept the word lengths. Moreover, since COMPLETE VICTORY was a key known to be in use by the Confederates, it could be tried and was found correct. Yet, even if that key had not been known, this message, probably the most secure Confederate message extant, would have been speedily solved by a modern cryptanalytic unit. Note that there are repetitions of the following polygraphs:

ABXC	and 105 letters later	ABXC
KFG	and 165 letters later	KFG
IU	and 30 letters later	IU

The factors are as follows:

105:	5, 7, 15
30:	5, 6, 10, 15
165:	5, 11, 15

Both 5 and 15 appear in all three intervals. Solution could proceed on either assumption; actually, the number of alphabets was 15, since COMPLETE

VICTORY has 15 letters in it.

-- By performing the decipherment, the reader will discover that the cipher reads as follows:

The President deems it advisable that you should be charged with the military operations on both banks of the Miss., and that you should endeavor as promptly as possible to cross that river with as large a force as may be prudently withdrawn from your present Dept. You will accordingly extend your command to the east bank of the Miss., and make arrangements to bring to this side such of your present force as you may deem best.

Lee's cipher clerk was not always so careful as to eliminate from his telegrams plain text of a revealing nature. The following message, enciphered by the key COME RETRIBUTION, (ominous, in view of the date) will serve as an illustration:

Confederate States of America, Military Telegraph.
Dated Head-quarters, February 25, 1865. Received
at Richmond, Va., 12:25 minutes, A.M.

To Hon. J. C. Breckenridge, Sec'y of War:—I recommend that the
TSYSBEE FN COUTP REATVWLP UEMACBQTM EXFVKJ and ISWAOJRU KTMFL
are not of immediate necessity, UV KPGFEBPGR MPC THELFL LKONTSP.

R. E. Lee.

At once KTMFL suggests WHICH, and this is correct, as will be seen from the decipherment:

I recommend that the removal of public property, machinery, stores, and archives which are not of immediate necessity, be commenced. All powder should be secured.

The only example⁸ of the use of the key IN GOD WE TRUST is found

8. Brown, 211-212.

in a message of which the date and correspondents are unknown:

Key: INGODMETRUSTINGODMETRUSTINGODMETR
 Plain: LONGSTREETISMARCHINGONFISHERSHILL
 Cipher: TBTUVXVAVNALUNXOJERZFDLBAUKFVDEEC

This cryptogram differs from others in that the encipherer found his key letter at the top, the plain letter at the left, and the cipher letter at the intersection.

During the trial of the accomplices of John Wilkes Booth considerable attention was given to evidence tending to show that Booth's intentions were known to President Davis and other Confederate leaders. On Booth's body and also in his trunk in the National Hotel there were found after his death copies of "an alphabet square cipher". This is described by Bates as identical with those known to have been used by Davis and Confederate generals, as well as with another found on 6 April 1865 by Charles A. Dana, Assistant Secretary of War, in the office of Judah P. Benjamin, Confederate Secretary of State. This evidence, so Bates (page 298) says, makes it "inconceivable that Booth was not supplied with this cipher-code by the Confederate government." The evidence does not now seem so conclusive: if Booth merely had a cipher square of the Vigenère type, his knowledge of the system may have been independent. If, however, Booth also possessed one or more of the key phrases mentioned, the evidence is much better.

B. The Cipher Cylinder

The Confederates found that the operations of enciphering and deciphering a message using the Vigenère square were laborious, and Captain William N. Barker, of the Confederate Signal Corps, devised a cipher cylinder⁹ by which this type of operation could be speeded. The cylinder was mounted in such a way that it could be made to revolve horizontally on a shaft fitted with a crank. On its outer surface a Vigenère square was pasted and a fixed pointer was attached in such a way as always to point to the left hand column. There was also a movable pointer which could be slid along a bar to point to any other column. The operator began encipherment by turning the cylinder until the first line of the square was opposite the movable pointer. He then slid the movable pointer until it indicated the key letter. The cylinder was then turned until the fixed pointer would indicate the cipher letter to be used. Myer illustrates this cylinder on Plate 7, figure 4.¹⁰ Another illustration (Brown, p.212) is entitled "Confederate Cipher Machine." This machine is much simpler, and lacks the pointers. The cylinder is enclosed within a box which has a slit to permit the operator to view only one line at a time. Obviously,

9. See Figure 2. One of the cylinders is on exhibit in the ASA Museum; another is in the Lincoln Museum, Tenth Street Northwest, Washington. It is described as having been found in the Confederate War Department in Richmond, and probably is the cylinder referred to by Brown as in the War Department at Washington.

10. See Figure 2.



the operator using such a device would be forced to mark the proper column in some way. Brown says that "a model of this apparatus is preserved among the Confederate records in the War Department at Washington." He himself possessed another.

Neither device involved any cryptographic principle different from the hand-operated Vigenère square.

C. The Running Key

Following his description of the Confederate Vigenère table, Fyer describes (pages 300-302) another cipher which may have been used by the Confederates though Fyer does not specifically say so. It is perhaps the most interesting cipher in the Manual. The procedure is as follows: the letters of the alphabet are numbered consecutively from 1 to 26:

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
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

Then, by using these numbers, the key is converted to digits, thus:

Key in letters: A D I S C O V E R Y
Key in digits: 1 4 9 19 3 15 22 5 18 25

Encipherment is performed as follows:

Plain text in letters:	S	E	N	D	M	E	P	O	W	D	E	R
Converted to digits:	19	5	14	4	13	5	16	15	23	4	5	18
Numerical key:	1	4	9	19	3	15	22	5	18	25	1	4
By addition:	20	9	23	23	16	20	38	20	41	29	6	22
Subtracting 1: ¹¹	19	8	22	22	15	19	37	19	40	28	5	21
Where more than 26, subtracting 26:	19	8	22	22	15	19	11	19	14	2	5	21
Converting to letters:	S	H	V	V	O	S	K	S	N	B	E	U

11. This is done merely to add complications!

The decipherment proceeds as follows:

Cipher text in letters:	S	H	V	V	O	S	K	S	N	B	E	U
Converting to digits:	19	8	22	22	15	19	11	19	14	2	5	21
Key in digits:	1	4	9	19	3	15	22	5	18	25	1	4
Subtracting: ¹²	18	4	13	3	12	4	15	14	22	3	4	17
Adding 1:	19	5	14	4	13	5	16	15	23	4	5	18
Converting to letters:	S	E	N	D	M	E	P	O	W	D	E	R

The operation is complicated, but says Myer, it can be speeded in direct proportion as the operator is able to commit the numbers to memory. Thus, if the operator can through memory subtract digits from letters, some of the operations can be omitted.

D. Confederate Espionage Systems

As is well known, Confederate agents were active in Canada, perhaps, as was suspected by the Federal Government at the time, with the connivance of the Canadian authorities. With these agents communication was maintained by means of a secret messenger who regularly passed through Washington on his way from Richmond to Canada.¹³ If not a member of the United States Secret Service, this messenger was at least willing to permit inspection in Washington of the contents of his messages. It is possible that like many another spy, the man was willing to sell himself to both sides at the same time and that he also furnished the Confederates the results of

12. Where minuend is less than subtrahend, add 26 before subtracting.

13. Bates, Century, 298-299.

his observations of Union territory. In any case, Bates (298-299) makes the claim that the cipher messages in his possession were from time to time solved by the War Department cipher clerks, though he does not give either the text of the messages or details of the solution.

In December 1863¹⁴ the Post Office in New York intercepted two letters addressed to a man named Alex. Keith, Jr., Halifax, Nova Scotia. The first was dated 18 December and the second the 22nd. Both were in cipher using arbitrary symbols. The text¹⁵ is printed in Bates' article in Harper's (June 1893), and another transcription is printed by Plum (I, 41): whether either is a photograph of the original letter is not clear; probably both are transcriptions. According to Plum, the first message was passed around the War Department to various clerks who could do nothing with it until it came to the cipher operators who were able to solve it. As Plum was not an eyewitness of the events, it seems better to follow Bates, one of the men who did solve the message, and state that the letter reached the cipher clerks without much delay. The document was obviously a letter, beginning with the place and date, the name of the addressee, and ending with a signature in three symbols. The symbols, however, were a mixture of many types: there were some which resembled script; some were geometrical figures, musical notations, dots and dashes

14. Bates, Century, 299-302.

15. See Figure 3.



of the Morse code, and at least one symbol was a caricature of a man's face. Perhaps by error, near the bottom of the letter the writer had failed to encipher two words "reaches you" and this proved the entering wedge. In Plum's version the words of the message are set off with commas; in Bates, they are run together. As Bates, Tinker, and Chandler studied the message, with President Lincoln looking over their shoulders, it appeared that the encipherer had used symbols of a single type for each word. It was therefore possible to mark the word lengths by noting where different types began and ceased. In front of the words "reaches you" was another word of four letters and in front of that another of six letters in which the second was identical with the sixth: i.e. it formed the following pattern ABCDEB. On the basis of this pattern and the plain words, the experts hit upon the phrase "before this reaches you," which proved to be right. From that point on, solution was rapid, the entire solution taking only four hours.

The letter when deciphered was as follows:

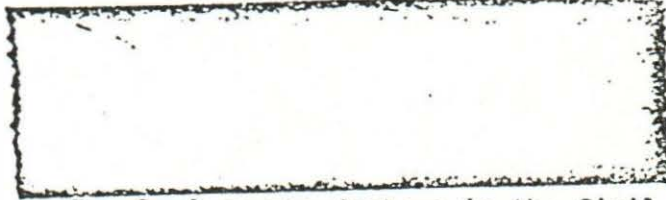
New York, Dec. 18, 1863.

Hon. J. P. Benjamin:

Willis is here. The two steamers will leave here about Christmas. Lamar and Bowers left here via Bermuda two weeks ago. 12,000 rifled muskets came duly to hand and were shipped to Halifax as instructed. We will be able to seize the other two steamers as per programme. Trowbridge has followed the President's orders. We will have Briggs under arrest before this reaches you; cost \$2,000. We want more money; how shall we draw? Bills are forwarded to Slidell and receipts received. Write as before.

J.H.C.

070 096



This message was, of course, intended to be forwarded from Halifax to Richmond, and the initials signed to it were those of J. H. Cammack, a Confederate agent in New York City. Acting upon the intelligence obtained from the letter, the Federal authorities were able to prevent the accomplishment of the designs which Cammack and the others had in mind.

Four days after Cammack mailed his first letter, he sent a second, this time addressed to Benjamin H. Hill, another member of President Davis's cabinet. The text of this message is not preserved by any of the sources, but the same system was in use as with the letter to Secretary Benjamin. Thus, the solution was rapid and resulted in the following decipherment:

New York, Dec. 22, 1863.

Hon. Benj. H. Hill, Richmond, Va.:

Dear Sir:-Say to Meringer that Hilton will have the machine all finished and dies all cut ready for shipping by the first of January. The engraving of the plates is superb. They will be shipped via Halifax and all according to instructions. The main part of the work has been under the immediate supervision of Hilton, who will act in good faith in consequence of the large amount he has and will receive. The work is beautifully done and the paper is superb. A part has been shipped and balance will be forwarded in a few days. Send some one to Nassau to receive and take the machine and paper through Florida. Write me at Halifax. I leave first week in January. Should Goodman arrive at Nassau, please send word by your agent that he is to await further instructions.

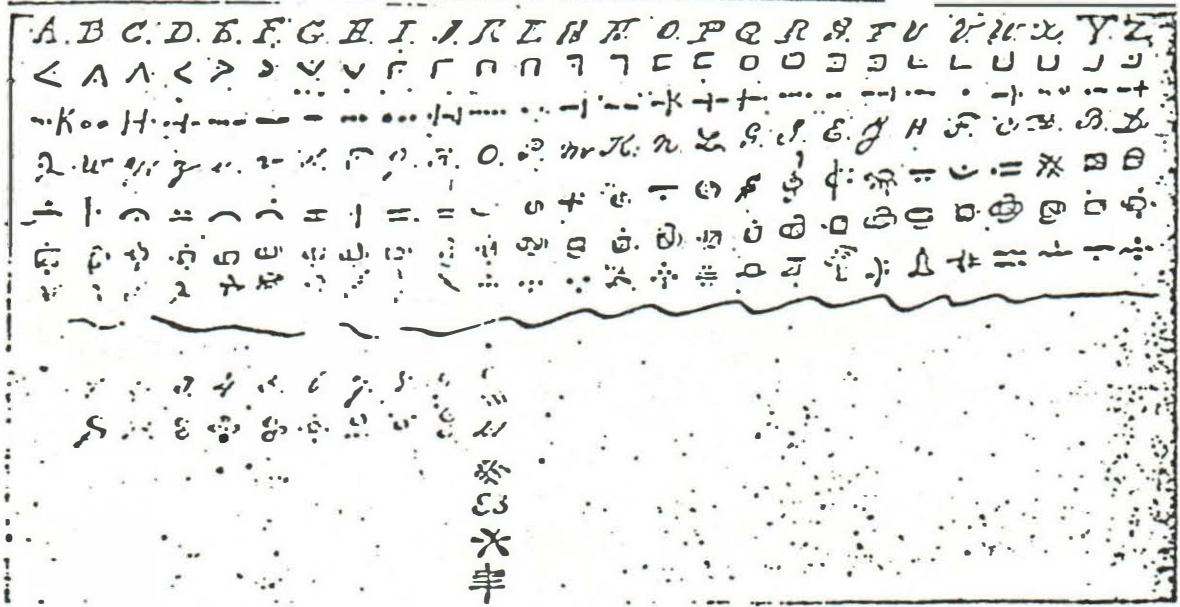
Yours truly, J. H. C.

After the capture of Richmond in April 1865, the Assistant Secretary of War, Charles A. Dana, found in the Confederate State Department a document¹⁶ which proved to be the key to the Cammack letters. The system is, in effect, polyalphabetic substitution, though the fact that each of the six alphabets is made up of symbols of a different type defeats the fundamental purpose of that type of substitution, namely, to conceal the identity of the different alphabets and thus prevent the preparation of a homogeneous frequency distribution. Cammack had used the alphabets in an enep~~t~~ way: he had used a single alphabet for each word, but had he been more skillful and mixed the alphabets thoroughly, still the essential difference of the various alphabets would have aided solution.

The nature of these alphabets will be clearly seen in Figure 4. Some confusion might be experienced in separating the fourth from the fifth alphabet in a message: a few characters in each resemble some in the other. A good deal of attention is paid by all the writers to the fact that a few of the symbols show some resemblance to the cryptogram said to be on a tombstone in Trinity Churchyard, New York, in which the Rosicrucian or pigpen cipher appears, but the resemblance is merely accidental—the Cammack letters are definitely not in the Rosicrucian cipher.

16. Bates, Century, 300: a photograph of the document, reproduced as Figure 4.





Facsimile of the Confederate cipher-code found on April 6, 1865, by Charles A. Dana, among the archives of the Confederate State Department in Richmond, printed for the first time in "Century Magazine" for June, 1907

This cipher was used in the correspondence between the highest Confederate officials and the Confederate agents in Canada and New York City. The letters signed "J. H. C." on pages 74 and 75, were written in a combination of these six sets of hieroglyphics. From a consideration of such intricacy the reader may judge how remarkable was the feat of the cipher operators in translating these messages without any other clues than those derived from ingenuity and patience.

Figure 4. Confederate Cipher Key Captured at Richmond (April 1865).



070 149

E. An Appraisal of Confederate Cryptography

The Vigenere square cipher was of a type of cryptography considerably more mature than the monoalphabetic substitutions and route transpositions in use by the Federals. Where the Confederates failed was in their clumsy use of the device which had many more possibilities for security than they ever exploited. One of the worst faults was the failure to encipher the entire message: only one extant Confederate cipher message avoids this fault, and even that has an unenciphered address and complimentary close which aids the cryptanalyst, at least to a limited extent. Secondly, there were too few keys and these were not changed with regularity. Furthermore, the cipher clerks made no effort to see that repetitions of the same plain text within a message did not fall into the same phase. The skillful cipher clerk who uses such a polyalphabetic substitution will first underline all repetitions in the plain text of the message. He will then take the time to copy the text into columns under the key word or phrase and make sure that none of these repetitions appear in the same column. If they do, all that is necessary is to insert nulls to throw the repetition out of phase. But such skill was beyond any Confederate cryptographer. In their favor, it should be pointed out that, except for the single letter from Colonel J. H. Alexander, all of the testimony concerning the Confederate system comes from Union sources.



Fig 4: Confederate Cipher Key found in Richmond in 1865 by Charles A. Dana (after Bates).



An appraisal of the espionage system used by Cammack has been given above in paragraph 15. That such a device was thought suitable for a letter which would have to pass through the United States mails shows considerable naiveté on the part of the compiler. An open code would have been more suitable. Possibly the Confederates did not consider the possibility of a thorough censorship, or of their cover address in Halifax becoming known to the U.S. Secret Service. Their own inability to solve cryptograms may have led them to a trustful confidence that relatively weak systems were "absolutely indecipherable," as in the case of many another beginner in cryptography.



CHAPTER V. A DIPLOMATIC SYSTEM OF THE CIVIL WAR PERIOD

Little is known of American diplomatic systems from the Revolutionary period until the invention of the telegraph and the laying of the Atlantic cable provided a means of rapid communication between Washington and the European capitals. Nor is it possible to say much about the diplomatic systems used with the first messages sent over the cable when it was first laid in 1866. For a full account, the files of the State Department would be necessary.

Haswell, who was a State Department employee for many years discusses in the article already mentioned,¹⁷ the State Department system of the period (pages 88-90). His statements are to be accepted with extreme caution, as it is not known how he obtained his information or whether it is authentic. The following is a transcription of the pertinent paragraphs:

Shortly after this¹⁸ another cipher was adopted by the Government, which continued to be used by the Department of State after the inauguration of the Government under the Constitution, down to as recent a date as 1867. It was very seldom used, however, after the War of 1812. It was constructed upon the principle of a combination of numbers ranging from 1 to 1600, each number representing either punctuation-marks, letters, syllables, or in some few instances complete words. It was a cumbersome, laborious cipher, suited, perhaps, to ordinary correspondence, with the merit of being easily deciphered by an expert. It was found not only very inconvenient for corresponding by means of the cable, but exceedingly expensive. A similar cipher, however, is now being used by at least one of the principal powers of Europe.

17. Century, LXXIV (1912-1913), 83-92.

18. That is, shortly after the Revolution.




In 1864 the French government under the Emperor Napoleon III, taking advantage of the Civil War in the United States, occupied Mexico and placed Maximilian on the throne as emperor. As soon as the war was over, Mr. Seward took steps to force the French to retire from that country, and by that means enabled the people to choose between Maximilian as emperor and Juarez as president, without being influenced by the presence of the French military forces. A cabinet meeting was called, at which General Grant was present by invitation. The result of the conference was that an instruction was prepared by Secretary Seward to our minister at Paris that plainly stated the sentiments of the United States, which was to the effect that the French must evacuate Mexico at once, or the United States would send her troops into that country and help the forces of the republic. The Atlantic cable had only just been completed, and the president of the company wanted the patronage of the Government to aid the enterprise. He called upon Mr. Seward and requested him to use the cable, promising that the rates would be entirely satisfactory to the Government, notwithstanding those to the public were ten dollars per word. In addition to the ordinary charge, the cable company imposed double rates upon all messages in which a cipher code was used. The instruction was given to the writer¹⁹ to put it into cipher, when he called the attention of the secretary to the great expense that would attend its transmission by cable, as each syllable in the instruction would be represented by four figures,²⁰ and the cable company considered each figure as an equivalent for a word, and charged double rates accordingly. Having in view the assurances of the president of the company that the charges would not be excessive, Mr. Seward gave directions to have the instructions put in cipher and sent by cable, which was done. The instruction would occupy in print about a page and a quarter of an ordinary congressional document. The bill of the cable company was afterward submitted, and it amounted to over \$23,000, which Mr. Seward, not considering it reasonable, refused to pay. The rates were soon reduced to the public one half, and several other reductions followed, but the bill which Mr. Seward refused to pay was never paid.


During the occupation of Mexico by the French, cipher telegrams were sent to General Bazaine, commander of the French forces. Some of these coming into the possession of the authorities of the United States were deciphered by an army officer and much valuable information was obtained.

19. Haswell was evidently a State Department cipher clerk.

20. This was obviously a form of dinomic substitution, i.e. of a dinome for a syllable.



The value and importance of secret writing is of course obvious, but the advantages which have accrued from it, while easily surmised, have become known only in a vague and general way. A specific illustration of a particular benefit derived from it by the United States in a very important matter and at a very critical time relates to the treaty of 1871 between this country and Great Britain, whereby the so-called "Alabama Claims" were to be adjusted by a tribunal of Arbitration at Geneva, and which came very near being nullified in consequence of our presentation to that tribunal of what was known as "indirect claims," namely, claims not for actual losses, but for the deprivation of prospective profits, etc. Great Britain sought to use the presentation of these claims as a ground for setting aside the jurisdiction of the tribunal, and consequently subverting it. Our agent before the tribunal, Judge J. C. Bancroft Davis, devised a plan for saving the case of the United States and preserving the ~~the~~ tribunal. The nature of this plan was such as to require the approval of the President before it could be put into operation, and had to be communicated to him quickly as well as secretly. In anticipation of some such emergency, the writer, at Mr. Davis's request, had prepared for him, just before his departure for Geneva, a cipher which, while perfectly secret, could be easily managed and the key of which could be memorized. Mr. Davis and Secretary Fish had recourse to this cipher for the purpose of the important correspondence above referred to, which could not have been conducted openly and which resulted in the maintenance of the Geneva Tribunal. An amusing feature of this correspondence was the perturbation it caused our minister at London, General Schenck. The messages were relayed through his office and he, not being in the secret of the cipher, insisted upon having them repeated, because, as he said, he found them to be only "a jargon of unmeaning words."



CHAPTER VI. CRYPTOGRAPHIC PROGRESS 1865-1917

A. The Telegraphic Code 1885

Following the Civil War the Military Telegraph Corps was abolished. In the Signal Corps, however, Myer, by this time a Colonel, continued as Chief Signal Officer until his death in 1880, soon after he had been promoted to the rank of Brigadier General. The use of cryptography for military purposes went into a decline during the long period of peace, broken only by the short Spanish-American War of 1898.

The earliest extant War Department Telegraph Code was one called "Telegraphic Code to Insure Secrecy in the Transmission of Telegrams," compiled in 1885 and published by the Government Printing Office in the following year. It was issued by the authority of the Secretary of War and was the work of Lieutenant Colonel J. F. Gregory, A.D.C. It was not, however, a completely independent compilation but a revision and adaptation of a widely used, public code prepared by Robert Slater, Secretary of the French Atlantic Telegraph Company. The code contained 25,000 words, numbered consecutively from 00001 to 25000. The vocabulary proper extended from 00001 to 24200, the remainder being geographical names, personal names, names of forts, etc. There were no blanks for addenda. The compiler intended that only the words and not their equivalent serial or code numbers be used, a limitation which meant, of course, that only enciphered code messages could be transmitted. The procedure was this: each word in the message was looked up in the code book and its serial number written



070 136

down. Then a fixed number was added to or subtracted from the serial number, and the word standing opposite the result was transmitted as the code group. If the additive were such that the minuend was smaller than the subtrahend, then 25000 had to be added; when a subtractor was used, a similar compensation was necessary. In addition to encipherment by addition or subtraction, it was suggested that encipherment could be by transposition of the digits of the serial number. The resultant transposition would then indicate which word was to be sent. Apparently, no one thought of sending the serial number instead of a word. Had this been done, the code would have possessed a greater security than most, if not all, of those systems in use by governments during the First World War. This is the only American code known to have been used between the Civil War and the Spanish-American War, a period of thirty-three years.

B. The Spanish-American War

During the Spanish-American War a telegraph and cipher bureau was maintained at the Executive Office of the President for communications between the Commander in Chief of the Army and Navy and his subordinates.¹ This office, which not only performed telegraphic services but also was responsible for encoding and decoding all traffic, was under the direction

1. Report of the Chief Signal Officer for 1900, p. 50; Report for 1901, p. 23; Report for 1902, p. 42; Report for 1903, p. 33.

of Captain (later Major) Benjamin F. Montgomery, of the Signal Corps Volunteers, whose special report is printed as Appendix No. 11² of the Report of the Chief Signal Officer for 1901. The report, however, gives no information concerning the cipher work performed by the bureau.

Little other information concerning the use of cryptography during the Spanish-American War has survived, and that little is to be found in the pages of the annual Reports of the Chief Signal Officer beginning with the year 1898. The following passages are taken from the Report for 1898:

[Private] Cipher dispatches by mail were also forbidden to and from any part of the West Indies, as otherwise information injurious to the United States would have been possible. . . The Chief Signal Officer was not oblivious of the fact that secret information could be sent in plain text by concerted code,³ but it is to be said that while such messages were frequently accepted, it was often the case that they went quietly into the waste basket and not over the wires to the proposed destination. On the other hand the Chief Signal Officer appreciated fully the advantages to be derived from careful examination of the thousands of messages of unfriendly or neutral character that passed through the hands of his subordinates. From newspaper correspondents, blockade runners, Spanish agents, commercial messages, personal dispatches, etc., there was reaped a rich harvest of information.⁴

The report goes on to refer specifically to special messages in "cipher"—what type is not stated—but presumable what was really meant

2. Pp. 144-147.

3. "Concerted code" is now called "open code."

4. Report of the Chief Signal Officer to the Secretary of War for the Fiscal Year ending June 30, 1898 (Washington, Government Printing Office, 1898). pp. 21-22. Substantially the same facts are given by Captain Howard A. Giddings in his book, Exploits of the Signal Corps in the War with Spain (Kansas City, Hudson-Kimmerly, 1900), pp. 113-120.

was the code of 1885, though reference was made to a new code to be described below.

Herbert O. Yardley, whose testimony should be accepted with the greatest caution for reasons to appear later, alludes⁵ to "the so-called additive or subtractive method for garbling a code telegram (used during the Spanish-American War) [as] about as effective for maintaining secrecy as the simple substitution cipher which as children we read in Poe's The Gold Bug." This probably is a reference to the type of system already described as embodied in Gregory's Telegraphic Code of 1885. Yardley goes on to tell how he had attempted to educate "a higher officer of the Signal Corps who had just been appointed a military attache to an Allied country" in better security measures. The attache was not impressed by Yardley's contentions and said, so Yardley quotes him:

That's a lot of nonsense. Whoever heard of going to all that trouble? During the Spanish-American War we didn't do all those things. We just added the figure 1898 to all our figure code words, and the Spaniards never did find out about it.

If any credence can be placed in the story, this was what would now be called a fixed additive, a very insecure system indeed.

At this point it will be well to note the solution of a number of cipher messages sent by the Filipino insurrectionist, Emilio Aguinaldo, to various chieftains under him in February 1901.⁶

5. The American Black Chamber (Indianapolis, Bobbs Merrill, 1931) pp. 41-42.

6. Frederick Funston, Memories of Two Wars (New York, Scribner's, 1911), chapter vii: "The Capture of Emilio Aguinaldo."

The messages had been brought to General Funston from Lieutenant J. D. Taylor, Twenty-Fourth Infantry, who had succeeded in capturing the bearer, one Cecilio Segismundo, at Pantabangan, Luzon.

The cipher letters completely barked us for many hours. They seemed to be made up of a jumble of letters of the alphabet, making words in no particular language. Captain Smith, Lazaro Segovia, the versatile and courageous Spaniard who for nearly a year had done such excellent secret-service work for me, and I took off our coats and even other things, in fact, stripped for action, and with pencils and pads of paper seated ourselves around a table and racked our brains. . . . Dawn was at hand before the peerless Segovia, whose knowledge of both Spanish and Tagalo now stood us in such good stead, found the key word of the cipher, which was in the latter language, having done it by ransacking his brain for every word in that Malay dialect that he had ever heard of. Among us, we then slowly unwound the mess, and mess it was when there are taken into consideration the difficulties of reducing a cipher and of rendering it through two languages to get the letters in which it was written into English.


Unfortunately, General Funston gives no more details but goes on to explain how the decipherment helped to locate Aguinaldo and bring about his capture.

C. The War Department Telegraphic Code 1899

In the Report for the year 1899 appears ⁷ the following paragraph:

Under the provisions of General Orders, No. 9, Adjutant-General's Office, January 16, 1899, the Chief Signal Officer of the Army has undertaken the preparation of a suitable telegraphic code for the official use of the Army. The extraordinary telegraphic expenses to which the War Department has been lately subjected made this a matter of great importance. Unfortunately the conditions were such that the preparation of this work devolved upon the Chief Signal Officer of the Army personally, this resulting from the fact that

7. P. 18.




a satisfactory performance of this work required a practical knowledge of telegraphy, a thorough familiarity with the necessities of the special vocabularies to be used; also a knowledge of working methods in vogue and regulations in force on the various cable lines of the world. It was evident that perfected work of this kind could not be completed except after many months of labor, but on the other hand, it was important that tentative and temporary steps should be taken to reduce the enormous cable expenses then devolving upon the Department. The first act was to adopt, temporarily, such commercial code as might be best suited to the uses of the Army, which proved to be a new code known as "Western Union Telegraphic Code."

By assiduous personal application the Chief Signal Officer of the Army succeeded in constructing within sixteen days after the date of order a publication for emergent use, which, known under the title of "Preliminary War Department Telegraphic Code," has been printed and distributed to the Army. This code contains general and special instructions concerning the preparations of ordinary messages, as well as those in code and in cipher, and also points out to officers concerned the most important features for Army use of the "Western Union Telegraphic Code." The "Preliminary War Department Telegraphic Code" contains, alphabetically arranged, nearly 4,000 sentences that are of more or less frequent use in military correspondence. It is believed that the savings made to the United States by this code for the eight months ending September 30, 1899, exceeded the sum of \$50,000. In one case a single cipher word conveys a sentence of twenty-four words, a phrase frequently telegraphed. On an average each cipher word represents about seven words in plain text.

The Chief Signal Officer still continues, as rapidly as is possible, his personal labors on a perfected code, which, it is hoped, will be available for distribution by December 31, 1899. As a saving to the Government this code will utilize as supplementary the main body of the "Western Union Telegraphic Code."

In the preparation of the permanent War Department Telegraphic Code very great care has been taken to omit words which, either in the Continental Code or American Morse, are of such character as to lead to errors, whether in the transcription of the cipher messages or from defective transcription.

The copy of the Preliminary War Department Telegraphic Code which has survived shows that the plain equivalents included a few frequent phrases and geographical and military terms. Its use, of course, gave no security



whatever, the only object in adopting it being, as the Report quoted admits, the effecting of economy in telegraphic expenses and in code compilation. As was predicted in the Report, the new War Department Telegraphic Code appeared either late in 1899 (the date on the title-page) or on 16 January 1900, as is indicated by a stamp on the leather binding. This code was in use at least as late as 24 December 1904, for an unknown officer marked the copy now under examination (No. 445) as received by him on that date. Paragraph 2 of the introduction is as follows:

Through lack of time it has been impossible to incorporate in the War Department Telegraphic Code all desirable phrases, and in consequence the first 471 pages of the Western Union Telegraphic Code now in use by the Army will continue in use as a supplementary code. This affords the Army the telegraphic use of 100,000 code words, of which numbers 1 to 78, inclusive are in the Western Union Telegraphic Code and numbers 78, 201 [sic] to 100,000 are in the War Department Telegraphic Code.

This code was one-part in arrangement and employed as code groups both bona fide and artificial words of irregular length. The bona fide words were in many different languages (e.g. NAVIGABAT), while the artificial words tended to be constructed so as to make them seem authentic (e.g. NAVISSET). They probably were taken from the Beruë (International) vocabulary. That part of the code which was a new compilation contained the following sections:

- a. acknowledgements, inquiries, and references to telegrams;
- b. annual and quarterly accounts, returns, estimates, etc.;
- c. errors and corrections;
- d. miscellaneous phrases indicating time: hourly, weekly, etc.;

- e. Monthly calendar;
- f. numerals to be used in cabling amounts, weights, quantities, etc.;
- g. quantities;
- h. cipher phrases;
- i. appendixes
 - (1) military organizations;
 - (2) military posts, etc.;
 - (3) officers' names (not complete list).

After these sections, a copy of the Western Union Telegraphic Code was bound in the same volume. The security reached by such a makeshift affair was not high: it was one-part and unenciphered, but even the security which would have been achieved with a code of this type, if an entirely new compilation, was vitiated by the fact that the public could easily obtain a copy of the vocabulary used. Only the special sections would have required any cryptanalytic study for solution.

This code was again referred to in the Report of the Chief Signal Officer for 1900.⁸ The chief point that is made is again the economy effected by its use.

From time to time appendices have been issued, as the code is not yet in its perfected condition. . . . While primarily a code for commercial purposes, yet the War Department Telegraphic code is so arranged that it can be used for enciphering important confidential messages where secrecy is desired. Each code word has a number, so that any method of enciphering by key numbers can be readily used, either simple or complex.

The Report for 1901⁹ cites paragraph 1741 of Army Regulations for the authority granted to the Chief Signal Officer to prepare the War Department

8. Pp. 47-48.

9. P. 22.

Telegraphic Code, but the other details there given are largely the same as in the preceding year. The Report for 1902¹⁰ again repeats the same statements and so does the Report for 1903.¹¹

D. The Cipher of the War Department 1902

Some sort of dissatisfaction may have been felt with the 1899 code, for in 1902 another was issued by direction of Major General H. C. Corbin, Adjutant-General of the Army. This was inaccurately called "The Cipher of the War Department" in spite of the fact that it was a code. It was prepared by W. H. Allensworth and W. G. Spottswood, of the Adjutant-General's Office, and was printed at the Government Printing Office in 1902. The arrangement in this code was also one-part, and each plain equivalent was given two code groups, one of which was a five-digit group, the other a word. For example, the plain word abandoning could be transmitted as either 10077 or aberrance. The compilers expressed their opinion¹² that digit groups were preferable for traffic transmitted by cable, since "if the word code is used, vexatious and other serious mutilations of original messages are committed by operators ignorant of each other's language." Each page has a hundred groups, numbered by the digit sequence 00-99, and the first page is numbered 100. The main vocabulary stops with the plain word Zouaves which has the digit group 77138. Then there are blank lines

10. Pp. 65-66.

11. P. 27.

12. Pp. iii-iv.

to 77999, and after that an appendix, dated 1 March 1902, which contains lists of arsenals, banks, days of the year, companies, headquarters, units, and organizations down to and including companies, stations, officers of the Army, railroads, phrases of reference, steamship companies, surety companies, telegraph and cable companies, and transports. The last page in the book is blank and is numbered 850, so the size of the code, including the blank lines, is 75,100 groups. Following the vocabulary is a spelling table, which is a normal Vigenère square except that the horizontal plain alphabet is a reversed standard, rather than a direct standard alphabet. The method was to search for the plain letter in the horizontal alphabet, the key letter in the vertical alphabet, and the cipher letter at the intersection of the row and column. The keys were to be distributed: they were not included in the code book. This code marked a distinct improvement over its predecessor in that it was an entirely new compilation and showed no relationship to any public code; it was also superior in having either code words or digit code groups for each plain equivalent. The sections also were the most elaborate of any that had appeared in a War Department code up to that time.

E. The War Department Telegraph Code 1906

The code just mentioned is the only one ever published by the Adjutant General's Department. By 1904, the Chief Signal Officer (General A. N. Greely)

was planning a revision of the War Department Telegraphic Code of 1899. His Report for the year 1904¹³ mentions that during the current fiscal year (1904) Appendix No. 3, which was nothing more than a list of Army officers with code groups for each, had been issued.

A much-needed general revision of the code is now under consideration. Steps have already been taken to utilize the extended privileges as to code words authorized by the International Telegraph Conference of 1903. It is planned to use only such code words as are free from characteristics that facilitate telegraphic errors in either the American or continental Morse alphabets..

The new code had a slightly different title, War Department Telegraph Code, a designation which was destined to remain constant through many revisions. The volume was bound in leather with gilded edges and a flap. It is expressly stated in the introduction that the purpose of this code was to produce both secrecy and economy. For secret messages the code was to be enciphered—how is not stated. The code clerk was permitted to use synonyms wherever the exact word did not appear in the text. The use of commercial codes by the Army was also permitted when desired. The users might also compose a message partly in plain code groups and partly in enciphered code groups. Perhaps benefiting by acquaintance with the "Cipher" of 1902, General Greely supplied with each plain equivalent a six-letter code group and a digit group for an alternative. The arrangement is one-part except for the sections at the beginning, which include

13. Pp. 41-42.

an Army list (names of officers), military organizations, posts and stations, numerals, arrivals and departures, dates, indorsements, letter acknowledgments, requisitions, telegram acknowledgments, mails, shipments, transports, miscellaneous items, vessels, geographical, and radio stations. The vocabulary begins on page 89 with 10467 = ASIFIK, the two code groups for the indefinite article A or an. There are many blanks left for addenda. The last group is 62000 = TESADU, so the size of the code is 62,000 groups, including the blanks.

F. The War Department Telegraph Code 1915

For the next nine years no new code appeared,¹⁴ but in the Report of the Chief Signal Officer for 1913, there appeared on page 35 the statement that the Chief Signal Officer had taken up the task of revising the War Department code book, that is, Greely's 1906 edition. The old code was regarded as inadequate because there were too many letters in the groups, and, besides, revision was needed to bring the material up-to-date.

14. That is, so far as is now known. There still exists a typewritten copy of an "Insular Bureau Supplement, prepared in the Insular Bureau of the War Department, October 1909." The code groups are formed of digits ranging from 24025 to 107244, and the arrangement is one-part. The nature of the code groups makes it unlikely that this supplement was intended to be used either with the code just described in the text or with the Tabular Code issued by the Office of Isthmian Administration, Washington, September 1905, since both of these used words as code groups. Rather was it intended, it would seem, to be used as a supplement to the so-called Cipher of the War Department, issued by The Adjutant General in 1904, the highest code group in which was 77138.

An "expert in code work" had been obtained for this purpose. His name is not stated, and his identity is long since forgotten. On the following page the Chief Signal Officer proposed that an Interdepartmental Code be prepared for use by the War Department, the Navy Department, and the State Department. He recommended that \$10,000 be appropriated as the War Department's share in this task. Evidently a committee was already studying the project, for representatives of the Office of the Chief Signal Officer are stated to have served on the committee thus far.

In the Report of the Chief Signal Officer for 1914 is a statement¹⁵ that the new War Department Telegraph Code was then being completed, and that it was to have 30,000 new phrases, 10,000 of the older code phrase being eliminated as obsolete. The principle of the two-letter differential was to be used and the pages were to be printed on loose leaves to permit revision. An expert had been working for several months on the Tactical Code, but this code was to be only a shorter form of the larger code. The Tactical Code was to have 25,000 groups and be distributed to all officers above the grade of lieutenant. Little progress was reported on the Interdepartmental Code and the appropriation of \$10,000 was again recommended.

In his Report for the year 1915 the Chief Signal Officer announced that the War Department Telegraph Code had been printed and was ready.

15. Pp. 54-55.

for distribution in the fall of 1915, but no further progress had been made on the Interdepartmental Code, for which the appropriation of \$10,000 was recommended a third time. No mention is made in this report of the Tactical Code: it was probably abandoned and in any case was not used during the First World War.

The War Department Telegraph Code 1915, prepared under the direction of the Chief Signal Officer of the Army and published by authority of the Secretary of War, bears on its title-page the imprint of the Government Printing Office, but it was actually printed in a commercial establishment in Cleveland, Ohio! In addition to the possibility that the code was compromised even before it was issued—note that the European phase of the War was already in progress before the printing began¹⁶—the code was also insecure in being one-part in arrangement. The code groups were composed of five-letters, and the code contained 114,000 groups, the last, a blank, being YSGKH. As was predicted in the Report of the Chief Signal Officer for 1914, the two-letter differential was used, and there was a mutilation table, but the proposed loose-leaf feature was not used. The groups were not pronounceable, and the failure to have the groups conform to International Telegraph Regulations resulted in great cost to the Government.

16. On this point see Chapter II, note 3.

In addition to the general vocabulary there were sections for the following:

- a. blanks for emergencies;
- b. organizations;
- c. departments, etc.;
- d. radio and telegraphic stations;
- e. vessels;
- f. Naval officers;
- g. geographical names;
- h. Mexican geographical names;
- i. special persons and firms;
- j. dates, etc.;
- k. hours and minutes;
- l. numerals;
- m. railroads;
- n. cables and cable companies.

The presence of a special section for geographical names in Mexico reflects, of course, the rising interest of the United States in Mexico at that period.

This code then represented all the preparation for the security of major circuits of United States Army communications which had been made prior to the outbreak of the First World War. For low echelon traffic there was a cipher system known as the repeating key system, which used a simple celluloid device called the "Army Cipher Disk," the basic principles of which were understood and described as far back as the year 1500; and a cipher system called the Playfair cipher, which had been frankly copied from the British, who had used it as a field cipher for many years before the [First] World War and continued to use it during the war.¹⁷ With such inadequate preparation in the field of compilation the Army entered the greatest war ever fought up to that time.

17. William F. Friedman, American Army Field Codes in the American Expeditionary Forces during the First World War (Washington, United States Government Printing Office, 1942), p. 1.

G. Suggestions from Inventors

The War Department, from time to time, has received from independent inventors outlines of cipher devices and other cryptographic systems, believed to be "absolutely indecipherable." One such device is known to have been submitted for adoption during the period under discussion.¹⁸ The inventor was Benjamin Myrrick Des Jardins and his patented device was submitted by R. E. Kimball & Co., 274 Wabash Avenue, Chicago, Illinois, who wrote on 7 July 1905, to Major W. D. Beach, General Staff, Washington, D. C. enclosing an outline of the Des Jardins invention. The device was known as the "Permutator" and the usual claim of indecipherability was made. The Permutator was a watch-like affair with two standard alphabets printed on the circumference of two revolving disks, each of which could be fixed at any juxtaposition. No matter what juxtaposition was chosen, only monoalphabetic encipherment would result. Des Jardins appears not to have been aware that his device differed only in unessential details from the cipher devices used by the Federal Army in the Civil War. Needless to say, even though Des Jardins came to Washington for an interview with Captain (afterwards Major General) Ralph H. Van Deman, Military Intelligence Division, General Staff, and with the Chief Signal Officer, his device was not adopted for Army use.

18. See IR 4388.

H. The Eve of the Conflict


If the Army was without adequate cryptographic systems for preserving the security of its own communications, it also possessed no cryptanalytic bureau, though there were among its officers a number who had studied this phase of cryptology to some extent. Certainly as early as the school year ending in June 1913, and continuing until the outbreak of the First World War, cryptography had formed part of the curriculum of the Army Signal School, Fort Leavenworth, Kansas. On 10 July 1916, the Chief of the War College Division, Brigadier General M. M. Macomb, wrote the following paragraph in a letter to the Army Service Schools at Fort Leavenworth:

2. The War College Division is frequently called upon to decipher various messages and, as it has no one who is an expert in work of this description, we would like to have the names of such officers as have shown special aptitude in such work in order to utilize their services.¹⁹

This request ultimately reached the desk of the Acting Director, Army Signal School, Fort Leavenworth, who replied on 13 July 1916, by the following second indorsement:

1. Captain Parker Hitt, 19th Infantry, is undoubtedly the best cipher man in our service.
Lieut. Joseph O. Mauborgne, 8th Infantry, has done some excellent work in this line and should be of value to the War College.
Lieut. Charles A. Lewis, 9th Infantry, has taken an interest in cipher work and if given something to do in this line should develop into a valuable man.

19. Letter 4131-14, copy now filed in IR 4241.



Lieut. Edmund R. Andrews, 13th Infantry, made a good record at the school and conducted the class in ciphers during the school year ending June, 1914.

Lieuts. Charles E. Swartz, 22nd Infantry, Clyde L. Eastman, 20th Infantry, and Karl Truesdell, 25th Infantry, showed talent as cipher men while at the school.

Lieut. Frank Moorman, 18th Infantry, is interested and would be glad to undertake the work of this kind.

Had this indorsement not been signed by Lieutenant Moorman as Acting Director of the Army Signal School, it is probable that his name would have appeared higher on the list and with a more positive statement of his abilities. Captain Hitt (now Colonel, Signal Corps, retired) was the author of a text on cryptanalysis entitled "Manual for the Solution of Military Ciphers,"²⁰ a brochure of 101 pages, which was the first text of its kind in the English language and excellent for its day. It exhibits considerable acquaintance with the literature of cryptography, and discusses the solution of both transposition and substitution ciphers.

Lieutenant Mauborgne, afterwards Major General Mauborgne, was Chief Signal Officer at the time of his retirement in 1940. Lieutenant Clyde L. Eastman, afterwards Colonel Eastman, was Executive Officer to the Chief Signal Officer before his retirement early in the Second World War. Of the others mentioned, only Lieutenant Moorman had any connection with the cryptanalysis of enemy communications during the First World War. As

20. Fort Leavenworth, Kansas, Press of the Army Service Schools, 1916.



a lieutenant colonel he was Officer in Charge of the Radio Intelligence Section (G-2, A-6), of the General Staff, at General Headquarters, American Expeditionary Forces, in France, 1918. Colonel Hitt, though he served primarily as Assistant Chief Signal Officer in France, was as such responsible for the work done in Code Compilation and was one of the inventors of the M-94 Cipher Device, now obsolete.²¹

The Mexican Expeditionary Forces, which occupied parts of Northern Mexico from 15 March 1916 to 5 February 1917, greatly increased the growing interest in Mexican communications.²² From time to time arrests along the border produced information concerning the types of Mexican cryptography currently in vogue. The earliest such arrest now known took place on 5 October 1908. At times espionage activity produced further information. Most of these systems were monoalphabetic substitutions using letters or arbitrary symbols for the cipher forms. A favorite type was a cipher table in which letters placed in the cells, were enciphered by two digits representing the row and the column of the letter desired. The monoalphabetic substitutions were in some cases based on key words, that is, the cipher alphabet was generated by writing down a word and the remaining letters after it. On occasion, Mexicans would be found to be using commercial codes or short lists of code words especially prepared for their purpose.

21. See Chapter VIII.

22. On this topic, see IR 5049: Mexican Cryptographic Systems Prior to 1929, a paper (1945) of the Historical Unit of the Signal Security Agency.

In 1916 an agent of the Department of Justice, Victor Weiskopf, was sent to Texas and in September he succeeded in intercepting and solving some simple monoalphabetic substitution ciphers of a military nature. Weiskopf remained in Texas at least until October 1917, for in that month he solved some financial messages of the Mexican Monetary Commission. His work in Mexico would not now be worthy of note were it not for the fact that during the war he was a member of the staff of the Cipher Bureau, which will be described in succeeding chapters, and until 1929 maintained his activity as a Government cryptanalyst.

During the Mexican expedition a number of Mexican ciphers were intercepted and solved by various intelligence officers on duty in the Southern Department.²³ Yet the experience with Mexican systems was not such as to develop much skill in cryptanalysis. The ciphers themselves were far too simple to be challenging.²⁴ Persons having slight acquaintance with the basic principles of cryptography could, with a little practice, solve any Mexican system then current: Captain Hitt and his colleagues at Fort Leavenworth had already advanced far beyond this stage in their training program, even though, when compared with modern developments, their cryptanalysis was rudimentary.

23. See IR 4450 for the keys and circuits.

24. The cryptanalysts of the Riverbank Laboratories (see Chapter II) did much work on this type of intercept and had nearly 100% success.

Fig. 1: Plate V of Lyer's Manual of Signals (1866).

070 125

Fig. 2: Plate 7 of Myer's Manual of Signals (1866).

012 127



INDEX.

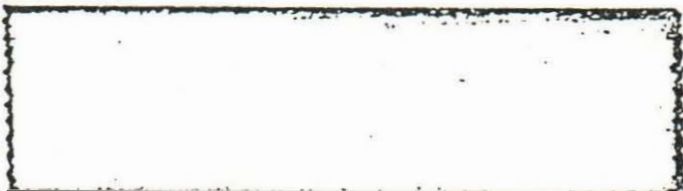
Adams, Abigail	2	American diplomatic system	96-98
Adams, John	2	American Morse	104
Adams manuscripts	3	American Morse alphabet	109
Additive	102	American Philosophical Society	2
fixed	102	André, John.....	18, 19
Adjustment letter	71	Andrews, Edmund R.....	116
Agents, confederate	87	Anton's Cipher Device ...	44
Aguinaldo, Emilio..	102, 103	Arbitrary	71
"Alabama Claims"	98	"Arbitrariness, list of" ...	73
Alexander, P. E..21, 41,	75	Army of the Potomac ...21,	68
Alexander, J. H.....	75, 93	Armies, Confederate	76
Alexander's manual	76	Arnold, Benedict	18, 19
Allensworth, W. H.....	107	Arrangement	
Alphabet	3, 14	one-part.....17, 51, 106, 107	109, 110, 112
American Morse	109	two-part	17
cipher.....2, 43, 76, 117		Atlantic cable	96, 97
Continental Morse	109	Bailey's Dictionary ..	19, 20
direct	15	Barker, William N.....	85
plain	2, 108	Bates, David Homer	
transposed	1	25, 26, 27, 28, 47, 50, 53	
Alphabetic code	40	60, 64, 72, 78, 84, 88, 89	
American diplomatic code	10		



Bazaine, Achille F.....	97	Cannack, J. H....	91, 92, 95
Bazeries, Etienne	4	Cannack letters	92
Beach, W. D.....	114	Cannack's Cipher Message	90
Beal, T. F.....	63	Canby, E. R. S.....	63
Beauregard, Pierre G.	21, 76	Carnegie, Andrew	27
Beckwith, S. H.	30-33, 53 60, 63, 71	Chandler, Albert B.	28, 53, 89
Benjamin, Judah P.	84, 89, 91	Check word	71
Blackstone, Sir William..	19	Chief Signal Officer	21, 99, 101, 103, 104, 106 108, 110, 111, 112, 114, 116
Booth, John Wilkes	84	Office of the	111
Breckenridge, J. C.....	83	Cipher	9, 15, 18, 29, 33, 35, 37, 41, 47, 48, 49, 53, 54, 59, 63, 71, 75, 76, 78, 79, 80, 83, 84, 86, 88, 96, 101, 103, 104, 115.
Brown, J. Willard	21, 24, 34 76, 85, 86	Cipher	
Brown, Samuel M.....	27	Confederate	75
Buell, D.C.....	54, 55, 57	grille	16
Bulled	71	home-made	69
Bureau		monoalphabetic	1, 2
Cipher	100, 118	Playfair	113
Cryptanalytic	115	"Rosicrucian on pig pen"	39, 92
Cryptographic	73	Rosignol	9
Burgoyne, John	12, 16	Route Transposition	48, 53
Burnett, Edmund C	1-9		
Burnside, A.Z.	67, 68, 69, 70		
Cameron, Simon	64, 73		

substitution 102
 "The Court" 77
 transposition 67
 CIPHER—
 alphabet ... 2, 43, 76, 117
 book 67
 books 31
 bureau 100, 118
 clerk 25, 26, 83
 clerks 24, 29, 53, 88, 93
 Federal 75
 War Department 88
 code 84, 97
 Cylinder 85
 device 4
 Anton's 44
 Hawley's 44
 M-94 5, 117
 Thomas Jefferson's ... 4
 devices 114
 disk 22, 39, 43
 Army 113
 Navy 45
 disks 78

Cipher—
 key 30, 68
 Confederate 94
 letter ... 80, 84, 85, 108
 letters 3
 "Machine, Confederate" 85
 Message, ~~Carmack's~~ 90
 No. 1 60
 No. 2 61
 No. 3 63
 No. 4 63, 66
 No. 6 54
 No. 7 54, 55
 No. 9 57, 58, 60
 No. 10 58
 No. 12 .. 56, 57, 58, 64
 of 1902 109
 of the War Department 110
 of the War Department
 1902 107
 operator 60, 82
 operators 70, 83
 phrases 106
 sequences 4



Cipher —

Square..... 84
 Vigenère 75
 system 113
 table..... 44, 117
 telegrams 30
 test 3, 14, 43, 46,
 55, 75, 81, 87
 variants..... 4
 word..... 104
 words 51
 Ciphers8, 32, 53, 60, 67
 116, 118.
 Confederate..... 28
 "Departmental" 67
 Mexican..... 118
 monoalphabetic
 substitution..... 118
 route transposition.... 70
 substitution 116
 transposition 116
 Civil War
 26, 27, 40, 45, 71,
 72, 75, 95, 97, 99,
 100, 114
 Clinton Papers,..... 14
 Clinton, Sir Henry 13, 16, 18

Code

6, 8, 9, 15, 19, 48
 65, 71, 99, 100, 102
 104, 105, 106, 107, 108
 109, 110, 111, 112, 113
 alphabetic..... 40
 American diplomatic.... 10
 cipher 84, 97
 concerted 101
 continental 104
 dictionary 5, 7, 13,
 17, 19
 eight-element..... 36
 enciphered.....74,99,109
 Federal..... 73
 five-element..... 38
 "General Service
 Homographic"..... 37
 Interdepartmental..111,112
 Morse..... 36,89
 numerical..... 7, 8, 9
 open..... 95
 plain..... 20, 109
 signal 35
 tabular 110
 tactical..... 111,112
 telegraphic 103



Code	Comstock, Cyrus E. 30, 31, 32
two-element	37, 43
Code—	
book	99, 108
War Department	110
clerk	109
compilation	117
group, six-letter	109
groups 107, 109, 110, 112	
of 1685	102
"of two Elements" ...	35
phrase	111
word	106
words 53, 56, 60, 61, 65, 66	
73, 105, 109, 117	
Codes	13, 17, 74
commercial	117
Commencement word	71
Commentaries on the	
Laws of England	19
Commission, Mexican	
Monetary	118
Committee of	
Correspondence	12
Committee of	
Secret Correspondence..	5
Committee on	
Foreign Affairs	2
Compilation, code	117
Concerted code.....	101
Confederacy	73
Confederate—	
agents.....	87
armies.....	76
cipher	75
key	94
machine	85
ciphers	28
cryptanalysts	72
cryptographer	93
cryptography	25, 93
espionage systems ..	87, 92
government	84
message	82
Signal Corps	85
Signal Officers	75, 76
State Department	92
systems	75—95
Vigenère table	86
Confederates	
40, 66, 72, 73, 76, 77,	
82, 85, 87, 93, 95.	
Continental Code	104
Continental Morse	
alphabets	109

Conversion	36	Cryptography	13, 22, 23, 24, 26, 34, 64, 77, 93, 95, 99, 101, 115, 118
Corbin, H.C.....	107	Confederate	25, 93
"Countersign Word"	42, 71	Federal	72, 73
"Court cipher, The".....	17	Mexican	117
Crimean War	26	Cryptology	115
Cryptanalysis ...	41, 115, 118	"Culpers, The "	79
Cryptanalyst	42, 93, 118	Cypher.....	10
Federal	78	Dana, Charles A ...	84, 92, 94
Cryptanalysts ...	25, 72, 80	Davis, J.C. Bancroft	98
Confederate	72	Davis, Jefferson	84, 91
Cryptanalytic bureau	115	Deane, Silas	11
Cryptanalytic unit	82	Decipherment	52, 59, 81, 83, 87, 91, 103
Cryptogram ...	37, 70, 84, 92	"Decypher of Mr. L"	14
Cryptograms	26, 35, 95	Dennison, Governor of Ohio ...	47, 48
Cryptographed dispatches..	28	"Departmental Ciphers" ...	67
Cryptographer	13	Differential, two-letter	111, 112
Confederate	93	Diplomatic systems,	96
Cryptographers	72, 75	American	
Cryptographic —		Doyle, Sir Arthur Conan ..	37
bureau	73	Drake, William H.....	55
devices	35		
processes	10		
systems..	1, 5, 26, 28, 36 76, 114, 115		

Eckert, Thomas T....	28, 53	"General Service Homographic Code".....	37
Eddy, C. G.....	63	Geneva Tribunal	98
Eight-element code	36	Gilmore, James R.....	28
Emperor Napoleon III	97	"Gold Bug, The"	102
Enciphered code 74, 99, 109		Grant, Ulysses S	
Enciphered letters	35	29, 30, 31, 33, 60, 65, 71, 78, 97	
Encipherment. 29, 35, 49, 70, 78, 79, 85, 86, 100		Greely, A. N.....	108, 109
monoalphabetic	114	Gregory, J. F.	99, 102
Entick's dictionary 1, 6, 17		Grille	16
Espionage system.....	95	Grilles	13
Eastman, Clyde L.....	116	Halleck, Henry W	
Federal systems	21-74	31, 32, 33, 54, 55, 57, 59, 63	
First World War..74, 100, 112 113, 115		Haswell, John H....	25, 45, 96
Five-element code	38	Hawley, Edwin H	45, 44
Fixed additive	102	Hawley's Cipher Device ...	44
Four-disk device	41	Henry, Patrick	8
Fort Leavenworth	115	Hill, Benjamin H	91
Franklin, Benjamin	2	Hitt, Parker.....	4, 115-118
Freeman, D. S.....	73	Hurlbut, S.A.....	59
Freemont, John Charles ..	50	Indicator	49, 55, 58, 65
Fuller, W. G.....	63	Indicators 51, 54, 56, 61, 66	
Funston, Frederick	103	key	60
Gates, Horatio	3	Ink	
		invisible	12, 19





Ink

secret 10, 13, 18, 19
 sympathetic 11
 Interdepartmental
 code 111, 112
 Jardins, B. M. 114
 Jay, John 1, 6, 11, 12
 Jay, Sir James 11, 18
 Jefferson, Thomas 3, 4, 8, 9
 Jefferson's Cipher Device 4
 Johnston, J. E. 78
 Juarez, Benito 97
 Keith, Alex. Jr. 88

Key

2, 8, 10, 15, 19,
 40, 42, 58, 60, 78,
 79, 80, 81, 82, 83,
 84, 86, 87, 92.

Confederate cipher 94
 numerical 86
 running 86

Key--

book 60
 indicators 60
 letter 80, 85, 108
 numbers 106
 sequence 58
 system, repeating ... 113

Key--

word 2, 3, 42, 44,
 75, 76, 93, 103
 words 49, 117.
 Keys 48, 77, 93, 108
 Kimball, R. E. 114
 Lafayette, Marquis de ... 8
 Lander, F. W. 52
 Lee, Arthur 5, 6
 Lee, Richard Henry 6
 Lee, Robert E. 68, 70, 73
 81, 82, 83
 Lee, William 1, 6, 15
 Lee's Army 21
 Library, William L. Clements
 13
 Lincoln, Abraham
 25, 28, 64, 69
 70, 71, 73, 89
 "List of Arbitraries" 73
 Livingston, Robert... 3, 6, 8
 Lovell, James 2, 3, 15
 M-94, Cipher device... 5, 117
 Macomb, M. M. 115
 Madison, James... 3, 7, 8, 9
 "Manual for the Solution of
 Military Ciphers".... 116
 Markoe, Frank 72





Mauborgne, Joseph O. 115, 116	Morse Alphabets
Maximilian, F. 97	American 109
McClellan, G.W. 47, 49, 50, 52	continental 109
Meade, George Gordon 64	Morse, American 104
Metcalf, F. M. 41	Morse Code 36, 89
Mexican -	Mutilation table 112
cryptography 117	Myer, Albert James
Expeditionary Forces.. 117	21, 22, 34, 38, 41;
Monetary Commission... 118	42, 43, 46, 48, 72,
systems 118	73, 75, 85, 86, 99.
Military Telegraph Corps	Myer's Manual 77
24, 25, 29, 34,	Napoleonic Wars 10
35, 50, 99.	Norton, L. B. 41
Monoalphabetic -	O'Brien, Richard 27
cipher 1, 2	Odell, Jonathan 18, 19
encipherment 114	One-part arrangement 17, 51, 106, 107, 109, 110, 112.
substitution	Open code 95
1, 2, 15, 14,	Peckham, Howard H. 13
15, 35, 38, 42,	Pemberton, J. C. 78, 79
46, 72, 76, 93,	Permutations 38
117	"Permutator" 114
substitution ciphers 118	Pinkerton, Allan C. 48
Monroe, James 8, 9	Plain letter 45, 84, 108
Montgomery, Benjamin F. 101	
Moorman, Frank 116	
Morgan, John H 54	
Morris, Robert 1	



Plum, W. R...	23, 26, 29, 34, 47, 49, 53, 60, 62, 63, 64, 67, 72, 79, 81, 85, 89, 90.	Secret Ink	11, 13, 18, 19
Poe, Edgar Allen	102	Secret Service, United States.....	87,
Polyalphabetic substitution	42, 43, 44, 45, 72, 75, 76, 92, 93.	Secret writing.....	13
Potomac, Army of the..	21, 68	Segismundo, Cecilio.....	103
Pratt, Fletcher	25	Segovia, Lazaro.....	103
"Preliminary War Department Telegraphic Code"	104	Sheridan, Philip H.....	63
Randolph, Edmund	38	Sherman, W. T.	59, 63
Randolf, John	7	Signal, Visual	36
Repeating key system ...	113	Signal—	
Riverbank Laboratories..	116	Corps.....	24, 34, 35 44, 99.
Robinson, Stephen L.....	56	Confederate	85
"Rosicrucian or pig-pen cipher".....	39, 92	Corps Volunteers	100
Rossignol, Antoine.....	9	Disk.....	39
Rossignol cipher	9	Officers, Confederate	75, 76
Route transposition	46, 48, 72 73, 74, 93	School, Army.....	115, 116
cipher	48, 53, 70	Signals.....	21, 22, 34, 35
Running key.....	86	Slater, Robert.....	99
Scott, Thomas A.....	27	Smith, E. Kirby	56, 80, 81, 82
Second World War.....	116	Spanish-American War.....	99, 100, 101, 102
		Spottswood, W. G.....	107
		Square	78

Square		Sympathetic ink	11
Cipher	84	Tabular code	110
Vigenere ..	85, 86, 93, 108	Tactical code	111, 112
Vigenere cipher	75, 75	Tagalo	103
Stager	30, 31, 33, 47, 48; 49, 50, 53, 54, 55, 58, 67, 73.	Taylor, J.D.....	103
Stansbury, Joseph.....	19, 20	Telegraph	24, 26
Strouse, David.....	27	Telegraphic Code of 1885 99-100, 102	
Stuart, J.E.B.....	21	"Telegraphic Code to Insure Secrecy in the Transmission of Telegrams".....	99
Substitution		Telegraphy	26
Monoalphabetic..	13; 14; 15, 16, 35, 38, 46	Text	
Polyalphabetic...	43, 44, 75, 92, 93	cipher	3, 14, 43, 46, 53, 73, 81, 87.
Substitution.—.....	2	plain	4; 14, 35, 36, 55, 57, 58, 62, 70, 77, 79, 80, 81, 83, 86, 93, 101, 104.
Cipher.....	1, 102	Thomas, G. H.....	55, 63
Ciphers.....	116	Tinker, Charles A.	28, 53, 89
Substitutions.		To put up...;.....	71
Monoalphabetic	1, 2, 42, 72, 76, 93, 117	<u>Traicté des chiffres ou</u> <u>secrets manières d'escrire</u>	75
Polyalphabetic...	42, 45, 72 78, 118.	Transposed alphabet	1
Subtractive.....	102	Transposition	15, 35, 47, 49, 56, 58, 67, 70, 72, 100.
Swartz, Charles E.....	116		
Symbols.....	88, 89, 92		
two-element.....	36		

- Transposition
 Columnar 48
 Route 46, 48, 72,
 73, 74, 93
- Transposition—
 cipher 67, 116
- Truesdell, Karl 116
- Two-element code 37, 43
- Two-element symbols 36
- Two-letter
 differential 111, 112
- Two-part
 arrangement 17
- United States Military
 Telegraphic Corps
 24, 26—34, 99
- Van Deman, Ralph H. 114
- Van Doren, Carl 18
- Van Nostrand, D. 23
- Variants 2, 9, 37, 38
 43, 49, 51, 61
- cipher 4
- Vigenère, Blaise de 75
- Vigenère—
 Cipher square .. 73, 75, 84
 table 13, 14, 75
 77, 80.
 table, Confederate 86
 square 85, 86, 93, 108
- Vigenère's book 75
- War
 Civil... 21—98, 26, 27, 40,
 45, 71, 72, 75, 96,
 97, 99, 100, 114
- Crimean 26
- First World ... 74, 100, 112,
 113, 115
- War of 1812 96
- Second World 116
- Spanish-American
 99, 100—103
- War College Division 115
- War Department
Telegraph Code 1906 ...
 108, 110
- War Department
Telegraph Code 1915...
 110—113
- War Department
 Telegraph office 28
- War Department
Telegraphic Code 1899...
 103—107
- Washington, George 8, 10, 11
- Weiskopf, Victor 118
- "Western Union
 Telegraphic Code,"
 104, 105, 106
- Wilson, J. J. S 50
- Yardley, Herbert O 102

SRH-001