2021

The History of American Cryptology Prior to World War II

Robert Sawyers

The History of American Cryptology Prior to World War II

Foreword

Throughout the semester, I was captivated by the ciphers and cryptanalysis techniques (the German Enigma, the Japanese PURPLE, and the American SIGABA) used during World War II on account of their many mechanical intricacies, complexities, and resulting strong security. During this war, cryptology grew exponentially in tandem with technology. Technology allowed humans to mechanize encryption and decryption systems, tremendously increasing the efficiency and security of any cipher. Furthermore, cryptology developed out of necessity. When at war, a weak cipher or failed cryptanalysis attack can cost hundreds of lives or crucial loss of territory, intensifying the need to maintain secret communication and avoid leaking information. Subsequently, entire cryptology organizations became a relevant battle tool, which is most clearly depicted by the American women codebreakers during World War II. World War II proved to be a notable turning point in the grand scheme of cryptology; it was the end of first-generation cryptology and beginning of modern cryptology. Yet, cryptology also depended on an established foundation that allowed its advancement. The foundation for modern cryptological techniques was established during World War II and the Cold War. Therefore, I wondered what the cryptological foundation was prior to World War II and, more generally, the era of modern cryptology.

Having studied the American women codebreakers, I was curious to research the United States' cryptological roots and the foundation which was built for modern cryptology. To preserve some parallels between the two eras of cryptology, I focused on wartime cryptology which led me to two instrumental wars in American history: the Revolutionary War and the Civil

War. This paper will explore these two tremendously influential events in the history of American cryptology, which laid the foundation for World War II and modern era cryptology.

Throughout the Revolutionary War, cryptology took many different forms. American cryptology possessed similar traits as seen with the four classical ciphers we studied—the Caesar cipher, the Playfair cipher, the Rail Fence cipher, and the Columnar Transposition cipher. These ciphers share a simplistic encryption method which retains the ability to hand encipher messages in an intricate and secretive way. Since cryptology spread to Europe much earlier than to the United States, the U.S. was not yet experienced in this field. Nonetheless, American cryptology steadily grew. The perception of threat was the driving factor in cryptology's development as a war for independence requires sending secure, secret messages to avoid disaster.

The Civil War was the optimal environment for cryptology to grow and advance due to the invention of the telegraph. An added level of complexion comes into play because both the Confederate and Union armies stemmed from the same origins. Each side knew its adversary inside and out, thus novel and innovative methods of communications were more crucial than ever.

The Revolutionary War

"British attempts to assert tighter control over its North American colonies and the colonial resolve to pursue self-government" ignited rising tensions between Britain and her colonies and more importantly, "a colonial independence movement and the Revolutionary War" (AP, n.d.). A little more than a decade before, Britain defeated France in the Seven Years War, which spanned from 1756 to 1763. France was forced to relinquish its control of North American territory, and Britain hoped to reinforce its authority over the colonies. The Proclamation of 1763, a regulation which restricted colonists from expanding westward past the Appalachian

Trail, was the first of many British attempts to reassert its dominance (AP, n.d.). Additionally, the debt which Britain plummeted into because of the Seven Years War was a more concerning issue, prompting Britain to implement numerous taxes on the colonies in an attempt to recover their financial losses. With each act the colonists rioted, fueled by exacerbated anger towards Britain. In 1764, the Sugar Act was imposed which placed a tax on sugar and molasses. One year later, the Stamp Act taxed official documents. The American backlash prompted Britain to repeal the act but simultaneously impose the Declaratory Act, which stated that Britain could "make laws binding on the American Colonies 'in all cases whatsoever'" (Britannica, 2017). Subsequently, the colonists fought back on the grounds of "no taxation without representation," arguing that because the colonists had no representation in the British Parliament, there were no grounds upon which Britain could tax the colonies. The last notable act, the Tea Act of 1773, resulted in the first major retaliation performed by the colonists, more specifically a resistance group called the Sons of Liberty. On the night of December 16, 1773, the Sons of Liberty threw 342 chests of tea into the Boston Harbor (History, 2009). Throughout these years, American sentiment of separation from Britain thrived in the colonies and further gained popularity through John Locke's perspective on natural rights and Thomas Paine's *Common Sense*. John Locke proposed that all humans deserve natural rights and the government should protect those rights. In order to maintain equilibrium between the people and government, Locke constructed the idea of a "social contract." The people obey the government who protects them in return; this is a mutualistic relationship because of the equal, beneficial exchange between each party. However, if the government fails to uphold the contract, the people no longer feel obligated to uphold their side of the contract and may rightfully rebel against the government. Thomas Paine echoed Locke's ideas in *Common Sense*, a pamphlet published in early 1776, which justified

growing American sentiment against Britain because Britain had broken their side of the "social contract" (AP, n.d.). *Common Sense* gained huge support and became one of the best selling texts in the Colonies, further promoting revolutionary ideology (AP, n.d.). When "the shot heard around the world" rang out at the Battle of Lexington and Concord, the Revolutionary War commenced.

Cryptology in America

The Revolutionary War served as the perfect catalyst for cryptology's growth. This enticing field of study had only recently reached the colonies as "the traditions of cryptography established in Western Europe moved slowly to the United States… after 1775" (Weber, 1993). Accordingly, cryptology struggled to grow at first. Weber describes this struggle as "[a]n embryonic and besieged United States in 1775 lacked the sophistication, skills, and European diplomatic traditions so integral for successful secret communications systems" (1993). The colonies still had no governmental structure in place, thus cryptology also lacked a proper foundation. Meanwhile in Britain, there were "black chambers," private sectors which focused on cryptanalysis (Doyle, 2017). These divisions would duplicate a letter's seal, thus enabling them to open the letter and read its contents. Having collected any valuable information, the letter would be resealed, making it appear as though the letter had not been touched. Contrarily, in the colonies, there was no formal organization or bureau of cryptology, nor were there any "peacetime professional codebreakers in the United States" (Weber, 1993). The difference between cryptology's popularity in the Western and Eastern hemispheres was immense. Due to the lack of any formal structure, cryptology in America depended entirely on the interest of individuals (Weber, 1993). Some prominent names within the American cryptology sphere were Charles W. F. Dumas, George Washington, Thomas Jefferson, James Madison, James Monroe,

and John Quincy Adams, alluding to the belief that cryptology was a sophisticated field and could only be understood by educated figures given the stature of these men's reputations. However, cryptology also interested everyday citizens as other cryptologists "were 'civilians in uniform,' volunteer soldiers…learned men, clergy (familiar with Greek, Latin, Hebrew), mathematicians, scholars -- some were statesmen" (Weber, 1993). Because of America's inexperience with cryptology, "American leaders struggled to learn the ways and means of secret correspondence," and the British undoubtedly had the advantage in terms of code making and breaking (Weber, 1993).

In spite of the lack of organized cryptology in the U.S., the Revolutionary War sparked cryptology's initial growth in America. Due to the contemporary circumstances of the United States—America was a weak collection of colonies ravaged by war and internal conflict—secret communication was essential in order to have a chance in their fight against the British. Revolution was perfect for the development of espionage and secret communication, and the colonies recognized that. Moreover, these conditions prompted America's leaders to push for cryptological development as their outlook shifted, "cryptology '[was not] employed for purposes of evil and cruelty' but rather as an instrument for protecting crucial information during wartime" (Weber, 1993). This development in perspective highlights some key progression in cryptology as American leaders started to strive to understand the art of encrypting and decrypting messages.

Revolutionary Era Ciphers

Revolutionary War ciphers ranged in complexity and form. While these ciphers were not extremely intricate, with the exception of Thomas Jefferson's wheel cipher, these rudimentary instances of cryptology contributed to its foundation and advancement in America. When

examining these ciphers, it is crucial to use a historical outlook rather than a modern outlook to properly assess their value, given the technological growth since this time.

Both the British and Americans used invisible inks, a form of steganography, to conceal their messages. Usually composed of a mixture of ferrous sulfate and water, the secret message was written in between the lines of a cover letter. Invisible inks were one of the simpler techniques used during the war as a message's content could easily be exposed via heat or a chemical substance like sodium carbonate (Philbrick, n.d.). Nonetheless, General George Washington took a liking to invisible inks because they were so easy to use. Invisible ink could be written on any unsuspecting surface such as a pamphlet or a book. He believed that the ink "not only render[s]… communications less exposed to detection, but relieve[s] the fears of such persons as may be entrusted in its conveyance" (Philbrick, n.d.). Mask letters, another steganographic cipher, were of similar value to invisible inks. This technique employs a seemingly innocent letter whose intended contents can be revealed by placing a "mask" over the letter. British General Sir Henry Clinton used an hourglass shaped mask, shown in figure 1, when corresponding about the Saratoga campaign in 1777 (Dooley, 2018). Both techniques provided sufficient security, as the methods for breaking one of these messages were possible but tedious. More importantly, these introductory techniques of encryption support an underlying increase in enthusiasm for cryptology throughout this war.

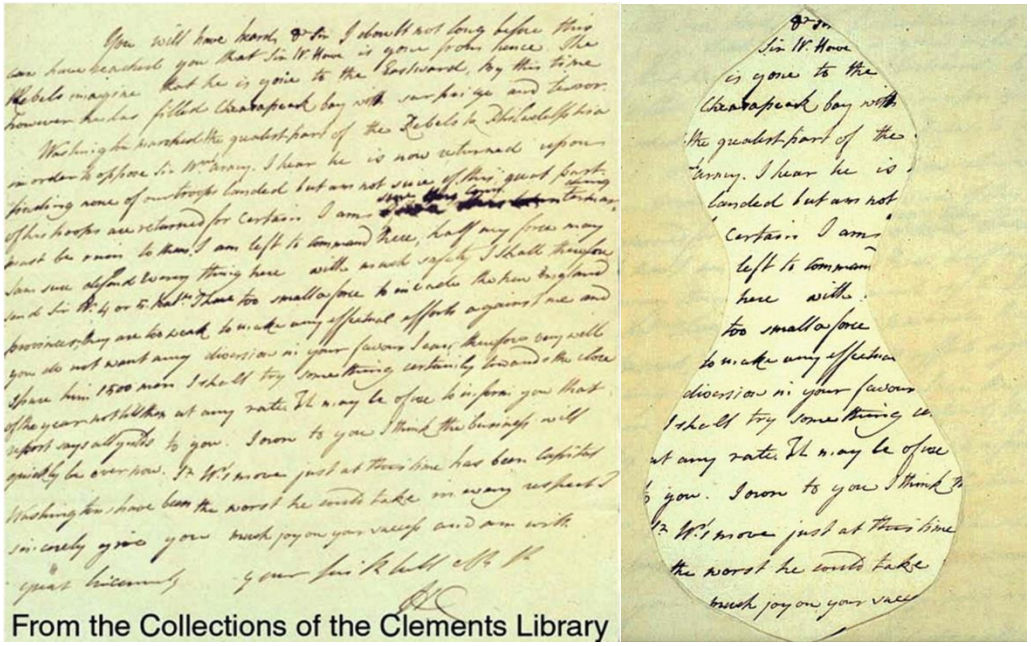

Figure 1: Sir Henry Clinton's mask cipher (Dooley, 2018)

One of the first substitution ciphers, titled the United Colonies' Cipher, was used in correspondence between Charles William Frederic Dumas, one of America's best secret agents, and Benjamin Franklin. Stationed in Europe with the purpose of informing America of any European espionage, Dumas desperately needed some form of secret communication to transmit any important information to the colonies. The cipher contained two lists: the enciphering list had numbers assigned to letters of the alphabet and the deciphering list had letters of the alphabet arranged in numerical order. In total, the lists contained six hundred eighty-two symbols. There were also some slight adjustments to certain letters. W's were to be replaced by two u's and k's were to be substituted by c's (Weber, 1993). When properly used, the United Colonies cipher provided greater security than previous forms of encryption due to its distribution of numbers for each letter: there were one hundred twenty-eight different numbers for 'e', sixty-three numbers for 'r', sixty numbers for 's', and so on (Weber, 1993). Subsequently, words could be enciphered in numerous fashions allowing for a cipher which does not fall victim to frequency analysis.

American cryptology was progressing, but the subsequent advantages were not being used to their full potential. When communicating, Dumas did not randomly choose numbers, but rather frequently chose the first numbers, therefore degrading his cipher's security.

Major General Benedict Arnold and John Andre's book cipher exhibits signs of advancement in American cryptology's complexity. Book ciphers were "employed rather extensively, particularly in the earlier part of the period" due to their simple encryption methods and valid security as long as the book that the cipher was based on did not fall into enemy hands (Burnett, 1917). At first, Arnold and Andre's cipher was based on *Blackstone's Commentary on the Laws of England*; however, they later switched to *Bailey's Dictionary* (Dooley, 2018). Their system of encryption followed the pattern of page number, column number, and word in that column. For example, Mr. Moore, Arnold's alias at the time, was enciphered as "Mr. 172.19.12" (Dooley, 2018). Both the United Colonies Cipher and Arnold and Andre's book cipher displayed the development of US cryptology as their respective ciphers protected their correspondence to the required extent. These ciphers showed glimpses of cryptology's true ability through their substitution methods. Being held back by the lack of mechanization, substitution ciphers only reached a certain intricacy before they were too complicated. The complexity of these ciphers was less notable because of cryptology's introductory state at the time. The introduction of substitution ciphers and book ciphers served as the foundation for code books to be popularly used later.

As previously mentioned, cryptology had reached a limit. Ciphers were restricted in their complexity so that the contents of the message could be deciphered. James Lovell, an American cryptographic tutor and cryptanalyst, intensely studied encryption and decryption. Throughout his studies, he created the Lovell cipher which is based on the first two or more letters of the

keyword. Figure 2 depicts an example of Lovell's cipher. There are three columns with twenty-seven rows and each row contains three letters of the alphabet including '&'. As figure 2 shows, if the keyword is "PEOPLE," the first column of letters would start with 'p' and end with 'o', the second column 'e' through 'd', and the third column would be 'o' through 'n'.

1 PEO	10 YNX	19 GWF
2 QFP	11 ZOY	20 HXG
3 RGQ	12 &PZ	21 IYH
4 SHR	13 AQ&	22 JZI
5 TIS	14 BRA	23 K&J
6 UJT	15 CSB	24 LAK
7 VKU	16 DTC	25 MBL
8 WLV	17 EUD	26 NCM
9 XMW	18 FVE	27 ODN

Figure 2: An example of James Lovell's cipher

More subtle adjustments could also be added. For instance, instructions for the cipher to be done in reverse, thus instead of "PEO," it would be "OEP," or nulls could be attributed to the numbers 28, 29, and 30 (Weber, 1993). This cipher was the first to use a keyword which added another layer of security. This security stems from the unique tables that the first three letters of the keyword produce. "ROB" and "JAC" create distinct tables because the letters are assigned to different numbers. However, Lovell's cipher ended up being too complex to be practically incorporated. Lovell was described as having "tried to force his system on the best minds of the country – even they didn't understand it, and the system failed" (NSA, 2011). For the first time, cryptography had been limited by the lack of technology. American cryptologists could not

continue to create more advanced ciphers because they had to retain an appropriate level of simplicity to be able to decrypt their own messages.

Shifting focus to cryptanalysis, cryptography and steganography's counterpart, Lovell's contribution to cryptology comes from his work with breaking ciphers. Code breaking is equally as essential as encryption, and Lovell illustrated cryptanalysis's value through his deciphering of some of Lord Cornwallis's communications. Lovell instantly discovered a flaw in the British encryption system, as he stated, "the Enemy make only such changes in their Cypher, when they meet with misfortunes, as makes a difference of Position only to the same Alphabet" (NSA, 2011). In other words, the British were using a monoalphabetic substitution cipher which would change positions every so often. Lovell used this knowledge to gain intel of British army movements stationed in Yorktown, allowing the Americans to implement appropriate countermeasures (NSA, 2011). James Lovell and his cryptanalytic feat was one of the first instances that displayed cryptanalysis's power.

Another notable instance of a successful cryptanalysis attack was centered around Dr. Benjamin Church, a well-known Boston physician and member of the Massachusetts Provincial Congress, who communicated with Britain (Weber, 1993). Church had used a monoalphabetic cipher, displayed in figure 3, which included a mixture of Latin and Greek symbols but did not assign every letter of the alphabet to a counterpart; the five least used letters in the English alphabet, 'j', 'k', 'q', 'x', and 'z' all represented themselves. In 1775, George Washington received an enciphered letter which was to be delivered to Dr. Benjamin Church Jr.. Due to Church's refusal to decipher his letter, Samuel West, Elbridge Gerry, and Elisa Porter led the successful cryptanalytic attack. The deciphered message provided information about previous attempts of communication, American army movements and details, casualty numbers, the

colonial economies, increased support for American independence, and explicit instructions on how to reach him (Weber, 1993). For his actions, Church was imprisoned and later hanged. Deciphering his message was a significant cryptanalytic victory and increased cryptanalysis's popularity as a valuable wartime instrument.

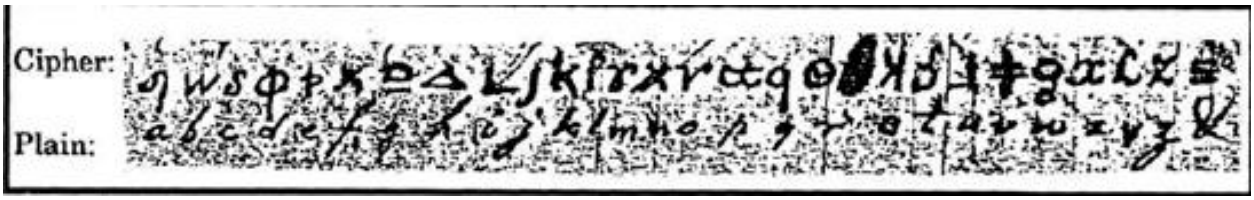

Figure 3: Dr. Benjamin Church's monoalphabetic cipher (Weber, 1993)

By far the most impressive cipher designed during this time was Thomas Jefferson's wheel cipher. David Kahn described it as "so far ahead of its time, and so much in the spirit of the later inventions," testifying to the magnitude of this cipher's strength (1996, pg. 111). Moreover, a similar version of Jefferson's cipher was adopted by the U.S. Army much later in 1922, further supporting this wheel cipher to have been too advanced for its time (Doyle, 2017). Jefferson's wheel cipher utilized transposition. Letters are not substituted for other symbols, but rather they are rearranged. The cipher device contains twenty-six different wheels with the alphabet inscribed on each one. When encrypting a message, each wheel represents a letter in the phrase, for example if one were to inscribe "tomorrow we will attack," the first wheel would be a "t", the second an "o", the third a "m", and so on. Once the phrase has been enciphered, there are now twenty-five other lines of letters which are completely scrambled. Sending any of these jumbled lines would allow the intended recipient to align these letters and the phrase "tomorrow we will attack" would emerge at one of the twenty-five other lines. To much disappointment, just as how Lovell's cipher was never used, Jefferson's wheel cipher similarly found little use. However, this ingenious creation "would have endowed [America] with a method of secret

communication that would almost certainly have withstood any cryptanalytic attack of those days," as Kahn stated, nevertheless commending Jefferson's cipher for its ingenuity given the year in which it was created (1996, pg. 113).

The Civil War

Cryptology went through its first major transformation during the Civil War. Sparked by the secession of South Carolina, this war was "the greatest threat to the survival of the young republic" (Weber, 1993) and secret communication was nothing short of necessary. Along with the invention of the telegraph, encryption systems had to be correspondingly revolutionized, and thus cryptology was mechanized. America saw the formation of entire organizations with the purpose of mastering the telegraph; for the North, there was the U.S. Military Telegraph (USMT) and for the South, there was the Confederate States Military Telegraph (CSMT) (Weber, 1993). The creation of these telegraph bureaus was necessitated by the increase in the number of encrypted messages being sent as well as their growing complexity. Revolutionary ciphers were now outdated as book ciphers and codebooks had become inefficient. Cryptanalysis prevailed during the Civil War as it was simple to tap into a communication wire. Considering both the North and South stemmed from the same technological origins, each side had to create novel ways of deception. These dueling creation processes lead to the Civil War being America's war with significant advancement in cryptography. Because of the telegraph, this was the first time ciphers rearranged the words of a message. Illustrated in Anson Stager's cipher, words would be placed into columns, subsequently shuffling the order. Adding nulls created diffusion as the intended words were spread out by the meaningless words (Dooley, 2018). Along with the knowledge gained about how ciphers could be changed, cryptanalysis played a key role in

gaining vital information which parallels cryptolanalysis's role in World War II. Cryptology continuously progressed throughout the Civil War, subsequently strengthening America's cryptological foundation and subsequent rise to global cryptology experts.

Conclusion

Both the Revolutionary War and Civil War proved to have accelerated cryptology's growth. Secret communication was and remains essential as military intel of an army's tactics, movements, troop reinforcements, or supply distribution can change the outcome of a battle. Yet, cryptology's value does not only apply to war situations; it has weaved throughout our everyday lives. The growth of cryptology follows the same pattern as an exponential curve. Growing very slowly at first, with each war America fought, cryptology advanced. The Revolutionary War laid a sturdy foundation for Civil War cryptology, and the Civil War provided the same for twentieth century conflicts. With World War II technology, humans realized the tremendous power of cryptology, rendering it yet another crucial point in cryptology's growth. These wars boosted cryptology's growth in America by highlighting its worth in the terms of safety, freedom, and human life. The future of cryptology is creeping into view with quantum computers on the rise and America's foundation for modern cryptology will enable us to reach new heights.

Bibliography

AP Committee. (n.d.-a). *AP US History Binder*.

Britannica, T. Editors of Encyclopaedia (2017). *Declaratory Act*. *Encyclopedia Britannica*. https://www.britannica.com/event/Declaratory-Act-Great-Britain-1766

Burnett, E. C. (1917). Ciphers of the revolutionary period. *The American Historical Review*, *22*(2), 329. https://doi.org/10.2307/1834965

Confederate Cipher Disc. (n.d.). https://www.cryptomuseum.com/crypto/usa/ccd/index.htm#:~:text=The%20Confederate%20Cipher%20Disc%20was,War%20(1861%2D1865).

Documents from the Continental Congress and the Constitutional Convention. (n.d.). [Web page]. Library of Congress, Washington, D.C. 20540 USA. https://www.loc.gov/collections/continental-congress-and-constitutional-convention-from-1774-to-1789/articles-and-essays/timeline/1766-to-1767/

Dooley, J. F. (2018). Crypto goes to war: The american revolution. In J. F. Dooley, *History of Cryptography and Cryptanalysis*. Springer International Publishing. https://doi.org/10.1007/978-3-319-90443-6_4

Doyle, R. B. (2017). *The founding fathers encrypted secret messages, too*. The Atlantic. https://www.theatlantic.com/science/archive/2017/03/h3ll0-mr-pr3s1d3nt/521193/

Edwardsc. (2017). *Technologies effect on cryptography – cryptography*. https://derekbruff.org/blogs/fywscrypto/2017/09/19/technologies-effect-on-cryptography/

Founders online: Description of a wheel cipher, [before 22 march 1802]. (n.d.-a). http://founders.archives.gov/documents/Jefferson/01-37-02-0082

Founders online: From thomas jefferson to robert r. Livingston, 18 april 1802. (n.d.-b). http://founders.archives.gov/documents/Jefferson/01-37-02-0220

History.com Editors. (2009a). *Boston tea party*. HISTORY. https://www.history.com/topics/american-revolution/boston-tea-party

History.com Editors. (2009b). *Revolutionary war*. HISTORY. https://www.history.com/topics/american-revolution/american-revolution-history

Kahn, D. (1979). *The codebreakers: The story of secret writing* (9. print). Macmillan. file:///Users/rsawyers21/Downloads/Kahn,%20David%20-%20The%20CodeBreakers.pdf

NSA. (2011). *The American Revolution's One-Man National Security Agency*. NSA. https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/crypto-almanac-50th/the-american-revolution.pdf

Philbrick, N. (n.d.). *Spy techniques of the revolutionary war*. George Washington's Mount Vernon. https://www.mountvernon.org/george-washington/the-revolutionary-war/spying-and-espionage/spy-techniques-of-the-revolutionary-war/

The Colonial Williamsburg Foundation. (n.d.). *The American Revolution*. http://www.ouramericanrevolution.org/index.cfm/page/view/prq0003

Weber, R. E. (1993). *Masked dispatches: Cryptograms and Cryptology in American History, 1775-1900*. Center for Cryptologic History.