American Systems in the Revolutionary War

A Brief History

This is a chapter from an unpublished history written by members of the staff of the U.S. Army Signal Security Agency during World War II. The complete history is to be published as part of the United States Cryptologic History series.

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 Lee 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."[1]

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. 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 monalphabetic 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 Z. The cipher alphabet was apparently a series of numbers, probably in numerical order. Burnett 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."[2]

Robert Livingston used this cipher in his first correspondence with John Adams, who apparently did not understand it. 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." 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

[1] Edmund C. Burnett, "Ciphers of the Revolutionary Period," *The American Historical Review*, vol.XXII (1916–1917), 330, citing Ford's edition of the *Letters of William Lee*, vol. II, 417, 666.

[2] p. 351.

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 probable word method in America. Madison's footnote giving the key word was later found: it was probably, according to Brunett, "Cupid," the name of a slave who used to serve Madison.

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. 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 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 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 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.

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 Correspondence. 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*, a dictionary suggested for this purpose also by John Jay.

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.

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 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. The Virginia delegates to Congress in 1782 wrote officially to their governor in such a numerical code, the code groups being the numbers 1–846. A great deal of the private correspondence between James Madison and John Randolph during the year 1782 was transmitted in this code. 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." 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 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; "Edmond 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. [3]

[3] p. 333.

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 existence and permit the reading of letters otherwise undeciphered. Using the printed forms which Robert Livingston 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.

"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.

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,"[4] 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 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.

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.[5]

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.

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.[6]

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 in invisible ink "the first authentic account which Congress received, of the determination of the British Ministry to reduce the Colonies to unconditional submission. By the

[4] Antoine Rossignol, a sixteenth century cryptographer. See Fletcher Pratt, *Secret and Urgent* (Garden City, 1942), pp. 127–128.

[5] John C. Fitzpatrick, *The Writings of George Washington* (United States Govenment Printing Office, Washington, 1931–1944), vol. XXX, p. 169.

[6] Victor Hugo Paltsits, "The Use of Invisible Ink for Secret Writing during the American Revolution," *New York Public Library Bulletin*, vol. XXXIX (1935), p. 362; Haswell, p. 87–88.

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.