How I Broke the Confederate Code
(137 Years Too Late)

KENT D. BOKLAN

Abstract We study a previously undeciphered Civil War cryptogram, limiting ourselves to pencil and paper, and discover not only a missive of military importance, but in the process, identify a new Confederate codeword. Our methods rely not only upon cryptanalysis of the encryption method but also on the exploitation of an elementary mistake.

Keywords Baltimore, Bragg, confederate code, Kirby-Smith, Mumfordville, Mumfordsville, new key, Vigenère

Dedicated to the Memory of Lydia M. Kawka

In the spring of 1999, I received a catalogue for a sale of Fine Books and Manuscripts Including Americana that Sotheby’s was to hold in New York on June 22. Lot 79 was described as:

Kirby-Smith, Edmund, C.S.A. General
Letter signed (“E.K.S.”), 1 page (10 × 7 7/8 in.; 254 × 200 mm), n.p., 14 September n.y. [1862], to an unidentified recipient; the text of the letter in pencil, tiny chip to right margin.

A LETTER OF INTELLIGENCE, PARTIALLY WRITTEN IN CONFEDERATE CODE. The first eleven lines of this intriguing document are in undeciphered code, but the last paragraph provides pertinent information regarding the Union army and its movements. “…A part of Genl Grant’s army is reported to have arrived at Louisville. [General] Buell was expected to come on in advance of his army, and to arrive there yesterday. Several old batteries have arrived there within the past few days.”

“General Smith and his forces…were waiting to join forces with [General] Bragg before advancing on Louisville. “…Bragg’s advance…pushed on towards Louisville, and on the 14th [of September], two brigades under… General Duncan…encountered a little more than 2000 National troops, under Colonel T. J. Wilder at Mumfordsville…Duncan…demanded an unconditional surrender. It was refused, and…the next morning the Confederates drove in the National pickets. A battle began…and raged for about five hours, when four hundred of the Fiftieth Indiana…came to the aid of the garrison. The assailants were repulsed with heavy losses.

Address correspondence to Kent D. Boklan, Department of Computer Science, Queens College, CUNY, 65-30 Kissena Boulevard, Flushing, NY 11367-1597, USA. E-mail: boklan@boole.cs.qc.edu
Assured of final success, the Confederates remained quiet until the 16th, when a large portion of Bragg’s main body... appeared [and overpowered the Union forces] ....” [2, p. 238]

The letter was pictured (Figure 1). I thought that it would be good fun to (try to) decrypt the message and a few days later I traveled from my home, then in Baltimore, Maryland, to New York City. I visited Sotheby’s and expressed my desire to break the code. I was forewarned that I would not be paid if I succeeded.

On the train ride back to Baltimore, I realized that accurately transcribing the very deliberate penmanship of the cipher clerk was going to be a challenge. A single error, I expected, would render a good deal of the message undecipherable. Fortunately, I was able to compare the cipher characters against the plain text characters in the last paragraph of the letter. But there were other problems. In the left margin of the third line of the text, there was a capital Z in a different hand. I didn’t know if this was a part of the cipher. And not only had a few letters faded but there was a very unusual looking character that resembled a spermatozoon.

I performed my initial investigations on the train, first counting the number of appearances of each of the cipher characters (the letters and that one odd symbol) in the body of the roughly 280-character long encrypted section. Twenty-five of the twenty-six English letters were employed. The letter ‘g,’ however, was not present and, so, I surmised that the ‘o’ with a tail was indeed the cipher clerk’s own stylish way of writing a ‘g.’ Now, had the method of encryption been a mono-alphabetic substitution whereby each distinct cipher character would have been a unique representative of a plain text letter (so the ciphertext alphabet is a simple permutation of the plaintext alphabet), it would have been exceedingly unlikely that all twenty-six letters would have appeared in so short a message. And it was at this point that I concluded my first analysis since the canter of the railroad car was making me feel ill.

Figure 1. The Letter, Lot 79 (Image courtesy of Sotheby’s).
The character counts for Lot 79 were too flat, too even, for a simple mono-
alphabetic method; a more sophisticated technique was employed. This point is also
immediately evident when one considers the cipher “word” TTTET. I did notice,
before my train arrived home, that the parsing of the cipher words in Lot 79 cipher
seemed reasonably natural to English—but I did sense an abundance of long words.

My next step was to do a bit of research to see if I could discern which types of
encryption techniques were employed during the War (that is, the Civil War or the
War of the Northern Aggression depending upon your point of view). I consulted
David Kahn’s excellent resource, The Codebreakers [1] and what I found was very
interesting:

The rebels reposed their major trust, however, in the Vigenère, sometimes
using it in the form of a brass cipher disc. In theory, it was an excellent
choice, for so far as the South knew the cipher was unbreakable. In prac-
tice, it proved a dismal failure. For one thing, transmission errors that
added or subtracted a letter...unmeshed the key from the cipher and
caused no end of difficulty. Once Major Cunningham of General
Kirby-Smith’s staff tried for twelve hours to decipher a garbled message;
he finally gave up in disgust and galloped around the Union flank to the
sender to find out what it said.

So here was direct evidence that Kirby-Smith’s staff had used the Vigenère scheme.
I read on:

Lincoln’s three young cipher operators—Tinker, Chandler and
Bates...solved it. It proved to be Vigenère, key MANCHESTER
BLUFF...This was only one of a number of Confederate cryptograms
solved by the triumvirate...it [the solution] provided the three young
men with a Confederate keyword, of which the South apparently used
only three during the war...MANCHESTER BLUFF...COMPLETE
VICTORY (a phrase the Confederates clung to long after that cherished
hope had dissipated)...[and at] about the same time that Booth and
others were being hunted down and captured, Jefferson Davis was using
the third Vigenère key to compose the last official cryptogram of the
Confederacy...COME RETRIBUTION.

Now I was almost convinced (a touch of skepticism always kept in reserve) that Lot
79 was indeed encrypted by the Vigenère method.\footnote{It may be of interest to note that a Vigenère table was found in John Wilkes Booth’s
room at the National Hotel and was used at the trial of the eight sympathizers charged with
conspiracy to assassinate President Lincoln.}

If Lot 79 in the Sotheby’s sale was encrypted by the Vigenère scheme and Kahn’s
suggestion that only three keywords were used by the Confederacy was correct, test-
ing each of MANCHESTER BLUFF, COMPLETE VICTORY and COME RET-
RIBUTION should lead to a proper decryption of the message. So I wrote the Lot
79 cipher on graph paper on a width of fifteen as all three putative keywords had
length fifteen characters. I did this twice—with the Z on line three present and with-
out it. Since the cipher text had two one-letter words, Z and U, I naturally surmised
that these corresponded to either a plaintext A or a plaintext I. The Vigenère table (Figure 2) demonstrates that if a cipher Z is the encrypted form of a plaintext A, there must be a Z in the keyword. But none of the three keys we were considering had Z’s—so this was not the case. If a cipher Z is derived from a plaintext I, there is a corresponding R in the key. And this was a possibility as all three keys had R’s. If the spaces in Lot 79 were indeed indicative of breaks between words, the cipher word Z was followed by the cipher word WIAWE. Our line of reasoning would then suggest that one of the key fragments BLUFF, YCOMP, ETRIB, and IBUTI should yield a decrypt of WIAWE. And trying this out, the four “decrypts” are, respectively, VXGRZ, YGMKP, SPJOD, and OHGDW. These are not good; they’re pretty clearly not English words and not even nearly English words.

![Figure 2. The English Vigenère table.](image)

The key for Lot 79, I realized, was not one of the three known Confederate keys.

Throughout the course of my investigation, I was conscious of the fact that there were likely to be garbles—sporadic errors—that had been accidentally introduced into the cipher (noted with square brackets to signify the plaintext letter to which a cipher letter should have decoded). If the true key length had been fifteen or a divisor of fifteen, the cipher characters in each column on my graph paper would have been generated from a single row in the Vigenère table. That is, each of my fifteen columns would have followed a mono-alphabetic substitution scheme. So I considered these columns of about eighteen characters each. The letter frequency counts were, again, very flat with no apparent disposition towards causality (that is, some deterministic language as the distribution bias of the most common English letters ETNORIAS would suggest—even in so small a sample). This new key, I thought, did not have length fifteen (or five or three).

I could have then tried variable widths in order to gauge the key word length but there was only a small amount of cipher. Setting aside my awareness that the true value might not shine prominently because of this, I was also growing weary of recopying the cipher on graph paper. Since I stubbornly refused the aid of a computer (since no such device had been available to Tinker or Chandler or Bates), I decided that it was a good time to make use of an apparent signature in the cipher, the initials QYJ.
Once a method of encryption has been identified, the most potent weapon in a cryptanalyst’s arsenal is to exploit mistakes and lapses. The last part of the Lot 79 letter was not encrypted and was signed EKS for Edmund Kirby-Smith (Figure 3). Perhaps this signature QYJ, then, was the encrypted form of EKS. If this was the case, the Vigenère table provides the related key fragment MOR.

And then I made a small leap of faith, an educated guess, based upon the observation that I had made on the train ride home, that some of these ‘long’ words in the cipher were names and locations. Since Louisville was mentioned prominently in the plain text part of the Lot 79 letter, so might it be in the cipher section too. The first ten-letter word in the cipher was EWGWJMjLWX and if this was the encrypted form of Louisville, I determined that the (associated) key must be TIMORRBALT. So I shifted IMOREBALT (making an educated correction for key length nine) ahead nine spaces and again and tried to decrypt the next part of the cipher—to see if English would come out. And out came AND COVINGTON THEY ARE.

So BALTIMORE it was. BALTIMORE is a new Confederate key word, a fourth key.

But why Baltimore? Perhaps the key choice was a portent of what would occur near Baltimore only three days later on the 17th of September, the Battle of Antietam.

With a Vigenère table to the left of me and graph paper and colored pencils in front of me, the drama unfolded after 137 years. The first two words of the cipher, UHP XVQAP became THE ENEMY and my excitement was suddenly tempered with a sense of the scope and intimacy of history.

Kirby-Smith’s missive, Lot 79, was probably sent to General Bragg who was headed towards Mumfordsville (Munfordville) to join forces before marching to

Figure 3. Gen. Edmund Kirby-Smith (Image courtesy of the Library of Congress, Prints and Photographs Division, LC-B813-2013A).
Louisville. The Union troops had set up a garrison at Mumfordsville (Munfordville) and had repelled the initial Confederate attack. The siege lasted from the 14th until the 17th of September. Bragg’s troops arrived on the 15th and 16th and surrounded the garrison. On the 17th, they suddenly appeared and overwhelmed the Union:

THE ENEMY RAPIDLY CONCENTRATING AT LOUISVILLE AND COVINGTON. THEY ARE CONFIDENT OF SOON CRUSHING MY FORCE HERE. IT IS IMPORTANT OUR COMMUNICATION WITH EACH OTHER SHOULD BE KEPT OPEN. I SHALL PRESENT A BOLD FRONT IN ORDER TO DECEIVE THE ENEMY AS LONG AS POSSIBLE AND WHEN COMPelled I SHALL FALL BACK UPON YOU. MARSHALL IS STILL FAR BEHIND. E.K.S.

About the Author

Kent D. Boklan is, by trade, a cryptographer and a mathematician. He received his SB from MIT and PhD from the University of Michigan (in analytic number theory) and designed his first [public key] cryptosystem in 1988. He worked for the National Security Agency (1996–1999) where he was professionalized as a cryptologic mathematician. He has written more than a dozen research papers in cryptography and cryptanalysis [but most of them are CLASSIFIED]. He recently lived in Iceland, spending much of his time identifying inversions in the human genomic sequence and bumming around downtown Reykjavik. Presently, Dr. Boklan is on the faculty of Queens College and the City University of New York Graduate Center. He also provides data security and cryptographic consulting services and his clients include the NYC Police Department, Sanitation Department, and the Department of Information Technology and Telecommunications.

Acknowledgement

The author would like to thank Mr. David Gaddy, a student of Confederate cryptography, for noting [private communication] the distinction between main line (i.e., high level) key usage and use within a department (military territorial command) or field army. During the War, Richmond authorities specified a fixed key-length for encrypted communications to and from the seat of government. Lower echelon military authorities were not required to adhere to this, internally, and the nine letter key, BALTIMORE, is an example of this type of hierarchical structure – implying that Kirby-Smith was communicating to a commander included in his cryptonet, his key family.

“Marshall” is probably not a cover name but a reference to Humphrey Marshall of KY (1812–1872) who was in Bragg’s Fall, 1862 Kentucky campaign. Kirby-Smith had sought his cooperation.

References

Copyright of Cryptologia is the property of Taylor & Francis Ltd and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.