The First U.S. Government Manual on Cryptography

DAVID W. GADDY

It is always risky to claim a "first," especially in such an esoteric field as cryptography, and government cryptography at that. But mounting evidence points to a small book with the simple title *Cipher* as a prime candidate for the U.S. government's first manual on the making and breaking of ciphers, predating by a half century or more the army manual by Parker Hitt which has been accorded that position. Carrying no explicit evidence of the publisher, date, or place of publication, the book is a reprint of a lengthy encyclopedia article on the subject penned by an English surgeon and amateur student of cryptography, William Blair, around 1807. It exists in two editions, a 117-page version (*presumed* to be the earlier) and an expanded, 156-page version, which alludes to practices during the American Civil War. The book was evidently printed by and for the Chief Signal Officer of the U.S. Army in the mid-nineteenth century and was used as a text in the instruction of signal officers.

Around 1807, Dr. William Blair (1766-1822) wrote for Abraham Rees's *Cyclopaedia* a lengthy article (some 35,000 words) under the heading of "Cipher."[1] According to internal evidence, the forty-one-year-old surgeon was an amateur drawn to the subject by a museum exhibit that kindled his interest. For three years he must have read everything he could get his hands on, in English, French, Latin, Greek, and possibly other languages. Dissatisfaction with the treatment of the subject in available authorities (such as *Britannica*) led him to undertake a superior presentation, and in that he ably succeeded. David Kahn, in his monumental work *The Codebreakers* (1967), characterized Blair's "superb article" as "the finest treatise in English on cryptology" until Parker Hitt's military manual was published by the U.S. Army in 1916. [2] Rees issued his work in parts, comprising thirty-nine volumes, over a period of eighteen years, the Blair article

[1] An excellent overview of the work of Dr. Abraham Rees (1743–1825) is contained in Harold R. Pestana, "Rees's *Cyclopaedia* (1802–1820), A Sourcebook for the History of Geology," in the *Journal of the Society for the Bibliography of Natural History*, Vol. 9, No. 3 (1979), 353–61. The *Cyclopaedia* was issued serially in eighty-five parts over two decades, two parts intended to comprise a volume (except for XXXIX, which required three parts), plus plates. Individual pages are not numbered. From extant library copies, some subscribers did not take the trouble to bind the parts as intended. That, plus the fact that individual articles are not signed, might well have caused a casual reader to overlook the fact that William Blair was identified in the preface (v) as the author of the article on "Cipher," but a careful reader would have discovered his identity buried in the text.

[2] David Kahn, *The Codebreakers: The Story of Secret Writing* (New York: The Macmillan Company, 1967), 788, echoing the *British Dictionary of National Biography*, "incomparably the best treatise in the English language on secret writing and the art of deciphering" (V, 168). Parker Hitt, *Manual for the Solution of Military Ciphers* (Fort Leavenworth, Kansas: Press of the Army Service Schools, 1916, First Edition).

appearing in May 1807. An American edition followed on the heels of the London edition.[3] One reader who evidently digested its contents was Edgar Allan Poe, popularly regarded as a cipher expert because of "The Gold Bug" and other writings in the late 1830s/1840s.[4] Yet, while American Civil War contemporaries of the 1860s cited "The Gold Bug" as the basis for their familiarity with letter-frequency in cipher solution,[5] Rees's half-century-old encyclopedia seemed to have fallen out of use and common knowledge by that time. Ironically, Blair (citing Falconer and other authorities) described the principal cryptosystems that would be used by the two sides in the American Civil War – the Confederacy's dictionary cipher, the Vigenère (as it is generally known today) and the grille, as well as simple substitution ciphers, and the Union's word-route transposition cipher – and suggested ways of solving them. In the last case, that of the route transposition – perhaps the earliest American cipher designed specifically for the telegraph – contemporaries ascribed its origin to Anson Stager, creator of the U.S. Military Telegraph Department (later "Corps"), evidently never having heard of the Earl of Argyll (1685), James Falconer (1685), or Blair.[6]

[3] Pestana, "Rees's *Cyclopaedia*," 356–57. The American edition appears to have commenced in 1806, expanded to include items considered to be of specifically American interest. Robert A. Gross, *Books and Libraries in Thoreau's Concord* (American Antiquarian Society, 1988), 415, lists in that library Rees's "First American Edition, Revised, Corrected, Enlarged, and Adapted to this Country" in 1825, with eighty-three "volumes" [*sic*: probably unbound parts], whereas the actual title page states forty-one volumes. Precise dating of components of the work is of interest mainly in establishing potential availability of its information to readers, e.g., was the "Cipher" article in the library at West Point when cadet Edward Porter Alexander, 1835–1910, USMA Class of 1857 (who introduced the Vigenère into Confederate service) might have had an opportunity to see it? (In characterizing the Blair extract as "the first U.S. government manual on cryptography," I am reserving "first American" for the Confederate confidential pamphlet (Richmond, 1862), compiled by Alexander and his brother, until that distinction is successfully challenged. No copies of that work, the Confederate equivalent of Myer's *Manual*, are known to exist today. See "Friedman's Lecture IV" in the forthcoming *The Friedman Legacy*, National Security Agency, Center for Cryptologic History, 1992, or SRH-004, Record Group 475, (National Archives.)

[4] W.K. Wimsatt, Jr., "What Poe Knew About Cryptography." *Publications of the Modern Language Association of America*, LVIII, 3 (September, 1943), 754–79, supersedes William F. Friedman, "Edgar Allan Poe, Cryptographer" (*American Literature*, VIII (November, 1936), 266–80. See also Kahn, *The Codebreakers*, 783–93. Both Wimsatt and Kahn had consulted with Friedman to gain his insights. Overseas, British Admiral Sir Francis Beaufort ("who was himself a great influence in developing and modernizing cryptography for Naval Intelligence") is quoted as having said that the Rees-Blair article "attracted much attention in London intelligence circles and then came the influence of Edgar Allen [*sic*] Poe" (Richard Deacon, *A History of the British Secret Service*. New York: Taplinger Publishing Co., 1969, 143).

[5] For example, S.H. Lockett, "The Defense of Vicksburg" in Robert Underwood Johnson and Clarence Clough Buel, eds., *Battles and Leaders of the Civil War* (New York: The Century Co., 1884, 4 vols.), Vol. 3, "Retreat from Gettysburg," 482–92, at 492: "Our signal-service men had long before worked out the Federal code on the principle of Poe's 'Gold Bug,' and translated the messages as soon as sent."

[6] See William Plum, *The Military Telegraph During the Civil War in the United States* (Chicago: Jansen McClurg & Company Publishers, 1882, 2 vols.; reprinted, New York: Arno Press, 1974, with introduction by Paul J. Scheips), 44ff., and David Homer Bates, *Lincoln in the Telegraph Office* (New York: The Century Co., 1907), 49 ff. The author is persuaded that the principal appeal of the cipher was that the telegrapher was able to deal with recognizable words, instead of "sound" copying of Morse and, confronted with line interference, this was an all-important consideration. The system was one "of, by, and for" telegraphers, rather than having been devised by a cipher expert. Through trial and error, it evolved during the war, and was approaching two-part code status at war's end, by a variety of variant routes. Post-1865 replacements evidently continued to serve government (or, at least, War Department) cryptography into the seventies, and probably until the appearance of the 1885–86 telegraphic code compiled under the direction of Lt. Col J.F. Gregory, aide to commanding general Phil Sheridan, based upon the 1870 commercial code of Robert Slater (London).

With respect to the Civil War period, the first Signal Officer of the U.S. Army (1860), Albert James Myer (1828-1880), inventor of the "wig-wag" system of visual signaling, was "bounced" from his position as Chief Signal Officer in 1863, in the middle of the war, and was not restored until 1867, two years after the fighting ended.[7] In 1864 Myer had hastily printed a signal manual to which he appended, as a section on ciphers, an article drawn from a popular journal of 1863. After the war, he enlarged on the provisional text, producing the first in a series of copyrighted editions that made up the principal manual and reference ("Myer's Manual") for military communicators for the remainder of the nineteenth century, but he retained the 1863 cipher article. Like Blair, Myer, the "Father of the Signal Corps" (and Weather Bureau, among other accomplishments) was also a surgeon, with a scientific background. He pushed his people into the study of electricity and electromagnetic telegraphy, into balloons and aeronautics, into meteorology, and into telephony. His appreciation of signal or communications security stemmed from wartime experience with an able adversary who had jumped the gun on him in his chosen field. But he seemed to lack anything better on the subject of cryptography than a popular journal article. Perhaps that is an incorrect impression.

The small book that constitutes our subject appears in David Shulman's *An Annotated Bibliography of Cryptography* (1976), with the authorship correctly interpolated (William Blair's name had been used as a example in the text), as was the fact that it is a reprint of the Rees article. He notes a copy of the 117-page version in his personal collection (subsequently placed in the New York Public Library), plus one in the Harvard University Library, and another, enlarged edition (156pp., vice 117) at the latter place. Inquiry in 1990 disclosed that Shulman was in error in listing Harvard and that the Boston Public Library was the actual repository. According to the Rare Books staff in Boston, their copy of the earlier edition has been missing since 1936, but their other copy – the expanded edition – bears the identification of "Philip Reade, 2nd Lt, 3rd Inf; Actg Signal Officer, San Diego, 1875."

Recently a private collector has reported the acquisition of a copy of the expanded version that clarifies some aspects of this book, while raising other questions. It bears a handwritten inscription on the flyleaf as follows:

> This little volume is of interest,
> being the textbook of the
> Signal Officer class of 1869, of
> which I was, fortunately, the only
> officer to pass successfully the
> final examination.

[7] See Max L. Marshall, ed., *The Story of the U.S. Army Signal Corps* (New York: Franklin Watts, Inc., 1965). Myer is considered to have based his signal code on the two-element Bain telegraphic code, with which he was familiar as a young telegrapher, rather than the four-element American Morse system. On the other hand, the Myer code (a simple substitution cipher, cryptographically) was similar to one depicted by Blair as an example of a two- or three-element system. (See page 26 of *Cipher.*)

/s/ A.W. Greely
Lieut 36th US Inf
Acting Signal Officer [8]

In 1989 a copy of the shorter (presumed earlier) edition was donated to NSA. Curiosity prompted this study. The book is marked in red ink on the front fly leaf "Office Copy" and, both on the title page and first page, "Signal Department USA No. 18." It has been hand corrected in pencil where typographic errors appear in the text, showing careful study (but overlooking a typo misspelling "Vigenère" as "Vigeuere" in one place). There is a copy of this same edition, privately rebound, and with no marking, in the William F. and Elizebeth S. Friedman Collection at the George C. Marshall Research Library in Lexington, Virginia, without elucidation in the card catalog beyond the fact that it was a reprint of Blair, suggesting that Mr. Friedman appreciated it only as a historical curiosity. The Library of Congress also holds a copy of this edition, transferred there from the "W.B. [Weather Bureau?] Library" in 1917 and re-bound by the Library of Congress. [9]

The difference between the two editions is that the smaller one is a verbatim, type-reset and paginated reprinting of the 1807 Blair article from the Rees encyclopedia or its American counterpart. The expanded version (to be dated at least by 1869) appends some later information and observations based upon experience during the American Civil War. A record of the course of instruction for the 1869 signal officers' class notes the use of the Myer manual and a cipher manual, which would accord with Greely's notation.[10] But if Greely is to be taken literally, that the expanded version in which he wrote was the one used in his class just four years after the war ended, and if our speculation is correct that the shorter version predated it, we are left wondering . . . by how many years? The cryptologic state-of-knowledge of Civil War participants does not appear to be consistent with the comprehensive basis afforded by Blair. Further research in the correspondence and contracting records of the Chief Signal Officer at the National Archives might fix dates and specifics and thereby shed more light on a dim chapter of early American cryptography.

Having continued in postwar editions of his manual to use the 1863 journal article as if he knew of no superior treatment of cryptography, the Chief Signal Officer, one might speculate, subsequently learned of the Blair piece and had it printed to offer his men a concise supplemental reference on cryptology, much as a modern instructor might refer his

[8] Adolphus Washington Greely (1844–1935), Chief Signal Officer from 1887 to 1906, was a soldier-scientist of distinguished career, commencing with Civil War service as a volunteer and culminating with his receipt of a rare "lifetime" Medal of Honor as major general. Meteorologist-climatologist, polar explorer, founder of the National Geographic Society, Greely was also, as chief signal officer, compiler of the 1906 War Department Telegraphic Code, among other accomplishments.

[9] The United States Weather Bureau stemmed from the systematized recording, reporting (via telegraph), and study of weather conditions commenced by the Signal Corps after the Civil War. Gen. Myer's intense interest in the prospect of predicting the weather led to the somewhat derisive nickname, "Old Probabilities." The weather service function was transferred from the Signal Corps to the Department of Agriculture in 1891.

[10] Information provided to the author by Ms. Rebecca Raines, signal corps historian, U.S. Army, Center of Military History, May 1992.

students to the classic encyclopedia articles by William F. Friedman or Lambros D. Callimahos. Modern practices would expect identification of the source and authorship, however, and in this case, neither was given (if known). Perhaps this was considered not plagiarism, but a "lifting" for limited "official use only," thereby accounting also for the evidently small number of surviving copies.[11] In any event, Myer's use of "the finest treatment of the subject in English" remains a tribute to the professionalism he sought to instill in the Signal Corps and affords new insight into American military knowledge of cryptography during what had been regarded as the cryptographic "dark ages" of the mid-nineteenth century. And, in turn, one is left wondering . . . was Parker Hitt aware of Blair and "the little black book," or was there yet another gap in institutional memory?

Acknowledgment: I am indebted to [redacted] *of the NSA Library staff for her research assistance, including the discovery of the Pestana monograph cited in the notes.*

(b)(3)-P.L. 86-36

[11] The possibility that source and/or authorship were unknown to the "extractor" cannot be ruled out: see Footnote 1 above. Rees evidently is "rediscovered" at intervals: In 1970, two extracts comparable to *Cipher.* appeared, i.e., Rees's *Clocks, Watches and Chronometers, 1819–20*: a Selection from *The Cyclopaedia: of Universal Dictionary of Arts, Sciences and Literature* (Rutland, VT: C. E. Tuttle Co., 295 pp.) and *Rees's Naval Architecture (1819–20)* (Annapolis: United States Naval Institute, 183 pp.). As a basic repository of information, the Blair article offers a satisfactory answer to the question posed back in the sixties by the author to the late Lambros Callimahos: "How do you suppose the Confederates hit upon the Vigenère for their main cipher – how would an American in 1861, striking out on his own, have known about that system?" His response was, "Oh, probably from some encyclopedia, . . ." which may well have been the case.

~~(FOUO)~~ Mr. Gaddy is NSA's Chief Historian and a frequent contributor to Agency publications. He began his career in cryptology as a cryptanalyst (foreign language) in 1953 and served in a variety of staff and line management capacities in Operations, at the Pentagon, the National Cryptologic School, and the Director's Senior Council, before being given the opportunity to create the Center for Cryptologic History in 1989, and heading it during its first three years, concurrently serving as publisher of *Cryptologic Quarterly*. A charter member of the Senior Cryptologic Executive Service, he is a graduate of the Armed Forces Staff College and the National War College. He holds degrees from Mars Hill College (A.A.), the University of North Carolina, Chapel Hill (B.A.), and the George Washington University (M.S.). He also chairs NSA's Cryptologic History Committee and its World War II fiftieth anniversary commemoration. Dually certified in Language and Intelligence Research, he was NSA's second recipient of the National Foreign Intelligence Medal of Achievement, awarded by the DCI. In his "outside life," Mr. Gaddy is a recognized specialist in mid-nineteenth century military history, concentrating on the Signal Corps, cryptography, and secret service of the Confederate States. He was a coauthor of the 1988 *Come Retribution: The Confederate Secret Service and the Assassination of Lincoln*, co-winner of the 1988 National Intelligence Study Center "best book" award for intelligence literature.