The National Cryptologic Museum Library

Eugene Becker

Last year, a widely published German technical author, Klaus Schmeh, e-mailed the library of the National Cryptologic Museum from his home in Gelsenkirchen, Germany. He needed information for an article on the Kryha cipher machine, a device popular in the 1920s. Librarian Rene Stein found articles about the machine but, even more useful, she found unpublished correspondence between Alexander von Kryha, the machine's inventor, and a German who had invested in the machine. She photocopied the files and sent them to Schmeh, who used them for a talk at the 2009 Cryptologic History Symposium and for an article in *Cryptologia* magazine. Thus the museum advanced knowledge of the history of cryptology.

When scholar Chris Christensen needed information on the US Navy cryptology correspondence courses for his article on William Wray, an early NSA mathematician, he contacted the museum library. From its collection of Special Research Histories, he obtained copies of the courses produced by the Navy between 1937 and 1946.

In researching his book on the vocoder, which played a role in speech scrambling, David Tompkins met at the NSA Museum with Frank Gentges, a vocoder consultant during the Cold War. Gentges and his partner, the late David Coulter, had contributed their collection of speech cryptodevices to the museum. Gentges took Tompkins on a Cold War "Secure Voice" tour, explaining the HY-2 vocoder and the STU-II and STU-III phone systems. (The museum's audio history of secure voice was also helpful.) Because Tompkins was primarily interested in the replica of the extremely secure World War II SIGSALY voice encryption system, he and Gentges spent most of the day in the library going through declassified SIGSALY files. The librarian provided technical manuals, Signal Corps logs, and noted cryptologic historian David Kahn's notes for a SIGSALY article in the IEEE publication Spectrum), as well as photos of the SIGSALY terminals. All of this provided much-needed backbone for the SIGSALY chapter of his book.

In dozens of ways like these, the museum and its library, with the support of the National Cryptologic Museum Foundation, is becoming a world center of historical intelligence research. Daily, the museum responds to historians seeking answers to questions in intelligence history, primarily cryptology. It has expanded its original focus of displaying cryptologic artifacts to educating the public about cryptology and its vital role in national defense.

The museum grew out of the US Army's collection of captured Axis cryptographic equipment and the Army Signal Intelligence Service's Research and Development Museum of older cryptographic devices and books. At first these were merely displayed

All statements of fact, opinion, or analysis expressed in this article are those of the author. Nothing in the article should be construed as asserting or implying US government endorsement of its factual statements and interpretations.

in cases in the halls of NSA. When around 1990, the history-minded Vice Admiral William O. Studeman, then the director of NSA, established the Center for Cryptologic History and NSA acquired a motel adjacent its headquarters, space for a real museum became available. Earl J. "Jerry" Coates and another NSA employee, Jack E. Ingram, helped by an NSA graphics team and construction workers, converted one of the buildings into a museum and library. On Coates' retirement, Ingram took over as director. The doors were opened on 15 July 1993 to NSA employees, then, in December, to the public.

The museum, whose story has been well told by Ingram in "The Story of the National Cryptologic Museum," *Studies in Intelligence* 47, No. 3 (2003), displays some of America's most valuable cryptologic artifacts. Among the most dramatic is the museum's huge bombe—the World War II electromechanical device that tested German Enigma-machine intercepts with possible cribs to see if any produced a valid Enigma key so German messages could be read. Visitors queue up at the museum's Enigma cipher machine—perhaps the most famous in the world because of its use by the German armed forces and its solution by the Allies. They stare at the museum's polished brass Hebern cipher machine—the first to utilize the rotor principle, which became the world's most used cryptosystem, at the Civil War cipher table mounted on a cylinder, at the replica of a World War I intercept station. The museum has on display the first printed book on cryptology—the 1518 *Polygraphiae libri sex* of the Benedictine monk and mystic Johannes Trithemius.

For those who pursue that history, the museum library has proven to be a mother lode of valuable resources. Perhaps first among these are the declassified oral histories of such cryptologic pioneers as Frank Rowlett, the "foreman" of the team that cracked the Japanese PURPLE diplomatic cipher machine and who ran a major Army codebreaking element in World War II. He later became an assistant to successive directors and his reminiscences are exceptionally useful and interesting because they include much about agency personalities. Other gems consist of the British technical studies of the breaking of the German Enigma and other cipher machines and some of the Allied TICOM studies—the American-British reports, based on captured documents and postwar interrogations, of Axis code-making and code-breaking. These provide a remarkable source for a rounded history of cryptology in World War II.

The core of the library book collection was gathered in the years before World War II when resources for cryptologic study were scarce. Under the direction of William F. Friedman, Chief of the Army's Special Intelligence Service, books were collected wherever they could be found regardless of age or language. Thus the library has many rare and hard-to-find items that were used for study. In his book *The Story of Magic*, Frank Rowlett, the first junior cryptanalyst hired by Friedman, tells how his cryptologic training began. On his first day of work, Rowlett watched as Friedman removed four books from a vault; two were in German and two were in French. Rowlett was only able to read German so he began with F.W. Kasiski's *Die Geheimschriften und die Dechiffrirkunst* and later went on to Andreas Figl's *Systeme des Chiffrierens*. The library holds both of these famous books as well early cryptanalytic training materials such as *Elements of Cryptanalysis* (Training Pamphlet No. 3), and Friedman and Lambros Callimahos's three-volume *Military Cryptanalytics*.

In addition to these, the library's book collection contains 6,000 books, covering all aspects of cryptology from technical manuals and how-to books on codes and ciphers to histories that describe the development and impact of code-making and codebreaking as well as their use by spies and foreign governments. The library also has one of the largest collections of commercial code books. These codebooks were used by businesses to

reduce the cost of cable communications by substituting short code groups for words and phrases in telegrams. Modern communications and encryption methods have made them obsolete and mainly of historical interest.

The library is also home to a collection of hundreds of scientific articles on communications, computer security, electronic equipment, key management, mathematics, intelligence, and cryptologic history collected during the 1970's and 80's. Because they predate articles covered in full-text databases, they are difficult or impossible to find in one place elsewhere. The collection is called the Disher Collection, named for its compiler.

In addition to books and articles, the library houses a number of historical declassified documents: special research histories, Japanese "Red" messages, Venona messages, MASK messages, and ISCOT messages. Special research histories or SRHs are of naval, military, intelligence, diplomatic, and technical studies prepared largely by the US military utilizing decoded and translated enemy communications. The bulk of the material deals with World War II, though some studies cover topics ranging from World War I to the attack on USS Liberty in 1967. These documents describe military operations, intelligence organizations and activities, communications security and intercepts, code breaking, codes, and ciphers.

During the 1930s, the Japanese enciphered their diplomatic messages using a machine that US intelligence named "Red." The library holds 3,338 decrypted messages dating from November 1934 to October 1938.

The Signals Intelligence Service began a secret program in February 1943, later codenamed VENONA. The mission of this small program was to examine and exploit Soviet diplomatic communications, but after the program began, the message traffic included espionage efforts as well. The first of these messages were declassified and released in July 1995. Over the course of five more releases, all of the approximately 3,000 VENONA translations were made public. The library holds copies of all of the released VENONA messages.[1]

The British Government MASK messages are thousands of secret COMINTERN (Communist International) messages between various capital cities and Moscow from 1934 to 1937, which give a wealth of detail about Moscow's control of the various national Communist parties (including the American Communist Party). ISCOT was the codename for the British program to intercept and decrypt clandestine radio messages between Moscow and COMINTERN (Communist International) outstations in German-occupied Europe and in China from 1943 to 1945. The library holds a complete set of both the MASK and ISCOT messages.

Early this year, the Museum Foundation purchased a collection of children's books on cryptology for the library's younger researchers. Among them are books on Native American Code Talkers and codes and ciphers.

An event that moved the museum to the forefront of historical intelligence studies was the donation by David Kahn, the author of *The Codebreakers* and a 1995 NSA scholar in residence, of his considerable collection of books, articles, interview notes, and docu-

[1] See https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/venona-soviet-espionage-and-the-american-response-1939-1957/venona.htm

ments on cryptology to the library. This enormously expanded the range and value of the holdings of the library. Of David Kahn's several careers—historian, journalist, author—it is as a collector and researcher that he has made perhaps his most important contribution to the esoteric field of cryptology. Kahn began buying books on the subject as a young man, starting with readily available trade works and soon adding rare books such as Blaise de Vigenère's 1587 *Traicté des Chiffres* and Johannes Frederici's 1684 *Cryptographia* and journal articles on cryptology, as well as letters and interviews he had gathered while writing his books. Realizing that his two sons were not interested in cryptology or his by-then vast and valuable collection, he decided to donate his books to the National Cryptologic Museum through the National Cryptologic Museum Foundation.

Among the most interesting items in the Kahn Collection are the papers of an early 20th century American cryptanalyst, Colonel Parker Hitt, and some papers of Dr. Lester Hill, who first proposed polyalphabetic algebraic ciphers—though, regrettably, nothing about the cipher machine that he patented for that system. There are also some very rare items such as photocopies of a historical study of French cryptology from about the 1880s to a little past the end of World War I, based on documents that no longer exist and a personal memoir by Givierge, telling his life story as a leading figure in French cryptology and giving his colorful impressions of personalities in that field.

All of Kahn's books have been cataloged and are now available for reading and research in the library. However, because of their vast number, the papers are still being processed. Recently the library began to digitize Kahn's very valuable notes from correspondence and interviews conducted while researching his books and articles. Among these is an interview with retired Captain A. J. Baker-Cresswell, commander of the Royal Navy destroyer Bulldog that had captured a German Enigma machine and its book of settings from the U-110. The detailed story of the capture would never have come to light but for the interview. Yet to come from Kahn are his collection of photographs of cryptologic and intelligence personnel, equipment, and places. Such illustrations will enhance the value of the museum to television producers and internet users.

The library was further enriched last spring by the aquisition of the personal collection of the late Louis Kruh, a nationally known collector and colleague of Kahn. Among the 60 boxes and three file cabinets is a correspondence addressed to Alexander Hamilton in 1796 prepared in a shorthand system of concealment. Later, in May, the library received the archive of Chaocipher material from the estate of inventor John Byrne. Chaocipher is the name Byrne gave to a cipher system he invented in 1918. The Chaocipher is on a list of infamous unsolved codes and ciphers, and it remains both a cryptologic curiosity and legend—one of today's premier unsolved cipher challenges.

Information about the museum's hours, its services, and contact telephone numbers can be found on the Internet at http://www.nsa.gov/about/cryptologic_heritage/museum/ and at http://www.cryptologicfoundation.org.

**The idea for this article originated with Dr. David Kahn. I also wish to acknowledge the helpful assistance of the museum library staff in its preparation.*

❖ ❖ ❖