United States Cryptologic History

"Give to Ferner"
The Untold Story of an American Master Cryptanalyst

Special Series | Volume 14 | 2023
Center For Cryptologic History

This publication presents a historical perspective for informational and educational purposes, is the result of independent research, and does not necessarily reflect a position of NSA/CSS or any other US government entity.

This publication is distributed *free* by the National Security Agency. If you would like additional copies, please email history@nsa.gov or write to:

Center for Cryptologic History
National Security Agency
9800 Savage Road, Suite 6886
Fort George G. Meade, MD 20755

Cover: Robert O. Ferner, Arlington, VA, circa 1944-1945, courtesy of Mrs. Jean Ferner

“Give to Ferner”

The Untold Story of an American Master Cryptanalyst

Brenda J. McIntire

Center for Cryptologic History

2023

And then, at a certain length, it said, "Give to Ferner." Oh yes. He was the only one that could solve them if they were really short. Only Ferner.[1] — Arthur J. Levenson

Prologue

In July 1936, a young college graduate from Alliance, Ohio, began working for the US Army in Washington, DC. He was joining an organization that would play a critical role in assuring America's security during the coming global war and beyond. Without ever firing a shot on a battlefield, this man personally enabled numerous attacks and defenses in a most secret war: a war fought not with kinetic weapons but with weapons of the mind. The man was Robert Orestes Ferner, and the battlefield was the realm of cryptology.

Much of the story of US Army cryptology in the 1930s and the impact of American cryptology during World War II is well known. For decades, leaders such as William Friedman and successes such as the Allied breaking of the German Enigma machine have risen to fame. More recently, the cryptologic workforce—including thousands of "code girls"—has received increased public attention. But the stories of other major contributors remain to be told. Robert O. Ferner is one of these.

This account is a step toward better understanding the work and impact of one of America's most outstanding cryptanalysts of the 1930s and 1940s—and most likely far beyond. Because of his involvement with many, if not most, army cryptanalytic problems during this period, the study of his life and cryptologic work also illuminates the broader story of US Army cryptanalysis.

To understand Ferner's work, one must first understand the state of US Army cryptology in the 1930s.

Formation of the Signal Intelligence Service

In 1930, the army's sole cryptographer-cryptanalyst in Washington, DC, finally obtained long-sought permission to hire several assistants. The man was William Friedman, a civilian employee of the US Army Signal Corps. The decision to allow Friedman to build his workforce had its roots in an event from the preceding year.

From the end of World War I until 1929, the United States had sponsored a covert cryptanalytic presence in New York City. This organization had sprung from a wartime group with a similar mission. Its leader remained the same: Herbert O. Yardley, a former cipher clerk for the Department of State. During World War I, Yardley successfully led MI-8, the unit responsible for solving codes and ciphers within the larger Military Intelligence Division. The State Department and US Army jointly funded a continuation of the capability after the war, with State providing the majority of funding.

In 1929, Secretary of State Henry Stimson suddenly terminated the effort, stopping activities and releasing personnel. The organization's legacy, in the form of records and expertise, shifted to the Signal Corps office in Washington, DC. In July of 1929, the War Department decided to establish the Signal Intelligence Service (SIS), which encompassed not just cryptography and cryptanalysis, but also the related disciplines of intercepting communications and developing secret inks.

As the new organization began operations, Louise Newkirk reported to work on March 1, 1930, as an assistant cryptographic clerk. In April, three additional technical workers arrived: Solomon Kullback, Frank Rowlett, and Abraham Sinkov. All were high school mathematics teachers, hired through the civil service system into a new role of junior cryptanalyst. Friedman's original vision had been for the junior cryptanalysts to double dip: they would be mathematicians, but they also would collectively provide language expertise in

French, German, Spanish, and Japanese. He got his wish for three of the four languages, lacking only Japanese. In May, John Hurt, a brilliant Japanese linguist, reported as a cryptanalyst aide.

Over the next few years, several more individuals joined SIS as typists, clerks, and a stenographer. But Friedman had no authority to hire any other junior cryptanalysts. Not, that is, until an opening arose at the SIS headquarters.

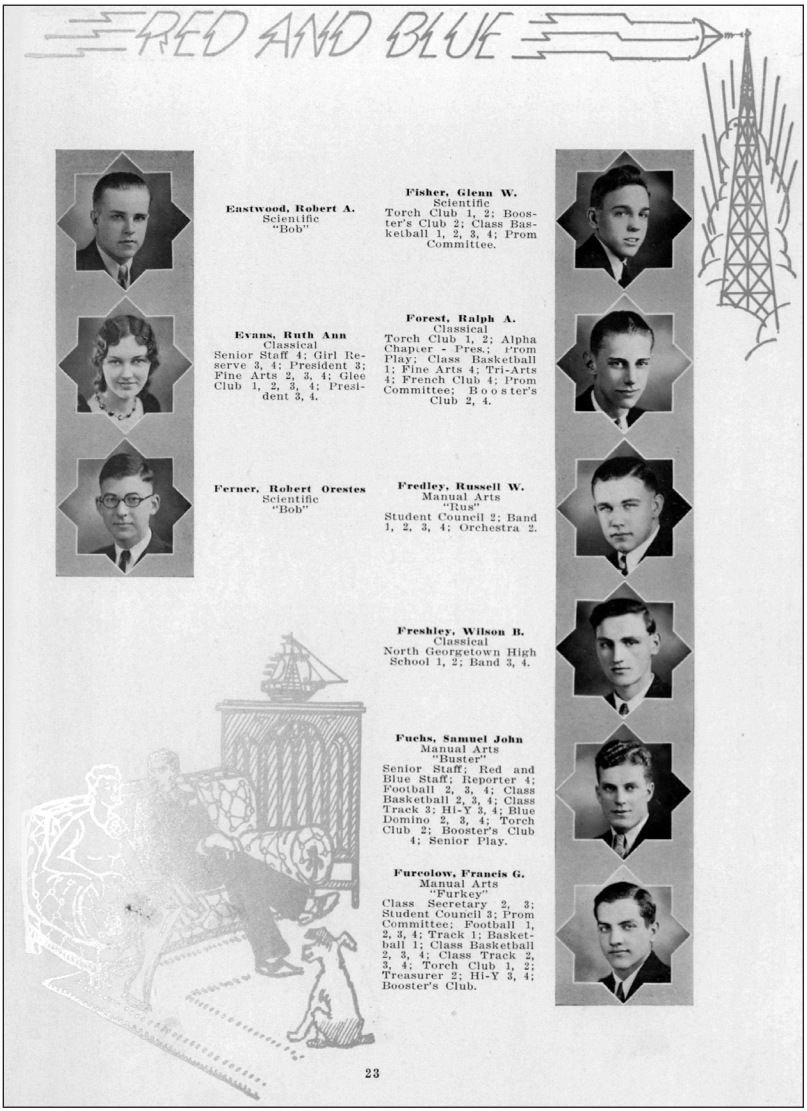
In early 1936, Sinkov, one of the original junior cryptanalysts, was transferred to an American base in Panama. He was to provide cryptanalytic support and training to the personnel on site. As a result, Friedman gained permission to hire a junior cryptanalyst to fill Sinkov's position in Washington. The man selected was a recent physics graduate from Alliance, Ohio, Robert Ferner.[2]

Ferner's Background

Robert Orestes Ferner was born in Clear Spring, Iowa, on May 15, 1915. His father, Orestes Asa Ferner, was an educator, whose genealogical studies traced the first Ferner's arrival in America from Switzerland in the mid-1700s. Robert's mother, Marie Pfund Ferner, was also of Swiss ancestry. Robert was the youngest of three surviving brothers; the firstborn son had died when still a child.[3]

During Robert's early years, the family moved to a farm near Alliance. While Orestes continued working in education, the real farming enthusiast in the family was middle son Terrence, whose high school yearbook noted his "ability to run a 100-acre farm."[4] Robert's mother also had farm-related skills of her own, winning a local "nail driving contest for women."[5] Despite the family's best efforts, the impression left with Robert Ferner's daughter years later was that neither the Ferner farm nor the Ferner family income had prospered greatly during these years, due in large part to Orestes's reluctance to invest in the farm's infrastructure.[6]

Despite the opportunities offered by living in the countryside, Robert's severe asthma prevented his spending much time outdoors. But his health did not affect his academic life.



I. Robert Ferner's high school yearbook entry, 1931.
Courtesy of the Alliance School District, Alliance, Ohio

Robert graduated in 1931 from Alliance High School at age 16, near the top of his class.[7] He went on to study physics at Mount Union College (now the University of Mount Union) in Alliance,

SENIORS

John W. Fairless

Alpha Kappa Pi — Massillon, Ohio

Football 2, 3, 4; Junior Prom Committee; Class Day Committee; Inter-Fraternity Council 3, 4; Glee Club 4; Oratorio 4; A Capella Choir 4; Intramurals 1, 2, 3, 4.

Robert Ferner

Alpha Kappa Pi — Alliance, Ohio

Physics Lab Assistant 2, 3, 4; Psi Kappa Omega 3, 4.

Mary Louise Fitch

Cortland, Ohio

Phi Sigma 3, 4; Pi Gamma Mu 3, 4; W. A. A. Board 3.

J. William Foltz

Sigma Alpha Epsilon — Canton, Ohio

Junior Prom Chairman; Class President 4; Pres. Student Senate; Class Treasurer 3; Inter-Fraternity Council 3, 4; Dynamo 1, 2; Unonian 2, 3; College Social Committee; Intramurals 1, 2, 3, 4.

29

II. Robert Ferner's college yearbook entry, 1935. *Courtesy of the University of Mount Union Library, Alliance, Ohio*

ALPHA KAPPA PI—FOUNDED AT NEWARK
CHAPTER HOUSE AT 536 WEST STATE STREET

SENIORS:

Eric Brady, John Fairless, Theodore Earl, James Thomas, William Thacker, Eugene Benedetto, Robert Ferner, Joseph Lasse, Frank Leyda.

JUNIORS:

Ralph Curtis, John Yaggi, Ennio Juisti.

SOPHOMORES:

John Woods, Kenneth Eckert, Hamill Hartman, Charles Hart.

FRESHMEN:

Robert Bryden, Wilson Snyder, Dean Crawford, Melvin Waltz, Darl Dolan, Francis Bartchy, James West, Allan Adams, Wendell Graening.

90

III. Alpha Kappa Pi group photo, 1935. Ferner is seated in the front row, left-hand side. *Courtesy of the University of Mount Union Library, Alliance, Ohio*

graduating in 1935. Here he served as vice president of the local chapter of Alpha Kappa Pi, an engineering fraternity; joined Psi Kappa Omega, a local fraternity honoring academic achievement; and also found time to assist in the physics laboratory.[8]

While at Mount Union, Robert met Erma Pauline Woodward whose gregarious nature complemented Robert's quieter personality. The morning after Erma graduated in June 1937, she married Robert in a small, family-only ceremony on the Mount Union campus. After a celebratory wedding breakfast, the couple departed, but not, it seems, for their honeymoon. Instead, as the local Alliance newspaper noted, "the couple left immediately for Washington, D.C." where "the bridegroom … is in the employ of the War Department."[9]

Ferner's Early Years at SIS

And indeed he was. Ferner had joined SIS on July 1, 1936, aged 21. His starting salary as a junior cryptanalyst was $2,000—exactly that of the first three junior cryptanalysts hired in 1930.[10] Although Sinkov was still in Panama and Kullback would soon depart for a similar tour in Hawaii, Rowlett was still in Washington.

By the time Ferner arrived, the original junior cryptanalysts had six years of experience. Friedman had developed on-the-job training for the earlier junior cryptanalysts, based on a combination of his own writings; World War I-era encryption problems; real-life projects from the dusty files of the Cipher Bureau; and current encrypted messages, contingent upon SIS's new collection capabilities.[11] Rowlett commented some years later that he and his peers had passed along their training to the new hires. Hurt also ran in-house training in Japanese, which Ferner attended.[12]

Organizationally, as late as March 1937, SIS still numbered only around a dozen employees. There was an Administrative and School Section numbering five people and the Code and Cipher Solution and Compilation Section comprising Friedman and six others, including Ferner.[13] By 1938 though, four distinct cryptanalytic units had emerged, dedicated to the diplomatic traffic of Japan, Germany,

Italy, and Mexico, respectively; the latter unit eventually expanded to include other countries using Spanish and related languages.[14] It is not certain which of these sections became Ferner's home base, but, in light of his ongoing association with Rowlett and the Japanese problems under Rowlett's direction, the Japanese "J section" seems most likely. Regardless of the exact administrative location, Ferner's career was progressing well. By February 1938, he was characterized as a "cryptanalyst of considerable ability."[15]

Within this intimate atmosphere of SIS, Ferner and Hurt became good friends. The Ferners and the Hurts often socialized together outside of work. Robert and Erma's daughter Jean later recalled that the Hurts shared their love of opera with the Ferners—something the musically inclined Erma probably appreciated more than Robert did.

Japanese Red and Purple Machines

During the 1930s, the SIS cryptanalysts expanded their understanding of encrypted Japanese diplomatic communications. For some time the Japanese had employed superenciphered code systems, overlaying a robust codebook with a level of encipherment. Both levels could be cryptanalytically and linguistically challenging. Even after solving an encryption system, the American cryptanalysts had to re-solve aspects of the puzzle each time the Japanese changed current settings or modified the underlying system.

Within a few months of joining SIS, Ferner developed a system of indexing encoded Japanese diplomatic messages. This index was an efficient way to correlate mentions of certain messages within other messages and also provided continuity when the Japanese moved to new codes.[16]

Early Japanese diplomatic systems were all traditional manual systems, enciphered and deciphered by hand. But in the early 1930s, the Americans discovered the Japanese had taken a quantum leap: they were encrypting high-level diplomatic communications by machine.

Machine encryption was not a new concept in the 1930s. Individuals from several countries had already developed and marketed machines claiming to produce secure ciphers. During World War I and in the 1920s, Friedman had solved several of these systems, including the Navy Cipher Box.

The Japanese called the first of their machines Type A; the Americans, using a different color to identify each encryption device, called this machine Red.[17] This machine appeared by at least 1932.[18]

Red gave SIS cryptanalysts an opportunity to examine contemporary real-world communications encrypted by machine. In the early SIS, such a problem would have been an all-hands-on-deck affair. Rowlett, the lead on Japanese diplomatic communications, personally worked on Red, and Ferner did as well.[19] To communicate using typewriters and similar machines, the Japanese converted their language's characters into the romanized letters of the English alphabet. While solving Red, SIS realized that the machine's cryptography was influenced by the English alphabet's division into vowels ("the sixes") and consonants ("the twenties"). This insight would prove most useful in combatting the next development in Japanese machine cryptography.

Although SIS fully understood the Red machine by 1936, the cryptanalysts still had to keep up with changes to the machine's settings, some of which were daily.[20] The Japanese did not give the SIS cryptanalysts much opportunity to rest on their laurels. On February 20, 1939, Japanese diplomatic posts began communicating in a new cipher, known to the Japanese as Type B and to the Americans as Purple. Purple was similar to Red in preserving a distinction between the "sixes" and the "twenties," but overall the Japanese had significantly improved the machine's security. It took a year and a half to the very day (September 20, 1940) for the SIS cryptanalysts to resolve the last sticking point in their understanding of how the machine worked. After that, it was a matter of scaling up the effort to apply the discovery to all possible machine settings. On September 27, the first Purple translation based on the recent breakthrough appeared. SIS subsequently developed a machine of its own to dupli-

cate the Japanese capability to decrypt Purple messages. All of this was accomplished without ever having seen the Japanese device itself. It was an amazing achievement.[21]

Several weeks after the Purple breakthrough, Friedman documented the success, naming key contributors. At the head of that list, he began with two key players:

> The specific direction and coordination of all studies on this project was the joint work of Cryptanalyst Frank B. Rowlett and Assistant Cryptanalyst Robert O. Ferner. Their indefatigable labors and brilliant analytical work testify and are a credit to their cryptanalytic skill, training and experience.
>
> To their joint direction and efforts are due the extremely fruitful analysis of the cryptographic mechanics underlying the operation of the B-machine as a whole, the theory of its operation, and the development and solution of the "6's" at [an] early date in these studies.
>
> They were also extremely active in pushing the solution to a successful conclusion by organizing and directing the reconstruction of the developments or wirings of the switches for the "20's."[22]

Cryptologic historians and others recounting the Purple story have rightly recognized the contributions of Friedman, Rowlett, cryptanalyst Genevieve Grotjan (later Feinstein),[23] and engineer Leo Rosen. But one significant name has fallen by the historical wayside. Future accounts of the Purple success should reinstate the pivotal role of Robert Ferner, the man who, with Rowlett, provided the essential technical leadership and expert analysis that enabled the entire SIS team's success.

And what of the value of Purple? Technically, Friedman considered the success "to have been by far the most difficult cryptanalytic problem successfully handled and solved by any signal intelligence organization in the world."[24] And the intelligence value? Friedman continued, "so far as [Arlington Hall Station] is concerned, this has

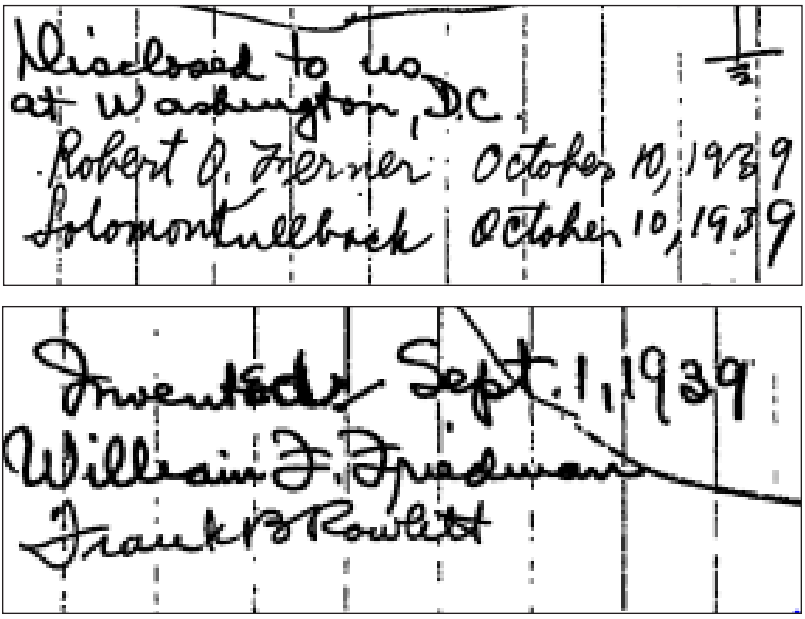
been and still is the most important source of strategically valuable, long-term intelligence." One well-known user of Purple illustrates this value: Japan's ambassador to the Third Reich, Lieutenant General Oshima Hiroshi, had broad, firsthand access to Hitler's plans and capabilities.[25] For the duration of the war and across all theaters of action, Oshima faithfully kept the Japanese leadership apprised of his observations and insights. His Purple-encrypted reports encompassed remarkable breadth and depth, ranging from tactical preparations, operations, and weapons development to strategic partnerships and intent.[26] Unbeknownst to him, he was faithfully reporting, in equal measure, the same vital information to the Americans.

SIS Prepares for War

In response to Germany's invasion of Poland on September 1, 1939, Britain and France declared war on Germany. These world events triggered—almost immediately—what a decade of pleas from Friedman had been unable to accomplish. In September 1939, the US Army at long last approved funding to increase SIS's workforce substantially. The new recruits began arriving in October.[27]

It was a busy time within SIS. Even as SIS was training the new workforce and wrestling with cryptanalytic problems, the cryptologists were still responsible for developing cryptographic solutions to protect America's own communications. In September, Friedman and Rowlett completed a patent application documenting their joint invention for securing "electrical printing telegraphy." Kullback and Ferner were their witnesses.[28]

In late 1941, the SIS reorganized—a theme that would repeat throughout the war—as SIS tried to keep up with an exponentially expanding workforce and an evolving wartime mission. The Cryptanalytic Section was now one of four major sections within SIS, alongside sections devoted to administration, cryptography, and a secret ink and photographic laboratory. Initially the Cryptanalytic Section had six subsections; by May of 1942 this grew to 10. Again, it is not yet possible to place Ferner organizationally during these moves. It is certain, however, that his continuing interest in the



IV. With Kullback, Ferner witnessed Friedman and Rowlett's patent application for a cryptographic invention.

Japanese diplomatic target had found a new objective. This time, the challenge was not a machine but a fiendishly difficult enciphered code.[29]

Japanese Transposition-Enciphered Code

On July 1, 1941—five years to the day since Ferner had come to SIS—the Japanese deployed a new enciphered codebook system. Like Purple, this system was used by Japanese diplomats, but, unlike Purple, this was not a machine cipher. Although SIS was familiar already with the initial underlying codebook, it soon changed. The real problem, however, was the superencipherment: a complex transposition system using matrices of variable widths, including blank cells in patterns that changed every 10 days. The diplomatic users of the system were grouped into four sets, each with its own daily

changing key.[30] Friedman himself initially described the system as "impregnable."[31]

A Japanese message announcing the update to all diplomatic users also alerted the SIS cryptanalysts to the impending release of the new system. As SIS began seeing the traffic operationally, they soon realized this encryption would be more of a challenge than its predecessors. Once again, Rowlett and Ferner tackled the problem, along with a third cryptanalyst, Albert Small, who had joined SIS as part of the cadre arriving in the fall of 1939.[32]

The cryptanalysts recognized that the new system might share similarities with a code active in another place and time: the ADFGVX system used by the Germans during World War I. Friedman had incorporated the older code into his training curriculum for his cryptanalytic new hires, who had documented their success against this system in an early SIS technical paper.[33]

The army was not the only American service organization closely following Japanese cryptographic developments. Since the 1920s, the US Navy had also been successfully decrypting Japanese systems. And so it came about that the first real breakthrough against the new enciphered code was not through pure cryptanalysis. Rather, the broader US Navy provided help in another form. In a covert operation, naval operatives had acquired photographs of both the code and the transposition matrices. Navy cryptanalysts recognized the potential for the army's cryptanalytic experts to further the effort and shared the new information with SIS. The purloined material enabled the army to decrypt current and some past messages—for the time being.

SIS leadership realized it was just a matter of time until the Japanese would change the system settings. Working against that day, SIS divided the cryptanalytic effort between current decryption and new research into the underlying cryptography, according to Rowlett's later recollections. Ferner and Small were responsible for the research effort.

Rowlett, who still oversaw SIS's cryptanalysis of Japanese diplomatic communications, detailed in his memoir *The Story of Magic* the

successful collaboration among Ferner, Small, and himself to fully understand and exploit this system. In addition, Rowlett also talked about it in several oral histories. The SIS cryptanalysts astounded their navy colleagues by demonstrating their ability to predict future keys, proving they had completely unwrapped the system's secrets.

Even this full understanding of the system did not eliminate the hard, and sometimes tedious, work of recovering new settings. Part of the process for recovering the transposition settings was a step called *anagramming*, whereby the columns of the transposition matrix were rearranged back into their original order. Anagramming was a mix of "eyeballing" and employing language-based statistics. It required seemingly endless repetitive and mind-numbing calculations.

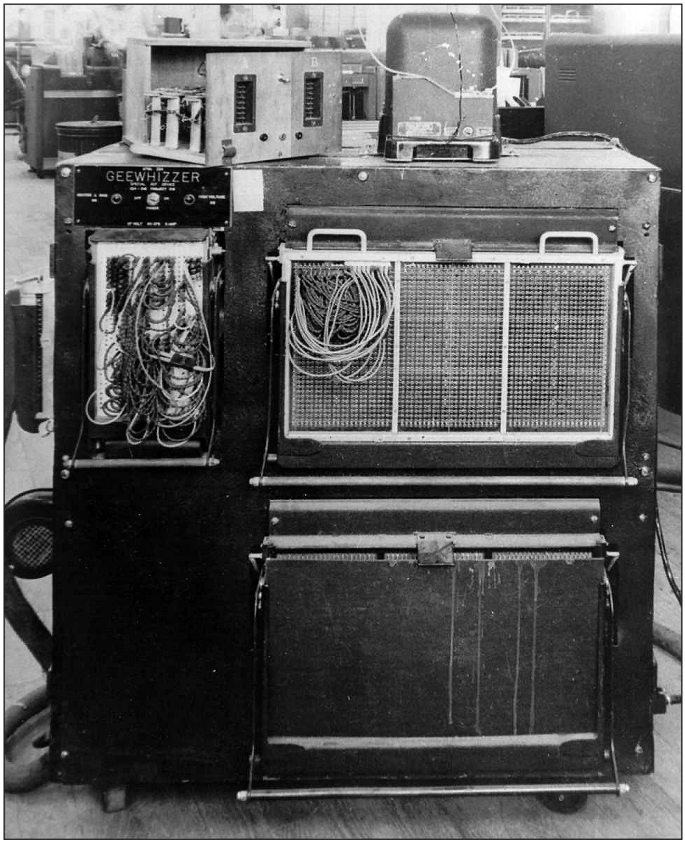
By 1941, SIS possessed machines to assist the cryptanalysts. By today's standards, the capabilities were basic indeed: sorting, ordering, and similar processes. Nevertheless, the cryptanalysts appreciated each advance that reduced the number of repetitive steps they would otherwise have to do by hand. Much of this equipment was developed for SIS by IBM, whose representatives were on site to make any required modifications to the machinery. SIS personnel were not authorized to alter the equipment.

Regardless, the IBM machines were indeed altered—and not by the IBM representatives. After Small envisioned an innovative way to perform the anagramming calculations, the trio eventually modified the IBM equipment to test his approach.[34] Small, Ferner, and Rowlett each brought individual and combined talents to bear on the refinements that produced a successful operational capability. Rowlett believed they had pushed the mechanical devices to new frontiers, approaching the brink (and perhaps crossing the line, in his opinion) of becoming true computing capabilities. The resulting device was formally known as the Electromechanagrammer, although it would always be the "GeeWhizzer"[35] to Rowlett, the recorder of these events.

SIS enjoyed success against this enciphered code used by Japanese diplomats worldwide for several years. The Japanese finally removed the system from service in July 1943.[36]

Ferner and Small brought complementary skills to this and the other projects they tackled together. Rowlett later summed up what made their teamwork so effective:

> Small … lived with the machines and he … was the new idea man to develop new programs using the machines and Ferner was just a doggone good cryptanalyst and mathematician and he could take Small's … brilliant glimpses and … he enhanced these into practical applications and he made them real. He'd sort out the … glint in Small's eye.[37]



V. Several generations of GeeWhizzers. The version devised by Rowlett, Ferner, and Small is probably the small box sitting on the left top of the larger version. *Collection of the Center for Cryptologic History*

Halfway through America's involvement in the war, Friedman wrote a set of award recommendations for personal cryptanalytic successes. Of this project, Friedman confirmed:

> For the development of the techniques and procedures in solution and for the mechanization of those techniques and procedures, major credit belongs to Major Rowlett and Messrs. Ferner and Small.[38]

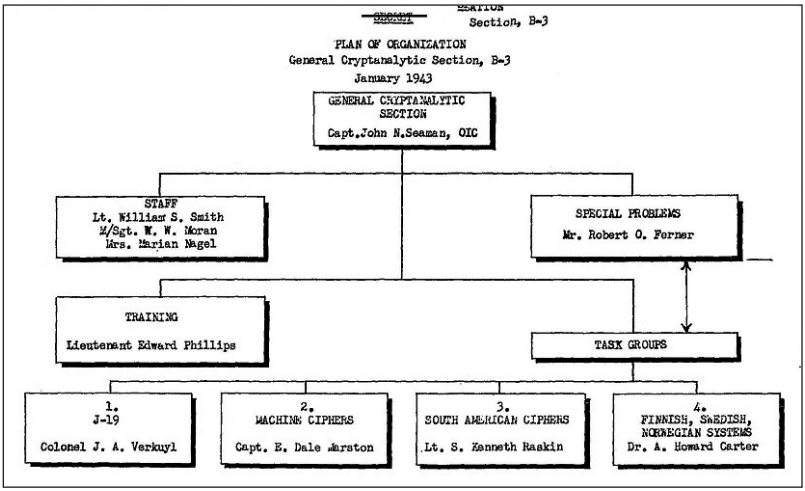
German Enigma

The SIS of mid-1942 would have been unrecognizable to somebody who had last seen it in the mid-1930s. First, the name had changed. After several short-lived variations, in July 1943 the organization became the Signal Security Agency or SSA.[39] The location had changed too. During the summer of 1942, the organization moved from the national mall in Washington, DC, to the campus of Arlington Hall, a former girls' school in Arlington, Virginia. And its size had certainly changed: SSA was now a workforce of not dozens or even hundreds but literally of thousands.

Once again the cryptanalytic workforce was reorganized. This time the Cryptanalytic Section was divided into two large subsections mirroring the major divisions of cryptography: codes and ciphers. Rowlett was initially in charge of B-3, an organization responsible for solving all ciphers, along with all code encipherments other than additive.[40]

By November 1942, Rowlett had become the head of Arlington Hall Station's (AHS) training program. Captain John Seaman became officer in charge of B-3.[41] Ferner was responsible for B-3 Special Problems, with a direct relationship to Task Groups.[42] It is likely that these Task Groups were similar to or perhaps the forerunners of the Technical Consultants Group that would be formalized later in 1943.

By 1942, the army cryptanalysts, like their navy counterparts, had the German Enigma machine in their sights. Initially a 1920s commercial development, the Enigma had been adopted and adapted by the German government and military. Its usage was pervasive during the war.



VI. B-3 organization chart, early 1943

American interest in Enigma was fueled by increasing levels of cryptanalytic exchange with the British, a partnership initiated in earnest by the groundbreaking Sinkov mission of 1941.[43] The exchange of liaison officers and technical experts furthered the relationship.

With a view to establishing their own effort against Enigma, US Army cryptologists developed plans to build an Enigma-decrypting machine. Army cryptanalytic leaders knew about the US Navy's rotor-based *bombe* technology but chose to base their own proposed system—also called a *bombe*—on relay switches.[44] The army had experience with cryptanalytic use of switches, having based both the Purple analogue[45] and the Electromechanagrammer on this technology.[46] The army engaged Bell Laboratories to build the system.[47]

Events progressed quickly. After a proof-of-concept demonstration in late 1942, the army commissioned a large section of the actual system to be delivered in two installments during 1943. Army leaders made overtures to the British to obtain crucial technical information, in exchange for offers to employ the new machine against the Enigma problem on behalf of the Allies.[48]

In parallel with efforts to build the machine, Arlington Hall Sta-

tion trained members of the cryptanalytic workforce to decrypt Enigma. In November 1942, a group of top AHS cryptanalysts, including Ferner, designed and taught a course on machine cipher systems. The training was something of a roll call for existing machine encryption devices, including, among others, several Enigma variations, the Japanese Red and Purple devices, and several commercial machines.[49]

In 1943, army representatives met with their navy counterparts for technical discussions about strategies for exploiting the commercial version of Enigma. Ferner, Seaman, Small, and Rosen were among the participants. These discussions were not without complications: the navy surprised the army with revelations of existing projects, and the army tried to preserve their right to keep to their terms for sharing information with the British.[50]

As it turned out, the army's preparations to combat Enigma did not materialize as foreseen, owing to one major deficit: the army was unable to establish its own regular feed of Enigma collection. As a result, the army did not participate in the division of effort to decrypt the massive volume of daily Enigma communications with the British. That would fall to the navy.

However, SSA's *bombe* prototype did play an important role in Enigma solutions of a specialized kind. By mid-July 1943, the first section of the AHS machine, known as Bombe 003 or just 003, was ready for operational use. British cryptologic leadership had agreed to send to Arlington Hall Station certain Enigma messages with anomalies that prevented them from passing through normal *bombe* processing. The army targeted the 003 against these messages requiring additional work. In effect, "the section at the Signal Security Agency actually functioned as a subsection of the British unit."[51]

One type of anomalous Enigma message resulted from Germany's introduction of a pluggable reflector. The initial solution devised by British and American cryptanalysts was an extremely time-intensive manual process called *scritching*. The intelligence was valuable, but the diversion of cryptanalysts' time was alarming, as "the efforts of the entire Cipher Section were devoted for several weeks to scritching."[52]

Once again, Ferner and Small contributed to the design of a time-saving cryptanalytic device. Their role was to define the problem that resulted in automating the scritching processes. This time they did not have to personally design—or surreptitiously install—the hardware implementation; Arlington Hall Station's Development Branch took care of that. The resulting machine was dubbed the Autoscritcher.[53] Dr. Howard H. Campaigne, a future chief of the National Security Agency's (NSA) Office of Research, later referred to the scritching devices as "quite close to being digital computers and were probably the most ingenious machines built during the war."[54]

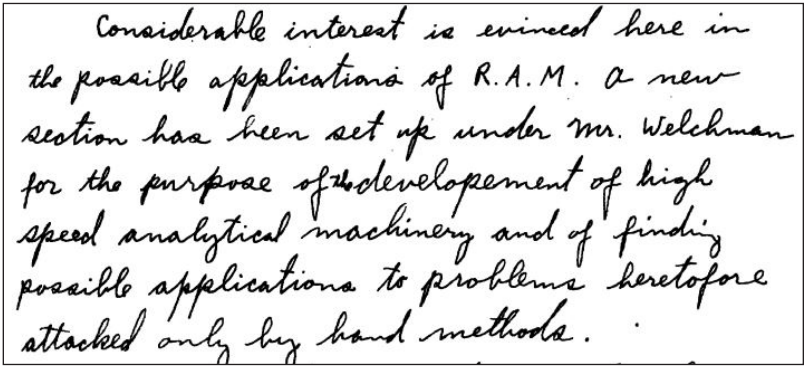
Travel to England

In mid-1943, Seaman and Ferner became the latest AHS experts to undertake an extended visit to Bletchley Park, the center of British cryptanalysis during the war. Ferner stayed for several months; Seaman remained longer, becoming the first SSA liaison assigned to Bletchley Park. During this trip, Ferner focused especially on machine ciphers, including Enigma.[55]

While at Bletchley Park, Seaman and Ferner learned of cutting-edge British cryptanalytic developments. The pair sent regular updates on their findings to Arlington Hall Station. The example below, in Ferner's own hand, describes British efforts to incorporate rapid analytical machinery (RAM) into Bletchley's cryptanalytic work.

In October 1943, while Seaman and Ferner were still in England, Friedman corresponded with one of his British counterparts, Colonel C. V. L. Lycett. At the end of this letter, he inquired whether Lycett had met several visiting Americans, including Seaman and Ferner. Friedman wrote, "Captain Seaman I think you would like very much as an all-round scholar. Ferner is very quiet but extremely able."[56]

Brigadier John Tiltman, a renowned diagnostic cryptanalyst who became Britain's chief cryptographer in 1942, later recalled Ferner as "a very good cryptanalyst" who "made a big contribution to all the diagnostic cryptanalysis."[57]


Considerable interest is evinced here in the possible applications of R.A.M. A new section has been set up under Mr. Welchman for the purpose of the development of high speed analytical machinery and of finding possible applications to problems heretofore attacked only by hand methods.

VII. Ferner's handwritten account of the latest British cryptanalytic developments.

Research: The Technical Consultants

The army's cryptanalytic organization changed yet again in 1943, both to improve internal collaboration and, especially, to reallocate resources in light of a major success against Japanese Army communications. The designators B-2 and B-3 remained (now usually notated as B-II and B-III), but the organizations' purposes had changed. B-II was devoted to the Japanese Army problem. B-III, now the General Cryptanalytic Branch, was responsible for nothing less than all other targets.[58] Although there were other reorganizations during the war, this two-fold division of cryptanalytic targets remained for the balance of the conflict. Rowlett returned from the training program to lead the B-III organization.[59]

Upon Ferner's return from England in November 1943,[60] he assumed leadership of a section within the B-III General Cryptanalytic Branch. This organization was called variously Research or Technical Consultants, and both titles were accurate.[61]

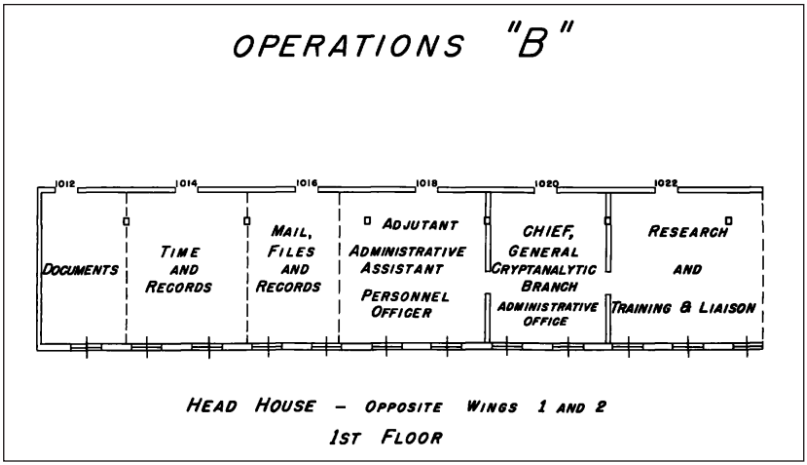
Ferner's small research staff comprised a handful of SSA's best cryptanalysts, characterized as "expert cryptanalysts for the most difficult problems encountered by the operating sections."[62] These

VIII. Working spaces, most likely in Arlington Hall Station, B-III; Robert Ferner is in the back row on the right. *Collection of the Center for Cryptologic History*

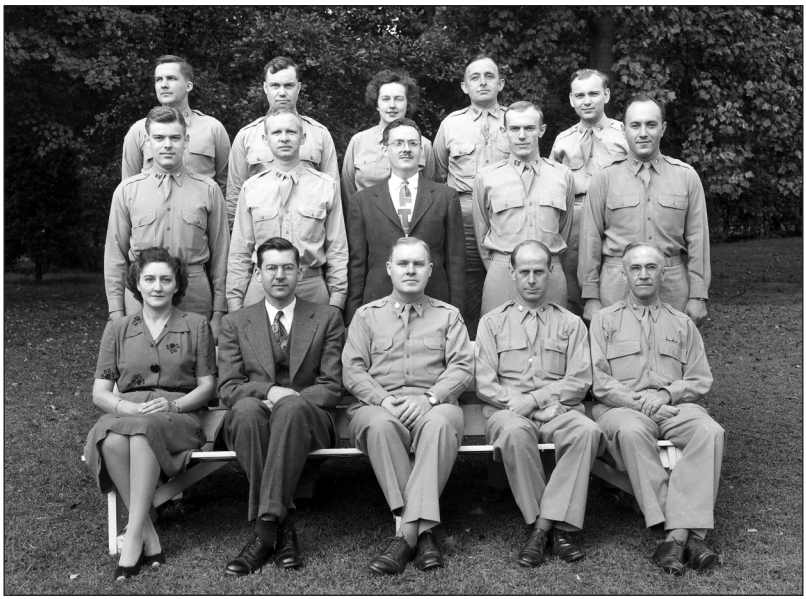
troubleshooters assisted SSA's operational elements with diagnosing and solving especially important and perplexing cryptanalytic problems. They also developed cryptanalytic techniques and new ways of using machines for cryptanalysis. Their remit included testing of US encryption systems to ensure these were secure.[63]

In fact, the Technical Consultants concept came about through a cryptographic, not a cryptanalytic, assignment, when four top-notch cryptanalysts had assisted in evaluating and strengthening an American cryptographic machine.[64] The concept had worked so well that the group's function became permanent, even though individual members rotated into and out of the small organization.

This was to be Ferner's final wartime move. A major reorganization in August 1944 left the overall B-III organization largely unchanged. Ferner appears to have found an organizational home



IX. Floor plan of B-III (SPSB-III) front office in August 1945. Note location of Research under Ferner directly next to the Chief (Rowlett).



X. B Branch Staff, Arlington Hall Station. *Left to right, back row*: unidentified, Maurice Collens, Dorothy MacCarthy, William Smith, Dale Marston. *Middle row:* Robert Packard, C. P. Collins, Albert Howard Carter III, William Hazlep, Maurice "Mo" Klein. *Front row:* Mary Louise Prather, Robert O. Ferner, Frank B. Rowlett, Franklin Bearce, William F. Edgerton. *Collection of the Center for Cryptologic History*

that reflected what he had been doing all along: applying his cryptanalytic expertise to a wide swath of Arlington Hall Station's technical challenges. In addition to the major accomplishments mentioned above, Ferner participated in successful cryptanalytic team efforts yielding solutions of codes and ciphers, machines, and hand systems across a broad range of wartime targets, as well as helping to improve America's own cryptographic protection.[65] In short, he was a consummate technical expert with knowledge of the entire target set and whose influence extended across the organization.[66]

German Diplomatic[67]

The Technical Consultants, under Ferner's leadership, demonstrated the effectiveness of their technical leadership against another German target: an encryption system used by German diplomats since the mid-1920s. Because this system used keypads with disposable pages designed to be used only once (one-time pads), AHS cryptanalysts for many years had considered it to be secure. Even after the FBI captured actual one-time pads in 1940, the system still remained unsolved. The project was set aside for more-promising cryptanalytic priorities.[68]

In 1943, the situation changed. The cryptanalysts of B-III's German Diplomatic Section examined recent intercepts and realized the key might not be secure. SSA's postwar history noted, "This discovery was like a shot in the arm to the personnel of the German Diplomatic Section."[69]

Soon this project had gone from a figurative place on the back shelf to a very tangible position of cryptanalytic priority. Cryptanalysts from other targets converged to reinforce the resources of the German Diplomatic Section. All of the Technical Consultants were among those additions.

Ferner had previously worked on German diplomatic communications in the late 1930s.[70] Now he returned to this target as a leader of the group, which in turn headed the technical effort to finally break through the system's defenses: "[c]ryptanalytic activities there

were directed by Mr. Robert Ferner, Captain Walter Fried, and other members of the Research Group."[71]

It took a year for the resource-intensive combined cryptanalytic effort to yield a successfully decrypted message in January 1945.[72] Although late in the war, "[T]heir [the Research Section's] assistance made it possible to supply a great amount of useful intelligence before V-E Day as well as afterwards."[73] This "useful intelligence"—obtained with the help of IBM machinery—was of "utmost importance in the spheres of politics, scientific advance, technical data, and production" of war materiel.[74]

As with Purple, the story of the solution of this German diplomatic system is familiar within cryptologic history circles. The initial cryptanalytic detective work by members of the German Diplomatic Section, including Juanita Moody and Thomas Waggoner, has been the focus of the story; without their efforts, there might have been no story to tell. But the full account should acknowledge the contributions of experts in the Machine Cipher Section and the technical leadership of the Research Section, headed by Ferner, in ultimately defeating the hard encryption used to secure the German diplomats' communications. This project epitomizes the role of the Technical Consultants in coming alongside operational offices to overcome some of Arlington Hall Station's hardest cryptanalytic challenges.

Coordination Across Organizations

As a technical expert now in a formal leadership role, Ferner supported SSA senior line managers in cross-organizational efforts, both within Arlington Hall Station and with external partners. In September 1944, Mark Rhoads, assistant director of Communications Research, proposed forming a high-level internal committee to ensure good cross-communication among major agency elements. Participants would represent both the intelligence-producing mission and the defense of American communications.

This committee's mandate would be to address the large-scale

growth of the army's cryptologic service. In the memo proposing the committee, Rhoads wrote, "When the organization was small, the two functions, cryptography and cryptanalysis, were concentrated in the same people, but mushroom growth has segregated them into two entities in direct proportion to the growth."[75] Several examples of the benefits of cross-organizational integration cited contributions of the B Branch cryptanalytic experts in studying American cryptographic machines.[76]

The proposed committee was to be chaired by Friedman. Most members would be appointed by virtue of their current positions as senior leaders within the participating organizations. But when it came to including technical experts to serve as needed, Rhoads identified these individuals on a by-name basis, including Ferner, Small, and then-Sergeant Walter Jacobs from the Technical Consultants.[77]

Outside of Arlington Hall Station, during 1944, army and navy cryptologists put formal structures into place to help cross-service coordination. The Army-Navy COMINT Coordinating Committee (ANCICC) first met on April 18, 1944; senior cryptologic leaders from each service attended the meeting.[78]

Later that year, a new ANCICC subcommittee was formed: the Army-Navy Sub-Committee on Cryptanalysis, which first convened on October 20, 1944. Principals for the army were Kullback and Rowlett. Ferner and cryptanalyst Frank Lewis also attended, likely as technical experts. The group's focus was to be "cryptanalytic theory, procedure, techniques, and research"—in other words, a perfect fit with Ferner's expertise and his role as head of the Technical Consultants Group.[79]

After the War

As the war ended in stages during 1945, the Signal Security Agency began preparing for the postwar era. On September 6, 1945, four days after Japan formally surrendered, the army's cryptologic agency again changed its name, this time to the Army Security Agency (ASA). The changes were not just a matter of nomencla-

ture: the organization now fell under a different reporting hierarchy within the army. Most importantly, there were large-scale personnel changes, as many left cryptologic service to return to their prewar livelihoods.[80]

ASA formalized its postwar reorganization in November 1945. The major mission elements were to be Operations (WDGSS-90), home of the communications intelligence (COMINT) or signal intelligence mission; Security, responsible for cryptography (WDGSS-80); and, for the first time, an agency-wide Research and Development (R&D) organization (WDGSS-70). This centralized R&D effort supported the cryptographic security and intelligence missions.[81]

At the war's end, Ferner initially remained in charge of the Research Group of Technical Consultants. In December 1945, at the creation of the ASA under the new organizational plan, Ferner moved to the newly created R&D Division.[82]

Ferner's organizational home within R&D would have been familiar to him. ASA R&D had adopted the Technical Consultants model, setting up a Technical Consultants Staff (SS-71-C) within the overall Technical Staff (WDGSS-71) of the R&D Division. It is unclear whether or not Ferner had a designated leadership role in this organization of some nine consultants with various specialties. With cryptanalyst Lewis, Ferner is listed as a cryptologic consultant. Presumably, Ferner may have been moved to help R&D's implementation of this concept start off on a firm footing.[83]

Although Ferner left the Operations organization, the original Research Group that he had led remained. Known once again as the Technical Consultants Group, it continued in Operations under the designator WDGAS-93-X. Small was the group's first leader within the ASA construct.[84]

In 1946, army cryptologic leadership established a rotational program to diversify the professional experience of high-ranking managerial and technical personnel.[85] In one of the earliest implementations of the scheme, Ferner moved from R&D to Operations;

Small moved from Operations to [cryptographic] Security; and J. H. Douglas, another technical leader, moved from [cryptographic] Security to R&D.[86]

Ferner's move to Operations took him back to a familiar but expanded role. He became chief of a new Operations Technical Staff, which included the Operations Technical Consultants as well as several one-off functions. Perhaps influenced by the R&D model, Operations had established a broader Technical Staff during fiscal year (FY) 1947, which ended June 30, 1947.[87] The Operations Division designator at this time was WDGAS-90, later changing to CSGAS-90. Within that organization, the Technical Staff was WDGAS-96 or simply AS-96.[88]

On paper, at least, this move placed Ferner in his highest level of organizational leadership yet. The Technical Staff was one of six organizations reporting directly to Rowlett, now chief of the Operations Division. During FY 1947, the Technical Staff had from 23 to 32 members, of whom around 10 to 14 were "skilled cryptanalysts." Since the other disparate functions within the staff still reported directly to Rowlett, most of Ferner's attention may have gone toward leading the Technical Consultants within the larger Technical Staff.[89]

All records discovered to date indicate Ferner remained in this role for the duration of his cryptologic career.

Leaving Cryptologic Service

And then, in 1948, the year in which he turned 33, Ferner decided to leave army cryptanalysis. A letter of reference written by Friedman to the University of Colorado Boulder several years later explained a major reason for Ferner's departure, along with SIS/SSA/ASA's reaction:

> I am happy to reply to your letter of 19 January 1950 in regard to Mr. Robert Orestes Ferner. I have been associated with Mr. Ferner for about twelve years. At the end of this period he had become one of the most outstanding technical workers of the Army Security Agency, which sustained a

> great loss when he had to leave this climate for the sake of his health.
>
> With all of his ability, he is a modest and retiring man, even-tempered, and gets along exceeding well with his co-workers. Everyone at the Army Security Agency had the highest regard for him, and professional jealousy of him was unknown.

Friedman continued:

> He is a man of the highest character, of unquestioned loyalty, and anyone employing him is to be envied.

From William Friedman, this is high praise indeed.[90]

On June 10, 1950, Ferner received a bachelor of science degree in electrical engineering, with honors, from the University of Colorado Boulder.[91] He was a member of numerous professional organizations: the Tau Beta Pi engineering honor fraternity; Eta Kappa Nu, a national electrical engineering honor society; Sigma Tau, a national honorary engineering fraternity; and the American Institute of Electrical Engineers–Institute of Radio Engineers.[92]

Even as he graduated, Ferner had a position awaiting him at Sandia Corporation in Albuquerque, New Mexico. He had been granted a Q clearance in May 1950.[93] The move took place in short order, with Sandia's *Lab News* welcoming him aboard on July 7, 1950. At Sandia, he was hired by the Instruments and Measurements Group in the Weapons Effects Department, Model Studies Division.[94]

By mid-1954, Ferner again heard the westward call. In August and September, he advertised his house for sale in the Sandia *Lab News*.[95] As recalled by his daughter, this was when the family moved to the San Diego area. Ferner subsequently worked for Convair (later part of General Dynamics) and then in naval research. California—with its asthma-friendly weather—was to be his home for the rest of his life.

A Brief Return to Washington

In 1949, the cryptologic elements of the US Army, US Navy, and the new US Air Force had combined to form a new joint agency: the Armed Forces Security Agency (AFSA). Early on, AFSA leaders assembled a high-powered technical advisory group known as the Special Cryptologic Advisory Group (SCAG).[96] SCAG members came from academia and industry, and were recognized as foremost authorities in the highly technical disciplines needed to support AFSA's work. Pioneering information theorist Dr. Claude Shannon was representative of the SCAG's level of expertise.

At the third meeting of the SCAG, Ferner's name appeared as a potential member.[97] It is not clear whether Ferner ever attended a SCAG event. It is certain, however, that he did return to work with his former colleagues at least once. Dale Marston, another veteran of the B-III General Cryptanalytic Branch, had led units responsible for cryptanalysis of machine ciphers and also for operation of Arlington Hall Station's cryptanalytic machines. In 1952, Marston submitted to AFSA leaders an urgent plea to obtain Ferner's help in analyzing a high-profile problem.[98]

Marston's language is unusually strong for a government memorandum, especially one working its way up the management chain to ultimately reach an agency head:

> Mr. Ferner is considered by the undersigned to be the outstanding cryptanalyst of the past decade. This opinion is shared by all who have worked with him.

Marston continues later:

> This is more than a request. If we, as a working party, were in the position to demand, we would do so. We feel so strongly that Mr. Ferner is the one person most apt to help us along to success on this problem that we would go to any extreme to get his services.[99]

Endeavoring to address every possible impediment to the visit, Mar-

ston even suggests the time of year with the least likelihood of seasonal allergies to affect Ferner's asthma.

It is not entirely clear whether Ferner came as part of a SCAG delegation or instead came individually. But there is no doubt as to AFSA's opinion of the visit's success. Major General Ralph Canine, AFSA director, personally wrote to thank the president of Sandia Corporation for making Ferner available to work with AFSA for two weeks.[100] He also suggested that a similar future visit would be welcome. The record is for now silent as to whether Ferner ever returned, or whether the mid-1952 visit was the last time he worked with his cryptologic colleagues.

The Ferner Family

And what of the Ferner family? In Washington, DC, Robert and Erma's first child was born: a daughter, Jean. Their son Thomas was born in Albuquerque. Sadly, Thomas was born with serious heart problems, which ultimately took his life in 1960 when he was eight years old.[101]

The effect of Thomas's death upon the Ferner family was profound. Erma, struggling to cope with his loss, began working outside the home. Beginning as a physical therapy volunteer, she discovered that she was gifted in this area. She quickly became a consultant in that field, a career that she enjoyed well into her mid-seventies.

For his part, Robert became more involved in supporting their daughter throughout her high school years (not surprisingly, to include helping her with her less-than-favorite subjects of mathematics and science). Decades later, Jean viewed this as the time when she really got to know her father.

Robert semi-retired at a relatively young age, partially thanks to yet another successful application of his analytical thinking—this time to his own finances in the stock market. His daughter recalled that he took more classes and taught for a while at a junior college. Finally, he retired for good. He remained a thoughtful and contem-

XI. Robert, Erma, Jean, and Thomas Ferner, New Mexico, around 1953. *Courtesy of Mrs. Jean Ferner*

plative man, and thankfully in his later years had some relief from the asthma that had plagued him throughout his life.

On August 8, 1982, Robert Ferner died from a sudden heart attack. He was sixty-eight years old.[102] While the family knew of his intellect, they did not know the extent of his professional contribu-

tions. To them, however, he excelled in another way—one which had nothing to do with cryptanalysis. To his daughter, Jean, he was simply "the kindest person I ever knew."[103]

Legacy

Today, the earliest members of the Signal Intelligence Service (SIS) are well known within the cryptologic history community. William Friedman and the first three junior cryptanalysts all played foundational roles in the history of US Army cryptology. It is important to acknowledge the contributions of these early leaders who provided continuity and expertise in the years after World War II and through NSA's first decade.

Similarly, there has been much emphasis in recent years on the thousands who served the nation in cryptology during the Second World War. In particular, the work of the women who came from around the country to Washington to serve has gained wide public recognition through books such as Liza Mundy's *Code Girls: The Untold Story of the American Women Code Breakers of World War II*. While it is impossible to recognize each individual, by setting forth the life and career stories of selected women, Mundy has paid tribute to all of the women who made possible America's cryptologic support to the war.

And what of those who arrived in the in-between period—after the first hires of 1930 but before the major expansion of the war? Here too, some of these individuals have been highlighted and recognized. The Cryptologic Hall of Honor includes Samuel Snyder (hired in 1936) and Genevieve Grotjan (hired in 1939), for example.

Certainly for the war years, and even for the earlier, quieter atmosphere of SIS in the 1930s, it is unlikely that each cryptologist will ever be honored personally. Upon learning of new stories, the cryptologic historian can only marvel at the level of expertise, dedication, and accomplishment that characterized so many.

And yet, when encountering the story of Robert Orestes Ferner, one cannot help but recognize that this is a cryptanalyst who is in a

different league. Although acknowledgments for the work of peers abound in oral histories of many World War II cryptologists, the consistent superlatives used to describe Ferner stand out.

Two things seem to have argued against the preservation of Ferner's cryptologic legacy: possibly, his quiet personality and lack of self-promotion and, certainly, the fact that he left cryptologic service in 1948. Frank Rowlett, who worked with Ferner for decades, described Ferner's normally staid nature by highlighting the exceptions. At Grotjan's discovery of the final piece of the Purple cryptanalytic puzzle, Rowlett colorfully wrote that "Ferner, who was usually very quiet and not very much inclined to show enthusiasm, clapped his hands, shouting 'Hurrah! Hurrah!'" And again, at a crucial success in developing machine techniques to combat the transposition-enciphered Japanese code, Rowlett recalled, "Ferner and Small came charging into my office carrying a machine display. Ferner usually did not display much excitement, but this time he was as jubilant as Small."[104] Recall that Friedman, in his recommendation letter to the University of Colorado Boulder, also had referred to Ferner as "a modest and retiring man"[105] and in his letter to Colonel Lycett as "very quiet."[106]

Once again, however, Jean Ferner rounds out the picture with details not included in official military histories. Apparently the exceptionally quiet Robert was known—in his family, at least—for his sense of humor, which "inclined toward the irreverent."[107]

As to Ferner's expertise, there are other contemporary voices to add to those already mentioned. World War II cryptologist Ed Fishel, in a short account of his own entry into the US Army, mentioned being surprised to cross paths with "two fellow townsmen and college mates." One of them was "Bob Ferner, remembered as an Einstein among cryppies."[108]

World War II cryptanalyst George Hurley also later reminisced:

> Bob Ferner who I would say was the leading cryptanalyst that the United States has ever had. … take your Rowletts and your Sinkovs and your Kullbacks, and your Ravens and your Frank Lewises and they're all marvelous and there

XII. Presentation of Commendations for Exceptional Civilian Service at Arlington Hall Station, May 1946. Left to right, front row: Mark Rhoads, Genevieve M. Feinstein, Brigadier General P. E. Peabody, USA, Frank W. Lewis, and Colonel Hayes, USA; second row: Thomas A. Waggoner, William H. Erskine, Paul V. Gerhard, Albert W. Small, Robert O. Ferner, and Martin Joos. *Collection of the Center for Cryptologic History*

> may be a couple of obscure people like Genevieve Grotjan Feinstein or Al Small and so forth. All brilliant, but give me Ferner.[109]

Arthur Levenson, another World War II cryptanalyst and later senior cryptanalytic leader now included in the Cryptologic Hall of Honor, recounted in his 1980 oral history his work on the 1941 Japanese transposition-enciphered code discussed earlier, and how the length of the message determined the difficulty of the solution.

XIII. At the Commendations for Exceptional Civilian Service ceremony, May 1946, Robert and Erma Ferner (second and third from right). *Collection of the Center for Cryptologic History*

> And Bob Ferner was the genius on that, as he was on many other problems. A terrific cryptanalyst. And they had a little table, that if the message was a certain length, anybody could do it. If it was a little shorter, then you had to be a little better or more clever. And then, at a certain length, it said, "Give to Ferner." Oh yes. He was the only one that could solve them if they were really short. Only Ferner.[110]

In 1982, NSA's KRYPTOS Society announced an inaugural list of 14 Distinguished Members, chosen from more than 100 names under consideration. This recognition was "based solely on cryptanalytic skills and achievements." All cryptanalysts "retired since 1935 from the 'official cryptanalytic community' of any of the Five-Eyes

partners" were eligible. The 14 cryptanalysts—all men—on this initial list included Friedman, Kullback, Sinkov, and their equally well-recognized counterparts from the US Navy. Others, now less remembered, were also among these select cryptanalytic greats who were recognized by their own community for technical prowess. Among these was Robert Ferner, one of the original 14 KRYPTOS Society Distinguished Members.[111]

Now, nearly 75 years after Robert Ferner left cryptologic service, it is time to restore him to his rightful place in American cryptologic history. With this renewed understanding of his contributions, it is, using Arthur Levenson's words, again time to "give to Ferner" the recognition due this man who was one of America's most outstanding early cryptanalysts and perhaps well beyond—truly, a cryptanalyst's cryptanalyst.

Epilogue

Robert Orestes Ferner became a member of the NSA Cryptologic Hall of Honor in 2022. The story of this American master cryptanalyst is untold no longer.

Glossary

These definitions were used by William Friedman, with some slight edits for length. See William Friedman, "Six Lectures on Cryptology," *The Friedman Legacy: A Tribute to William and Elizebeth Friedman*, third printing (Ft. Meade, MD: Center for Cryptologic History, 2006), 6-8. Terms are listed in the order they appear in the Friedman book.

Cryptology: The doctrine, theory, or branch of knowledge that treats of hidden, disguised, or secret communications. It has two main branches: cryptography and cryptanalysis.

Cryptography: The science of preparing secret communications.

Cryptanalysis: The science of solving secret communications.

Encrypt: To convert or transform a plaintext message into a cryptogram—a message in secret language—by following certain rules, steps, or processes. To **decrypt** is to reconvert or to transform a cryptogram into the original equivalent plaintext message by a direct reversal of the encrypting process. Encrypting and decrypting are accomplished by use of codes and ciphers.

Ciphers: In ciphers, cryptograms are produced by applying the cryptographic treatment to individual *letters* of the plaintext messages. There are two types of ciphers: transposition and substitution.

Transposition: The letters of the plain text retain their original identities and merely undergo some change in the relative positions.

Substitution: The letters of the plain text retain their original relative positions but are replaced by other letters or symbols.

Codes: In codes, cryptograms are produced by applying the cryptographic treatment generally to entire *words, phrases, and sentences* of the plaintext messages.

Notes

1. Arthur J. Levenson, interview by Robert D. Farley, NSA-OH-40-80 (November 25, 1980), 12, accessed April 7, 2022, https://media.defense.gov/2021/Jul/15/2002763471/-1/-1/0/NSA-OH-40-08-LEVENSON.PDF.

2. Edward Barnett, memorandum for the Executive Officer, January 30, 1939, 4-7, Document Reference ID A61782, accessed January 7, 2022, https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/correspondence/FOLDER_001/41758469079760.pdf.

3. Roy Y. Ferner and O. A. Ferner, *Ferner – Farner – Furner Families* (Alliance, OH: private publication, 1941), 2, 3, 10, 31. Copy provided by Dave Tyler. Orestes Asa Ferner, Robert Ferner's father, completed this detailed genealogical study begun by his relative Roy Ferner. The family branch with the "Ferner" spelling was

presumed to be Swiss. Robert's ancestral tree on the Ferner side dated back to one Daniel Ferner, who arrived in America around 1750 and later served in the Continental Army. Another Ferner ancestor was named George Washington, who was born in 1842 and served in the Union Army. A page, which documented family members who had been or were currently in military service, did not include Robert's silent civilian service in the War Department.

4. *Alliance High School Chronicle*, June 1927, 55, accessed December 14, 2021, https://www.alliancememory.org/digital/collection/p16335coll4/id/24178/rec/1. Collection of Rodman Public Library and Alliance Historical Society.

5. *The Alliance Review and Leader*, December 29, 1924, 9, accessed December 14, 2021, http://www.ohiohistory.org/digital/collection/p16007coll36/id/43544/rec/8. Collection of Rodman Public Library and Alliance Historical Society.

6. Jean Ferner, telephone interviews (August 27 and 30, 2021) and follow-up emails, Center for Cryptologic History (CCH) Historian Projects File, Ferner-McIntire. Unless otherwise indicated, information about Robert's life before and after his cryptologic career was provided by Mrs. Ferner, Robert and Erma's daughter.

7. *Alliance High School Chronicle*, June 1931, 18, accessed December 14, 2021, https://www.alliancememory.org/digitalcollection/p16335col4/id/2751/rec/3. Collection of Rodman Public Library and Alliance Historical Society.

8. 1935 *Unonian*, 29, 90-91, 94, University of Mount Union Library collection.

9. Jean Ferner, phone interviews; "Couple Wed in Mt. Union Garden Early Wednesday," *The Alliance Review*, June 16, 1937. Article received August 24, 2021, from Reference Department, Rodman Library, Alliance, Ohio.

10. Barnett, memorandum for the Executive Officer, 7.

11. This training is documented in the oral histories of Frank Rowlett (NSA-OH-1976-1-10), Solomon Kullback (NSA-OH-17-82), and Abraham Sinkov (NSA-OH-02-79). All are available at https://www.nsa.gov/Helpful-Links/NSA-FOIA/

Declassification-Transparency-Initiatives/Historical-Releases/Oral-History-interviews/.

12. John B. Hurt, "The Japanese Problem in the Signal Intelligence Service (Later Signal Security Agency) 1930-1945," November 20, 1956, 4, 7, Document Reference ID A58132, accessed October 8, 2021, https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/reports-research/FOLDER_212/41760749079991.pdf.

13. *History of the Signal Security Agency, Volume 1, Organization 1939-1945*, April 13, 1948, 11-13, Document Reference ID 4222114, accessed April 1, 2022, https://media.defense.gov/2021/Jun/29/2002751406/-1/-1/0/HISTORY_OF_THE_SIGNAL_SECURITY_AGENCY_VOL_ISRH364.PDF. Date of the cited chart is March 2, 1937.

14. *History of the Signal Security Agency, Volume 2, The General Cryptanalytic Problem*, January 15, 1947, 2-3, Document Reference ID 6554247, accessed January 9, 2022, https://media.defense.gov/2021/Jun/29/2002751477/-1/-1/0/HISTORY_VOL_2.PDF.

15. Major W. S. Rumbough, "Personnel Now Available for Signal Intelligence Work and Degree of Training of Each Specialist," January 28, 1938, 1, NSA Archives, Accession 48421, Document Reference ID A2332199.

16. *History of the Signal Security Agency, Volume 5, Traffic Analysis and Control*, Part Two, 1946, 3, NSA Archives, Accession 2369, Document Reference ID A76078.

17. Not to be confused with the Japanese enciphered code known by American cryptanalysts as the Red Code.

18. *History of the Signal Security Agency, Volume 2*, 26, 29.

19. *History of the Signal Security Agency, Volume 2*, 29 (footnote 9).

20. *History of the Signal Security Agency, Volume 2*, 30.

21. Friedman, "Preliminary Historical Report on the Solution of the 'B' Machine," October 14, 1940, 1, 6-7, Document Reference ID A67848, accessed January 9, 2022, https://www.nsa.gov/

Portals/75/documents/news-features/declassified-documents/friedman-documents/reports-research/FOLDER_077/41709249074857.pdf.

22. Friedman, "Preliminary Historical Report," 8. This document shows the success against Purple was a collaborative effort requiring the talents and diverse skills of an entire team. Although early histories such as Ronald Clark's *The Man Who Broke Purple* (Boston: Little, Brown and Company, 1977) largely credited Friedman with the success, currently available sources and research now show there was no single "man (or woman) who broke Purple."

23. When David Kahn asked Genevieve Grotjan Feinstein why she had been the one to make the Purple breakthrough, she recalled (as manually transcribed by Kahn) that "Ferner might have done it but he was working on something else. [Albert] Small and Ferner and [Leo] Rosen were also working on ways to mechanize it." See Feinstein, interview by Kahn, June 25, 1995, 5, National Cryptologic Museum Library collection.

24. Friedman, "Recommendations for Legion of Merit and Medal for Merit Awards," September 27, 1943, 3, Document Reference ID A4148494, accessed October 8, 2021, https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/correspondence/FOLDER_529/41771309081039.pdf.

25. Somewhat ironically, Japanese diplomats very likely knew far more about the military activities of their German allies than of their own nation's military activities and plans. See Frederick D. Parker, *Pearl Harbor Revisited: U.S. Navy Communications Intelligence 1924-1941,* 3rd edition (Ft. Meade, MD: Center for Cryptologic History, 2013) for more details concerning the limited access to Japanese military information available through Purple.

26. See Carl Boyd, *Hitler's Japanese Confidant: General Oshima Hiroshi and MAGIC Intelligence, 1941-1945* (Lawrence: University Press of Kansas, 1993).

27. *History of the Signal Security Agency, Volume 1*, 39.

28. Friedman and Rowlett, set of patent papers, May 16, 1942, 69, Document Reference ID A71739, accessed April 7, 2022, https://

www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/patent-equipment/FOLDER_097/41711449075075.pdf. The device, known by the army as "M-228" or "SIGCUM," went briefly into production in the 1940s but was withdrawn for security concerns. See Stephen J. Kelley, 'The SIGCUM Story: Cryptographic Failure, Cryptologic Success," *Cryptologia* 21, no. 4 (1997): 289-316.

29. *History of the Signal Security Agency, Volume 2*, 3-5.

30. *History of the Signal Security Agency, Volume 2*, 52-53.

31. Friedman, "Recommendations for Legion of Merit and Medal for Merit Awards," 1.

32. Wilma Davis, interview by Robert D. Farley, NSA-OH-25-82, 5, accessed April 6, 2022, https://media.defense.gov/2021/Jul/15/2002763435/-1/-1/0/NSA-OH-25-82-DAVIS.PDF. Based on my research, Grotjan came to SIS in 1939; compared with this reference, I established 1939 as the date when Al Small arrived.

33. Rowlett, *The Story of Magic: Memoirs of an American Cryptologic Pioneer* (Laguna Hills, CA: Aegean Park Press, 1998), 174-176. See also Signal Intelligence Section, *General Solution for the ADFGVX Cipher System* (Washington, DC: Government Printing Office, 1934), Document Reference ID A68203, accessed November 12, 2021, https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/publications/FOLDER_269/41784769082379.pdf.

34. According to Rowlett, Small's brilliant breakthrough was to perform the calculations using logarithms, which allowed multiplications to be handled as additions. Later documentation describes the device as an adaptation of an IBM tabulator designed to "compare a sequence of cipher text with other sequences and show at what position digraphs most likely to occur could be produced." *History of the Signal Security Agency, Volume 2*, 53.

35. *History of the Signal Security Agency, Volume 2*, 53-54. See also Rowlett, interview by Vincent Wilson, Coates, Henry Schorreck, and David Goodman, NSA-OH-1976-1-10 (August 31, 1976), 274-285, accessed April 6, 2022, https://media.defense.gov/2021/Oct/05/2002868610/-1/-1/0/NSA-OH-1976-1-10-

ROWLETT.PDF. Rowlett discusses the navy covert action in his other set of interviews (NSA-OH-1974-1-12), 27. Exact details on what the navy obtained are from Rowlett's book, *The Story of Magic.*

36. *History of the Signal Security Agency, Volume 2*, 53.

37. Rowlett, interview (August 31, 1976), 276.

38. Friedman, "Recommendations for Legion of Merit and Medal for Merit Awards," 3.

39. See "Records of the National Security Agency/Central Security Service," https://www.archives.gov/research/guide-fed-records/groups/457.html, for a detailed chronology of the Agency's names and organizational location. Accessed February 25, 2022.

40. *History of the Signal Security Agency, Volume 2*, 7-8.

41. *History of the Signal Security Agency, Volume 2*, "Evolution of the General Cryptanalytic Branch," unnumbered page 445.

42. *History of the Signal Security Agency, Volume 2*, "Plan of Organization General Cryptanalytic Section, B-3, January 1943," unnumbered page 448.

43. For an introduction to the Sinkov mission, see David Sherman, *The First Americans*: *The 1941 US Codebreaking Mission to Bletchley Park* (Ft. Meade, MD: Center for Cryptologic History, 2016).

44. *History of the Signal Security Agency, Volume 2*, 257.

45. *History of the Signal Security Agency, Volume 2*, 46.

46. Rowlett, *Magic,* 220.

47. *History of the Signal Security Agency, Volume 2*, 257-258.

48. *History of the Signal Security Agency, Volume 2*, 259-261.

49. *History of the Signal Security Agency, Volume 2*, 235.

50. Captain E. E. Stone, USN, "Suggested Solution of Commercial Enigma," May 15, 1943; and Friedman, Director of Communications Research, untitled memorandum to Commanding Officer, Arlington Hall Station, July 3, 1943, Document Refer-

ence ID A4146658; both accessed February 4, 2022, at https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/patent-equipment/FOLDER_521/41790359082935.pdf.

51. *History of the Signal Security Agency, Volume 2*, 262-263.

52. *History of the Signal Security Agency, Volume 2*, 242-243, 268-269.

53. *History of the Signal Security Agency, Volume 2*, 235-236, 269.

54. Leroy H. Wheatley, "Description of Analytic Machinery," May 1953, 4, Document Reference ID A60928, accessed April 8, 2022, https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/reports-research/FOLDER_107/41743419078275.pdf.

55. *History of the Signal Security Agency, Volume 2*, 20-21.

56. Friedman, letter to Colonel C. V. L. Lycett, October 9, 1943, Document Reference ID A70004, accessed October 8, 2021, https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/correspondence/FOLDER_365/41733709077294.pdf.

57. Brigadier John Tiltman, interview by Henry Schorreck, Robert Louis Benson, and David Goodman, NSA OH-04-78 (November-December 1978), 17, accessed May 18, 2022, https://media.defense.gov/2021/Jul/15/2002763520/-1/-1/0/NSA-OH-04-78-TILTMAN.PDF.

58. *History of the Signal Security Agency, Volume 2*, 8-9.

59. *History of the Signal Security Agency, Volume 2*, "Plan of Organization General Cryptanalytic Branch, B-III," September 1943, unnumbered page 452.

60. *History of the Signal Security Agency, Volume 2*, 21.

61. While the organization is usually called Research in the B-III organization charts, the November 25, 1943, B-III chart labels it simply "Technical Consultants." See *History of the Signal Security Agency, Volume 2*, unnumbered pages 452, 454, and 456.

62. *History of the Signal Security Agency, Volume 2*, 280-285.

63. *History of the Signal Security Agency, Volume 2*, 280-282.

64. *History of the Signal Security Agency, Volume 2*, 280.

65. Rowlett, interviews by Vincent Wilson, Coates, Henry Schorreck, and David Goodman, NSA-OH-01-74 to NSA-OH-12-74 (June 26, 1974), 120, accessed April 7, 2022, https://media.defense.gov/2021/Dec/03/2002902964/-1/-1/0/OH_01-74_TO_12-74_ROWLETT_MDR_80299.PDF.

66. For more examples, see *History of the Signal Security Agency, Volume 2*, 140, and Friedman, "Recommendations for Legion of Merit and Medal for Merit Awards," 2, 4.

67. The official postwar history discusses the German diplomatic problem in three accounts: the German Diplomatic Section (83-90); the Machine Cipher Section (244); and the Research Section (280-282). Comparing these three accounts yields a more robust picture of the roles of Robert Ferner and the Research Section than any one of the individual accounts. See Juanita Moody's oral history transcript (OH-1994-32) for a first-hand account of the excitement accompanying the initial discoveries that the system might not be secure.

68. *History of the Signal Security Agency, Volume 2*, 83.

69. *History of the Signal Security Agency, Volume 2*, 88-89.

70. *History of the Signal Security Agency, Volume 2*, 89.

71. *History of the Signal Security Agency, Volume 2*, 244.

72. *History of the Signal Security Agency, Volume 2*, 90.

73. *History of the Signal Security Agency, Volume 2*, 285.

74. *History of the Signal Security Agency, Volume 2*, 92.

75. Mark Rhoads, memorandum for Director of Communications Research, "Proposal for an ABC Committee," September 22, 1944, 2, Document Reference ID A4148557, accessed October 8, 2021, https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/reports-research/FOLDER_534/41772089081117.pdf.

76. Rhoads, "ABC Committee," 3.

77. Rhoads, "ABC Committee," 4. The memo names "Jacobson," but this is very likely Walter Jacobs, one of the Technical Consultants. After consideration, senior managers decided the necessary coordination could be accomplished by rotating key personnel. See "Security Division Executive Committee Minutes," October 2, 1944, 1, NSA Archives, Accession 21324, Document Reference ID A76960.

78. Robert Louis Benson, *A History of US Communications Intelligence during World War II: Policy and Administration* (Fort Meade, MD: Center for Cryptologic History, 1997), 134.

79. "Minutes of the First Meeting of the Army-Navy Sub-Committee on Cryptanalysis," October 20, 1944, 1-2, NSA Archives, Accession 17525, Document Reference ID A179060.

80. *Summary Annual Report of the Army Security Agency, Fiscal Year 1946*, 2, 4-5, Document ID 6579558, accessed March 4, 2022, https://media.defense.gov/2021/Jun/30/2002753623/-1/-1/0/SUMMARY-ANNUAL-REPORT-ASA-FY-1946.PDF.

81. *Summary Annual Report FY 1946*, 6-7, 15. The Security organization dealt with communications security, as opposed to personnel and physical security.

82. Army Security Agency, *Cryptanalytic Branch Annual Report 1945-1946*, 83-84, NSA Archives, Accession 32611, Document Reference ID A3166019.

83. "Research and Development Division," undated, 7, NSA Archives, Accession 35438, Document Reference ID A270473.

84. *Cryptanalytic Branch Annual Report 1945-1946*, 83-84.

85. "Rotation Plan Meeting," December 9, 1946, 2, Document Reference ID A67439, accessed February 15, 2022, https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/friedman-documents/panel-committee-board/FOLDER_468/41732969077220.pdf.

86. D. Glenn Starlin, "Minutes of Civilian Employment Board Meeting," September 6, 1946, 2, Document Reference ID A66697, accessed October 8, 2021, https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/

friedman-documents/panel-committee-board/FOLDER_471/41723629076289.pdf.

87. *Summary Annual Report FY 1946*, unnumbered page 3.

88. *CSGAS-90 Operations Division Annual Report, Fiscal Year 1948*, undated, unnumbered page 29, NSA Archives, Accession 14993, Document Reference ID A2806186.

89. *WDGAS-90 Operations Division Annual Report, Fiscal Year 1947,* December 11, 1947, 3-a and unnumbered pages 18, 19, 30, 32, NSA Archives, Accession 36332, Document Reference ID A68670.

90. Friedman, letter to R. Fred Chambers, February 9, 1950, Accession 47270, Document Reference ID A69090, accessed April 5, 2022, https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/correspondence/FOLDER_364/41731189077041.pdf. This letter initially appeared to be a letter of reference to the university; a better understanding of Ferner's chronology now makes it likely that this was a reference through the university to Sandia Corporation or perhaps another potential employer.

91. Commencement program, June 1950, per email from David M. Hays, archivist, University of Colorado Boulder Library, March 21, 2022, CCH Historian Projects File, Ferner-McIntire. Also per Hays, university directories place Ferner in local housing during the 1948–1949 and 1949–1950 school years.

92. *Coloradan* yearbook, 1950, per email from Hays, March 21, 2022.

93. Leslie H. Wyman, disposition form, subject "Robert O. Ferner," February 26, 1952, Accession 47270, Document Reference ID A65784, accessed November 27, 2020, https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/friedman-documents/panel-committee-board/FOLDER_393/41734129077335.pdf. Q is the Department of Energy's equivalent of the Top Secret clearance granted by other government agencies. See "Departmental Personnel Security FAQs," Department of Energy, Office of Environment, Health, Safety & Security, accessed October 21, 2021,

https://www.energy.gov/ehss/security-policy-guidance-reports/departmental-personnel-security-faqs.

94. Per email from Rebecca Ullrich, historian, Sandia National Laboratories, March 15, 2022, CCH Historian Projects File, Ferner-McIntire. Ullrich also noted that Ferner might have been involved with field testing of non-nuclear blast effects of various explosives. His work might have been in design, modeling, or both.

95. Ullrich, email.

96. There is some question as to exactly what the acronym SCAG stood for, as variations of this title appear in early SCAG documents. This is one valid candidate.

97. H. T. Engstrom, minutes of SCAG Conference, September 12-13, 1951, 4 [10], Accession 47270, Document Reference ID A66075, accessed November 27, 2020 (link updated April 5, 2022), https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/friedman-documents/panel-committee-board/FOLDER_392/41746519078572.pdf.

98. *History of the Signal Security Agency, Volume 2*, see references to Marston in index.

99. Oliver R. Kirby, "Request for Consultant Services of Mr. Robert O. Ferner," January 28, 1952, Accession 47270, Document Reference ID A65781, accessed November 27, 2020 (link updated April 5, 2022), https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/friedman-documents/panel-committee-board/FOLDER_393/41895859093477.pdf.

100. Ralph Canine, letter to Mr. Donald Quarles, June 20, 1952, Document Reference ID A65875, accessed October 8, 2021, https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/friedman-documents/panel-committee-board/FOLDER_393/41743069078227.pdf.

101. "Thomas Woodward Ferner," obituary, *The Alliance Review*, June 27, 1960. Article received August 24, 2021, from Reference Department, Rodman Library, Alliance, Ohio.

102. "Robert O. Ferner," obituary, *The Alliance Review*, August 9,

1982. Article received August 24, 2021, from Reference Department, Rodman Library, Alliance, Ohio.

103. Jean Ferner, interviews.

104. Rowlett, *Magic*, 152, 231.

105. Friedman, letter to Chambers.

106. Friedman, letter to Lycett.

107. Jean Ferner, interviews.

108. Ed Fishel, "Wanted: Personal Yarns," undated, 1, NSA Archives, Accession VI.S.1.1, Document Reference ID A313961.

109. George Hurley, interview by Robert D. Farley, August 13, 1981, NSA-OH-07-81, transcript, Center for Cryptologic History, Ft. Meade, MD, 139.

110. Levenson, interview, 12.

111. "KRYPTOS Society: Distinguished Members and New Seal," *Cryptolog* 9, no. 2 (December 1982): 17, NSA Archives, Accession 16566, Document Reference ID A546005.

List of Photos and Images

Station photograph collection, A-026-007, Center for Cryptologic History.

IX. Floor plan for B-III (SPSB-III) front office. Control Office, memorandum for Commanding General, Signal Security Agency, "General Cryptanalytic Problem [Control Office survey]," Document Reference ID A70871, accessed April 7, 2022, https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/reports-research/FOLDER_488/41718889075819.pdf.

X. Arlington Hall Station group photo (B Branch). Arlington Hall Station photograph collection, Center for Cryptologic History reference collection, SC-007-001, 1943. Identifications by Center for Cryptologic History staff.

XI. The Ferner family, New Mexico, circa 1953. Courtesy of Mrs. Jean Ferner.

XII. Exceptional Civilian Service ceremony group photo. Arlington Hall Station photograph collection, A-031-006, Center for Cryptologic History; reprinted with caption in *Cryptologic Quarterly* 1, no. 1 (Spring 1982): 67.

XIII. Exceptional Civilian Service ceremony with Robert and Erma Ferner. Arlington Hall Station photograph collection, A-031-001, Center for Cryptologic History.

Acknowledgments

Sincere thanks go to the following individuals and institutions that provided invaluable memories and materials about Robert Ferner's life: his daughter, Mrs. Jean Ferner, who generously shared insights into her father's life; Dave Tyler, who kindly provided the *Ferner – Farner – Furner* booklet; Reference Department, Rodman Public Library, Alliance, Ohio; Linda Poole, executive assistant, Superintendent's Office, Alliance City Schools; Alan Zahorsky, reference and instruction librarian, University of Mount Union; David Hays, archivist, University of Colorado Boulder Libraries; Rebecca Ullrich, historian, Sandia Laboratories; Robert Simpson, librarian, National Cryptologic Museum; and all of my colleagues from the Center for Cryptologic History, its Publications Team, and in other organizations who contributed in so many ways to improving the telling of Robert Ferner's story.

Brenda J. McIntire is a historian at the Center for Cryptologic History. She has served in the federal government since 1985, holding technical, leadership, and liaison positions. Ms. McIntire earned degrees in religious education, music, music history, and strategic intelligence.


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA