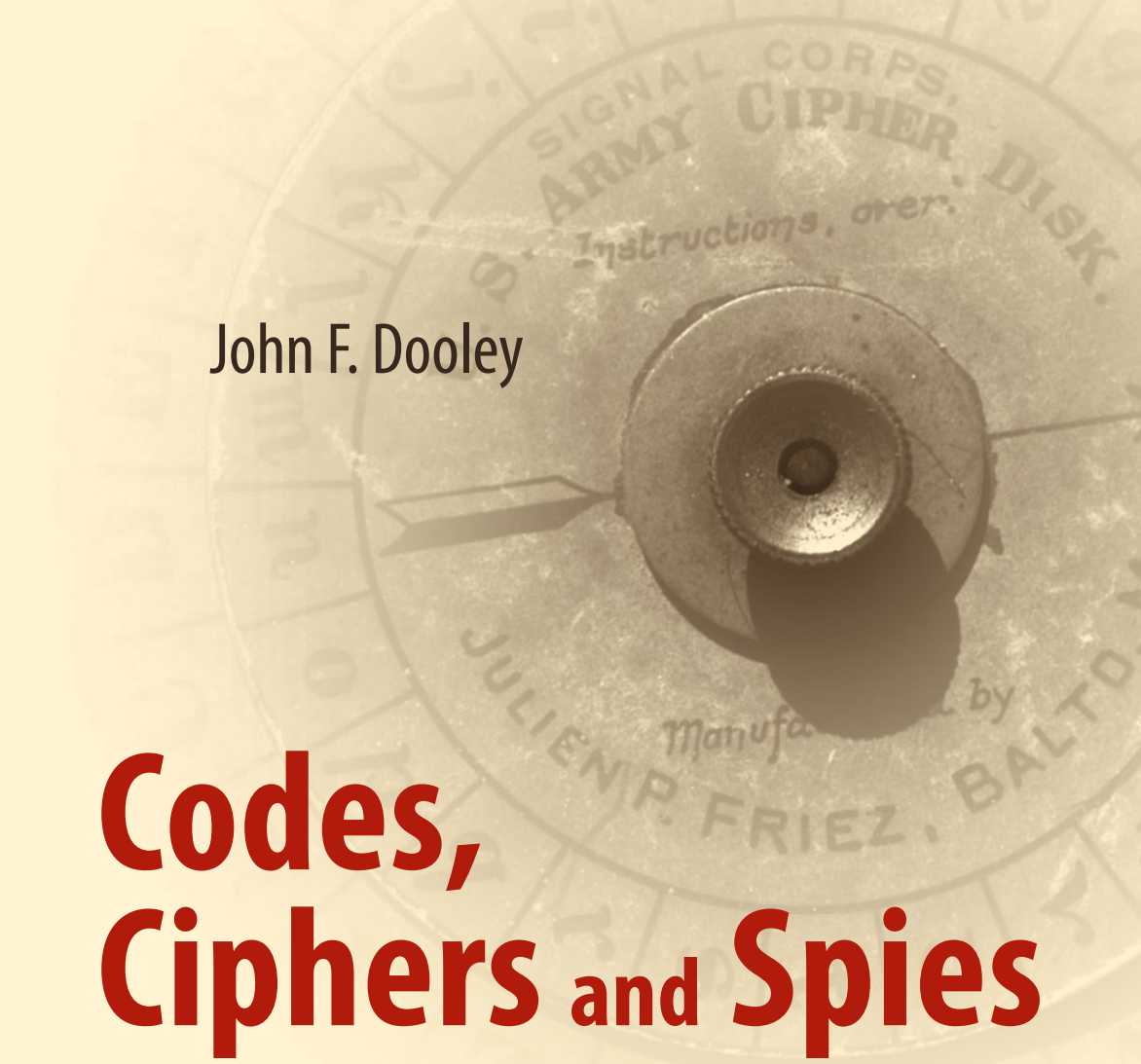


John F. Dooley

Codes, Ciphers and Spies

Tales of Military Intelligence in World War I

Springer

Codes, Ciphers and Spies

John F. Dooley

Codes, Ciphers and Spies

Tales of Military Intelligence in World War I

Copernicus Books
An Imprint of SpringerNature

John F. Dooley
Department of Computer Science
Knox College
Galesburg, Illinois, USA

ISBN 978-3-319-29414-8 ISBN 978-3-319-29415-5 (eBook)
DOI 10.1007/978-3-319-29415-5

Library of Congress Control Number: 2016933031

Published by Copernicus Books,
an imprint of SpringerNature.

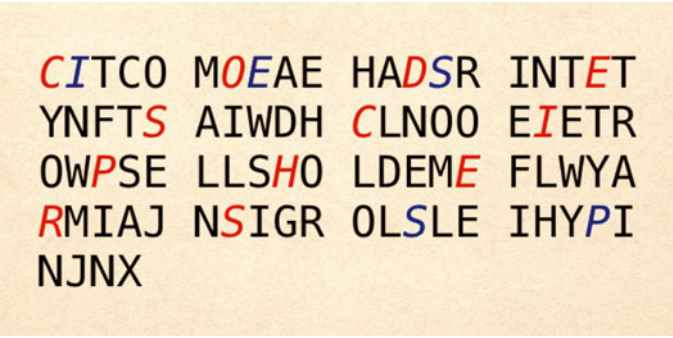
Copernicus Books
SpringerNature
233 Spring Street
New York, NY 10013
www.springer.com

Cover illustration: The cover image is copyright Dr. Nicholas Gessler, Duke University, and is used with his kind permission.

Printed on acid-free paper

This Copernicus imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

For Diane and Patrick


CITCO MOEAE HADSR INTET
YNFTS AIWDH CLNOO EIETR
OWPSE LLSHO LDEME FLWYA
RMIAJ NSIGR OLSLE IHYPI
NJNX

Preface

This book is about two different things. First, it started with the rediscovery of a series of a dozen articles written in 1927 on contract for *Collier's Weekly Magazine* about the cryptographic section of the Military Intelligence Division of the US Army during World War I by John Matthews Manly, a member of that division. These articles were never published, and they disappeared until recently, when copies were discovered in the William F. Friedman Collection at the George Marshall Foundation Research Library in Lexington, VA. The book describes how the articles were written, how they ended up in the Friedman Collection, and what they contain. The articles are presented; edited for grammatical, factual, and spelling mistakes (but spelling conventions from the 1920s are retained); and annotated to provide a context for their contents. The articles themselves contained no citations or bibliography, so these have been added where possible.

The second thing this book attempts to do is to put cryptology, particularly American cryptology, in the context of World War I. America was late in many ways in getting to the Great War. American cryptologists had to work very hard to catch up with their European counterparts who already had 3 years of experience in using code and cipher systems in a modern war by the time the Americans arrived in France in the summer of 1917.

The book is divided into four parts. Part I tells the story of the American Expeditionary Force (AEF), how it was organized and how it got to France, and gives us a peek into the military intelligence operations within the AEF during 1917 and 1918. For the entire 19 months that America participated in the Great War, the AEF was playing catch up to the Allies who had already been fighting for 3 years by the time that the first Americans arrived on the Western Front. The military intelligence organization was no different. A separate command from MI-8 (which handled domestic and diplomatic intelligence), the military intelligence unit in the AEF, designated G2-A6, had to be built from scratch and in the beginning was largely trained by their British and French counterparts. Manly provides us with insight into its operations and problems in three articles plus a separate essay to set the story for us.

Part II tells the story of MI-8 (Section 8, "The Code and Cipher Section," of the Military Intelligence Section of the Army General Staff), how it was organized and functioned, and how it dealt with domestic correspondence during the war. These articles focus on German espionage and civilian correspondence, including secret messages from German POWs interned in the United States. We learn how MI-8 acquired its intercepted messages, some techniques of decryption, and how MI-8 worked with the military intelligence counterespionage units within the Army.

Part III engages us with German efforts, largely through spies and sabotage, to hinder the supplying of American arms and ammunition to the Allies in the first 3 years of the war when the United States was still officially neutral. It's the story of German espionage and sabotage in the United States during the war. This includes a spy ring operating in New York, but run by German diplomats and embassy staff out of the German Embassy in Washington. It's the story of an unprepared German intelligence establishment trying to recruit competent spies and saboteurs in Germany and the United States and largely failing. Overall, the Germans were more an amateur or semipro team than an experienced group of professional intelligence agents. This story's central character is the infamous, but largely ineffective, female German spy Madame Marie de Victorica.

Finally, Part IV wraps up the narrative and brings the story back to John Manly.

Manly's articles provide us a window into his experiences in this environment, and the additional chapters attempt to flesh out the American experience in the war on both sides of the Atlantic. There is enough material in the various archives, even restricting ourselves mostly to cryptology, for several volumes. My hope is that this work will do justice to John Matthews Manly's contributions to the war effort and give the reader some insight into America's role in the last phase of the Great War.

Galesburg, IL, USA John F. Dooley

Acknowledgments

The copies of the Manly articles used here are in the public domain and are from Item 811 in the Friedman Collection at the George Marshall Foundation Research Library, Lexington, VA. They were ably scanned and transcribed by Elizabeth Anne King, Knox'13; any errors are mine.

I would like to thank the staffs at the Special Collections Research Center at the University of Chicago Library (which houses the papers of John Matthews Manly); the National Archives and Records Administration (NARA) at College Park, MD; and the George Marshall Foundation Research Library (where the William F. and Elizebeth S. Friedman papers are held) for their gracious help. Jeff Kozak and Paul Barron at the Marshall Library were particularly helpful and supportive. Rene Stein at the National Cryptologic Museum Research Library was, as always, very knowledgeable and helpful with my searches through the David Kahn Collection. I would also like to thank the research librarians at the Knox College Library, especially Anne Giffey and Laurie Sauer, for their kindness, patience, and help in digging up many obscure newspaper articles and books. Interlibrary loan is my savior. This research was funded in part by a grant from the Andrew Mellon Foundation and by grants from the Office of the Dean of the College at Knox College. As always, my wife, Diane, has been my inspiration, sounding board, and first and best editor.

Photo Credits

Figures 1.1 and 1.3 are from the John Matthews Manly Collection and are used with permission of the Special Collections Research Center at the University of Chicago Library. Figure 1.2 is used with permission of the New York Public Library. Figure 2.2 and Figs. 8.1 through 8.6 are used with permission of the American Battlefields Monument Commission. Figures 1.3, 2.3, 4.1, and 9.1 are from the William Friedman Collection of the George Marshall Foundation Research Library, Lexington, VA, and are used with permission. Figures 5.1 and 5.2 are copyrighted by Dr. Nicholas Gessler, Duke University, and are used with his kind permission. Figure 7.1 is from the David Kahn Collection at the NSA National Cryptologic Museum and is used with permission. Figures 13.1 through 13.5 and 14.1, 14.3, and 14.4 are in the public domain from the Library of Congress Prints and Photographs Division. All remaining figures are in the public domain and are from the National Archives and Records Administration, College Park, MD, or Wikimedia Commons.

Contents

Chapter 1
Introduction

Abstract In 1927, John Matthews Manly, former cryptanalyst for the Code and Cipher Section of the US Army Military Intelligence Division during World War I, wrote a series of a dozen articles intended for *Collier's* magazine. These articles are published here for the first time. This chapter gives a brief bio of John Manly and a short introduction to the internals of codes and ciphers.

In 1927, John Matthews Manly, a college English professor who had served in the Code and Cipher Section of the US Army's Military Intelligence Division (MID) during World War I, decided to write a series of articles about MID and his experiences during the war. Manly found a magazine interested in his idea and proceeded to write a set of twelve articles. Manly's articles were never published and were subsequently lost for more than 80 years. This book is the story of those articles, published for the first time here. It is also the story of MID, of German espionage in America during the war, the military intelligence unit of the American Expeditionary Force (AEF), spies, coded letters, plots to blow up ships and munition plants, secret inks, arms smuggling, treason, and desperate battlefield messages. The articles give us a uniquely American perspective on the Great War and provide a look at what the war was like both on the domestic and Western fronts for the Americans who lived it. The story all begins with John Manly.

1.1 John Matthews Manly: Early Life

John Matthews Manly was born on September 2, 1865, in Sumter County, Alabama, the eldest of seven children born to Charles and Mary Esther Manly. He came from a very successful and politically active Southern family. His great grandfather Basil Manly was president of the University of Alabama, and his grandfather, Basil Manly, Jr., was a minister and president of Georgetown College of Kentucky. In 1861 Basil Manly delivered the inaugural prayer when Jefferson Davis became the Confederate president. Manly's father, Charles, carried on the pastoral and educational traditions of his family and was a Baptist minister and the president of Furman University in Greenville, South Carolina.

J.F. Dooley, *Codes, Ciphers and Spies*, DOI 10.1007/978-3-319-29415-5_1

Fig. 1.1 John Matthews Manly (Used with permission of U. of Chicago Library)

John Manly was a precocious child and student, completing a master's degree in mathematics at Furman University in 1884 at age 19. He then taught mathematics at William Jewell College in Liberty, Missouri, for 5 years before heading to Harvard University to pursue his Ph.D. in philology. As Harvard did not have a department of philology, Manly put together his own program, rounded up a dissertation committee, and earned his degree in 1890. He then went to Brown University to teach English and stayed there until 1898 when he was lured by the new University of Chicago's first president, William Rainey Harper, to head the English Department there. With just the hiatus of his service during World War I, Manly would remain head of the department until his retirement nearly 40 years later (Fig. 1.1).

1.2 Manly and Chaucer

John Manly is primarily known as one of the world's premier Chaucer scholars. His masterwork, the result of a more than 16-year collaboration with Dr. Edith Rickert (1871–1938), one of his Chicago colleagues, is the eight-volume annotated edition of Chaucer's *The Canterbury Tales*, *The Text of the Canterbury Tales*, published just before his death in 1940 (Manly and Rickert 1940). Dr. Rickert had passed away in 1938 and never lived to see their magnum opus published.

Edith Rickert was first Manly's student, then his colleague in military intelligence during the war and finally, starting in 1924, his colleague in the English Department at Chicago. Rickert graduated from Vassar College in 1891 and taught at various high schools and later at Vassar before pursuing her graduate studies in English at the University of Chicago in 1895. She received her Ph.D. in English and philology in 1899 (Manly was on her dissertation committee). In 1900 Rickert moved to England and began a career as a novelist and journalist. While in England she published four novels, several research papers, and numerous newspaper arti-

Fig. 1.2 Edith Rickert (about 1905) (The Miriam and Ira D. Wallach Division of Art, Prints and Photographs: Print Collection. The New York Public Library.)

cles and short stories. She also worked as a professional researcher for a number of scholars including John Manly (Fig. 1.2).

Returning to Chicago in 1909, Rickert worked first as a magazine editor and in 1914 began teaching part-time in the English Department at the University of Chicago. During America's participation in World War I, she worked with Manly in the Code and Cipher Section of the Military Intelligence Division in Washington, DC. Rickert returned to Chicago after the war and continued her teaching at the university; she was named an associate professor of English in 1924. During this period, she and Manly wrote four textbooks on English and American literature and English grammar. It was also at this time that she and Manly began their collaboration on Chaucer.

From 1924 on, Manly and Rickert would spend the first 6 months of every year in England, tracking down reference after reference to Chaucer and manuscripts of *The Canterbury Tales*. In the summer and fall, they would be back at Chicago, teaching and supervising a staff of primarily graduate students that would collate and index their findings from England. Their goal was to find and annotate every single version of *The Canterbury Tales* in existence with the object of creating an authoritative text of the work, an effort that Manly thought, "would necessarily require several years" instead took 16. Rickert foresaw this early on in their collaboration. As Manly said in the preface to the set, "At a very early stage in our undertaking [Rickert] felt the great complication and size of it and often asserted that we could never finish it if we worked like normal human beings." While somewhat controversial 75 years later, their eight-volume *The Text of the Canterbury Tales* is still viewed by many scholars as the definitive work on this classic (Fig. 1.3).

1.3 Manly and Cryptology

In addition to the academic side of John Manly, his avocation was cryptology. From the time he was a teenager he was interested in secret codes and ciphers. Manly visited the Riverbank Laboratories in Geneva, IL, as early as 1915 to talk to the

Fig. 1.3 John Manly, Edith Rickert, and colleague David Stevens on board the *Europa* in 1932 (Used with permission of U. of Chicago Library)

owner, Colonel George Fabyan, about the alleged authorship of Shakespeare by Francis Bacon and the Baconian biliteral cipher. He also consulted with other scholars on cryptologic texts. For many years Manly maintained an active and friendly correspondence with Herbert O. Yardley, his commander during the war and the founder of the first permanent cryptologic organization in the War Department. William F. Friedman, widely regarded as the father of modern American cryptology, and Charles Mendelsohn, a historian and a colleague during World War I, were both close friends of Manly's. Their correspondence touched on many topics including cryptology, the Voynich manuscript and Roger Bacon, and, of course, Chaucer.

1.4 Manly in MI-8

Upon America's entry into World War I, John Manly, then 51 years old, volunteered for service in the US Army. He visited Major Ralph Van Deman, the head of the Military Intelligence Section, as early as March 1917 to offer his services. Van Deman contacted Manly at the end of September, and he was inducted as a Captain on October 3, 1917, and later promoted to Major. He served in the Code and Cipher Section of the Military Intelligence Division, designated MI-8, under the leadership of Herbert O. Yardley.

At the time of the American entry into World War I, the US Army did not have a formal intelligence organization nor did it have an organization to intercept and break enemy code and cipher messages. With each war or military conflict that the United States would find itself ensnared, the Army would create an intelligence organization and relearn all the skills and lessons required. Finally, in 1903 with the creation of the General Staff, the Army formed a formal military intelligence orga-

nization. This organization was short-lived, however, and was subsumed under the War College in 1908 with its separate identity eliminated. This first Military Intelligence Section did not include any personnel whose job it was to break enemy code and cipher messages.

With the American declaration of war, Major Ralph Van Deman, considered the "Father of American Military Intelligence," convinced the War Department that the United States needed a separate intelligence unit if it were to be a full partner in the war in Europe. So in May 1917 the Military Intelligence Section of the General Staff was created with Van Deman as its first head.

Herbert O. Yardley was a code clerk in the State Department and had developed a familiarity with State Department codes and ciphers. He also taught himself how to break those same code and cipher messages, much to the chagrin of his superiors. In early June 1917, and with his superior's reluctant assent, Yardley approached Major Van Deman with a proposal to create a Code and Cipher Section within the brand new Military Intelligence Section (Yardley 1931, pp. 34–36). With Van Deman's enthusiastic approval, Yardley created the Code and Cipher Section and continued its work as a civilian after the war. Yardley was an organizational genius, a slick and astute salesman, and a self-taught cryptanalyst who built the first permanent cryptologic organization in the US Army. Starting with just himself and a single clerk, Yardley built an organization that ended the war with more than 165 personnel and five subsections to handle shorthand messages, secret inks, code and cipher creation, code and cipher solution, and training. After the war his joint War-State Department Cipher Bureau—the Black Chamber—was the only US government organization devoted to breaking code and cipher messages during the 1920s. The Cipher Bureau was credited with breaking the main Japanese diplomatic code in 1920 and provided the US State Department with decrypted Japanese telegrams during the Washington Naval Conference of 1921–1922 (Yardley, 1931, pp. 283–317). These decrypted telegrams gave the United States a bargaining advantage in the negotiations on naval warship tonnage during the conference. With the change in administrations in 1929, Yardley's Cipher Bureau lost its funding, and he turned to other pursuits, including writing fiction, running a restaurant in Washington, DC, and writing nonfiction magazine articles about cryptology (Fig. 1.4).

Manly was 24 years older than Yardley, and their relationship was close during the war and would remain close at least through the early 1930s. Manly was practically the only person who defended Yardley after the publication of Yardley's tell-all 1931 book *The American Black Chamber* made him a pariah in the American cryptologic community.

In October 1917, Manly joined a fast-growing group under then Lieutenant Yardley in MI-8 as the head cryptanalyst, chief instructor, and second-in-command. Manly had an impact from the very beginning. He recruited several of his colleagues and students from the University of Chicago, including Dr. Edith Rickert, for MI-8 and began solving German military and diplomatic code and cipher messages.

Manly's greatest coup during the war was the solution of the Pablo Waberski cipher in 1918, a story told well, if not completely accurately, in Yardley's book, *The American Black Chamber* (Yardley 1931, pp. 140–171). Waberski was a

Fig. 1.4 Lt. Herbert O. Yardley (*Public Domain*. From RG 457 National Archives (NARA), the Yardley Collection.)

German spy who crossed into the United States from Nogales, Mexico, with a lengthy cryptogram in his possession. He was captured in Arizona on February 1, 1918, just after crossing the border, and the cryptogram was sent to MI-8 in Washington, where it languished unsolved for several weeks.

In early May 1918, Manly and Rickert spent the better part of 3 days breaking the cryptogram—a double transposition cipher—and Manly was later called to testify at Waberski's trial at Fort Sam Houston in San Antonio. The solution of the cryptogram was the damning piece of evidence that convicted Waberski and earned him a death sentence (later commuted; Waberski was released from prison and deported to Germany in 1924) (Kahn 2004, pp. 41–43).

When Yardley was sent to France in August 1918 and later assigned to supervise the cryptographic section of the American delegation to the Peace Conference in early 1919, John Manly became commander of the Code and Cipher Section and oversaw its demobilization after the Armistice, returning to the University of Chicago in mid-1919.

1.5 Manly After the War

Manly returned to the University of Chicago and resumed his post as chair of the English department. He and Edith Rickert published several more books together, including textbooks on English and American literature and a series of grammars for elementary schools in addition to their collaboration on Chaucer. While the remainder of Manly's career was primarily focused on literature, he still found time to work in cryptology.

Like many American cryptologists of the day including both Yardley and Friedman, Manly became interested in the Voynich manuscript (Kahn 1967, pp. 863–872). The Voynich manuscript is a 240-page illustrated vellum codex that is written in an unknown language and alphabet. It is named after Wilfrid Voynich, a Polish book collector and dealer who acquired it from a Jesuit monastery outside Rome in 1912. Nearly every page is a combination of text and illustrations. Of the approximately 170,000 letters in the manuscript, an alphabet of 20–30 symbols

would account for most of them. The vellum has been carbon-dated to the early to mid-fifteenth century, and the ink in which the text is written traced to a slightly later date. Professor William Newbold at the University of Pennsylvania announced a possible solution to the mysterious cryptogram in April 1921. He described the convoluted process requiring microscopes and a process of rearranging deciphered letters until they produced understandable Latin that he used to reach his decipherment. Manly began corresponding with Newbold and examining his claims and eventually came to the conclusion that Newbold's analysis was faulty and his decipherment incorrect. This led, later in 1921, to the publication by Manly of two papers on the Voynich, *Roger Bacon's Cipher Manuscript* (Manly 1921a) and *The Most Mysterious Manuscript in the World* (Manly 1921b). In these papers Manly laid out the various propositions about the manuscript and then analyzing Newbold's arguments and his process demolished them in their turn. Newbold would go on to publish a book on the Voynich manuscript in 1928 (Newbold 1928) in which he claimed to have deciphered the manuscript, and Manly would publish another paper shredding Newbold's techniques (Manly 1931).

1.6 The *Collier's* Articles

In the midst of his other scholarly work, Manly was also interested in telling the story of MI-8 during the war and of his own experiences as a member of the Military Intelligence Division. He was fully aware that much of what he could say was constrained by the secrecy demanded of everyone in MID with regard to their intelligence work during the war, but he thought he could tell enough of a tale to interest readers. In 1923 he contemplated writing an article for *Harper's Magazine* but eventually dropped the idea. Then in late 1926 the editor of *Collier's Weekly* magazine, Mr. William Chenery, wrote to Manly and suggested that Manly write a series of articles on the role of MI-8 during the war. Manly, who was about to head to England for his annual trip researching Chaucer, put Chenery off and said he would contemplate the series when he returned to the United States in June 1927.

Here is where our story really begins.

Neither Manly nor Chenery gave up the idea of the articles, and after some negotiations Manly eventually agreed to write a series of articles for *Collier's* on his World War I experiences (Manly 1927a). He was originally contracted to write up to six articles and finally between 7 and 12 articles, each 4,000 words, for *Collier's*, and was to be paid $2,000 for each article, a tidy sum for 1927 New York (Anonymous 1927).

In early September 1927 Manly went to New York, rented an apartment, engaged a secretary, and began to write. Herbert Yardley assisted him, although the extent of their collaboration is not completely known. By September 14, 1927, Manly had three articles on the Radio Intelligence Section in the American Expeditionary Force finished and sent them to *Collier's*. In a letter dated September 16, 1927

(Chenery 1927), Chenery indicated he was happy with the content of the articles but suggested they needed to be edited for the more casual style required for a general circulation magazine. By the end of September, Manly and Yardley had all 12 articles finished and were ready to get into the editing phase with an experienced magazine journalist that *Collier's* had engaged (Anonymous 1927, p. 6). Manly was also ready to be paid.

At this point, *Collier's* and Chenery began to back off. First of all, Chenery hadn't liked Manly's writing style in the articles he had seen—insisting it was too scholarly and not appropriate for the type of audience that *Collier's* catered to—and he assigned a freelance journalist named Davenport to rework the articles. Manly, Yardley, and Davenport had met in late September to discuss the content, and Davenport had gone off to rework the existing articles.

There was also an evolving dispute over the timing of payment for the articles. In the September 16, 1927, letter to Manly, Chenery had stated, "We pay on acceptance but in the case of a long series of articles are accustomed to space the payments over a certain period of time" (Chenery 1927, p. 1). Manly thought that he and Chenery had agreed that "pay on acceptance" meant "pay on delivery" and that Chenery had already agreed to "accept" the articles that Manly submitted (Anonymous 1927, p. 1). Every time during the latter half of September and the first half of October 1927 that Manly asked Chenery about payment, Chenery put him off (Anonymous 1927, p. 5, 7). Manly finally received a check for $2,000—one article—on October 10, 1927.

By late October—somewhere around the 20th—Chenery, Davenport, Manly, and Yardley met at *Collier's*, and Chenery informed Manly "…that the material was such that it was impossible for *Collier's* to accept the articles and offered to return the manuscripts of the twelve articles, with the understanding that Prof. Manly should keep the $2000.00" (Anonymous 1927, p. 7). After considerable discussion, on November 29, 1927, *Collier's* sent back the 12 manuscripts and John Manly kept the $2,000.

Apparently, John Manly sent the articles, unopened, to his attorney and at this point they disappeared. Manly never tried to get the articles published again.

John Matthews Manly passed away on April 2, 1940, having published his magnum opus on Chaucer but never having published a word on his experiences in MI-8 during World War I. Manly's younger brother Basil Maxwell Manly (1886–1950) was the executor of his estate, and it was apparently he who inherited the *Collier's* articles upon John Manly's death in 1940. Basil Manly was an economist and a longtime member of the Federal Power Commission. Rose Sheldon, in her annotated inventory of the William Friedman Collection (Sheldon 2000, p. 296), believes that Basil Manly was interested in seeing that the articles were published or included as part of a biography of his brother. This never happened.

Upon Basil Manly's death in 1950, the *Collier's* articles were apparently passed on to two US Army generals, Lt. General Alexander R. Bolling (see http://en.wikipedia.org/wiki/Alexander_R._Bolling) and Major General (GSC) F. L. Parks (http://en.wikipedia.org/wiki/Floyd_Lavinius_Parks), by an unknown source, possibly the executor of Basil Manly's estate. Bolling was then in command of the US Third

Fig. 1.5 William F. Friedman (Used with permission of George Marshall Foundation Research Library)

Army, which was the center of training for all new Army recruits. Parks was the head of the Army Information (read public relations) Department. These two gentlemen saw the value of the articles as historical artifacts and were interested in finding a permanent home for them (Anonymous n.d.). They proceeded to give the articles to William F. Friedman, then the head of the cryptographic division of the Armed Forces Security Agency (AFSA). Friedman evidently made a cursory examination of the articles, wrote up some brief notes, and then put them away, never to look at them again (Anonymous 1967) (Fig. 1.5).

In the late 1960s William and Elizebeth Friedman were making preparations to donate all their papers to the George Marshall Foundation Library, the *Collier's* articles among them. However, the Library does not hold the originals of the articles. Item 811 of the William Friedman Collection contains a set of photostatic copies of the articles along with a copy of the *Facts* memorandum that lays out the chronology of the creation of the articles during the last few months of 1927. None of the supporting documentation mentioned in the *Facts* memorandum or the originals of the articles themselves are present in the Friedman Collection, nor is their current location known. Neither the series of letters between Manly and Chenery nor the memoranda written by Herbert Yardley, described in the *Facts* memorandum, are in the Friedman Collection, nor are they in the John Manly Collection at the University of Chicago.

Curiously, the biggest story missing from the twelve articles is the Pablo Waberski story in which Manly played the leading role. There doesn't seem to be any reason to leave this story out. It has all the elements that *Collier's* may have been looking for—spies crossing the border, hidden messages, brilliant decryption work, and dramatic trial testimony. This story rates many pages in Yardley's *The American Black Chamber* (Yardley 1931, pp. 140–171), so why is it missing in these articles?

What is more, in the same folder in the Friedman Collection with the articles, there is a version of the story, apparently written by Manly after his testimony at Waberski's court martial in 1918. This 23-page document (included as Chapter

15 in the current volume) describes in detail how Manly broke the double transposition cipher message and also contains—apparently from memory—a transcript of Manly's testimony at Waberski's court martial at Fort Sam Houston in San Antonio, TX (Manly 1927b).

So this is the heart of our story. These 12 articles from 1927 give us a glimpse into German spies, US military intelligence, codes, ciphers, and secret inks and how America began to come of age in international relations, espionage, and signals intelligence as a result of World War I.

1.7 A Few Words on Codes and Ciphers

Secrecy in communications is known to have existed for close to 3000 years. As Kahn puts it, "It must be that as soon as a culture has reached a certain level, probably measured largely by its literacy, cryptography appears spontaneously – as its parents, language and writing, probably also did. The multiple human needs and desires that demand privacy among two or more people in the midst of social life must inevitably lead to cryptology wherever men thrive and wherever they write. Cultural diffusion seems a less likely explanation for its occurrence in so many areas, many of them distant and isolated" (Kahn 1967, p. 84).

Every discipline has its own vocabulary and cryptology is no different. This section does not attempt to be a comprehensive glossary of cryptology but rather gives the basic definitions and jargon.

Governments, the military, and people in business have desired to keep their communications secret ever since the invention of writing. Spies, lovers, and diplomats all have secrets and are desperate to keep them as such.

There are typically two ways of keeping secrets in communications. *Steganography* hides the very existence of the message. Secret ink, microdots, and using different fonts on printed pages are all ways of hiding the message from prying eyes. *Cryptology*, on the other hand, makes absolutely no effort to hide the presence of the secret message. Instead it transforms the message into something unintelligible so that if the enemy intercepts the message they will have no hope of reading it. *Cryptology* is the study of secret writing. A *cryptologic system* performs a *transformation* on a message—called the *plaintext*. The transformation renders the plaintext unintelligible and produces a new version of the message—the *ciphertext*. This process is *encoding* or *enciphering* the plaintext. A message in ciphertext is typically called a *cryptogram*. To reverse the process the system performs an inverse transformation to recover the plaintext. This is known as *decoding* or *deciphering* the ciphertext.

Steganography usually involves hiding the existence of the message physically in some innocent document or, recently, hiding it virtually in digital images. The most common form of steganography in history is the use of secret inks. The world of secret inks is divided into two types. *Organic inks* are those derived from the juices of fruits and vegetables—lemons, limes, oranges, and onions—and other

Table 1.1 The two dimensions of Cryptology

	Cryptography		Cryptanalysis			
Codes	1-part	2-part	Theft, spying	Probable word	Context	
Ciphers	Substitution	Transposition	Classical	Statistical	Mathematical	Brute-force
	Product cipher					

organic substances—milk, urine, blood, starches, etc. These inks can normally be developed using heat or water. *Sympathetic inks* are those that are normally derived from other chemicals and that must be extracted from compounds, including tannic acid, cobalt chloride, alum (aluminum potassium sulfate), iron sulfate, phenolphthalein, etc. Sympathetic inks require a separate chemical reagent as a developer.

The science of cryptology can be broken down in a couple of different ways; one is that it is concerned with both the creation of cryptologic systems, called *cryptography*, and with techniques to uncover the secret from the ciphertext, called *cryptanalysis*. A person who attempts to break cryptograms is a *cryptanalyst*. A complementary way of looking at cryptology is to divide things up by the types and sizes of grammatical elements used by the transformations that different cryptologic systems perform. The standard division is by the size of the element of the plaintext used in the transformation. A *code* uses variable-sized elements that have meaning in the plaintext language, like syllables, words, or phrases. On the other hand, a *cipher* uses fixed-sized elements like single letters or two- or three-letter groups that are divorced from meaning in the language. For example, a code will have a single *code word* for the plaintext "stop," say, 37761, while a cipher will transform each individual letter as in X=s, A=t, V=o, and W=p to produce XAVW. One could argue that a code is also a substitution cipher, just one with a larger number of substitutions. However, while ciphers have a small fixed number of substitution elements—the letters of the alphabet—codes typically have thousands of words and phrases to substitute. Additionally, the methods of cryptanalysis of the two types of system are quite different. Table 1.1 provides a visual representation of the different dimensions of cryptology.

1.8 Codes

A *code* always takes the form of a book where a numerical or alphabetic *code word* is substituted for a complete word or phrase from the plaintext. *Codebooks* can have thousands of code words in them. There are two types of codes, 1-part and 2-part. In a 1-part code, there is a single pair of columns used for both encoding and decoding plaintext. The columns are usually sorted so that lower numbered code words will correspond to plaintext words or phrases that are lower in the alphabetic ordering. For example,