

Cryptology: the Secret Battlefield of the Civil War



June 27, 2020



Ralph Simpson

Ralph@CipherHistory.com

Copyright © 2022
CC Attribution 4.0 International

All images and cipher devices in this presentation are from the collection of CipherHistory.com, unless otherwise noted

Cryptology in the Civil War

- Not much is written about cryptology in the Civil War
- No new crypto technology

Why should we study Civil War crypto?

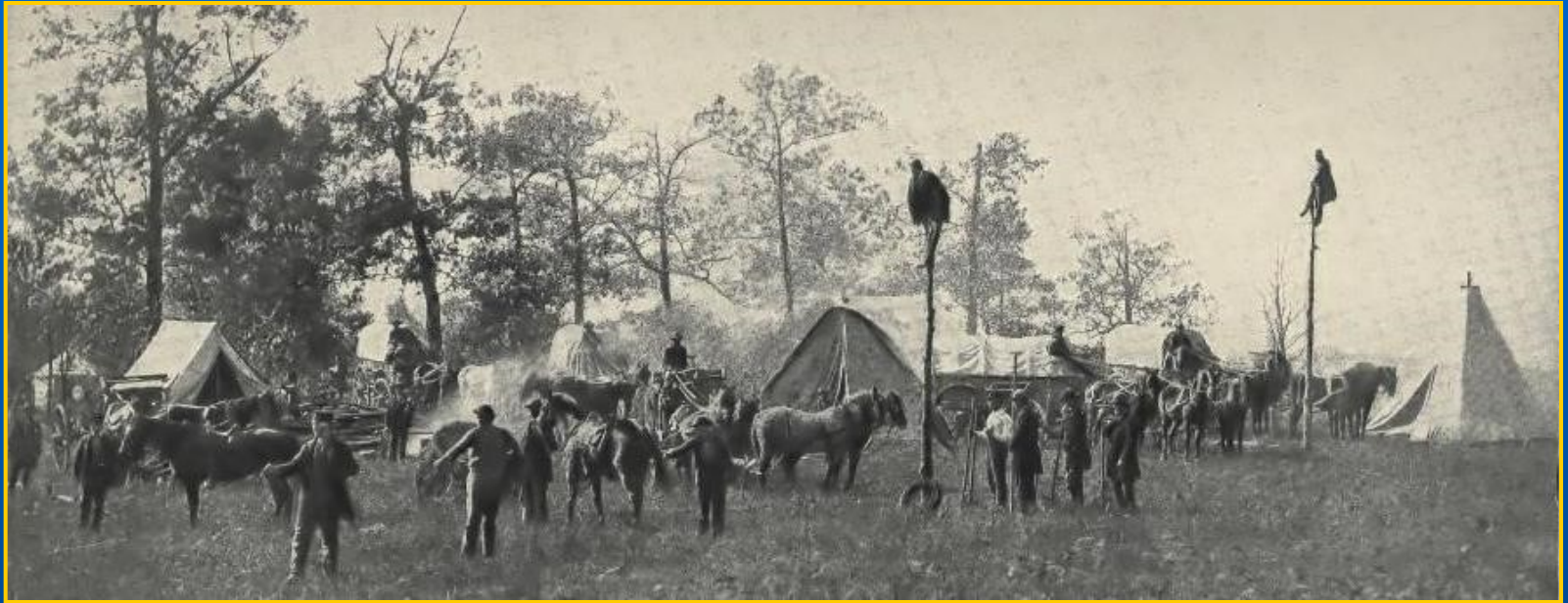
- Beginning of crypto warfare
- Birth of US Signal Corps
- Battles were won and lost based on crypto or cryptanalysis
- Lessons learned
- Lessons not learned, mistakes repeated in WW1

Civil War Crypto Landscape

- **Most widely used crypto:**
 - **Vigenère cipher**
 - **Transposition and substitution**
 - **Code books**
 - **Dictionary and other books as code book**
 - **Steganography (messages hidden in pocket watches, cigars, invisible ink, Cardano grille, etc.)**
- **Crypto was 400+ years old and worked in the days of couriers on horseback, but was now seriously compromised by the new technology of telegraphy**

New Message Technology in Civil War

Union Military
Telegraph
Construction
Corps
April, 1864



- Civil War - first major war to use telegraphy, revolutionized warfare
 - Generals have more control over battlefield strategy
 - Messages received immediately over long distances
 - Union sent 6.5 million messages over 15,000 miles wires
- Wigwag signal flags invented – digital aerial telegraphy
- For the first time, many messages were intercepted by the enemy

Birth of the US Signal Corps

- Albert J. Myers paid for medical school by working as a telegrapher
- Doctoral thesis - sign language for deaf
- Joined US Army in 1854 as surgeon
- Invented “wigwag” digital aerial signaling
- Wigwag used single flag as 1 or 2
- Lt. Col. Robert E. Lee headed the committee approving wigwag and Myers
- Myers was first Chief Signal Officer and headed new Signal Corps in 1860
- Second in command for Signal Corps was Lt. Edward Alexander, from Georgia



Gen. Albert J. Myers, US Signal Corps

Wigwag



Union wigwag platform near Antietam, Sept. 1862

- Single flag waved left or right for 1 or 2, “wig or wag”
- Four digits represents all letters
- Simple signaling, visible for up to 15 miles
- Lanterns used at night
- Digital system allowed for encrypting signal

Birth of the Confederate Signal Corps

- Lt. Alexander was assistant to Myers, joined South for Civil War
- Became Capt. and Chief Signals Officer for South in June 1861
- Direct competitor to his old boss
- Alexander quickly trained South in the wigwag system invented by Myers
- Also used spies in Washington DC and personally went in hot air balloons to find enemy positions
- Climbed poles to tap into telegraph messages
- Promoted to Lt. Col. by end of 1861, General in Feb. 1863



Capt. Edward Alexander, Chief Signals Officer, Confederate Signal Corps

First use of Wigwag by South

- Confederate Wigwag signals used in first land battle, First Battle of Bull Run, July 21, 1861
- North outnumbered South, 35,000 to 20,000
- Wigwag warned of Union flanking move, turning Union rout to Confederate victory
- Wigwag changed outcome of first battle
- North immediately started wigwag signaling



Bull Run Battlefield



Signal Corps – North vs South

- The South had a quicker start, at First Battle of Bull Run
- Myers was embroiled in politics with US Military Telegraphers Corps, headed by Anson Stager, co-founder of Western Union
- US MTC was civilian organization, reporting to Sec. of War
- Myers relieved of duty in Nov. 1863, reinstated after war
- By the end of the war, the Union Signal Corps had 3,000 men, the South had half that number
- Abraham Lincoln made extensive use of telegraph, changing generals often
- Jefferson Davis left war strategy to Robert E. Lee
- Both Myers and Alexander would attain the rank of General

Union Vigenère Cipher



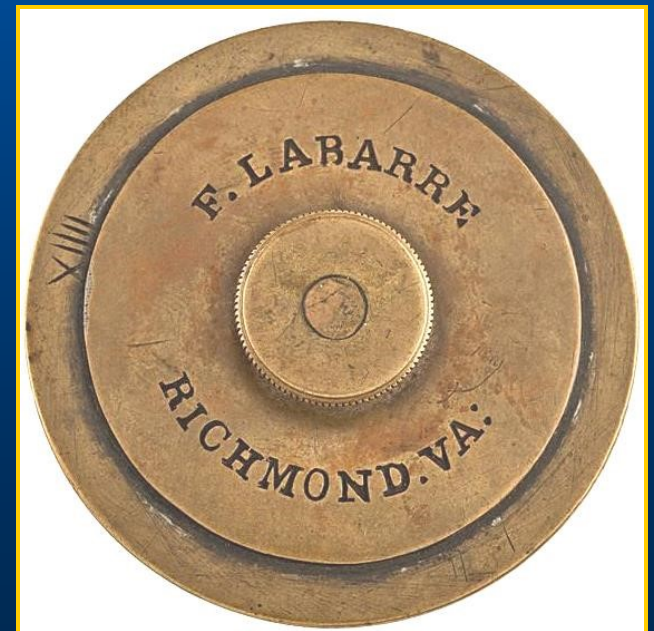
Union Cipher Disk

- “A.J.M.” is Albert J. Myers
 - Vigenère disk directly encodes wigwag signals
 - “8” and “1” used because they can be read in any orientation
 - “2” not used because it could be confused if partly obscured
 - 4 bit code gives 30 characters
 - Wigwag was relatively effective and secure
-
- Vigenère disk was also used for telegraphy and courier messages

Confederate Vigenère Cipher

“CSA S.S.” means Confederate States of America, Secret Service

- 57mm or 2.25in. diameter, designed by Francis LeBarre in 1862
- Only 5 known to exist:
 - One in Smithsonian
 - Two in Museum of the Confederacy in Richmond, VA
 - Two in private hands
- This one, serial # XIII, sold in 2014 for \$18,000 (one that got away!)



Confederate Vigenère Cipher

Confederate
cipher wheel at
NCM



- “Fred Flintstone” cipher wheel
- Only one known to exist, in National Cryptologic Museum
- Vigenère table with 2 pointers to find intersection point
- Appears to be a solution in search of a problem
- Highlights the lack of knowledge of cryptology

Civil War Codebreaking

- Both sides of the Civil War intercepted messages and broke enemy codes
- Union was more consistent and secure
- South only used 4 keywords throughout the war, and changed them only after proof of compromise
 - Complete Victory
 - Manchester Bluff
 - Come Retribution
 - In God we Trust
- First break by North was during Battle of Shiloh in April, 1862; solution published in the New York Herald
- Confederates changed keyword to Manchester Bluff

Union Codebreaking

- After the war, a Confederate crypto officer on Gen. Joseph Johnston's staff wrote:
 - “Col. E [Benjamin S. Ewell] taught me the cipher & the password, or keyword, to read the dispatches. . . . The system was only to put the most important words of a message into cipher - & occasionally an unimportant one to mislead - so as to prevent detection. I may of course now mention the keyword then in use. It was “Manchester Bluff.”
- During Battle of Vicksburg, Johnston sent message by courier for reinforcements, but cipher was mangled. 12 hours later courier returns to resend message, but it was too late
- South lost Vicksburg and Union found cipher messages
- July 1863 Confederates changed keyword to “Come Retribution”
- In the final weeks of the war, it was changed to “In God we Trust”

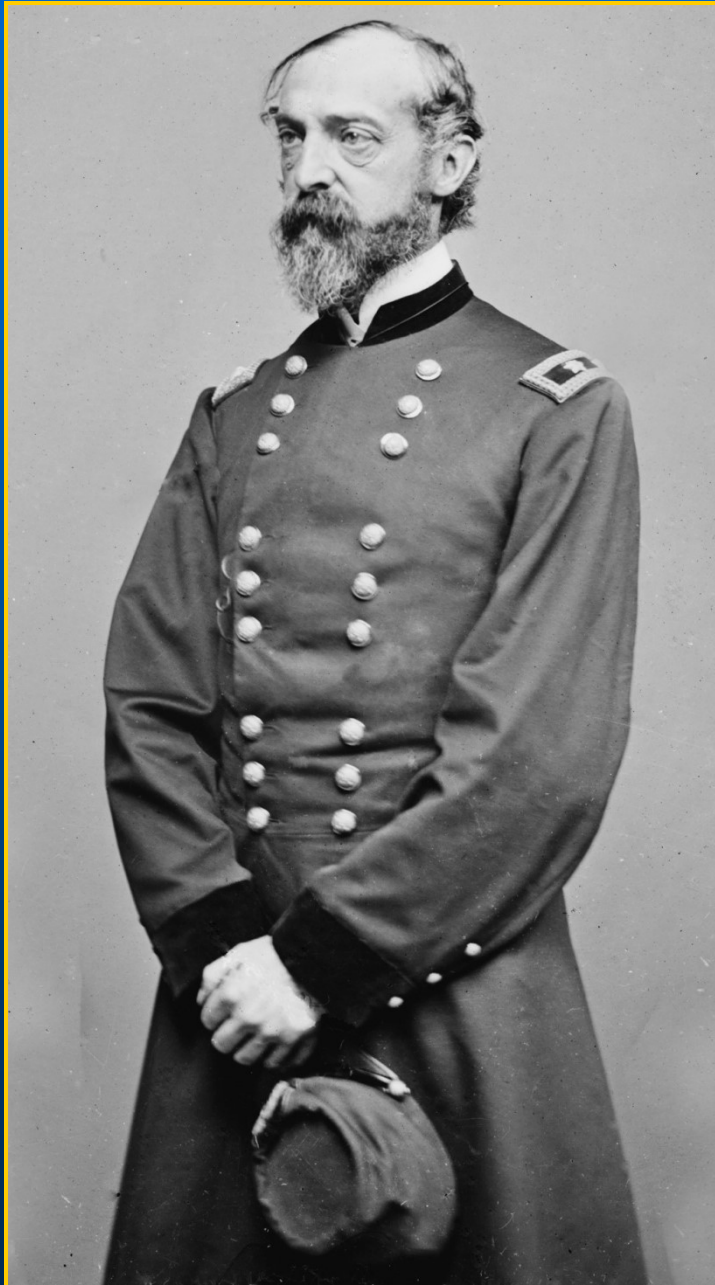
Confederate Codebreaking

- Confederates were not as successful as the North, but were known to break some Union Vigenère ciphers
- At Battle of Petersburg, Robert E. Lee gave his commanders the encrypted wigwag flag alphabet used by the Union Army
- The South still lost Petersburg and Richmond, leading to their surrender on April 9, 1865

**Confederate Capital
Richmond, VA
April 1865**



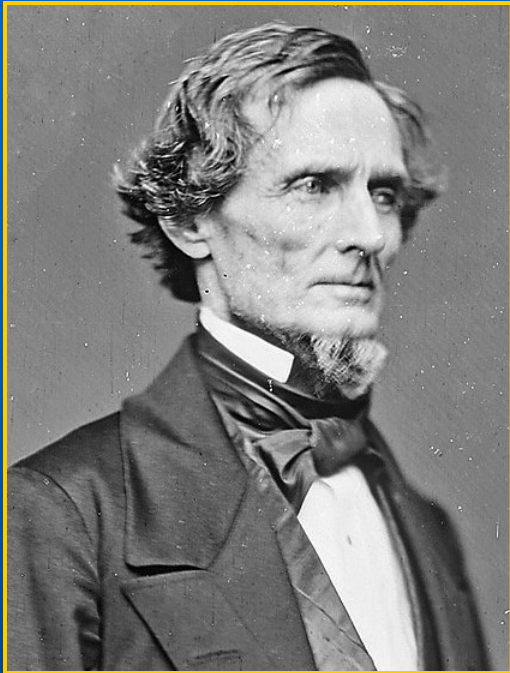
Value of Signal Corps



- Most soldiers knew the role of the Signal Corps but did not understand their value
- Union General George Meade place great value on the Signal Corps
- Meade known for winning the Battle of Gettysburg
- When he moved his headquarters location, he delayed the move until the telegraphers were operational at the new location
- Aptly, NSA headquarters at Ft. Meade is named for General Meade

Major General George Meade

Other Ciphers



Jefferson Davis
President of the
Confederacy



Anson Stager
co-founder,
Western Union

- Confederate President Jefferson Davis used a dictionary as his code book, not a very strong cipher
- Anson Stager took over from Albert Myers as Chief Signals Officer and mainly used transposition ciphers
 - Despite this being a weak cipher, it was not broken
 - Intercepted messages were published in newspapers with rewards offered, but they were never decoded

Lessons Learned... or Not!

- New invention of telegraphy transformed battlefield strategy
- Information, collaboration, intervention in war by government leaders
- Current cipher technology was 400 years old and inadequate when many messages are intercepted

What happened in WW1?

- New invention of radio and telephone transformed war strategy to include air force, navy, and army at all levels
- Information, collaboration, intervention in war by government leaders
- Cipher technology was the same as in the Civil War, but now with more known methods of cryptanalysis

Download this Presentation

Slides: CipherHistory.com/slides/civilwar.pptx

Article: CipherHistory.com/civilwar.html

