Fall 2019

# Secrecy in the American Revolution

Abigail N. Minzer
*Gettysburg College*

## Recommended Citation

Minzer, Abigail N., "Secrecy in the American Revolution" (2019). *Student Publications*. 770.
https://cupola.gettysburg.edu/student_scholarship/770

# Secrecy in the American Revolution

## Abstract

This paper analyzes how the use of various cryptographic and cryptanalytic techniques affected the American Revolution. By examining specific instances of and each country's general approaches to cryptography and cryptanalysis, it is determined that America's use of these techniques provided the rising nation with a critical advantage over Great Britain that assisted in its victory.

## Keywords

cryptography, American Revolution, Revolutionary War, Spies, Cryptanalysis

## Disciplines

Applied Mathematics | History

## Comments

Written for FYS 164-2: Cryptography: the Science of Secrecy.

Abby Minzer

Professor Glass

Cryptography

9 Dec. 2019

# Secrecy in the American Revolution

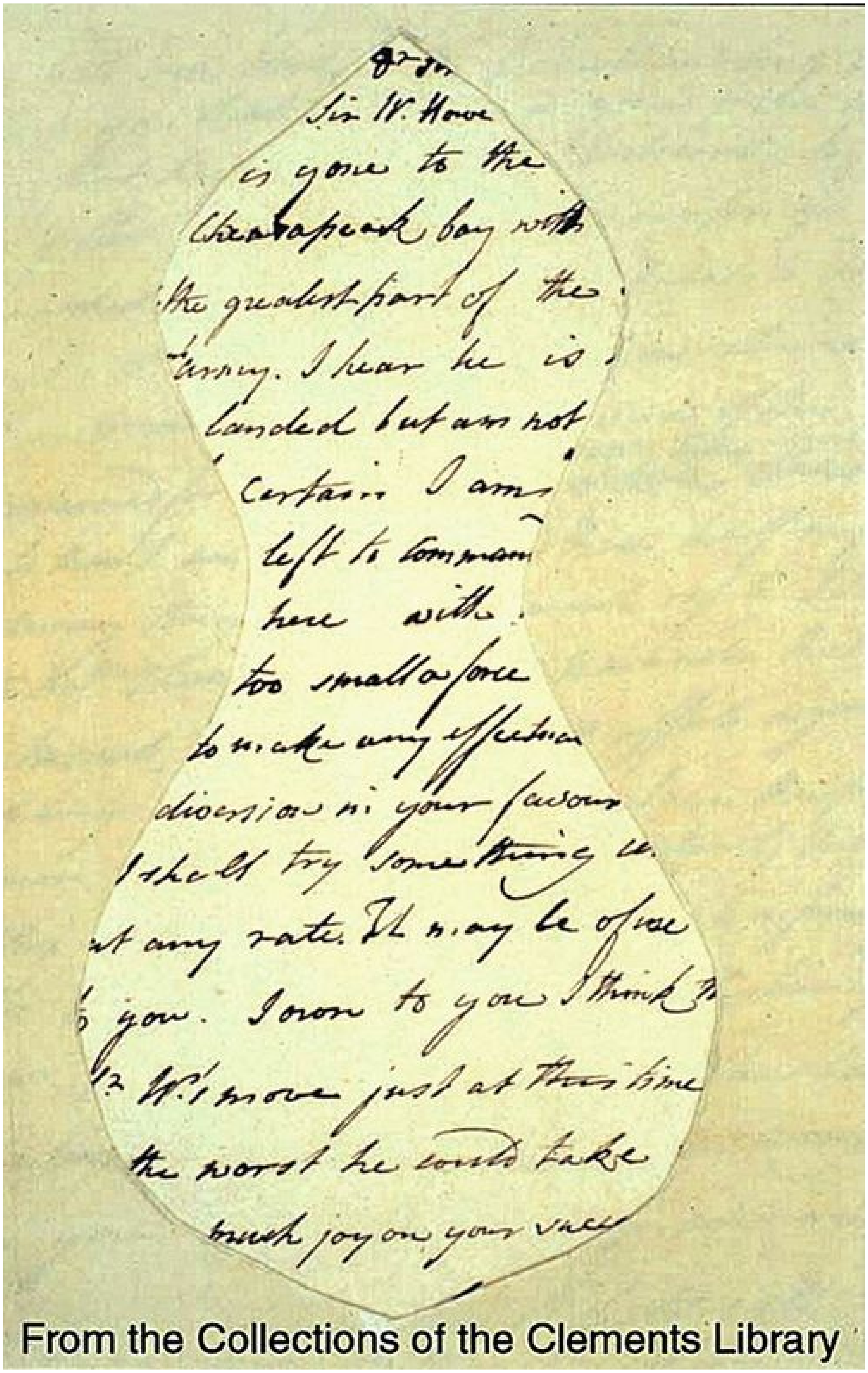
Throughout history and across the world, various types of cryptography have been used as a method for sending sensitive information while maintaining its secrecy. Many of the most prominent examples of cryptography that are studied occurred in military contexts. One lesser discussed, but exceptionally important, historical situation in which cryptography was used is now known as the American Revolutionary War. Various individuals such as John Jay and James Lovell were some of the main forces that propelled cryptography forward in America both during and after the war. While both sides in the American Revolutionary War used secretive techniques in their attempts to communicate vital war-related information discreetly, cryptanalysis and both military and personal uses of cryptography played a role in the Americans' eventual triumph over the British,

Historians studying the American Revolution generally acknowledge that neither the British nor the American forces were using the most advanced cryptographic techniques known at that time (Dooley 43-44). However, the cryptography that was used played important roles in several vital ways. Each side utilized types of cryptography that were both similar and different. For example, both sides used monoalphabetic ciphers, polyalphabetic ciphers, and invisible ink. Wilcox also discusses the ways in which each side used different forms of visual signals as codes (4, 35). Only the British forces are known to have significantly used book and dictionary codes and “masks,” while only the Americans are known to have used code words and homophonic ciphers (Dooley 45-56).

Of the many types of cryptography used during the American Revolutionary War, each had specific moments of crucial importance at various times when maintaining secrecy was either successfully achieved, leading to beneficial results for the side employing the cryptography, or failed and the message’s contents were read by opposing forces, which led to detrimental results for the side that employed the cryptography and beneficial results for the side that broke it. One specific use of cryptography was when Benedict Arnold, an American general in Washington’s army, secretly spied for the British and sent them information using a combination of book codes and invisible ink (Dooley 48-51). When they wanted to send messages to each other, Arnold and his British co-conspirator would first write out the plaintext of their messages. Then, they would look for each word of the plaintext in *Bailey’s Dictionary* and replace each word with the page number, column number, and the number indicating which word in the column was being referenced. An example of a word encrypted via this system would be 6.1.14, which would refer to the fourteenth word in the first column on the sixth page of the book (Wilcox 24-26). After the ciphertext was completely assembled, it would be written in invisible ink and sent via a courier (Dooley 49). Arnold was able to use this method of secret communication for more than a year. Eventually, however, Arnold’s British co-conspirator, who had been disguised as a civilian named John Anderson with a pass written by Arnold himself, was found by American soldiers with papers regarding West Point’s fortifications hidden in his boot. They were not encrypted, so he confessed his true identity as British Major John Andre after learning that the papers were being taken all the way up the chain of command to

Washington himself (Wilcox 30-32). Andre was tried and executed as a spy. The West Point papers he had hidden in his boots and Arnold's contribution to his disguise incriminated Arnold to the point where he fled behind British lines. This is an example where intercepting the enemy's use of cryptography was vital for the Americans, as Arnold had been planning a way to surrender West Point to the British (26-29). Unfortunately for the Americans, they too lost a valuable spy due to a similar incident of weak steganography. Nearly identically to Arnold's co-conspirator, an American spy named Nathan Hale was found behind British lines with incriminating, unencrypted papers hidden in his boots (10). He too was executed as a spy. However, Hale's loss to the Americans was not nearly so great when the British lost Andre and Arnold as the duo had provided much more concretely valuable information to the British and Arnold had been about to surrender significant territory to them (47).

A more complex use of steganography can be found in a letter sent by British General Sir Henry Clinton to British General John Burgoyne (Dooley 45-48). Clinton first wrote his real message by holding an hourglass-shaped "mask" over the page and writing only inside of its outline. From there, he filled in the rest of the page with words that made the letter seem innocent and misleading from its true purpose. Clinton sent the letter to Burgoyne with one courier and the "mask" via another, so that if one was intercepted without the other, it would be useless. This was an example of a successful steganographic communication during the Revolutionary War. Another British success involving a more advanced use of cryptography involves General Howe (Wilcox 11-12). He wrote a message describing his intent to change the course of his army's march on several "long, narrow" pieces of paper that he then hid inside of a quill feather that was hollowed on the inside.



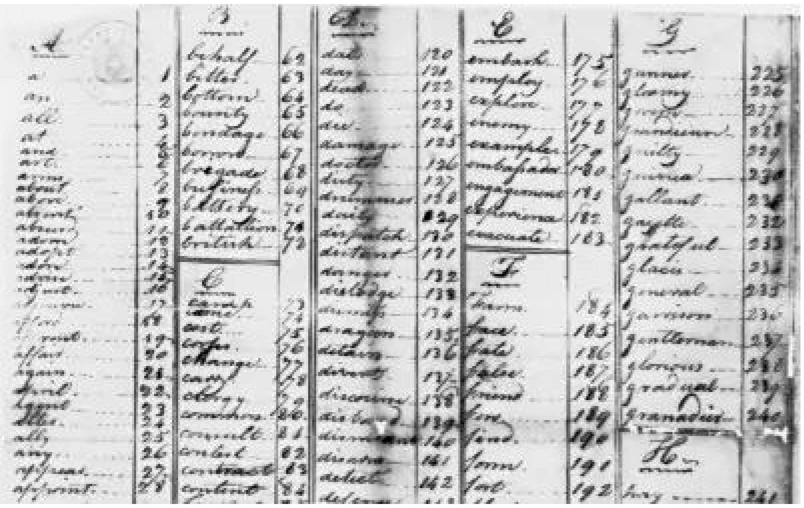
Dr Sr
Sir W. Howe
is gone to the
Chesapeak bay with
the greatest part of the
army. I hear he is
landed but am not
certain. I am
left to command
here with
too small a force
to make any effectual
diversion in your favour
I shall try something a
at any rate. It may be of use
to you. I own to you I think Si
W's move just at this time
the worst he could take
much joy on your succ

From the Collections of the Clements Library

*Clinton's hourglass "mask" (Dooley 47)*

On the American side of things, one of the most substantial accomplishments regarding cryptography was the creation of the Culper spy ring, which was a secret courier system used for sending important messages amongst the Continental Army without being intercepted by the British (Dooley 52-53). Because this spy ring consisted of a group of like-minded individuals dedicated to utmost secrecy, it became a breeding ground for many cryptographic developments. One such development was the creation of the "sympathetic stain" by Sir James Jay. Unlike other forms of invisible ink commonly in use at the time, Jay's creation consisted of using two chemical compounds, one to write the message and the other to brush over the invisible message and reveal it. For further secrecy, the spies would often write messages in invisible ink on one paper that they would hide in a stack of other papers, thereby using two steganographic techniques at once (Wilcox 22). One specific instance in which the Culper ring's use of efficient secret communications proved crucial occurred during the arrival of the French fleet to Newport, Rhode Island. It was later discovered that the British only knew about the details of the French fleet's arrival due to information passed along by Benedict Arnold. An American spy in the Culper ring named Robert Townsend discovered that 8,000 British troops were planning to attack and overwhelm the French force before they could make their landing ashore. He wrote a message on a piece of paper informing someone "that the goods he had requested were not currently available" (22-23). On the back, his real message about the British plan to intercept the French aid was written using the sympathetic stain. After the letter exchanged hands between a few other spies, Alexander Hamilton received the information on behalf of General George Washington. He knew about the Culper spy ring's cryptographic techniques and was therefore able to apply the correct chemical compound to the letter that allowed him to read its contents.

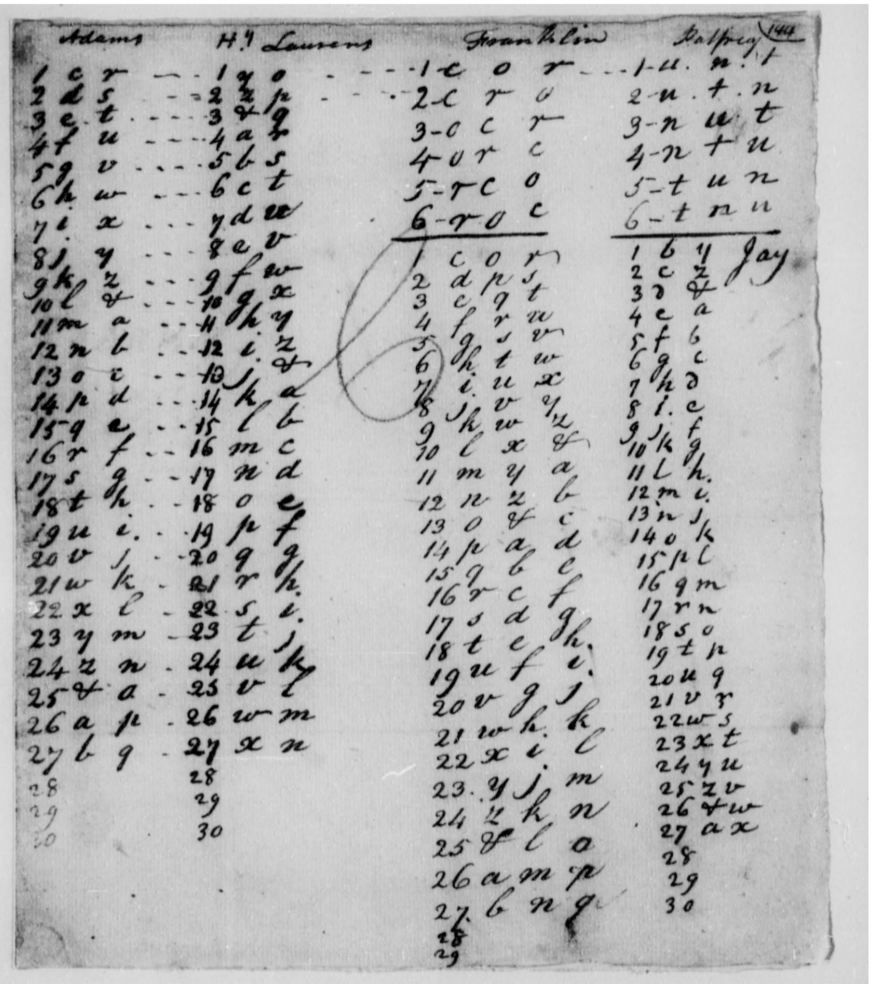
Hamilton was then able to warn the Americans who were awaiting the French fleet. When Washington was informed of the British plans, he decided to move his forces towards New York City as if he intended to take advantage of the British troops' absence to attack it. When the British forces rushed from Newport back to New York City to protect the British-controlled city, the French fleet was able to land successfully in Newport (24). Another way that the Culper spy ring concealed information involves the use of code words. They created alternate words for 763 commonly used words and then used a "mixed alphabet monoalphabetic substitution cipher" to disguise other words in their communications (Dooley 53-56).



| A |  | B |  | D |  | E |  | G |  |
|---|---|---|---|---|---|---|---|---|---|
|  |  | behalf | 62 | date | 120 | embark | 175 |  |  |
| a | 1 | better | 63 | day | 121 | employ | 176 | gunner | 225 |
| an | 2 | bottom | 64 | dead | 122 | explain | 177 | glory | 226 |
| all | 3 | bounty | 65 | do | 123 | enemy | 178 | [illegible] | 227 |
| at | 4 | bondage | 66 | die | 124 | example | 179 | [illegible] | 228 |
| and | 5 | borrow | 67 | damage | 125 | embassador | 180 | guilty | 229 |
| art | 6 | brigade | 68 | doctor | 126 | engagement | 181 | guinea | 230 |
| arm | 7 | business | 69 | duty | 127 | [illegible] | 182 | gallant | 231 |
| about | 8 | battery | 70 | drummer | 128 | [illegible] | 183 | gazette | 232 |
| above | 9 | battalion | 71 | [illegible] | 129 |  |  | grateful | 233 |
| absent | 10 | british | 72 | dispatch | 130 |  |  | glacis | 234 |
| absence | 11 | C |  | distant | 131 | F |  | general | 235 |
| adorn | 12 | camp | 73 | danger | 132 | farm | 184 | garrison | 236 |
| adopt | 13 | came | 74 | dislodge | 133 | face | 185 | gentleman | 237 |
| adore | 14 | cost | 75 | [illegible] | 134 | fate | 186 | glorious | 238 |
| [illegible] | 15 | corps | 76 | dragoon | 135 | false | 187 | gradual | 239 |
| [illegible] | 16 | change | 77 | detain | 136 | friend | 188 | grenadier | 240 |
| [illegible] | 17 | carry | 78 | direct | 137 | fire | 189 | H |  |
| [illegible] | 18 | clergy | 79 | discover | 138 | fund | 190 | hay | 241 |
| amount | 19 | [illegible] | 80 | [illegible] | 139 | form | 191 |  |  |
| affair | 20 | consult | 81 | [illegible] | 140 | fat | 192 |  |  |
| again | 21 | conduct | 82 | [illegible] | 141 |  |  |  |  |
| april | 22 | contract | 83 | [illegible] | 142 |  |  |  |  |
| august | 23 | content | 84 |  |  |  |  |  |  |
| alter | 24 |  |  |  |  |  |  |  |  |
| ally | 25 |  |  |  |  |  |  |  |  |
| any | 26 |  |  |  |  |  |  |  |  |
| appear | 27 |  |  |  |  |  |  |  |  |
| appoint | 28 |  |  |  |  |  |  |  |  |

*Some of the Culper spy ring's code words ("Culper Spy Ring Code")*

Other ciphers were developed for the purposes of American diplomatic affairs, which impacted the foreign aid that the Americans received during the war and contributed to their eventual victory. These ciphers included most notably a homophonic cipher and a polyalphabetic cipher, the first of which was developed by Charles Dumas (57). Although Dumas was neither American nor British himself, Ben Franklin paved the way for him to become an American-employed agent, leading Dumas to develop a homophonic cipher for use in American diplomatic encryption (Weber, “James Lovell” 75). He did this by taking a French essay by Emer de Vattel and numbering the letters up to 682 (Dooley 57). Each letter of the English alphabet then had multiple numbers associated with it, except for “w,” which was represented by two “v”s, and “k,” which was represented with a “c.” Whenever someone wanted to write a letter using this cipher, he or she had to replace each letter he or she wanted to use with one of the numerical values assigned to the letter by Dumas. In order for this cipher to live up to its potential for security, the numerical values would have to be chosen randomly; in reality, people who used this cipher often used the first few numbers assigned to each letter. James Lovell developed a polyalphabetic cipher intended for American diplomatic use as well (Weber, “James Lovell” 76). In Lovell’s cipher, one only needs to remember a keyword to use it. The first three letters of the keyword would be written out with a “1” written to the left of them. Underneath each letter, the user would simply continue writing out the alphabet vertically in three columns, labeling each row numerically, and including an ampersand in between “z” and “a.” The user would then have three 27-character alphabets side-by-side. One would encode the first letter in a message by looking for that letter under the first column and writing the number to its left. For the next letter, one would repeat that process in the second column, then the letter after that would use the third column, the fourth letter would go back to the first column, etc. While Lovell’s system, unlike Dumas’, seems like it ought to have been easily memorized and used, Lovell added complex rules involving the numbers 28, 29, and 30 that, when added to the already multi-step process of encoding and deciphering messages, often served to confuse and frustrate others trying to communicate with Lovell. For example, the three extra numbers were sometimes randomly added to messages as “balks,” but other times, 28 followed by 29 indicated that letters had been enciphered in the normal order of column 1, then column 2, then column 3, while 29 followed by 28 meant that letters had been enciphered in the reverse order of column 3, column 2, column 1. The complexity of Lovell's and Dumas' ciphers provided the Continental Army with secure means of communications with overseas diplomats who worked to persuade other nations to support the American cause. Without these ciphers, if these communications had been intercepted, Britain or other nations could have taken actions that may have adversely affected the outcome of the war.



144

| Adams | | |
|---|---|---|
| 1 | c | r |
| 2 | d | s |
| 3 | e | t |
| 4 | f | u |
| 5 | g | v |
| 6 | h | w |
| 7 | i | x |
| 8 | j | y |
| 9 | k | z |
| 10 | l | & |
| 11 | m | a |
| 12 | n | b |
| 13 | o | c |
| 14 | p | d |
| 15 | q | e |
| 16 | r | f |
| 17 | s | g |
| 18 | t | h |
| 19 | u | i |
| 20 | v | j |
| 21 | w | k |
| 22 | x | l |
| 23 | y | m |
| 24 | z | n |
| 25 | & | a |
| 26 | a | p |
| 27 | b | q |
| 28 | | |
| 29 | | |
| 30 | | |

| H.y Laurens | | |
|---|---|---|
| 1 | y | o |
| 2 | z | p |
| 3 | & | q |
| 4 | a | r |
| 5 | b | s |
| 6 | c | t |
| 7 | d | u |
| 8 | e | v |
| 9 | f | w |
| 10 | g | x |
| 11 | h | y |
| 12 | i | z |
| 13 | j | & |
| 14 | k | a |
| 15 | l | b |
| 16 | m | c |
| 17 | n | d |
| 18 | o | e |
| 19 | p | f |
| 20 | q | g |
| 21 | r | h |
| 22 | s | i |
| 23 | t | j |
| 24 | u | k |
| 25 | v | l |
| 26 | w | m |
| 27 | x | n |
| 28 | | |
| 29 | | |
| 30 | | |

| Franklin | | | |
|---|---|---|---|
| 1 | c | o | r |
| 2 | c | r | o |
| 3 | o | c | r |
| 4 | o | r | c |
| 5 | r | c | o |
| 6 | r | o | c |

| Palfrey | | | |
|---|---|---|---|
| 1 | u | n | t |
| 2 | u | t | n |
| 3 | n | u | t |
| 4 | n | t | u |
| 5 | t | u | n |
| 6 | t | n | u |

| | | | |
|---|---|---|---|
| 1 | c | o | r |
| 2 | d | p | s |
| 3 | e | q | t |
| 4 | f | r | u |
| 5 | g | s | v |
| 6 | h | t | w |
| 7 | i | u | x |
| 8 | j | v | y |
| 9 | k | w | z |
| 10 | l | x | & |
| 11 | m | y | a |
| 12 | n | z | b |
| 13 | o | & | c |
| 14 | p | a | d |
| 15 | q | b | e |
| 16 | r | c | f |
| 17 | s | d | g |
| 18 | t | e | h |
| 19 | u | f | i |
| 20 | v | g | j |
| 21 | w | h | k |
| 22 | x | i | l |
| 23 | y | j | m |
| 24 | z | k | n |
| 25 | & | l | o |
| 26 | a | m | p |
| 27 | b | n | q |
| 28 | | | |
| 29 | | | |

| Jay | | |
|---|---|---|
| 1 | b | y |
| 2 | c | z |
| 3 | d | & |
| 4 | e | a |
| 5 | f | b |
| 6 | g | c |
| 7 | h | d |
| 8 | i | e |
| 9 | j | f |
| 10 | k | g |
| 11 | l | h |
| 12 | m | i |
| 13 | n | j |
| 14 | o | k |
| 15 | p | l |
| 16 | q | m |
| 17 | r | n |
| 18 | s | o |
| 19 | t | p |
| 20 | u | q |
| 21 | v | r |
| 22 | w | s |
| 23 | x | t |
| 24 | y | u |
| 25 | z | v |
| 26 | & | w |
| 27 | a | x |
| 28 | | |
| 29 | | |
| 30 | | |

*James Lovell's polyalphabetic cipher keys for separate communications with John Adams, Henry Laurens, Benjamin Franklin, William Palfrey, and John Jay (Lovell)*

Visual signals were infrequent but important types of cryptography used during the American Revolution. One such example can be found with Paul Revere (Wilcox 4-5). He and his compatriots in Boston knew that if two lanterns were hung and lit in the North Church, it meant that the British were crossing the Back Bay. They would then send riders to warn revolutionists in Lexington. This system was used when the British did end up crossing the Back Bay. Its success in allowing the colonists to prepare for the arrival of British forces allowed them to have enough time to assemble a large enough militia to prevail at Concord, keep their supplies safe from British raids, and prevent the capture of prominent revolutionaries Sam Adams and John Hancock. The British used visual signals in a different way. During the Battle of the Chesapeake Capes, the British used flag signals to send messages from different ships (35). American spies managed to steal the codebook for the flag signals, which provided the American generals with an advantage that allowed them to win the battle.

There are some instances in which cryptographic developments were made during the Revolutionary War but for private rather than military use. However, these developments were related to the war in that the cryptography was being developed and used by prominent Americans who were discussing the future of the country that was fighting for its independence. One particularly intriguing example of this is found in letters exchanged between Elbridge Gerry and James Lovell (Billias 3). Both men were knowledgeable cryptographers and cryptanalysts. They began writing to one another using a code that is still believed to be uncracked today. It is suspected to have been a transposition code, a dictionary or book code, a homophonic cipher, a Vigenère-like cipher, or “a collection of words, syllables, and letters more or less arbitrarily arranged and numbered.” Another example of cryptography used in private correspondence at this time was displayed by John Jay (Weber, “A Masked Dispatch” 375-376). Brother to the James Jay who invented the “sympathetic stain,” John Jay was also a skilled cryptographer who took great care to ensure that his personal correspondence was securely encrypted. He briefly used a simple substitution cipher in which each letter of the alphabet was replaced by a number 1-26, though the numbers were scrambled so that “a” was not 1 and “z” was not 26. Soon after, John Jay insisted that he and his correspondent Robert Livingston use a dictionary code instead, where each word would be represented with the page number; column number, in which the first column was referred to as “c,” the second column as “a,” and the third as “b;” and the number of words it is from the top plus 7. While that code had used a French dictionary, Jay often chose to base a dictionary code on *Entick’s Spelling Dictionary* with other correspondents. When using that dictionary, he instructed them to refer to pages in reverse order and count words down from the top of the page. Instead of using an explicit letter to reference which column the word was in, they were supposed to place a dot over the first or second number to show whether the word was in the first or second column. For one acquaintance, he added that they had to add 20 to the page number and 10 to the number of words down from the top of the column the desired word was. While Jay seems to have been the most “demanding” in terms of his encrypted overseas communications, it also seems that his mistrust was warranted, as European nations regularly inspected foreign mail in acts of espionage. As America was not yet a strong independent nation, the individuals who were corresponding about it required the utmost privacy in order to ensure that neither the war effort itself nor the beginning of the United States after the war could be threatened by more powerful nations who had easy access to the correspondence of America’s most important individuals. Jay often tried to convince other prominent Americans of the importance of cryptography, but individuals such as John Adams, who had struggled immensely with James Lovell’s ciphers, were not keen on utilizing even more complex codes and ciphers (376-377).

Cryptanalysis was developing in tandem to cryptography in America during the Revolutionary War (Dooley 59). James Lovell was one of the main early contributors to this field. He successfully deciphered many British messages during the American Revolution, including some that proved highly relevant to America’s victory at Yorktown. Lovell was able to identify patterns of weakness in British ciphers that offered the Americans shortcuts in their decrypting (Weber, “James Lovell” 84). For example, he noticed that, rather than completely changing the keys to their mixed alphabet ciphers, the British would simply shift it so the same mixed cipher alphabet aligned with different letters of the plaintext alphabet. Lovell’s cryptanalysis played an especially important role near the end of the war, when the Americans intercepted a message from General Clinton to Commander Cornwallis. After two days, Lovell had successfully decrypted it and realized that Clinton would be unable to assist Cornwallis at Yorktown until a certain time. The Americans were then able to pass the message along and pretend that they didn’t know its contents. They began a siege at Yorktown while Cornwallis was desperately awaiting assistance from Clinton (Wilcox 40). As a result, the British soon requested to negotiate the surrender of York and Gloucester to the Americans. Not long after that, the Americans intercepted and decrypted a message from Clinton to Cornwallis stating that the former was sailing towards the latter with aid. But the Americans alerted the French fleet, which positioned itself to ward off potential attackers. This brought an end to the American Revolutionary War. Another vital example of cryptanalysis that occurred before the war’s end, however, was the discovery of a British spy (Wilcox 7-10). Dr. Benjamin Church was working as chief physician in the Continental Army. He was also sending letters to British General Gage, sending information about such things as the locations of the Continental Army's supplies, which ended up causing Gage to head towards Lexington and Concord, where the American Revolutionary War officially began. Eventually, one of Church's letters, addressed to British Major Cane, found its way to Washington's hands. It was encrypted, so they could not prove his guilt, and he refused to decrypt the letter himself. At that point, Dr. Samuel West, Elisha Porter, and Elbridge Gerry each offered to attempt to decrypt the letter for Washington. They all quickly determined that the letter had been encrypted using a form of monoalphabetic substitution in which each letter of the plaintext alphabet was replaced by a specific number, letter, or symbol. Although Church's use of numbers and symbols in his monoalphabetic substitution cipher was unusual, and therefore he may have believed it would provide extra security, it did not actually add any extra difficulty to the task faced by the cryptanalysts. Within a couple of days, they were able to provide Washington with the plaintext of the letter. This proved Church's guilt as a spy, and he was jailed and later exiled, where he presumably died in a shipwreck. The use of American cryptanalysis in revealing the contents of Church's letter saved the Americans from any further damage Church could have caused as a British spy. As the British placed no emphasis on cryptanalysis during the war, instances such as this gave the Americans an advantage.

When the war drew to a close, the use of codes and ciphers in America drastically declined and virtually ceased militarily (Dooley 60). However, they were still frequently utilized to ensure that communications with the nation's overseas diplomats remained secure. During these early years of the United States, some of the most frequently used forms of encryption were code lists, Dumas' cipher, and various systems designed by Lovell (Wilcox 41-46). Code lists were often generated from a pre-existing sheet that had a column of numbers on one side and a column of alphabetically-arranged words, letters, or syllables on the other side. In order to individualize the code, a user would randomly write the words, letters, or syllables next to the numbers and then fill in the corresponding numbers next to the words, letters, or syllables in the second column. This two-step process would ensure that it would be easy to encrypt messages using the column arranged in alphabetical order and decrypt messages using the column arranged by numerical order. Dumas' homophonic cipher, as discussed earlier, was also heavily in use for diplomatic communications at this time. Though James Lovell's systems confused and drew complaints from many, they were nonetheless frequently used for encryption. Though his polyalphabetic cipher, described earlier, could be memorized because of its use of a simple keyword, it often resulted in users making many errors, including by Lovell himself, who is noted to have once made five significantly confusing errors in encryption in one letter (Weber, "James Lovell" 83-84). Furthermore, the problem of key distribution meant that Lovell would send hints as to what the keywords were, and these hints were often so obscure that his correspondents could not figure them out and sometimes even went so far as to forward his letters to other people in hopes of receiving help. Also during and after the war, Thomas Jefferson began to try his hand at cryptography (Dooley 60). He often used nomenclatures, which were lists of pre-determined codes for specific words, or Lovell's polyalphabetic cipher when he wrote to James Madison and Edmund Randolph. In 1795, Jefferson created a tool that could encrypt messages polyalphabetically. This device was used by assembling 36 wooden disks on a metal dowel. Each wooden disk had a mixed alphabet engraved around its circumference. The key for someone using Jefferson's cipher wheel would be the order in which the disks were hung on the dowel. Once the disks were assembled in the order of the key and someone wanted to encrypt a message, they only had to turn each disk until the first 36 letters of the desired message's plaintext aligned in the same row on the 36 disks. Then, the user could pick a different row and use the first 36 letters of that row to begin the message. The recipient of a message that had been encrypted with this device would also have to possess an identical version of the device in order to decrypt it. Then, they could just put the disks in the order dictated by the key and rotate the disks so that the first 36 letters of the ciphertext all appeared in a row. From there, the recipient could simply search the other rows for messages that would make logical sense as plaintext.

The American Revolutionary War introduced Americans to the overall importance of encryption and set the stage for the new nation's later contributions in the field. During this period of conflict, both the British and American forces employed various methods of cryptography for military and private purposes; however, American cryptanalysis efforts contributed towards their eventual prevail over the British, at which point the continued use of cryptography in diplomatic communications offered the new nation a secure beginning.

# Works Cited

Billias, George Athan. “Elbridge Gerry's Letter Code.” *Manuscripts*, vol. 20, no. 4, 1968, pp. 3–13. *America: History & Life*.

“Culper Spy Ring Code.” *Mount Vernon*, Mount Vernon Ladies' Association of the Union, https://www.mountvernon.org/education/primary-sources-2/article/culper-spy-ring-code/.

Doodley, John F. *History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms*. Springer, 2018.

Lovell, James. “Lovell's Cipher.” *National Archives*, The National Archives of the United States, https://www.archives.gov/.

Weber, Ralph E. “James Lovell And Secret Ciphers During The American Revolution.” *Cryptologia*, vol. 2, no. 1, 1978, pp. 75–88., doi:10.1080/0161-117891852811.

Weber, Ralph E. “A Masked Dispatch.” *Cryptologia*, vol. 14, no. 4, 1990, pp. 374–380., doi:10.1080/0161-119091865048.

Wilcox, Jennifer. *Revolutionary Secrets: Cryptology in the American Revolution*. *Revolutionary Secrets: Cryptology in the American Revolution*, Center for Cryptologic History, National Security Agency, 2012.