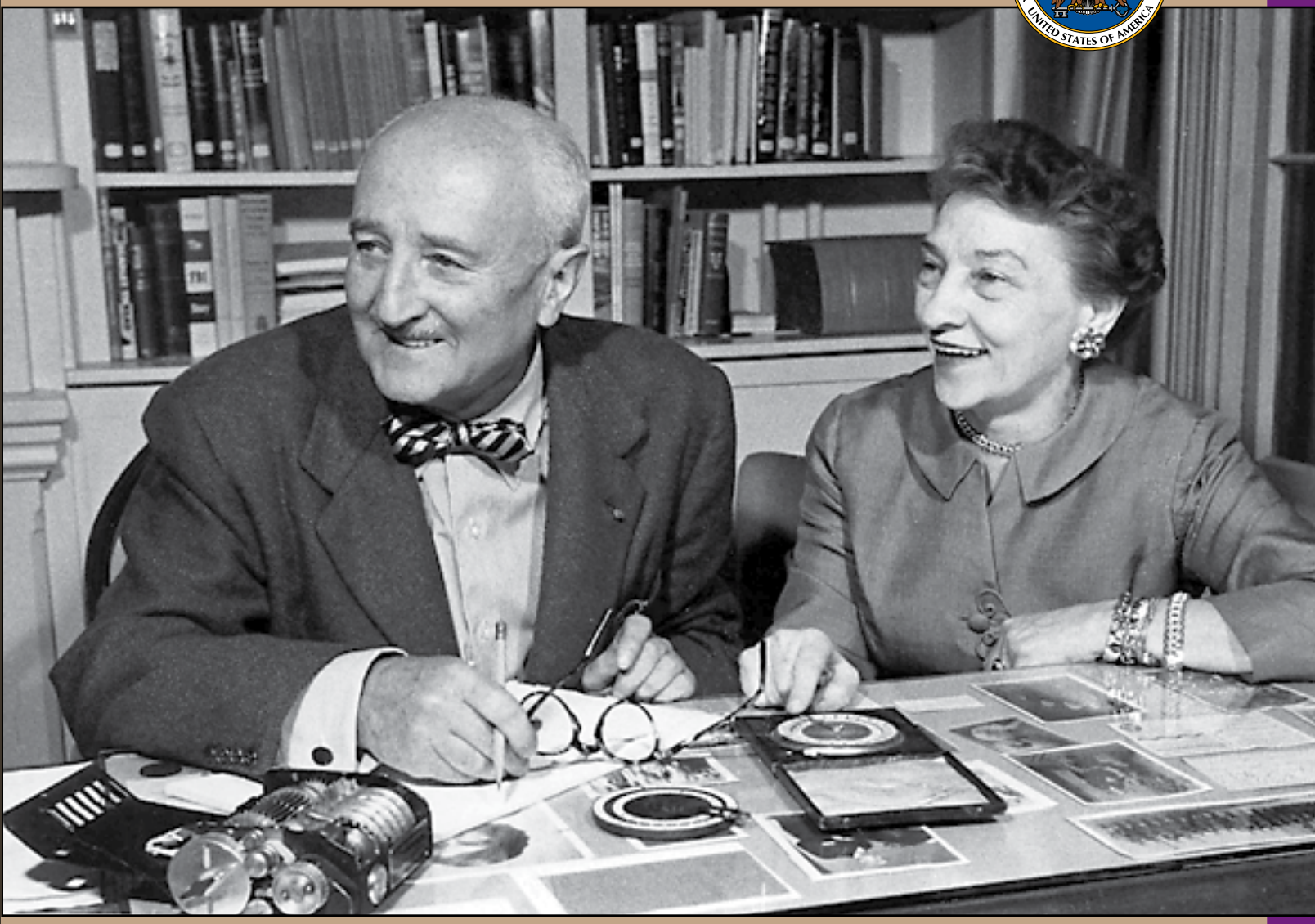
Cryptologic Quarterly



Release of the William and Elizebeth Friedman Collection

William Bundy at Bletchley Park

How Modular Arithmetic Helped Win World War II

Two Cryptologic Nights at the Cinema

2015-01 • Vol. 34

Center for Cryptologic History

Cryptologic Quarterly

Publisher: Associate Director for
Education and Training
Executive Editor: Barry D. Carleen
Managing Editor: Lu A. Greenwood
Associate Editor: Jennie Reinhardt

Editorial Policy. *Cryptologic Quarterly* is the professional journal for the National Security Agency/ Central Security Service. Its mission is to advance knowledge of all aspects of cryptology by serving as a forum for issues related to cryptologic theory, doctrine, operations, management, and history. The primary audience for *Cryptologic Quarterly* is NSA/CSS professionals, but *CQ* is also distributed to personnel in other United States intelligence organizations as well as cleared personnel in other federal agencies and departments.

Cryptologic Quarterly is published by the Center for Cryptologic History, NSA. The publication is designed as a working aid and is not subject to receipt, control, or accountability.

Contacts. Please feel free to address questions or comments to Editor, *CQ*, at history@nsa.gov.

Disclaimer. All opinions expressed in *Cryptologic Quarterly* are those of the authors. They do not necessarily reflect the official views of the National Security Agency.

Copies of *Cryptologic Quarterly* can be obtained by sending an e-mail to history@nsa.gov.

Comments. This is the first completely unclassified issue of this publication, and the *CQ* editorial staff would greatly appreciate all constructive comments and suggestions for improvement. Send to history@nsa.gov.

Cover: William and Elizebeth Friedman with part of their cryptologic collection. See The Editor's View, page 2, and article on page 4.

Contents

2015-01 • Volume 34

The Editor's View

Release of the Friedman Papers

In May 2015 NSA declassified and released to the public an enormous trove of documents from the William F. Friedman collection. While the originals, by law, had to go to the National Archives, copies of these documents have also been given to the Marshall Library in Lexington, VA. The Marshall Library has long had a magnificent collection of Friedman materials, donated to them by Elizebeth Friedman after her husband's death.

In this issue, Rose Mary Sheldon, professor of history at the Virginia Military Institute, describes the existing Friedman holdings in the Marshall Library. This collection was always an important source for understanding cryptologic history, and now it is even more so.

Let me on this occasion write a few unconventional thoughts about William Friedman.

If one were to ask the NSA/CSS workforce why we honor William Friedman, my guess is that a majority would answer something on the order of "He was the greatest codebreaker of his time." This, of course, raises the question of how anybody could measure this properly.

In my opinion, there are three better reasons for honoring Friedman.

As a scientist by education, Friedman early in the twentieth century recognized the need to apply scientific methods to cryptology. His ability to separate the steps composing the task of cryptanalysis (a word he coined, by the way) was central to the ability to expand American cryptology from a craft practiced by a few individuals, who performed all steps, into an industrial-style process. This was a necessary conceptual change as cryptanalysis had to meet the demands for range of coverage and speed of reporting in World War II.

Friedman recognized the importance of the past. His deep knowledge of the history of cryptology equipped him to understand the practical changes that had to be made for an effective national effort.

Friedman also recognized the future. He understood the trends in cryptologic thinking in his time

and where they would lead. He trained his employees on what they could learn from the past, then encouraged them to get an education that would equip them for the efforts that would be needed in the future; in his day that was the use of statistical analysis and a knowledge of machine support systems. Like the best teachers, he pushed his pupils to go further than he had.

My remarks have concentrated on William because of the recent events regarding release of his papers. His wife Elizebeth was no less a remarkable person. Read *The Friedman Legacy: A Tribute to William and Elizebeth Friedman*, published by the CCH, not only for William's lectures on cryptologic history but also for articles about Elizebeth Friedman's contributions to our profession.

◆ ◆ ◆ ◆ ◆

The Unclassified *CQ*

No glass ceiling is shattering, no ground is shaking, no sea of any hue is parting, but this current issue represents a major step forward.

This is the first totally unclassified issue of *Cryptologic Quarterly*. This is also the first issue of this journal released in its entirety to the public.

When NSA was first established in 1952, its personnel were discouraged from writing for outside journals, due to anonymity concerns. Then, as now, many members of the work force had been recruited from academia, where publishing was an accepted, even required, part of professional life. To help mitigate the policy about publishing, the director, LTG Ralph Canine, USA, established the *NSA Technical Journal* in 1954.

Over time, the Agency's leadership recognized that it would be desirable to have a publication that captured the wide varieties of experience at NSA apart from technical matters. Thus, in October 1969, came *Cryptologic Spectrum*.

Both journals were widely read within the work force, but the cost of publishing two issues regularly, with a separate staff for each, became a problem. Thus, in 1981, the two were combined into *Cryptologic Quarterly*.

Now that we have this precedent, we expect to publish one unclassified issue of *CQ* every year. This will include current articles and a generous sampling of classics from the back issues that have not previously been available outside NSA.

David A. Hatch, NSA Historian
[temporarily sitting in the editor's chair]

William F. Friedman: A Very Private Cryptographer and His Collection[1]

It is not possible to work for NSA without encountering the name William F. Friedman. Even if one only connects the name with an annex building, an auditorium, or a bust in the National Cryptologic Museum, it would be hard to pass through the halls and not see some reference to the dean of modern cryptographers or his wife, Elizebeth S. Friedman. They are two of the biggest figures in cryptologic history, and their legacy has been duly memorialized in the volume NSA published in 2006.[2]

The days are quickly passing when anyone who actually remembers William Friedman still walks the halls at Fort Meade, and those who did work with him may have only known him professionally or seen him in passing. This article presents the personal side of William Friedman as seen through his private library and the collection of books, papers, and cryptologic artifacts now housed at the George C. Marshall Library in Lexington, Virginia. The Friedman Collection has recently been systematized, and a reference guide to it can be accessed through the Marshall Library website: http://marshallfoundation.org/library/documents/The_Friedman_Collection_An_Analytical_Guide.pdf.

This article is based on the materials collected by the Friedmans and the comments they made about the materials. Although the Friedman Collection is a treasure trove of information on the history of cryptography, it really represents only what the Friedmans did in their spare time, rather than their professional work, much of which still remains classified [see editor's note at end]. No matter how much time one spends at the office, there must always be a personal side which one cultivates and even protects from the vicissitudes of the work world and its politics.

The general outline of William's life can be gotten from Ronald Clark's book *The Man Who Broke Purple*. Wolfe Friedman was born on September 24, 1891, in Kishniev, Russia. His family emigrated to the U.S. in 1892 and settled in Pittsburgh, where his name was changed to William. Although he had had no personal experiences of the persecution which had driven his parents from their homeland, his "historical memory" was affected by stories he heard from his parents about the pogroms in Russia. His daughter Barbara writes of "his deep ties to his early Jewish upbringing, especially his great love and respect for his own father, the 'Talmudic Scholar' who spoke nine languages." This father, Frederick Friedman, was from Bucharest and had worked as a translator and linguist for the Russian Postal Service. His mother was the daughter of a well-to-do wine merchant.

The Friedman Collection has hundreds of photos illustrating the life of the Friedmans. The ones included in this article represent only a fraction of what can be accessed at the Marshall Library. The earliest picture we have of William is his graduation photo from Pittsburgh's Central High School. Among his classmates were five Jewish students in the debating society called "The Emporean Philomath," who became imbued with the idea of a Jewish "back to the soil" movement. They would all attend Michigan Agricultural College (MAC) (which later became Michigan State University) in Lansing with the intent of becoming pioneering scientific agriculturalists.

Although William entered MAC in 1910, he left in 1911 when he was accepted to Cornell University as an undergraduate on a full scholarship. He was

William Friedman and Elizebeth Smith at Riverbank Estate in Illinois ca. 1916

William Friedman (l) with Jake Margolis, Nathan Gould, and unidentified student
at Michigan Agricultural College, 1910-1911

attracted to the new science of genetics resulting from the rediscovery of Mendel's work. In the summer of 1913 he helped Dr. D. H. Shull at the Carnegie Institution's Department of Experimental Evolution at Cold Spring Harbor, Long Island; he was 22. While there he fell in love with Verna Lehman, a young Jewish girl from Brooklyn, but felt he was not ready for a commitment since he was still in college.

William graduated from Cornell in 1914 with a BSc degree.[3] He then enrolled in the university's graduate program in the College of Agriculture. He studied plant breeding, plant physiology, botany, and chemistry. He taught undergraduates part time. He eventually registered for the Ph.D. program, but six months later switched to the Master of Science in Agriculture course. His record was described as "somewhat irregular."[4] Later in a letter he again talked about joining the "back to the farm" movement, but he felt unqualified. He always had nostalgia for what might have been if he had stuck with genetics. He titled a talk at the Cornell Club in March 1958 "From Biology to Cryptology: A Few Episodes in the Story of the Seduction of a Cornellian and Its Aftermath."

In 1915 William's supervisor, Professor Rollins A. Emerson, received a letter out of the blue from George Fabyan looking for a qualified per-

son to take over the Department of Genetics at Riverbank Labs in Geneva, Illinois. In June of 1915 Fabyan wrote William a letter offering him $100 a month and free room and board on the estate. William accepted the job and essentially said goodbye to the academic life. "Colonel" George Fabyan (the title was honorific) was a rich eccentric: for example, he bought an estate where he kept monkeys and caged vegetarian bears, and yelled at his employees while sitting in a chair suspended from the ceiling (called "The Hell Chair").

From 1915 to 1916 William was the director of the Department of Genetics, Riverbank Labs, and did experiments like planting oats by the light of the moon. Few details of his work as a geneticist have survived. During this time, he lived in the upper floor of a windmill on the estate.

Because of his abilities as a photographer and his facility with a darkroom, William was asked to do some work for Fabyan's cipher projects. George Fabyan and Elizabeth Wells Gallup both believed Francis Bacon wrote Shakespeare's works. The theory was based on a biliteral cipher that Mrs. Gallup supposedly detected in the Shakespearean folios. In order to see the letters more clearly, William had to produce large-format prints of the manuscripts that Mrs. Gallup was working on to illustrate the differences in letters she claimed to see. Within a few months he was drawn into their work with cryptography. Within less than a year, it was his main occupation, and a young female assistant was running the genetics lab for him.

"Colonel" George Fabyan in "The Hell Chair" from which he yelled orders to Riverbank Labs staff

Besides the introduction to cryptography, a good thing that came out of this job was that he met a young woman working in the cipher department named Elizebeth Smith, whom he eventually married. (According to a family story, Elizebeth's mother spelled her name this way to prevent anyone from nicknaming the child "Eliza.")

Neither of the Friedmans believed Mrs. Gallup's theory, and they would eventually write a book proving her wrong, but they never criticized the formidable Mrs. Gallup during her lifetime.[5] From 1916 to 1918 William had the title of director, Department of Ciphers and Genetics, Riverbank Labs. The department worked on many interesting projects. One was brought to Washington, DC, via

William Friedman's mother Rose (l) with Elizebeth Friedman, July 1920

Scotland Yard and then forwarded by the government to William's department at Riverbank Labs in 1917. It consisted of ciphered correspondence which had been passing between Hindu and German agents who were conspiring to launch a revolution in India while Great Britain was engaged in the war in Europe. William was asked to decipher the correspondence without the code books, which he did, and he appeared as a government witness in two trials. Eventually thirty Hindus and Germans were tried in Chicago; a second trial, with about 130 agents, was held in San Francisco. In the second case a Hindu who had turned state's witness was shot to death in the courtroom by another Hindu, a defendant, who had smuggled a gun into the courtroom.[6]

With America's entry into World War I, George Fabyan offered the services of his Department of Codes and Ciphers to the government. There was no federal department for this kind of work (although both the Army and Navy had had embryonic departments at various times). Colonel Joseph Mauborgne visited Fabyan in April of 1918, and on the 11th, five days after the U.S. had declared war on Germany, Mauborgne reported back that officers should be sent to Riverbank for training. He recommended that the team already working there under William Friedman should be used for official ciphering. Riverbank thus became the unofficial cryptographic center for the federal government. The Riverbank staff was given the task of training recruits. Eighty men were sent to Illinois and housed at the Aurora Hotel, the closest hotel to Riverbank. It was there, outside the entrance, that the officers were lined up for a photograph at the end of the course spelling out Bacon's axiom "Knowledge is Power" in code. [7]

William took two major steps in 1917. First, he and Elizebeth Smith married on May 21 in Chicago, a month after Germany declared war on the U.S. His brother Max said it was one of the first mixed marriages in the Pittsburgh Jewish community. You would have thought William had committed murder: "If he had still been living in Pittsburgh, he would have been ostracized."[8] The second big step was finally escaping from Fabyan's clutches. William did not want to be in Geneva, Illinois, working for Fabyan; he wanted to be in the war working overseas, and evidently the U.S. government wanted that too. Colonel Mauborgne had been trying to get William to Washington, but Fabyan had blocked the information by intercepting William's mail, which William never

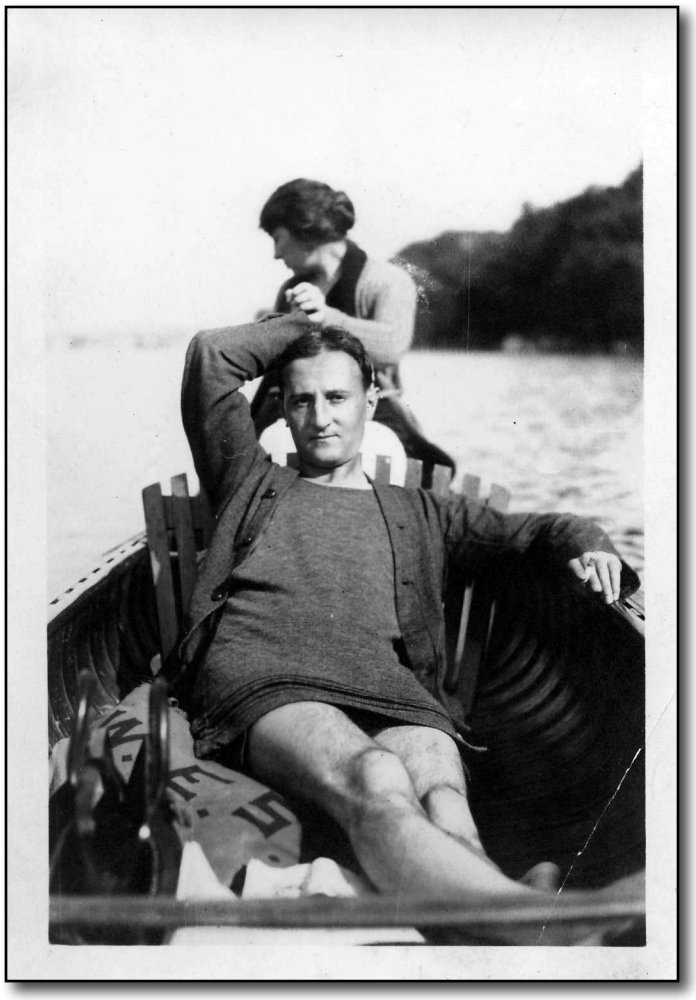
discovered until after the war. The Friedmans also believed that Fabyan's brother-in-law tried to block his enlistment.[9] For appointment to the regular army, William had to take a physical and intellectual achievement test at Camp Grant. George Fabyan's brother-in-law was in command at Camp Grant and had the doctor declare William 4F due to a "heart condition." William always felt he had missed out on one of the big opportunities of his life by not being commissioned earlier and making a name for himself.

Eventually, William escaped Riverbank, was commissioned, and crossed the Atlantic in July 1918. He reported for duty with Military Intelligence at General Pershing's headquarters. First Lieutenant Friedman served in the Code and Cipher Solving Section, G-2, General Headquarters, AEF Chaumont, France.

To support the training of department personnel, William produced a series of technical monographs. He had completed seven by early 1918. Among them is his most famous and important work, *The Index of Coincidence and Its Applications in Cryptography*, Riverbank Publication No. 22A. Among the people he served with was J. Rives Childs, who had been trained by William and Elizebeth at Riverbank in the autumn of 1917 and who later rose to the rank of ambassador in the U.S. Foreign Service.[10] William worked with many people in World War I whose work on codes is now in the collection, including Parker Hitt[11] and Frank Moorman, who headed the G-2, A-6—the German Code and Cipher Solving Section at General Headquarters (GHQ).[12] After the war, Major Moorman ordered William to remain at GHQ, write the history of the code-solving section, and eventually close the section. William returned to the U.S. in April 1919. Elizebeth had left Riverbank in the autumn of 1918 and returned to her family home in Huntington. She joined William in New York when he returned from the war, and together they visited the Friedman family in Pittsburgh. (The Friedman Collection has the first picture of the Friedmans taken together after his return to the U.S.)

1st Lieutenant William Friedman, ca. 1918

Neither of the Friedmans wanted to return to Riverbank in 1919; William was still looking for a job in genetics, but Fabyan kept trying to cajole them into coming back. Fabyan claimed that they were still under contract, that he had banked their salary for them while they were away, and that he would give them a raise if they returned. Of course, all of this would prove to be untrue. Still, the job market being what it was,[13] the Friedmans agreed to return under four conditions:[14]



Elizebeth and William Friedman boating on the Potomac River, Washington, DC, 1921-1922

1. They would not live at the Riverbank estate.

2. There would be no interference in their private life.

3. They had to be free to prove or disprove Mrs. Gallup's biliteral cipher.

4. Their names would appear on anything they published.

These conditions give a clear idea of their complaints about George Fabyan. The rapprochement did not last long. Within eighteen months they had left again, this time getting away from Riverbank with ultra-scheming to prevent Fabyan from knowing until they were packed for the train to Washington, DC.

They loved the nation's capital after the provincial Midwestern life they had been living. William had just read Sinclair Lewis's *Main Street* and said that he had to get out of the Midwest "before I turned myself completely to brick-red iron ore dust."[15] They had a wonderful life in D.C. Their first furnished apartment was in the home of a music teacher and had two pianos. They formed a musical quartet that included Major Mauborgne on the violin, Elizebeth on the piano, a friend from Geneva on cello, and a friend from the Army. People could hear them playing from the street when their window was open, and crowds formed to listen.[16] Both the Friedmans felt their disposition had improved now that they were doing work that was important and interesting. They had escaped the dull provincial life of the Midwest and, most importantly, they had escaped the clutches of George Fabyan. William wrote that Fabyan hated Elizebeth the most because she "saw through him and his wiles very early in the game."[17]

From 1920 to 1921 William served as cryptographer in the Office of the Chief Signal Officer, Washington, DC. Here he resuscitated two pieces of equipment from the AT&T Company. One, the Printing Telegraph Cipher that had been originally purchased by the Signal Corps but later warehoused after Riverbank, proved the double-key-tape was insecure. William used the equipment to compile Field Division Codes to be used in training or emergencies.[18]

In 1922 William became chief cryptographer for the U.S. Army Signal Corps. He joined the government's "Black Chamber," where he was placed in charge of researching new codes and ways of breaking them. This is where he met Herbert Yardley. Although both men were in the code-breaking business, no two people could be more unalike.[19] According to the Friedmans, Yardley was a drunk, womanizer, sloppy dresser, braggart, and had loose lips. He cheated at cards and plagiarized other peo-

ple's work.[20] What really upset the Friedmans and many others, however, was that when the Black Chamber was dissolved in 1929 for lack of funding, Yardley, in need of money, published a book in 1931 called *The American Black Chamber*, which many felt told too many American secrets. Yardley supported himself for years by writing pulp fiction and exaggerating his own exploits.[21]

Between the wars the Friedmans had a normal family life, raising two children, celebrating holidays, and going on vacation. About 1923 they moved into a rambling house on five acres in Maryland which they called Green Mansions. It was here that their daughter, Barbara, was born. The entertaining at this country house was a pleasant relief from the strain of work. But eventually the two-hour commute into D.C. each day became a strain, and they moved to a Chevy Chase house where their son, John, was born.

During the 1920s a series of new ciphers processed by machines gained popularity, based largely on typewriter mechanicals attached to basic electrical circuitry, that is, batteries, switches, and lights. The first such machine was the Hebern Rotor Machine, designed in 1915 by Edward Hebern. The Navy decided to buy the machine. One Navy employee, Agnes Meyer, went to work for Hebern and left the Navy completely, hoping there would be big money in the production side. Before the Navy would agree to shell out millions on this new invention, however, it had to be sure the machine could turn out secure communications. William was asked to break a code it produced.

He sat in front of the machine for six weeks in 1923, to the "point of black-out," thinking of a way to attack it. He used the index of coincidence and finally succeeded. William never did any more work on the Hebern machine, and the Navy took it away from Hebern, who was promised a huge sum of money but got nothing. The Navy decided not to use it, perhaps because William had discovered its weakness. When

William Friedman with AT&T printing telegraph cipher machine, 1919

Hebern died, his family sued the Navy for $50 million but settled for $50,000.

The 1920s saw both the Friedmans employed in important and productive work. In 1924 William cracked the codes used by the conspirators in the Teapot Dome Scandal in which Secretary of the Interior Albert B. Fall was convicted of renting government lands to oil companies in return for personal loans and gifts. In 1927 Elizebeth was appointed special agent on loan from the Department of Justice to the Coast Guard, which was struggling to enforce the Volstead Act against a flood of smuggled liquor coming in from Canada and the Bahamas. In the *I'm Alone* case she proved that a ship sunk by the Coast Guard was actually owned by American smugglers and not the Canadians, thus avoiding an international incident.[22]

The workload and the nature of his work caused William to consult Dr. Philip Crane, a young Washington psychoanalyst, for six months of treatment. The strain of having to maintain two separate lives—on the one hand the affable guest, devoted husband, and adored father, and on the other someone who had to think thrice before he spoke[23]—took its toll.

The Friedman family in Washington, DC, 1930s

In 1928 William was sent as an official delegate to the AT&T conference in Brussels. Elizebeth accompanied him at her own expense. His success at that conference made him a natural choice for the International Radio Conference in Madrid in 1932 at which he was both a technical adviser and the committee chairman.[24]

In 1929 when the American Black Chamber was dissolved, William moved to the Army Signal Intelligence Service in a similar capacity. While he worked as a cryptanalyst for the War Department in the 1930s, his life went on as usual. He felt that cryptologic literature in the 1930s was woefully inadequate and took up the task of having foreign works on the subject translated into English. During eight years in the 1930s, the members of the Signal Intelligence Section (eight people) wrote over sixteen textbooks. William systematized the art he had pioneered into the classic *Military Cryptanalysis,* Parts I-IV, which were classified but are now available on the NSA website. His other job was to train a new generation of codebreakers. He started in the spring of 1930 with four new recruits: Solomon Kullback, Frank Rowlett, Abraham Sinkov, and John Hurt. We have some early publications of theirs from before the war, but much of their later work is classified.

William Friedman was one of the first people to realize the importance that machine cryptography would have on the profession. In 1936, only after his continued insistence, the Army obtained its first IBM data-processing machines for cryptologic purposes.[25] Other countries were doing the same. In 1939 the Japanese introduced a new cipher machine system for their most secure diplomatic traffic to and from important embassies (replacing the Red code). The new one was called Purple.

Pearl Harbor and Beyond

Two years before Pearl Harbor, General Mauborgne called William into his office and complained that his people were getting nowhere with the Japanese codes. He wanted William to drop everything and work on them. It took eighteen months to solve the problem completely, but William and his team did it.[26] Purple did not use rotors, like the German Enigma or the Hebern design. It used step switches like those used in automatic telephone exchanges. William bought about $200 worth of telephone equipment, and by the end of 1940 Leo Rosen and his team had built a duplicate machine that worked.[27] One of the most amazing things about William's ability to keep a secret is that he never told his wife what they had done. He came home that very day and said nothing more than "What's for dinner?"

The pressure of the work once again took its toll. In January 1941 William was taken to the neuropsy-

chiatric ward of the Army's Walter Reed Hospital.[28] He was diagnosed with "extreme nervous fatigue" due to prolonged overwork on a top secret project. On March 22, 1941, he left Walter Reed and returned to active duty on April 1, 1941. Less than three weeks later he received a letter from the adjutant-general stating that he was being honorably discharged for reasons of physical disqualification ("incapacitated"). His commission in the Signal Corps was terminated. The letter was a shock because the medical board at the hospital had recommended a return to duty, and he had never appeared before the Retiring Board. He protested, but his protests were brushed aside; he was returned to his work, but as a civilian, for the rest of the war.

While William was helping to read the Purple traffic, in November 1941 Elizebeth was tasked with setting up a cryptographic organization for what was to become General William Donovan's OSS. America was still at peace when she was asked to prepare code and cipher material for Donovan's Office of the Coordination of Information. For three weeks she and her staff at Coast Guard Headquarters had laid the lines for cryptographic links between Washington and Donovan's London office. Two Hagelin machines would be used, but they did not arrive as expected, and one of Elizebeth's coups was to obtain for Donovan's use two machines which had been earmarked for other departments.[29]

In December 1941 Elizebeth moved into Donovan's organization, and for the rest of the month she and her staff prepared special keys, alphabet strips, and other devices for use in the field. She later wrote that this class of material was devised especially for Donovan and existed nowhere else. She began to recruit cryptographers for the organization and to lay down ground rules for the training in code and cipher which had to be given to Donovan's men going on secret operations. She also suggested they devise an oath for the entire organization. There is not a single word in the collection about this, just one brief notice of the Velvalee Dickinson case ("The Doll Woman").[30] Elizebeth's service record from St. Louis shows that she was on loan from the Treasury Department, but nothing more. The photograph of Elizebeth in 1934 gives us a tantalizing glimpse into her professional activities during the war, but that chapter has yet to be written and would be a serious lacuna for any biography unless further information is released.

Then on December 7, 1941, came Pearl Harbor. Elizebeth said that after the announcement of the attack, William wandered around the house saying, "But they knew, they knew." Years later, when one of his nephews wrote and asked him about revisionist theories, he wrote: "There were no messages which can be said to have disclosed exactly where and when the attack would be made. Hence I do not see how President Roosevelt could have avoided the attack by advance knowledge from reading such messages. In my opinion, only certain members of what may be called the Extreme Right Wing believe this fable."[31] William believed the information had been collected and processed, but not correctly analyzed or distributed. Although over the years people wrote to him asking for information about the Purple Code and the Pearl Harbor attack, he always respected his duty to the government. In a letter of January 14, 1961, he wrote to Eugene Bergman:

> I am sorry I cannot help you in regard to information about Japanese codes. It isn't permissible and I have rejected <u>all</u> requests so don't feel badly. The authorities are becoming more and more close-mouthed about all code matters and I must conform.

When his son John asked him what really happened, William pointed to the eighteen volumes of the Report and said "Read it. It's all there." The only statements he ever made were in congressional testimony.

In 1946 the breaking of Purple was revealed during the congressional hearings on Pearl Harbor. One of the most controversial phases in the investigation of the Pearl Harbor attack was the so-called

Friedman family at Christmas dinner, 1940, at their home in Chevy Chase, Maryland

"Winds Execute Message." Two officers, one naval and one army, believed that a "winds message" had been sent and intercepted before the attack.[32] Colonel Sadtler claimed he was told the message was destroyed on the orders of General George C. Marshall. Thousands of words of testimony were taken on this controversial point, and in the end there was only one person who remained convinced that such a message had actually been transmitted: Captain L. E. Safford, USN.[33] William testified that Safford had told him there was an intercept, but he never saw it and there were no copies. Safford's evidence has been refuted.

In the Friedman Collection there is a handwritten note made immediately after a talk with Captain Safford on 14 August 1946. The note is autographed to "Billy Friedman with deepest appreciation for the way in which he supported my testimony in an earlier investigation. L. F. Safford, August 14, 1946." According to Elizebeth's note on Item 354, Captain Safford's reference to "an earlier investigation" is to the Clark investigation, an "Inside the Armed Forces" report: "WFF never supported Capt. Safford in any of the latter's statements concerning this autographed message." In 2008 the Center for Cryptologic History at NSA published a volume called *West Wind Clear: Cryptology and the Winds Message Controversy—A Documentary History* (Eds., Robert J. Hanyok and David P. Mowry) covering everything there is to be known about the subject. The editors concluded there was no "winds message" received; however, this has not stopped conspiracy theorists from claiming there was.

British Liaison, 1942 Events

America's entry into the war in 1941 helped regularize the cryptographic collaboration with the British which William Friedman had been doing with his Navy counterparts for years. He visited the British code-breaking operations at Bletchley Park in 1941 and exchanged information on techniques for attacking Purple for British information on how they had attacked the Enigma. Here he worked with Alan Turing. William had been advocating for SIGINT cooperation with the British since 1940. The U.S. Navy's chief codebreaker, Commander Laurance Safford, was adamantly set against working with the allies. It was only after pressure from FDR finally broke the logjam that the so-called "Sinkov Mission" was sent to tour Bletchley Park and also visited outlying intercept stations. Safford believed these missions were a one-way street because the U.S. handed over the material on Magic but got nothing in return. Others believe this view was incorrect.[34]

In the summer of 1942 the Navy finally handed over its Purple machine to the Army along with all files and decrypts. From then on, it was the Army's job to intercept, decipher, and distribute all Japanese diplomatic messages. A huge increase in staff was involved in this transition. William's staff had been 300 by Pearl Harbor; by 1945 there would be 10,000 working for the Signal Security Service and then the

Signal Security Agency. Already by that summer the Munitions Building had become too small for William's operation. On June 10, 1942, the Signal Intelligence Service took possession of Arlington Hall where the code-cracking activities continued throughout the war.[35] The bulk of the training operations were shifted to Vint Hill Farms in Warrenton, Virginia, in the foothills of the Blue Ridge Mountains, fifty miles from D.C.

In the autumn of 1942 the Friedmans bought a house at 310 2nd Street, Capitol Hill. The first thing William did was to plant a talisman rose bush (a hybrid tea rose) by the house so it would climb around the door every summer. Throughout the remaining years of his marriage, he sent Elizebeth talisman roses on their anniversary.

William was under strain, overworked, and still under psychiatric treatment, but he kept his game face on. His morbid humor showed when asked why he had a coil of rope in his back seat. He said, "I'm looking for a tree to hang myself." At the desk next to him at Arlington Hall was his assistant, Lambros Callimahos. Callimahos described William as meticulous in his habits, whether on staff policy or in technical exposition. He was a stickler for precise and accurate terminology. He wasted little time or motion, and he never stopped working.

Postwar Years

Nineteen forty-four was a busy year. June brought D-Day. In the autumn William was awarded the War Department's Commendation for Exceptional Civilian Service. When the war finally ended in May 1945, a British regiment took over Japan's Berlin embassy. All cryptographic equipment had been removed. The same was true in Tokyo. All the Purple machines had been destroyed. A few broken metal parts were all that William ever got to see of the Purple machine that he had duplicated.

Following World War II William remained in government signals intelligence. From 1942 to 1947 he was director, Communications Research, Signal Intelligence Service (later the Army Security Agency). How ironic that when the Civil Service asked the new Army Security Agency for a list of those people who were its permanent employees, William was listed as temporary—after twenty-five years of service! He was technically not vetted properly for the work he was doing. Nevertheless, he was awarded the Medal for Merit (the civilian equivalent of the military Distinguished Service Medal). His office threw him a party and presented him with a black chamber pot (i.e., The Black Chamber!).

William was already in Europe by 1945. He visited Bletchley Park, where the shape of postwar U.S.-Britain cooperation was being hammered out. He moved on to Germany where he consulted on what kind of cryptographic service the occupation forces would need. He wanted to visit Boris Hagelin, the Swedish cryptologist who had lived in America during the war, but had no time. While in Germany, he was handed a mimeograph copy of his fourteen-lecture course on military codes and ciphers given to American officers in the 1930s; it had been used to train German officers.

In 1946, five years after William was asked to leave the Army, he got a letter from the adjutant-general admitting that he had been retired without the benefit of a Board hearing. Would he care to be reexamined? William returned to Walter Reed for a week, and after exhaustive tests and examinations, they concluded that he was not "incapacitated." The original diagnosis had been anxiety reaction, manifested by tension, insomnia, and stress due to prolonged overwork. He was declared fit for active duty and his commission was restored, but only at the grade he held in 1941, causing him to lose five years' seniority. The same thing had happened to soldiers who had spent four years in POW camps.

A two-week SIGINT conference was convened by GCHQ and its Commonwealth partners in February 1946. The following month, they met with the

Americans. William arrived in London on March 6, 1946, with the intent of delivering a revised version of the previous wartime agreements between the U.S. and Britain. A UK-USA technical conference followed in June 1946. The new material discussed dealt with agreements on security procedures for handling SIGINT.

Mental Illness and Recovery

Many of William's health problems that occurred in 1949-50 evolved from more work and more frustration. In 1949 he became head of the Code Division for the newly formed Armed Forces Security Agency (AFSA), but he was also involved in a legal dispute with the very government that was employing him. After the war William had looked into patenting his wartime machines. He asked for the declassification of a patent he and Frank Rowlett had filed in May 1941 (for the M-228),[36] but his applications were rejected and his request for counsel was ignored. AFSA said no to an outside lawyer—too much secret information would have to be released—but they also said no to an inside lawyer—you can't sue the government.

This frustration led to another health event. From 1947 to 1948 William became seriously ill and was out of commission. In his own words it was from "frustration from this and other sources connected with my work and personal situation." He consulted Dr. Paul Ewerhardt for advice on what he called "psychic giddiness" which attacked him while walking or playing golf. The treatment seemed to work. He had recovered by December 1949, but he was profoundly depressed again and in the following months of 1950 contemplated suicide. He voluntarily entered Mt. Alto Veteran's Hospital in Glover Park, Washington, DC, but disliked it intensely because he was placed with psychotic patients much sicker than he was. Movement to an open ward from which he could make weekend visits home did not help much. In March 1950 William was admitted to the Psychiatric Unit of George Washington University Hospital for electroshock therapy. He received six treatments without incident or complication. He made a dramatic and rapid recovery and was discharged on April 11, 1950. He was so happy, he kissed the nurses goodbye!

His 1951 retirement from the United States Army Reserve was not exactly voluntary and was probably due to his hospital stays. He returned to his usual busy schedule in the early fifties. He became the chief cryptologist for the newly formed NSA when it took over from AFSA in 1952. From 1951 to 1954 he was research consultant for NSA, along with his old colleagues Sinkov, Kullback, and Rowlett. From 1954 to 1955 he was special assistant to the director, NSA. From 1954 to 1969 he served as a member of the NSA Scientific Advisory Board. He also remained under contract to write lectures, books, and brochures. In 1954 he wrote the article on cryptography for the *Encyclopedia Brittanica.*

The Folger Prize and Heart Trouble

In the spring of 1955 William was in Europe, again on a secret mission. When he returned to the U.S. on March 28, he was told the Folger Shakespeare Prize would be announced on April 4, and that he and Elizebeth were the winners. Indeed, the headlines in the morning paper announced: "Washington couple wins Folger Shakespeare Prize," but before they could celebrate, William had a heart attack on April 3 while getting out of bed. He was taken to George Washington University Hospital where he was diagnosed with a severe coronary occlusion. Tests showed this was his second, not his first, heart attack. He had a third coronary occlusion in May 1955 and was finally brought home from the hospital in June. He was told to give up golf (which he didn't), to walk only short distances, and to carry nitroglycerine pills.[37] The Friedmans had an elevator installed in the house, and an intercom system was put in.[38] Very few people survive three attacks, yet William lived fourteen more active years and went on three more secret missions.

In a humorous letter dated 5 April 1955, John Ranleigh wrote to William:

> What an asinine thing to do [have a heart attack]. I suppose we can't hold you responsible. If only we could keep you from traipsing all over the place, and up and down mountains, and in non-pressurized USAF airplanes, there might be some chance of keeping you out of places like the one in which you now find yourself [the hospital].

E. E. Barker wrote to him on 7 April 1955, that

> These trips away from home have been, I fear, for you entirely too strenuous. I have known how you have been whirled from place to place, fast and furious in a party of men younger than yourself and more robust than you ever were. Well, don't let them do it again.

Active Retirement, Awards, and Bacon's Code

William's frailty probably led to his retirement from government service. In October 1955 the Agency gave him a retirement party complete with Army band. He was presented the Presidential National Security Medal by Allen Dulles. William Friedman is the only person (besides J. Edgar Hoover) to hold both the Medal for Merit and the National Security Medal. The medal part of the proceedings was kept so secret that even General Canine, NSA's director, did not know it had come through until the last minute. William was deeply honored by the award. He said he hoped that he could continue to do work for the Agency. He found the work "of deep interest" and hoped that the result would be of value to NSA and the country.

Letters of congratulations poured in from friends who could not attend the ceremony. Lester Bensinger wrote him in a letter on 4 May 1956, congratulating him and stating, "Our late friend Charlie Mendelsohn spoke often of you, and I am sure if he were here today, he would say, just as I do, that it is only partially what you deserve." Stuart Hedden wrote:

William Friedman with his roses at the house on 2nd St. in Washington, DC, May 1965

> Most men, even great men, can only learn how much their colleagues appreciate them by coming back to this sphere to read their own obituaries. You have had it . . . while you can still blush. . . It is a rare thing for men of extraordinary talents to retain over the years the affection, not the envy, of their colleagues. Your family must be bursting with pride.

Elizebeth added a note to the letter: "Indeed we are!"

William remained very busy because he felt the work was important, and thus he continued what he called his "juggling act." He did not want to have the reaction that one of his friends wrote about: "I fell victim to the rather frequent emotional reaction to retirement and I am still going through the psychic adjustment to this aspect."[39] He listed his hobbies as 1) writing books (unclassified); 2) golf; 3) listening to the HiFi [stereo equipment] his colleagues gave him

William traveling with his "better 9/10," as he referred to Elizebeth

as a retirement gift; 4) pretending he'd ever get around to fishing; 5) being chief engineer of the household, preventive maintenance man and too-late-for preventive maintenance chores in a house filled with "modern gadgets and gadgetry"; 6) taking his wife to the theater, concerts, a lecture or a movie now and then; 7) traveling to distant climes with his "better 9/10," as he referred to Elizebeth, or in other words: "Now I shall be able to think about what I believe to be interesting and important, instead of what other people think to be important."[40]

By 1956 the government's argument about William's ability to hire a lawyer to make a claim for his patents collapsed. He was finally able to hire a law firm, and they helped get a bill passed that would provide some remuneration for William's wartime work. Details of the inventions were not given to the lawyers, but William was awarded $100,000 for his inventions and patents in cryptography. Over the years he had discovered a number of problems common to most of the rotor machine designs. He used his understanding of the rotor machines to develop several of his own that remained immune to his own attacks. He eventually developed nine designs, six of which remain secret today. Since he was able to gain patents only years later, the government awarded him the $100,000 in lieu of what he could have made commercially.[41] The SIGABA machine, which became the U.S.'s highest security encryption system during World War II (which was similar to the British Typex machine), was never broken during World War II, or at all as far as we know.[42]

Also in 1956 William and Elizebeth turned their attention to the problem that had originally brought them together—examining Bacon's Code. For years they had been inundated with correspondence from Baconians. In a letter to Samuel B. Haskell dated 28 July 1947, William indicated that he did not wish to answer any more questions about the Bacon authorship. He said, "My position in the War Department makes commenting on cryptography problematic." And also, "When I retire I wish to write a book on the subject." Well, retirement had come, and in 1957 they wrote *The Shakespeare Ciphers Examined* [43] and won an award from the Folger Shakespeare Library for it.[44] Jacques Barzun wrote from Columbia University saying that it was "admirably conceived, composed and written." Barzun praised its "elegant lucidity" and called it a "model of courteous refutation." In 1958 the Friedmans were awarded the Fifth Annual Shakespeare Award from the American Shakespeare Festival Theater and Academy.

Another Secret Mission: 1957-1958

In August 1957, in the aftermath of the Suez crisis, the British became suspicious that the Americans were reading their traffic preceding the Anglo-French

invasion, something forbidden by the UKUSA agreement. There were also new cryptomachines being used by NATO countries. To breach the rift, William was sent to Europe on a top secret mission. His heart attacks and psychological breakdowns notwithstanding, NSA wanted William for the job because he was the only man who could do it. He was in London from 26 August 1957 through the autumn.

William shuttled between GCHQ's new site in Cheltenham and the Office of London Communications Security Agency on Palmer Street. The main focus of discussion was the collaboration against the western Europeans, and a key issue was the increasingly advanced machines being produced by Crypto AG in Switzerland and AB Crypto in Sweden. NSA wanted to continue having daily information that enabled them to read NATO countries' messages. Not surprisingly, William's subsequent destinations were Sweden and Switzerland.[45] He finally got to visit Boris Hagelin at his Swedish factory. The two had become good friends; they were both born in Russia and shared an interest in cryptography.[46] Elizebeth thought they were just making a social visit. Ronald Clark wrote in his biography that "a clearer picture of the significance of the secret missions of 1957 and 1958 is now emerging."[47] These were the operations which appear to have turned William Friedman against NSA. He just never adjusted to the U.S. spying on its allies or him having to manipulate his friends.

In January of 1958 the Friedmans went to Mérida in the Yucatan to study Mayan. William intended to return at least once every year, but he was pulled out for a special mission and returned to Europe. In April 1958 he flew to Frankfurt to confer with heads of NSA in Europe. In a letter to Walter Addicks dated 9 April 1958, he apologized for having to postpone his talk to the Cornell Club from mid-April to 1 May. In discussing the proposed title for his talk, William wrote: "I trust that none of my Cornellians are going to expect me to do a John Gunther 'Inside the Pentagon' cause I'm not. I want to stay out of jail." He

William Friedman on Oxford Street, London, 1957

wrote a letter to his son John saying he did not want any newspaper publicity. "The people to whom I owe allegiance are a bit down on me already for being too much in the spotlight recently."

Classification Quarrels

One of the biggest bones of contention between William and the government was the classification of historical information on cryptography. In 1960 the NSA got a new director, but the classification process became considerably stricter. William wanted to discuss cryptography with the public, but any mention of it, even in a historical context, resulted in a strong negative reaction from NSA.[48] In 1962,

for example, he gave a lecture on "Shakespeare's Secret Intelligence and Statecraft" at the annual meeting of the American Philosophical Society in Philadelphia, but it brought only more disapproval from NSA. ABC- TV was doing a documentary on Franklin Delano Roosevelt and asked William to appear. He told them they would have to take it up with the DoD.[49] He thought NSA considered him their "greatest security risk" and even hired a private investigator in 1961 to find out whether his phone had been tapped.

He experienced considerable negativity from the government whenever his name appeared in public. Although he was already listed in *Who's Who in America* and *American Men of Science*, when he was asked to submit a blurb for an edition of *Distinguished Leaders in the Nation's Capital* he had to get permission from the DoD, and "various positions I have occupied in the defense organization since 1921 had to be deleted for security reasons."[50] In a letter dated 17 September 1958, he said that he wanted to write a brochure on the American Revolutionary War ciphers, "that is, unless the authorities have discovered this material is still top secret." In another note, dated Thanksgiving 1960, he says "secrecy can be overdone."

When asked by E. G. Begle of Yale University to contribute a monograph on cryptology for high school students (12 September 1960), William wrote that he had to have the manuscript cleared with "the powers that be." He did not want to be guilty "by either conscious or unconscious violations of measures which I myself helped to establish for protecting our national security." In the end the Defense Department forbade him to do the monograph. In a letter dated 3 February 1962, William wrote,

> I have delayed embarking on a project by what I can only consider to be an absurd, foolish and dangerous attitude on the part of DoD authorities in regard to the publication of <u>any</u> sort of material on <u>any</u> phase of cryptology whatever. They seem to think that this whole subject is taboo, a private preserve, and poachers thereon will do so at their peril. And they have the laws and the means to enforce their views. I have in recent months tried to inject some new thoughts with a view to changing their attitude, but I am afraid I am making only very slow progress. … I am sure that their attitude is indefensible, but I do not wish to jeopardize my liberty in proving that it is.

William knew he was qualified to write the monograph, but he recommended finding someone else who had "never been in government service in a professional cryptologic capacity." He said that the project needed to be done in the furtherance of national security (i.e., to train a new generation) despite what the "authorities" thought. He found himself directed by "officials who were either so obsessed with security that they would hardly let him talk to his own wife" (herself an expert cryptologist) "or so pig-headed that they failed to use the priceless intelligence he provided."

The Price of Keeping Secrets

Keeping so many secrets took a great toll on William's health, both mental and physical. On the morality of reading other people's mail, he wrote: "I have often wondered whether a good portion of my psychic difficulties over the years are not attributable in part, at least, to that ambivalence." Having been asked whether it was necessary to be insane in order to be a cryptographer, William quipped to the Swedish cryptographer, Boris Hagelin, "it is not necessary but it helps." John Friedman felt his father's depression arose from being "continually put down and ripped off by his superiors." He was a man torn between wanting to leave a historical record, and not wanting to break his oath to his government.

Of all the petty humiliations William suffered, one of the worst, as far as the Friedman family was concerned, was the gutting of his library. The

Elizebeth Friedman being interviewed

"Restricted" classification used during World War II had been lifted by Executive Order No. 10503, effective 15 December 1953. This meant many of the items in the Friedman Collection could be made public. However, five years later DoD Directive 5200.1, dated 8 July 1957, raised all material related to cryptologic systems previously classified Restricted to the higher level Confidential. William did not even know about the DoD directive until told by NSA. He wrote in a document dated October 22, 1969, "What to do about those early writings of mine which are still held in the vaults of the NSA and copies of which I was not permitted to retain? I have practically given up hope of being able, at long last, to get those things released so that they might be integrated with the things included in my gift to the Marshall Library." All of the old Signal Corps Bulletins were affected, and William was unable to republish some of his earlier articles on topics such as the Zimmermann Telegram. The law also applied to his *Elements of Cryptanalysis* and his technical brochures.

William was not a great fan of the classification system used by the U.S. government. In Item 1102, for example, he cites an article on cryptography in the American Civil War that was marked "Unclassified" and yet an article on cryptography in Greek and Roman times was labeled "Restricted"! Why NSA would classify codes from World War I was incomprehensible to him. He wrote in Item 1405.1 that "the days when hand ciphers were all that were available are gone." Automation in cryptography had been used for over a dozen years when he wrote those words. "Even the smallest nations," he said, "don't care a fig about them." Yet the NSA hung onto all of the material. It seemed bizarre that NSA took copies of certain books from the Friedman Collection, and yet they remained available in the Mendelsohn Collection and from the Library of Congress. [See Editor's Note page 26.]

The Last Days

Throughout the 1960s the Friedmans kept up an active social life. William invented progressive dinner parties in which each part of the meal was at a different restaurant and the diners had to break a code to determine the next destination; the first team to make it home won a prize. William hosted musical evenings at which he played the violin and Lambros Callimahos played the flute. He spent time relaxing with his grandchildren and traveling. After surviving three heart attacks, on Sunday, 2 November 1969, William Friedman died quietly in his home and was buried with full military honors in Arlington National Cemetery. Elizebeth finished her career working for the IMF setting up a secure communications system. She oversaw the systematization of the Friedman collection and its transfer to the Marshall Library in 1970 and gave a number of interviews.

The Friedmans' gravestone at Arlington National Cemetery; it bears Bacon's axiom from their early Riverbank days, "Knowledge is power," and the flags and torch of the Army Signal Corps.

The Friedman Collection

William Friedman was always meticulous in keeping his office work secret. All the while he was working for various government agencies, his hobby was collecting anything he could find in print about cryptography ancient and modern. Much of what William did in his work is still classified, so I am talking primarily about his hobby, not his profession. There is precious little about his work in his library. In their retirement, the Friedmans continued to collect books, articles, papers, and curiosities: The 1,500 descriptive cards sent with the collection to the Marshall Library in 1966 show a full range of opinions on a variety of subjects. The collection even has embedded in it other people's collections. Among the people he worked with in World War I was Charles J. Mendelsohn, who had worked with Yardley in the Black Chamber solving German codes. Mendelsohn went on to become the greatest collector of literature on cryptography. He died prematurely in 1939, and William was named his literary executor. One of the most important segments of the Friedman Collection is the Mendelsohn papers, including the long correspondence and collaboration with William and copies of works that are housed in the Van Pelt-Dietrich Library at the University of Pennsylvania. The papers include cryptic remarks between the men about the Holocaust and William inheriting his father's *tefillin* (Jewish religious paraphernelia used during daily prayers) when he died.

William tried his hand at inventing games like "The Game of Secrecy" or "Spy and Counterspy," which he tried out on his son John. The game used certain elementary principles of cryptanalysis. The proposed game, simple in its operation as far as William was concerned, was too complex to interest game manufacturers like Milton Bradley in the 1930s.

The Collection contains cryptographic devices ranging from an actual Engima machine and the M-209 down to the promotional "cipher devices" given away by cereal manufacturers to children. Among them were the Captain Midnight cipher device, a Sky King Spy Detecto Writer, a Chex Agent, Little Orphan Annie Ring, and "A Space-O-Gram" birthday card which sent coded messages. It was received from Lambros Callimahos on 24 September 1956, William's 65th birthday.

William was interested in literary ciphers. The collection has works by and about Edgar Allan Poe, Jules Verne, and Casanova. His former World War I colleague, J. Rives Childs, retired from the U.S. Foreign Service and occupied much of his time in later years researching Casanova. In 1960 Childs asked William to write an article for his journal, *Casanova Gleanings*, which was published in 1961, called "Jacques Casanova, de Seingalt, Cryptologist."

William collected books on coded limericks and literary curiosities like a novel that did not use the letter *E*, the most common vowel in English. The collection has a book by Etienne Bazeries, the famous

French cryptographer, on specific ciphers in the correspondence of Louis XIV identifying the Man in the Iron Mask.

William was responsible for debunking numerous hoaxes. Among these were the Kensington Stone, discovered by Olof Ohman, a Swedish immigrant from Douglas County, Minnesota, while digging on his property in August 1898. It supposedly contained runic inscriptions that led some people to believe Scandinavians had explored that state in 1362. The stone later proved to be a forgery, although there are still amateurs who believe in its authenticity.[51] Other hoaxes include *The Beale Papers* that supposedly contain the secret map to a treasure buried in 1819 and 1821 near Bufords in Bedford County, Virginia, and which has never been recovered.[52] The Piltdown Forgery, an archaeological hoax launched in 1912, claimed to be the missing link to early human evolution. However, it was exposed in 1953 as a forgery, consisting of the lower jawbone of an orangutan that had been deliberately combined with the skull of a fully developed modern human.

Many professionals wrote to William with codes that needed to be solved. He helped the prison warden at Ohio State Penitentiary decrypt coded messages between inmates and their cohorts outside the prison planning a breakout. Some of the people who wrote to William with evidence of secret messages, however, came from St. Elizabeth's Hospital for the mentally ill in Washington, DC, and the letters were kept in the "nut file."

Some codes could not be broken at the time, but have since been cracked. William worked for years on Mayan glyphs and was convinced that Soviet linguist Yuri Knorozov was wrong in his theory about how to read them. Knorozov's work was in Russian and embedded in thick Marxist rhetoric. There was no way a cold warrior like William Friedman was going to admit the Russians were right. In the end, however, Knorozov's system became the key to reading ancient Mayan inscriptions.[53] (Other ancient languages and

The Mayan glyphs,
a long-term project of William Friedman

inscriptions kept their secrets. We still cannot read Linear A, Etruscan, the Phaistos Disk, or the Sator Rotas Square.[54])

The most enigmatic problem William worked on was the Voynich Manuscript. The Friedman Collection contains his earliest IBM computer printouts and the tape of one of his lectures on the subject. In 1962 he was working with RCA, which has the tapes in which he explains his solution, or at least the closest he would get to a solution. (We do not have the tapes.) The Friedman Collection also contains the papers and notes of Father Petersen, who spent his career trying to decipher the manuscript. To date, no one has yet deciphered this work, now housed at the Beinicke Library at Yale.

William collected copies of historical codes, including examples from Benedict Arnold, the Dreyfus Affair, British codes from the American Revolution, Monroe's cipher, and the Burr conspiracy. Some of these items are unique. He saved seven of the eleven cipher books used by the Federal Army in the Civil War. These books came into his possession by accident. They were about to be burned by personnel of the Old Records Division of the Adjutant General's Office, Munitions Building, because they were considered of no use or interest. William just happened to be walking by and saved them from the fire.

As brilliant as William was in the field of code-breaking, when it came to modern art or poetry, he was a traditionalist with a major blind spot. The writings of James Joyce and Gertrude Stein were incomprehensible to him. He lumped all such works together into a category he called "The Cult of Unintelligibility."

Gentleman Cryptographer

William was, as his son John described him, "a charming old-world type." To some people William came across as stiff and overly formal, but this was because he had a very strict sense of decorum. He wrote in a letter dated 8 June 1950 that he had never been back to a college reunion at Cornell. He said he wanted to wait for his 50th reunion to return because by then "I would imagine the boys would have settled down and gotten over certain jejeune ideas accompanied by juvenile behaviorisms."

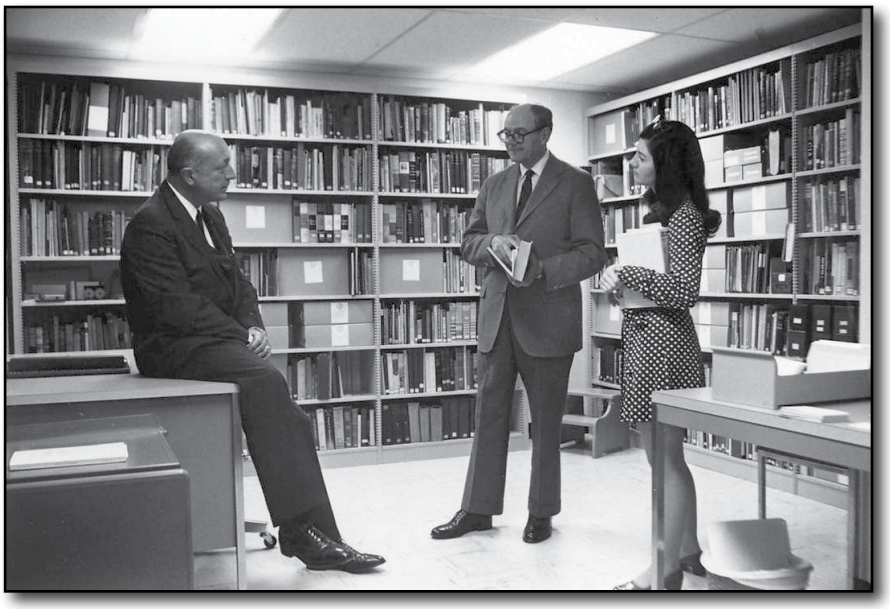
No doubt some of his psychiatric problems sprang from the knowledge that the government to which he had devoted his professional life was doing things he considered morally wrong. He did not like the trend toward polygraphing. He didn't like America spying on its allies, and he did not like wiretapping and electronic eavesdropping on American citizens. He was horrified when the Cambridge spies, Guy Burgess and Donald McLean, defected. He thoroughly disapproved of Joe McCarthy and the witch hunt he started. William and Elizebeth were both people of staunch principles. They described McCarthy as "a man who flouted the authority of the Senate, who overrode the Constitution while his followers cheered. Outside of America he was a gift to Russian propaganda" (see Item 1642). They did not like seeing minorities mistreated, and they hated the way Alan Turing was treated.

The one thing you did not question was William's honesty or integrity. A president of the American Cryptogram Association (R. R. Hammel, alias Hi-Fi) asked William to prove his statement that the Beale papers were a hoax. He accused William of suppressing the information to "discourage competition" or just because he was "incapable of solving it." William sent Hi-Fi a blistering letter in which he responded "with considerable annoyance and irritation" saying he considered himself under "no obligation to explain his opinion to anyone" and that he deeply resented the unwarranted and insulting implication that he was after money or that he was incapable of solving it. He went on to say that he had not worked on the Beale papers for more than twenty years except to deposit inquiries into his junk file, and that if Hi-Fi wrote to him again, that's where his letters would go! Then he gave Hi-Fi permission to publish his letter in *The Cryptogram* if he so desired. The conspiracy theory that William had an original copy of the Beale pamphlet published in 1885 was nonsense. There were many reproductions of the so-called "pamphlet," all of them with minor variations.

Both Friedmans could be scathingly critical of people they considered amateurs in cryptology or cryptologic history. They had nothing against such "amateurs" as long as they worked with open sources. What they didn't like were people who got the history wrong—like Ladislas Farago, whose book *Burn After Reading*, William suggested should have been titled *Burn Before Reading*.[55] Their reactions could range from a simple dismissive comment to a charge of "derangement" (see Item 1382) on the part of someone who claimed to have the solution to a cipher but did not use "scientific method." The Friedman Collection is littered with references to people whose method for deciphering some detected code was "subjective and arbitrary." When not getting a response that pleased them from William, these people would write to Elizebeth and she would tell them sweetly, "You don't need two opinions from the same family!"[56] The Friedmans had to deal with people whose convictions had more or less morphed into a belief system. One can see William's delicate sentiments when he said "one must be rather careful, in order to avoid subjecting them to needless shock."[57] Even when he writes that he had to be "pretty tough about

it" with someone, he was still always a complete gentleman. William was pursued relentlessly by people with pet theories. He wrote that, "these chaps take a good deal out of me because I cannot avoid a deep sense of sorrow in witnessing the breaking of a man's mind. I vow I will swear off seeing any more of these fellows." He was also annoyed by people who tried to pry information out of him that he had sworn to keep secret.

One reason I am fascinated by William Friedman is that very personality. As a life-long researcher, I am always grateful for access to people's personal libraries and the treasures they hold. William was an avid collector, a wide-ranging scholar and a polyglot. It has been my great pleasure to help in making the Friedman Collection more accessible to scholars everywhere.



The Friedman Collection, February 1971. L to R: Lieutenant General Marshall S. Carter, Foundation president; Dr. Forrest C. Pogue, director; and Nan Pascal, library research assistant

In our modern age of antiheroes, reality TV personalities, and an ever-present deluge of vulgarity on the airwaves, it is nice to contemplate someone who remained a true scholar and gentleman.

Some people found his sense of uprightness and honesty overbearing. President of CBS News Fred Friendly said that William had a ruthless, almost mathematical honesty. He never swore and he didn't allow his children to. In spite of his great achievements, he still remained exactly as Herman Wouk, the Pulitzer Prize-winning novelist, described him: "His effect on world history was incalculable, greater than kings and captains. Yet what a modest man."

In a world of moral ambiguity and relativism, William had a clear vision of the difference between right and wrong. He could also keep a secret—another lost art. He never revealed what he did for the government. It pained him greatly when he thought the government did not trust him. He was accused of discussing government work with his wife, but there is no evidence he ever did.[58]

William refused to ever take the easy way, and in an age where "near enough" seems to be considered a high standard, it is nice to read about a man who did not cut corners. He was truly a giant in his field and a hero whose work saved the lives of countless Americans and their allies. He should be remembered for "his unflagging dedication to his country's welfare and his unshakeable integrity."

The Future of the Friedman Collection

Although I knew of William Friedman's collection before coming to Lexington, not until I came to the Virginia Military Institute and had reason to go looking for a book in the Friedman Collection did I realize the collection was barely catalogued, that it had remained relatively untouched for thirty years, and that many items were missing. I decided there needed to be a guide to the collection. I was

fortunate to get a sabbatical leave during which I worked at the Marshall Library, and five years later we uploaded the guide onto the website of the Marshall where it is now available to everyone. As a historian, I am in the "information disseminating" business, not in the "classifying information" business like the Friedmans. Open access to historical knowledge matters to historians, especially when giving credit to the men and women who labor in secret on their country's behalf. People think that "full disclosure" means that intelligence historians want to know only about the failures being covered up. But it can also mean giving credit where credit is due. And since almost fifty years have passed since William's death, it may be time to look at some of the documents that trace his career.

Cataloguing the Friedman Collection has been a labor of love. My goal has been to reconstruct the original collection by finding replacement copies of lost open-source articles and books, and trying to "liberate" from the NSA the material taken so many years ago and which no longer needs to be hidden from the public. I am eternally grateful that Forrest Pogue's attempt to sell the Friedman books, referred to in a letter of 7 September 1970, failed. The Friedman Collection is in Lexington as a bequest to future generations of scholars and students from the Friedmans. I hope that we can augment it from time to time with newly released material from government archives.

Editor's Note

After this article was written, the NSA Archives finished its lengthy processing of declassified William Friedman documents, released thousands to the National Archives in College Park, MD, and posted them on NSA's website (nsa.gov, Public Information, Declassification and Transparency, William F. Friedman Collection of Official Papers).

Notes

1. I wish to thank Kent Sieg and the Center for Cryptologic History for their invitation to deliver the Schorreck Lecture at NSA May 24-26, 2011. My thanks also to Paul B. Barron, director of the Library and Archives, and Jeffrey Kozak, archivist and assistant librarian of the George C. Marshall Library, for all their help in preparing both my talk and this article.

   All pictures from this article come from the Friedman Collection and are published with the permission of the Marshall Library. I am grateful for the editorial help received from Jeffrey L. Aubert and Michael B. Phillips, my two favorite World War II readers.
2. Center for Cryptologic History, *The Friedman Legacy: A Tribute to William and Elizebeth Friedman*, Sources in Cryptologic History No. 3, Fort George Meade, MD: National Security Agency, third printing, 2006.
3. Although the Friedman Collection has his Sigma Chi pin, he was awarded this as an alumnus because of his work in cryptography. This was only after having been rejected once because Cornell did not teach "that particular science." His son, John Ramsay, also graduated from Cornell in 1950.
4. Ronald Clark, *The Man Who Broke Purple* (New York: Little, Brown, 1977), 7.
5. In correspondence between G. B. Curtis of Lehigh University (who had previously done code work in the American Expeditionary Forces) and William Friedman, she is referred to as "intelligent, high-minded and honest—but dead wrong." Another letter of 30 January 1952 says, "both Fabyan and Mrs. Gallup are dead and there is no validity to the biliteral cipher."
6. Friedman Collection Item 5; John Kidder Rhodes, "He Solves the Secrets of Cipher Writing," *The American Magazine*, 99 (January 1925), 37-39, 60-62; David Kahn, *The Codebreakers*, ch. 12, 371-374; Clark, *The Man Who Broke Purple*, 27.
7. Clark, *The Man Who Broke Purple*, 27; on the solution to the code in this picture, see William H. Sherman, "How to Make Anything Signify Anything," *Cabinet*, Issue 40, Winter 2010/11. www.cabinetmagazine.org/issues/40/sherman.php.
8. Clark, *The Man Who Broke Purple*, 21.
9. See letter to Elizebeth Friedman dated January 6, 1919.

10. The Friedman Collection contains a number of articles on cryptography by J. Rives Childs, including "The History and Principle of German Military Ciphers 1918," Part I, ch. 1-6, 1-110.
11. See Item 150.2, Parker Hitt, *The Star Cipher*.
12. See Item 43, Frank Moorman (Major USA), *A.E.F. Special Transposition Cipher*; and Item 150, Parker Hitt (Captain of Infantry, USA), *Manual for the Solution of Military Ciphers* (Fort Leavenworth, KS: Press of the Army Service Schools, First edition, 1916), 101.
13. On the anti-Semitism in the 1920s and the inability of Jews to get hired by any major employer but the government, see Stephen Budiansky, *Battle of Wits* (New York: The Free Press), 32.
14. Clark, *The Man Who Broke Purple*, 41.
15. Ibid., 61.
16. Ibid., 60.
17. Ibid., 61.
18. For a more detailed description of the duties of William F. Friedman's office in the Signal Corps, see Stephen Budiansky, *Battle of Wits*, 32-33.
19. See David Kahn's comments in *The Codebreakers*, 370. Cf. David Alvarez, *Secret Messages: Codebreaking and American Diplomacy 1930-1945* (Lawrence, KS: University Press of Kansas, 2000), 66-67.
20. Stephen Budiansky characterizes Yardley as follows: "He drinks a great deal and is obsessed with two topics: sex and a violent hatred for William Friedman." For a more sympathetic view of Herbert Yardley, see David Kahn, *The Reader of Gentlemen's Mail* (New Haven, CT: Yale University Press, 2004): "Their motivation differed fundamentally. Yardley sought money; Friedman knowledge. Friedman was driven not by egoism but by intellectual curiosity," 91. See also David Alvarez, *Secret Messages*, 66-67.
21. On the dissolving of the Black Chamber, see Budiansky, *Battle of Wits*, 31.
22. Clark, *The Man Who Broke Purple*, 76. On the Coast Guard's activities against the rum smugglers, see Commander Malcolm F. Willoughby, *Rum War at Sea* (Freedonia Books, 2001).
23. Clark, *The Man Who Broke Purple*, 82.
24. Ibid., 80.
25. On William F. Friedman's pleading for the IBM machines, see Budiansky, *Battle of Wits*, 211-212.
26. For a more detailed account of the team's efforts, see David Alvarez, *Secret Messages*, 81.
27. Ibid.
28. Budiansky, *Battle of Wits*, 175; Clark, *The Man Who Broke Purple*, 120.
29. I have been told by oral communications that the Coast Guard records have been declassified, but the Marshall Library has not yet acquired copies.
30. Item 1124 in the Friedman Collection is an article: Anonymous, *The Case of the Doll Woman—Velvalee Dickinson. Japanese Spy; only woman to spy for the Japanese and arrested in World War II.* Correspondence and article in *Liberty Magazine*, 16 December 1944.
31. The Friedman Collection contains a series of audio tapes made by Elizebeth Friedman about her life with William and her career in cryptography. In them she provides many of the quotations used in this article.
32. The Japanese foreign ministry developed coded "Winds messages" to be used as an emergency method to alert Japanese diplomats abroad that relations between Japan and the U.S., Great Britain, or the Soviet Union were about to take a downturn. The diplomats could then destroy cryptographic materials or sensitive messages. One method involved placing innocuous-sounding phrases about the winds in weather forecasts transmitted by short-wave radio.
33. Laurance F. Safford, Captain, USN, *Statement Regarding Winds Message by Captain L.F. Stafford, U.S. Navy before the Pearl Harbor Attack*, S. Con. Res. 27, 25 January 1946.
34. See Richard J. Aldridge, *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* (London: Harper Press, 2010); Budiansky, *Battle of Wits*, 174; *Idem*, *Bletchley Park*, 220.
35. On Arlington Hall, see Budiansky, *Battle of Wits,* 226.
36. For more detail on the machines and the declassification processes, see Kahn, *The Codebreakers*, 390-392.
37. In a letter dated 30 March 1958 he wrote to a friend, Max Bowers, that exercise was good for

avoiding coronaries. He said, "hard work and mental strain never brought on a coronary occlusion."

38. In a letter of August 8, 1956, he notes having "a kidney infection" after the heart attack and also having been fitted for dentures.
39. From a Peter Bayne letter dated 15 September 1955: "Personally I cannot feel that you are retired. I do not suppose that you are going to stop studying and thinking about cryptography. The only difference being that you can now do it in the quiet comfort of your study at home instead of amid the distractions of the Agency."
40. Letter of Peter Bayne to William F. Friedman quoting Archibald Gill.
41. Two were so secret the patent applications had never been filed. Four were held in secrecy in the Patent Office, three pertained to the M-134G rotor machine and one to the M-228 converter. See Kahn, *The Codebreakers*, 391-92. Safford got $100,000 in 1958 and Frank Rowlett a similar amount in 1964.
42. See Frank B. Rowlett, *The Story of Magic: Memoirs of an American Cryptologic Pioneer* (Laguna Hills, CA: Aegean Park Press, 1998).
43. He hated the title chosen by Cambridge University Press because he said it implied there were Shakespeare ciphers to be examined. His original title was "The Cryptologist Looks at Shakespeare."
44. See *TSCE*, Item 1691.
45. Clark, *The Man Who Broke Purple*, 185-89. The exact nature of the arrangements made in these "neutral countries" has never been made public. The exact nature of his arrangements with Boris Hagelin is also obscure. Their correspondence was removed from the Friedman Collection. By 1975, NSA was still involved in subverting the next range of Crypto AG machines. See Aldridge, *GCHQ*, 214.
46. Ronald Clark says it was because they were both neurotic. I don't think depression is a good basis for a friendship.
47. Clark, *The Man Who Broke Purple*, 189.
48. Even during his military service he was not allowed to put his name on documents he had written. When an edition of *Elementary Cryptanalysis* was published in 1939, the War Department forbade the use of William F. Friedman's name on the text that would later make him famous. He was only allowed to sign it "LTC Signal Reserve, principal Cryptanalyst." In a letter dated October 29, 1958, to William Friedman a member of the ACA said that the classifying of the ADFGVX cipher was stupid. "German military ciphers from [World War I] are *ancient history*." Most members of the ACA already had copies when they reclassified them. The Library of Congress (LC) had copies on their shelves, but when a request was put in for them in October of 1955, LC replied that "we will not give you a Xerox until the NSA says we can." NSA took the material off the shelves at LC.
49. Letter dated April 10, 1962.
50. Letter dated January 26, 1953.
51. See, for example, Alf Mongé and O. G. Landsverk, *Norse Medieval Cryptography in Runic Carvings* (Glendale, CA: Norsemen Press, 1967), 224 (Item 1157). For criticisms of her work, see Aslak Liestol, "Cryptograms in Runic Carvings–A Critical Analysis," *Minnesota History* (1968), 34-42, who points out, among other things, that certain markings on the stones they discuss were the result of working from bad xerox copies, and do not appear in the original inscription. See also Hans Karlgren, "Review of Mongé and Landsverk," *Scandinavian Studies* (1968), 326-330, who reviews the work that proved the Kensington stone a forgery and dismisses Mongé and Landsverk as a couple of amateurs. Most recently (November 2005) appeared *The Kensington Runestone: Compelling New Evidence* published by Richard Nielsen and Scott F. Wolter.
52. See Friedman Collection Item 518; http://bealetreasure.net/. Clark, *The Man Who Broke Purple*, 91.
53. Knorozov, Yuri V., selected chapters from *The Writing of the Maya Indians*, Cambridge, MA: Peabody Museum, 1967, 152.
54. On the Rotas Square, see R. M. Sheldon, "The Sator Rebus: An Unsolved Cryptogram?" *Cryptologia* 27, 3 (July, 2003), 233-287.
55. The Friedman Collection contains an autographed copy of Kahn's *The Codebreakers*, heavily annotat-

ed by Elizebeth S. Friedman. William F. Friedman never deigned to review it.

56. Letter of June 27, 1939, to a woman who believed she had found an inscription carved into a rock in Roman letters on Andros Island in the Bahamas that proved Baconian authorship!
57. Letter dated October 27, 1938.
58. The director of Military Intelligence himself accused William and Elizebeth of talking shop at home. William was surprised not only at the accusation but at the vehemence of the attack on him and his wife. They maintained a Trappist silence about their professional work. He later quipped that he was so taken aback he forgot to ask the general's permission to sleep in the same room and/or bed with Elizebeth Friedman.

Col. Rose Mary Sheldon is a professor of history at the Virginia Military Institute in Lexington, VA. She has a Ph.D. in ancient history and has written widely on intelligence and espionage in the ancient world. She also is the author of the guide to the Friedman Collection at the George C. Marshall Research Library in Lexington.

"Everyone's Ideal": William Bundy at Bletchley Park

Kent G. Sieg

The "Wise Men" were a group of venerable and trusted figures from industry, the military, politics, and the public sector who unofficially advised U.S. presidents on foreign policy over many decades during the last half of the twentieth century. Although an active government official during much of this time, William Putnam Bundy rightfully has been considered a junior member of this influential group. Notably, he was assistant secretary of state for Far Eastern affairs during the height of the Vietnam War, and following that was the long-time editor of the prestigious journal *Foreign Affairs*. Although he did hold seminal policy-making positions, in comparison with the giants of statesmanship represented in the Wise Men group, "Bill" Bundy was far less well known.[1]

While overshadowed by his supporting role in administering the difficult war in Southeast Asia through three presidential administrations, Bundy's accomplishments much earlier in his career may have had far more historical consequence. Not only had he cut his teeth as a military cryptologist, but he had played a key role in shaping the Allied signals intelligence (SIGINT) relationship while stationed at Bletchley Park in Britain during World War II. For that impact alone, history should hold a special place for him, and this article hopes to serve as a means of buttressing that assertion.

William Bundy was born on 24 September 1917 into a wealthy and socially elite eastern establishment family. His father, Harvey Bundy, had clerked for Supreme Court Chief Justice Oliver Wendell Holmes and had served in several White House administrations and in high-level posts within the Treasury, State, and War Departments. Harvey could count among his many friends the aged but energetic two-time Secretary of War and former Secretary of State Henry Stimson. Like his father, William Bundy was a graduate of prestigious schools, including Groton School, the preparatory school in Massachusetts, where he ranked at the top of his class, and Yale University, where he was president of its Political Union. He then completed a master's degree at Harvard University, awarded in 1940. Following a short-term job at the Library of Congress, he began studies at Harvard Law School, at this point still before America's entry into World War II.[2]

Much of the lack of popular knowledge about Bundy's communications intelligence (COMINT) contributions is a function of the penchant of those from his generation not to speak openly about the sensitive programs in which they were engaged. Only sparingly and much later in life did Bundy reveal some personal history from the war. Through such commentary we gain an insight into exactly what he did.

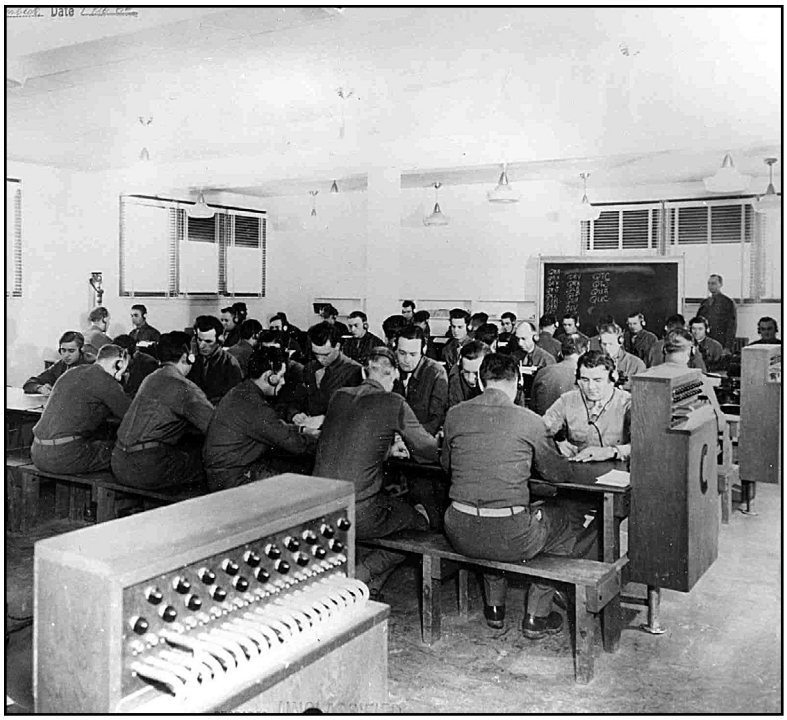
Bletchley Park mansion at the outbreak of World War II (Center for Cryptologic History files); right: Captain Bundy at Bletchley Park (from his personal collection)

Bundy realized that his time in cryptology had been the most satisfying and important of his long public service career. "It was a terrific human experience and I've never matched it since," he would comment. "I had other jobs with superb people, important and worthwhile pursuits but certainly for me personally this was the high point."[3]

It all started with his being accessioned into the U.S. Army during the summer of 1941. Within ten days of entering basic training at Fort Devens, Massachusetts, on August 3, he was plucked from his training course and, based on his high aptitude scores, placed into the Signal Corps. Bundy would later posit that although the aptitude tests were the sole criteria for selection, they were fairly predictive of problem-solving ability; thus the tests were necessary, as otherwise those recruits dumped into the "Crypt School" would continue to be persons "who had no visible talent or aptitude whatsoever for electrical work, or communications in the technological sense." Bundy's score on the Army General Classification Test was a previously unrecorded 161, with 162 being perfect.[4]

Bundy next entered the COMINT course at Fort Monmouth, New Jersey. Among his classmates was Lambros Callimahos, a flutist and later a cryptologist of great renown, whom Bundy recalled complaining that he would never be great in music again as his lip strength had deteriorated during Army training. December 7, 1941, marked a profound change in the regimen they faced. Bundy and the rest of the students immediately found themselves assigned to pack communications tapes as replacements for those lost in the Japanese attack on American stations in the Far East. Following completion of Officer Candidate School in April 1942, Bundy was commissioned as a Signal Corps officer. He immediately became an instructor for subsequent Crypt School classes, which were held at Vint Hill Farms, Virginia, and then at Arlington Hall.[5]

Beginning in early 1943, Bundy became involved with ULTRA, the government's most sensitive



Crypt School at Vint Hill Farms Station, Virginia
(U.S. Army photograph)

COMINT program, which involved decrypting and analyzing messages that the Germans transmitted on the ENIGMA cryptographic machine. Soon after Pearl Harbor, Solomon Kullback of the Signal Intelligence Service (SIS) had visited Bletchley Park, the site of Britain's Government Code and Cypher School (GC&CS), and thus had been the first American there. In succession, Captain Roy Johnson spent six months at Bletchley; Bundy would follow. Based upon the success of such tours, it was intended that a sizable number of Americans would be integrated into operations at GC&CS.[6]

The impressive young Bundy was earmarked for a principal role with this American contingent. By then an Army captain, he had been briefed by none other than notable Army cryptologist Frank Rowlett at Arlington Hall regarding "Yellow," the term used in the open to refer to the compartmentalized ULTRA program. Prior to that briefing, Rowlett had cautioned that "no one will leave this room a free man." Via a program known as Project BEECHNUT, Bundy was designated as the head of the first group of American integree codebreakers at GC&CS. "In reality, if not officially, they were guinea pigs," author Thomas Parrish has asserted, "and much attention would be paid to them by the British, by [cryptologic pioneer William] Friedman and Rowlett, and by the whole U.S. military establishment." Reportedly, Bundy was selected for this role not because of any specialized intelligence expertise but due to "his demonstrated ability and quietly effective personality, with its touch of Bostonian starch."[7]

Service as an instructor allowed Bundy to be in a vantage point to gain personal familiarity with topnotch American cryptologists. Thus, he was able to handpick his staff. Bundy was in charge of one of what became three companies sent overseas to Britain. On 4 August 1943, Bundy and the first contingent from his unit, numbering 19 men and known simply as "Shipment No. 0192-A," transited over to Scotland from Fort Hamilton in New York aboard the S.S. *Aquitania*. This Cunard liner still clung to the prewar trappings of luxury, although even the officers bunked twelve men to a state room. En route the group considered it necessary to invent a cover story, much used, that they were the Signal Corps "pigeon experts."[8]

They arrived at Bletchley Park on the day before the month ended, a date described by the unit history as that which "marked first penetration in force" by American personnel. Upon arrival in the area, the "Yanks" were placed in residence at a host of pubs and private homes in the vicinity. Originally, they formed part of the Signal Intelligence Division (Signal Section), Headquarters, U.S. Forces, European Theater of Operations. In February 1944, the companies received official unit designations, with Bundy's component becoming the 6813th Signal Security Detachment. As at Arlington Hall, troops eventually found

themselves in a former girl's school four miles to the north. On 29 March 1944, a post for them opened in the Manor House at Little Brickhill, Buckinghamshire.[9]

Ultimately, Bundy supervised nearly eighty-five Americans, including a number of scholars and professionals far more seasoned than their twenty-six-year-old commander. About twenty of those in support roles were stationed at Little Brickhill. The rest had been spread throughout GC&CS, with at least one American assigned to each of the sections in Bletchley Park's "huts." A large proportion of Bundy's troops worked ENIGMA traffic at Hut 6, the cryptanalytic section devoted to German army and air force traffic. No more than ten personnel ever ventured into Hut 3, where translation and intelligence analysis of the raw traffic from Hut 6 were performed.

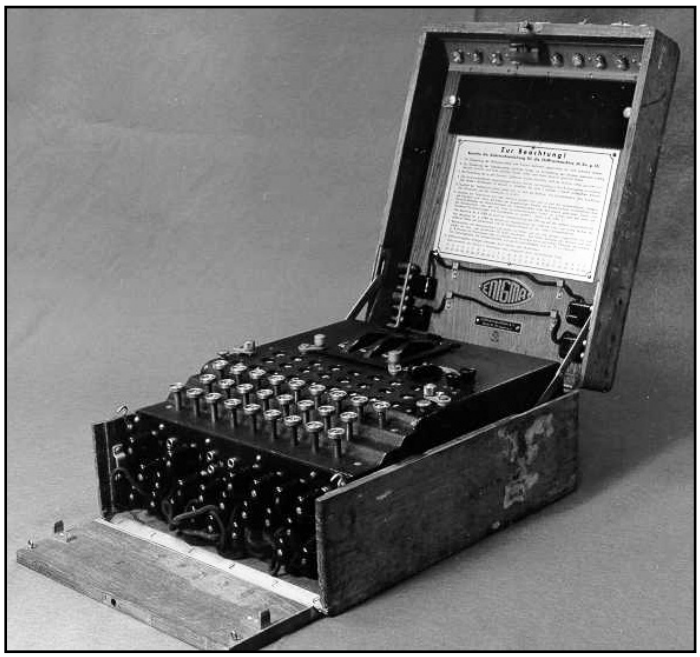
Others worked at Signals Intelligence and Traffic Analysis (SIXTA) in Hut 15 doing traffic analysis (TA). Although a "Quiet Room" maintained liaison between SIXTA and Hut 6, these operations were kept distinctly separated to ensure that TA provided its immense amount of information independently of any influence from Hut 6. A final cohort was in Block F, supporting cryptanalysis of "Fish," or non-Morse traffic on Lorenz-based cipher machines.[10]

The result of much prior wrangling was an agreement to share the task of decrypting ULTRA intercepts with SIS (later known as the Signal Security Agency, or SSA). Part of this decision was motivated by practical concerns. Due to limited numbers and the circumscribed run time of the British "bombes," much of the ULTRA material on which the Americans worked was sent back directly to SSA headquarters at Arlington Hall. American capabilities, buttressed by the nation's industrialized, automated know-how, were a great plus to the work at Bletchley. As a matter of course, solutions to such intercepts sent to Arlington Hall were often returned across the Atlantic to GC&CS within sixty to ninety minutes.[11]

Arlington Hall in Virginia during World War II
(U.S. Army photograph)

Even amongst the best of the best cryptologists, Bundy proved to be a skilled code-breaker; during orientation he had "distinguished himself at this stage by setting a new Hut 6 record for speed in the solution of the dottery exercise" (a pencil-and-paper method for determining the ENIGMA's plugboard settings). In a "complete fusion of effort," he directed all British and American personnel in his section. As a watch leader in Hut 6, Bundy was in charge of figuring out the settings used for the ENGIMA traffic by using cribs that arose, ascribing a priority to a potential result, estimating the likelihood of a given solution, and even determining which of the forty sets of German keys to try to break. It was a human capital-intensive effort, as Bletchley never acquired the labor-saving devices prevalent in American industry, compelling personnel at all levels to engage in routine mechanical activities. In spite of the complex drudgery, Bundy came to regard the setup "as near to perfect as anything I have ever been or ever expect to be associated with in a somewhat varied experience since then."[12]

In addition to operational support activities, Bundy played a role as diplomat. The importance



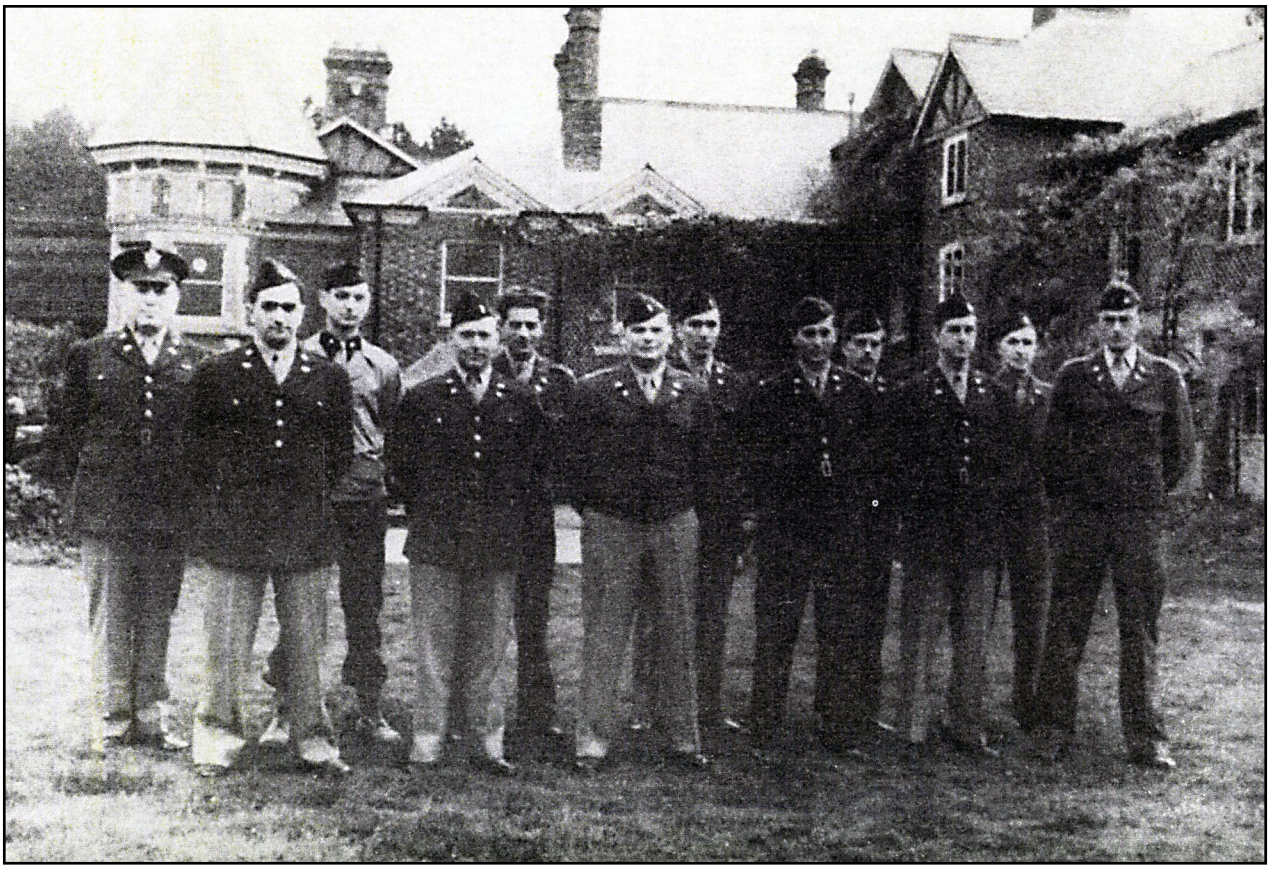
A German ENIGMA machine

of this function cannot be overstated, for as one of his subordinates later noted, "this was the first experiment in cooperating in the code-breaking business between any two countries." Tensions that might have run high had to be ameliorated, and that task formed a vital part of his job. The Americans' comparative wealth and apparent casual attitude toward operations security shocked their British counterparts and often were causes of resentment. On the other hand, the rank disparity between Americans and Brits doing the same job was great, as the British personnel were either civilians or by policy commissioned at the rank of senior lieutenant or above, while their U.S. counterparts were in most instances enlisted men—albeit specially picked—who as personnel in a U.S. Army support branch faced comparatively glacial promotion prospects.[13]

The young captain's management style personally lessened the atmosphere of pressure from carrying out such vital work. He did not insist on strict military protocol while his personnel worked at Bletchley, and he approached the vicissitudes of the duty in the context that the unit was pretty much a meritocracy. Everyone was on a first-name basis, and relative rank melted away as more experienced persons of any grade were those put in charge. The young commanding officer even championed efforts on the American side to share goods from the much better stocked U.S. post exchanges with their British counterparts. Additionally, while the Americans could enjoy themselves on the town, it was an accepted "good idea" for them to behave "in the most correct G.I. fashion for understood defense purposes" when they returned to their post in the evenings. As a result of this delicate oversight, Bundy was quite effective in imparting a sense of seriousness regarding security that dispelled some not-unfounded British concerns. Much potential discord was lessened simply by his individual direction.[14]

In short, Bundy was a leader much appreciated by his subordinates because he took care of them. He followed the British model and directed that U.S. personnel receive nine days of leave every three months, plus a free day here or there during the week. When the theater commander issued a prohibition against any leave beyond three days, Bundy, realizing his men greatly benefited from the rest and relaxation, came up with a way to work around it. He simply instructed his troops to send an extension request based upon an unexpected catching of any mild illness, including frequently the common cold, which would allow time for medical attention. He managed to maintain allotments of field rations for his desk-bound troops so that they had enough meals and snacks to keep them attentive. He even authorized a marriage of one of his officers even though it did not meet regulations. Further, the youthful leader supported diversions such as the organization of musical and theatrical groups from among his people. The groups performed so well that he and many others were genuinely convinced that his subordinates were talented enough at least for off-Broadway.[15]

The youthful American officer himself was extremely impressed by what he encountered at Bletchley Park. Bundy actually first offered a glimpse



Captain Bundy (far right) and his men at Bletchley (U.S. Army photograph)

into Bletchley's world in a 1959 classified article he wrote for a Central Intelligence Agency journal. He described in somewhat understated but nevertheless glowing terms the functioning of GC&CS:

> During the last war I was at a place called Bletchley in England. There, in three low brick wings of the same building, side by side—called, poetically enough, "huts"—were housed respectively a final producer apparatus, an intermediate processing apparatus, and a collection control apparatus. They were within easy walking distance, and the people in them knew each other by their first names and had been in their jobs long enough to have quite a knowledge of each other's problems. The result was a tremendously efficient collection operation, which balanced intelligence priorities and needs fully against the need to maintain assets for stand-by purposes, and all with what was—even by British standards—a minimum of red tape. As I recall, the weekly so-called control meeting used to take about an hour to dispose of all its business, including discussion and action on new ideas. I had never seen anything like it.[16]

In turn, GC&CS was just as impressed with him. Gordon Welchman, who was in overall charge of Hut 6, described Bundy, who headed the watch team there, as "a major contributor to the key-breaking achievements." Stuart Milner-Barry, also a key figure in Hut 6 for the entirety of the war, recalled that "No more admirable representative of our great new ally could possibly have been selected." According to

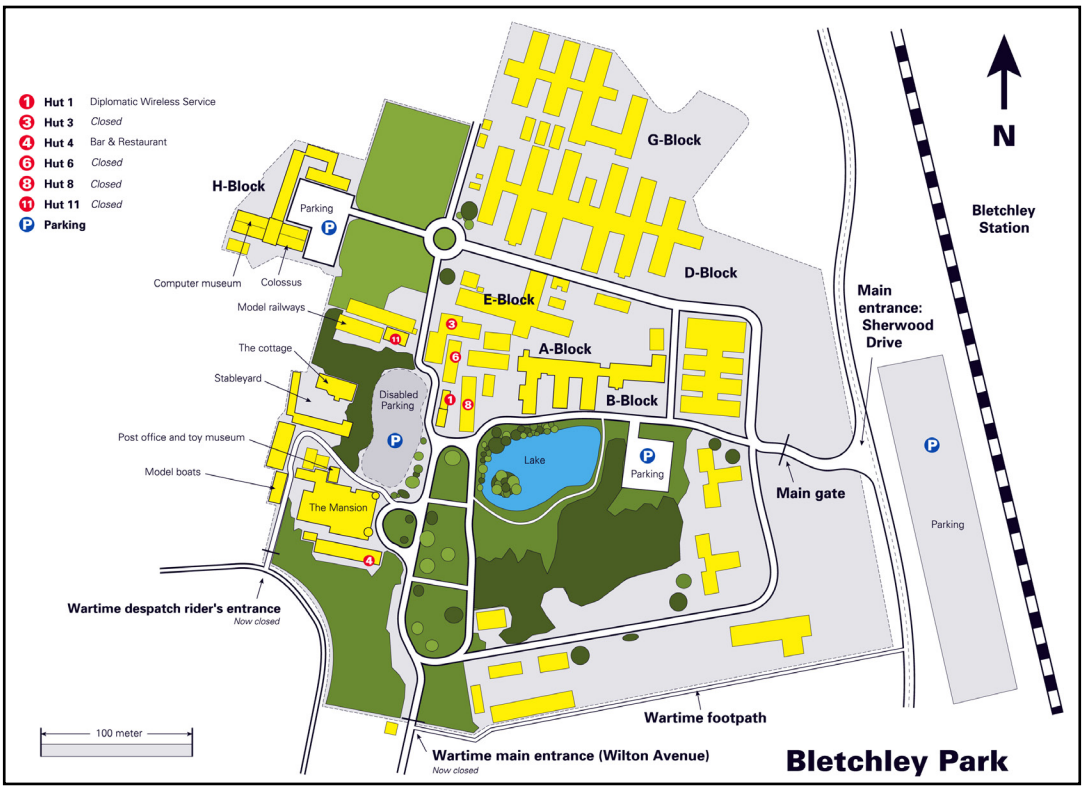
Hut 6 at Bletchley Park: (l) during World War II and (r) after the war (before restoration)

Derek Taunt, yet another influential Brit from Hut 6, Bundy was regarded as "everyone's ideal of the New England gentleman, tall, slim, handsome, fresh-faced, and courteous." Indeed, the U.S. troops circumspectly followed their commanding officer's example, and thus almost always appeared to be both modest and eager to help out. Consequently, the Americans rather easily integrated with and directly into the British staff. However, interaction by custom was minimal beyond one's assigned section. During his two years in England, Bundy, like most of the men in his unit, had minimal contact with British or even American personnel outside his area of oversight.[17]

Because once personnel were detailed to Bletchley they could not transfer, like his men Bundy remained there through the end of the war. They performed admirably, including providing invaluable service during D-Day. However, one hiccup occurred as the Battle of the Bulge raged in December 1944. Unlike as was done in previous operations, the Nazis chose to rely primarily on landlines for their tactical communications. That fact meant that the Bletchley codebreakers failed to discern indicators of the coming offensive in wireless traffic. With this exception, the intelligence flow from GC&CS continued unabated afterwards.[18]

The U.S. Army detachments at Bletchley began leaving Bletchley Park en masse soon after V-E Day. Their departure caused their British counterparts to openly lament. "I cannot let the American contingent pass from Hut 6 without trying to express, however inadequately, my sense of the debt which I myself and my colleagues owe to you," Milner-Barry wrote to Bundy on 10 May 1945. Along with the rest of the American personnel, Bundy received orders to prepare for transfer to the Pacific Theater. But with Japan's surrender and the specter of a massive invasion of the home islands ended, they were not needed in the Far East.[19]

Bundy was instead sent home, eventually being mustered out of active service on 27 February 1946. He ended the war as a major, in the process having been awarded the Legion of Merit and made a member of the Order of the British Empire. He had made a vital contribution to the war effort, one that certainly was then, and even is now, little known outside of the field of cryptologic history. The impact



Map of Bletchley Park today (courtesy the Crypto Museum)

of his leadership at Bletchley was felt long afterwards and in fact was often cited as seminal in the evolution of continuing cooperation among the Allies. In the words of one of the former soldiers serving there who later became a senior manager in the National Security Agency (NSA), the postwar Anglo-American relationship "got very thick indeed" as a result of the close wartime association Bundy had done so much to engender.[20]

Not widely understood is that Bundy's entire family had an important measure of involvement in cryptology during World War II. Like William, his younger brother McGeorge Bundy also graduated from Yale. Although saddled with poor eyesight, the younger brother memorized the testing chart in order to join the Signal Corps—just as his older brother had done! McGeorge likewise was a natural fit as a cryptologist, especially since he had majored in mathematics. He completed training at the Signal Corps school at Fort Monmouth but was not assigned to a cryptologic billet. Instead, Rear Admiral Alan R. Kirk, the Commander of Allied Amphibious Forces, chose the young Army officer—and family friend—as his personal aide. Moreover, Kirk designated McGeorge as his command's only officer responsible for using the one-time pad to decrypt ULTRA intercepts. McGeorge played an important role in providing intelligence during operations in Sicily and then assumed a similar position when Kirk was appointed commander of the Western Task Force for Operation OVERLORD, the cross-channel invasion of France.[21]

After the war, "Mac" Bundy was asked to help Stimson write his memoirs. As Stimson's ghost-writer, he had another significant impact on cryptologic history. In this capacity, he set down in print an infamous statement Stimson ostensibly made nearly two decades earlier: "Gentlemen do not read each other's

mail." Although only substantiated from a 1946 unrecorded oral history interview between McGeorge and Stimson, this statement became the stuff of legend. It would be attributed to the secretary of state as something he said in summarizing his reasoning when he withdrew funding for pioneering cryptologist Herbert Yardley, thus effectively shutting down the American Black Chamber in 1929. McGeorge Bundy later acknowledged that although Stimson had used the controversial phrase with him in preparation for the "autobiography," there is no solid evidence that it had been uttered earlier. Nevertheless, it has gone down in the annals of cryptologic lore; even Stimson came to regard it as a fairly accurate reflection of his beliefs at the time. Subsequent research has indicated that the statement may have been partly or wholly a manufacture of Yardley himself.[22]

The Bundy familial connection to the cryptology of World War II did not stop there. Throughout World War II, Harvey Bundy, who had been with Stimson at the State Department when the Black Chamber was shut down, remained the latter's principal special assistant. In this capacity, his purview ranged over the most important War Department programs, to include the Manhattan Project, and he accompanied the secretary of war to the most important Allied strategy conferences. He also oversaw the management of the military COMINT program including ULTRA, read all of the MAGIC intercepts of Japanese communications, and personally helped to arrange the divisions of labor between the American and British cryptologic organizations against the Germans. A significant aside: while clerking at the Supreme Court, Harvey Bundy had served alongside and come to know well Alger Hiss, the infamous high-level traitor discovered soon after the end of the war via the VENONA intercepts.[23]

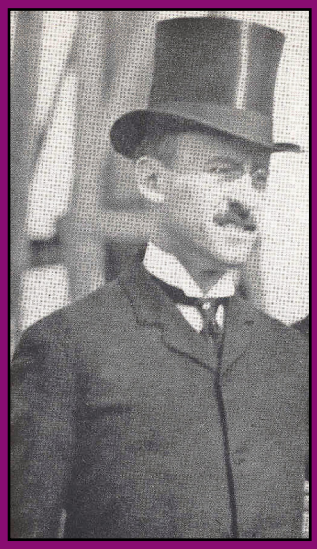
Somewhat astonishingly, William Bundy's mother similarly was engaged in wartime COMINT. With the help of her friend, the wife of the aforementioned Admiral Kirk, Katherine "Kay" Bundy became a bona fide cryptologist in her own right. Possessing a notable expertise in open codes, she worked for both the Navy's cryptanalysis office, Op-20-G, and the Army's SIS during the war. Kay Bundy was decorated for her important contributions, which included uncovering a significant security lapse: namely, that American messages sent from Central America were inadvertently alerting German U-boat submarines to the positions of American merchant shipping targets.[24]

A few more personal connections of William Bundy to cryptology are worth mentioning. At World War II's height, Bundy found time to hurriedly marry young Mary Acheson, daughter of then-Assistant Secretary of State Dean Acheson. Although just eighteen, Mary was bright and precocious. With her husband overseas and given the fervor with which the war effort was consuming her hometown of Washington, DC, she looked for employment in the military establishment. Her high potential and personal pedigree proved impressive enough that she landed a job at Arlington Hall. Like so many of the gifted young people who worked in COMINT there during the war, her varied talents would emerge throughout the balance of her life. In fact, in later decades she became an accomplished painter, and her work was featured in several significant exhibitions.[25]

Mary's father, of course, became secretary of state in 1949. In that role, Dean Acheson was a leading voice in the debate over the reform of cryptologic community. Acheson's efforts were intrinsic to the bureaucratic process that ultimately decided on centralization of cryptologic assets and capabilities outside of the strict control of the military, along with a clearly defined national mission beyond the Department of Defense. This new course for the nation's cryptologic community was epitomized in the creation of the NSA in 1952.[26]

As for William Bundy, once back home he availed himself of the G.I. bill to complete his Harvard law degree, which he was awarded in 1947. Following four years of private practice, he joined

Gordon Welchman was in overall charge of Hut 6 at Bletchley Park (Center for Cryptologic History files)



Henry Stimson as secretary of state (U.S. State Department photograph)

Former State Department official and Soviet spy Alger Hiss

the Central Intelligence Agency (CIA) as a GS-15 analyst on 26 June 1951, right at the height of the Korean War. At one point, his budding policy career was nearly derailed. During the era of Senator Joseph McCarthy's crusade to ferret out perceived communists from the U.S. government, it became public knowledge that Bundy had provided $400 in financial support to the older brother of a law partner, a man who was a venerated family friend. The recipient was none other than Alger Hiss, by then already defamed for lying before Congress but concomitantly held up as a sort of martyr against the then-prevalent Red hysteria. Luckily, various highly placed individuals, including Director of Central Intelligence Allen Dulles and later nemesis but then-Vice President Richard Nixon, rushed to defend and successfully shield Bundy from character and loyalty attacks by McCarthy.[27]

Beginning in 1951, Bundy sat on the CIA's National Board of Estimates. In this capacity, he oversaw the preparation of the crucial National Intelligence Estimate, which was the top analytical assessment of national security issues, for almost a decade. At the start of the Kennedy administration, he was appointed principal deputy assistant and then later assistant secretary of defense for international security affairs. He was eventually elevated as the senior official at the State Department for Far Eastern (later East Asian and Pacific) affairs from 1964 to 1969. He played a key role in supporting the policy of intervention in Vietnam. However, he would later express deep chagrin over both the lack of confidentiality in the divided wartime administration in Washington and the relative inability of the U.S. military to obtain the level of intelligence bounty that had existed in the effort he had been part of a generation earlier.[28]

William Bundy stayed on into the Nixon administration, providing essential overlap, but ultimately left an active role in the government on 1 May 1969, with twenty-two-and-a-half years combined federal

service. Subsequently he held several academic posts, as well as a consultancy appointment at the State Department that expired in 1972. He then became editor of *Foreign Affairs*, where he remained for eleven years. From this vantage point, he had an important impact on policy and academic circles regarding the key contemporary events in world politics. Naturally, he took special interest in often reviewing books on World War II-era COMINT operations published in the 1970s, works which for the first time publicly revealed ULTRA and other previously closely held intelligence-related programs. He passed away quietly on 6 October 2000 at the age of 83.[29]

William P. Bundy was a true Boston Brahmin, utterly embodying the most noble aspects associated with that term. He and his family members represented a long tradition of scions of wealthy, advantaged, and old-line families who, because of their providential bounty, felt morally driven to devote their energies toward politics and public service. At a time when the nation faced the specter of peril at the hands of fascist adversaries, Bundy stepped forward and made a tangible though little-known contribution to cryptology—as did the members of his immediate family. Indeed, the impact of his personal wartime role cannot be overstated. As he himself succinctly put it some thirty years after working at Bletchley Park, without ULTRA, "the chances of any Second Front whatever would have been small."[30]

Notes

1. Members included W. Averell Harriman, Dean Acheson, Robert Lovett, Charles Bohlen, John McCloy, George Kennan, Ellsworth Bunker, and Clark Clifford. See Walter Isaacson, *The Wise Men: Six Friends and the World They Made* (New York: Simon & Schuster, 1986).
2. For more perspective on the Bundy family within the context of the American patrician class and its internationalism, see Kai Bird, *The Color of Truth: McGeorge Bundy and William Bundy—Brothers in Arms* (New York: Simon & Schuster, 1998); and Burton Hersh, *The Old Boys: The American Elite and the Origins of the CIA* (New York: Scribner's, 1992).
3. Michael Smith, *Station X: The Codebreakers of Bletchley Park* (London: Channel 4 Books, 1998), 177.
4. William P. Bundy, "Some of My Wartime Experiences," *Cryptologia* (April 1987), 67; hereafter Bundy, "Wartime Experiences." Bundy also had an adequate grasp of German and French.
5. Ibid.
6. Bird, 73-139.
7. Thomas Parrish, *The ULTRA Americans: The U.S. Role in Breaking the Nazi Codes* (New York: Stein and Day, 1986), 100-102. Bundy knew Europe well, having made three long trips throughout the continent during the 1930s.
8. Bundy, "Wartime Experiences," 68.
9. "Technical History of 6813th Signal Security Detachment," 20 October 1945, sent as attachment to Memorandum from Capt. J. K. Lively to Director, Signal Security Division, 20 October 1945, Center for Cryptologic History (CCH) (hereafter 6813th Technical History).
10. (U//FOUO) American SIGINT activities in Britain during the war are detailed in Army Security Agency (ASA), *SRH-110—Operations of the Military Intelligence Service, War Department, London* (undated), CCH; 6813th Technical History; and Bradley F. Smith, *The ULTRA-MAGIC Deals and the Most Secret Special Relationship, 1940-1946* (Presidio: 1993), 165-167.
11. (U//FOUO) See ASA, *SRH-349—The Achievements of the Signal Security Agency in World War II* (20 February 1946), 29, CCH.
12. Described in the 6813th Technical History. See also Bundy, "Wartime Experiences," 70-74; Smith, *Station X*, 135; and Harold Deutsch, "The Historical Impact of Revealing the ULTRA Secret," *Parameters* (1977, Vol. VII, No. 3), 17-29.
13. See Arthur Levenson interview, CCH, OH-1980-40 (25 November 1980); see also Smith, 132-139.
14. Bundy, "Wartime Experiences," 69-72. For more on the atmosphere at Bletchley, see Public Broadcasting Service, "Decoding Nazi Secrets," NOVA, airdate 9 November 1999; "Oral History Interview with Nigel Forward," *Maybe Quarterly* (Autumn

2006); John Taylor, "Bletchley During World War Two: Everyday Life for the Townspeople & the Billeted Personnel from Bletchley Park" (Milton Keynes Heritage Association, 2007); and Christopher Grey and Andrew Sturdy, "Historicising Knowledge-Intensive Organizations: The Case of Bletchley Park 1939-1945," *Cambridge Working Paper Series* (August 2006).

15. Stephen Budiansky, *Battle of Wits: The Complete Story of Codebreaking in World War II* (New York: Touchstone, 2002), 299-302. For instances of what daily life at Bletchley was like, see Selmer Norland interview, CCH, OH-1980-20 (15 May 1980); Levenson interview, CCH, OH-1980-40; and J. H. Mann interview, University of North Carolina, Wilmington's William Madison Randall Library (26 September 2006).
16. William P. Bundy, "The Guiding of Intelligence Collection," *Studies in Intelligence* (Winter 1959), 37-53.
17. F. H. Hinsley and Alan Stripp, *Code Breakers: The Inside Story of Bletchley Park* (Oxford, U.K.: Oxford University Press, 1993), 95-98.
18. Smith, *Station X*, 168-169.
19. Excerpt of letter from Milner-Barry to Bundy, 10 May 1945, in 6813th Technical History.
20. See Levenson interview, CCH, OH-1980-40. His Legion of Merit award read: "Major Bundy was unusually successful in the accomplishment of his special signal operations requiring the highest degree of technical skill and mental concentration. Additionally, he supervised the operations and administration of a large detachment of signal specialists in most commendable fashion. Major Bundy's supreme efforts in both technical and administrative capacities were invaluable in the conduct of military operations on the continent." In addition to this award and the OBE, Bundy also received the World War II Victory Medal, the European-African-Middle Eastern Theater Service Medal with one Bronze Star, the American Theater Service Medal, and the American Defense Service Medal. He remained in the inactive reserve until resigning his officer's commission effective 21 October 1955. See his official service record at the National Personnel Records Center.
21. Barred from exposing himself to combat due to the sensitive nature of his duties, McGeorge Bundy finished the European war in relative comfort at Admiral Kirk's headquarters in Paris. Notably, though, he had managed to wrangle a transfer to an infantry unit involved in the planned invasion of the Japanese home islands. The dropping of the atomic bombs in August 1945 spared him from seeing action in the Far East. See Bird, 79-82.
22. For background on the "gentlemen" remark, see Henry L. Stimson with McGeorge Bundy, *On Active Service in Peace and War* (New York: Harper & Bros., 1948), 204. For additional details on the closing of the Black Chamber, see Louis Kruh, "Stimson, the Black Chamber, and the 'Gentlemen's Mail' Quote," *Cryptologia* (April 1988), 65-89. Interestingly, Kruh pointed out that in 1950 William Friedman, the former head of the Army's cryptography section, told Bill Bundy that Yardley had retreated from the contention that Stimson's ethical knee-jerk had been responsible for the closure. In fact, Yardley since had ascribed the termination of the Black Chamber's activities to President Herbert Hoover directly. These letters are held in the collection of Friedman's personal papers at the George C. Marshall Library; see Rose Mary Sheldon, *The Friedman Collection: An Analytic Guide* (Marshall Foundation: undated). As for McGeorge Bundy, he was so highly regarded that in spite of his young age and lack of advanced degrees he became a professor at Harvard and eventually became dean of faculty. In 1961 President John F. Kennedy appointed him assistant to the president for national security affairs. He remained as the national security adviser through the administration of President Lyndon Johnson, a tenure that included the key point of escalation in Vietnam. He left government in 1966 to become the president of the Ford Foundation, from which he retired thirteen years later; he died in 1996.
23. See Hodgson, *passim*.
24. Bird, 72.
25. Ibid., 73-74.
26. See Thomas L. Burns, *The Quest for Cryptologic Centralization and the Establishment of NSA, 1940-*

1952 (Ft. Meade, MD: Center for Cryptologic History, 2005), passim.

27. Douglas Martin, "William P. Bundy, 83, Dies: Advised 3 Presidents on American Policy in Vietnam," *New York Times* (7 October 2000).
28. "Obituary: William Bundy, 83, Vietnam Policy Aide," *Chicago Tribune* (7 October 2000). See also Andrew Preston, *The War Council: McGeorge Bundy, the NSC, and Vietnam* (Cambridge, MA: Harvard University Press, 2006); and David Halberstam, *The Best and the Brightest* (New York: Random House, 1972). See also Bundy's civil service personnel folder, National Personnel Records Center.
29. For instance, in the winter 1978-79 issue of *Foreign Affairs*, Bundy positively reviewed the books coming out on ULTRA, which he viewed as finally accurately describing "probably the most sustained intelligence success in the history of human conflict."
30. Bundy remained a respected commentator on the national scene until the end. A few years before his death, he published *A Tangled Web: The Making of Foreign Policy in the Nixon Presidency* (New York: Hill & Wang, 1998), an insightful critique of the Richard Nixon-Henry Kissinger foreign policy that was very well-received in academic and political circles.

Kent G. Sieg was formerly a historian at the Center for Cryptologic History. He holds a doctorate in history from the University of Colorado. He previously worked for the Department of State and the Army Corps of Engineers, and served on active duty with the U.S. Coast Guard.

How MODULAR ARITHMETIC Helped Win World War II

Craig Bauer

Abstract: The importance of modular arithmetic is demonstrated through an example having minimal prerequisites, namely the key role it played in SIGSALY, the top voice encryption system of World War II. It is presented here, along with the historic context, in the hope that it will be found to be a useful motivational tool for classes in which modular arithmetic is introduced.

Keywords: ciphony, Green Hornet, modular arithmetic, SIGSALY, voice encryption

Introduction

When introducing the concept of modular arithmetic, I, like everyone else, would talk about clock arithmetic and, as a second example, ask far-from-riveting questions like, "If today is Tuesday, what day will it be 1,000 days from now?" I was aware of more important applications, but they were not immediately accessible. Happily, my passion for cryptology led me to study voice encryption, and I discovered that modular arithmetic played a key role in the top system used during World War II. Even better, the concept can be conveyed quickly and requires no prerequisites.

Before getting to the heart of the matter, earlier voice encryption systems are discussed, along with the high price that was paid as a result of their insecurity.

Early Voice Encryption

Voice encryption, also known as ciphony, goes back as far as the 1920s, when an analog system was put into use by AT&T. During this decade, inverters swapped high tones with low tones, and vice versa. Expressing it more mathematically, the frequency p of each component is replaced with $s - p$, where s is the frequency of a carrier wave. The equation reveals a major weakness with this form of encryption. Namely, tones near the middle are hardly changed. So, that dull professor you remember not too fondly wouldn't be able to speak securely using an inverter, if his tone of choice was near the middle (Figure 1).

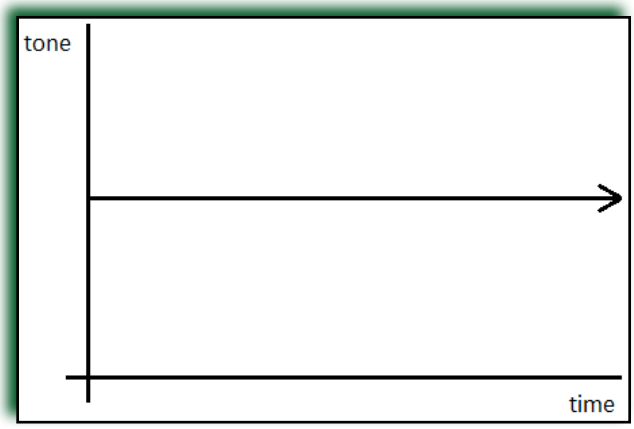


Fig. 1. Tone as a function of time for some professors

Actually, nobody could speak securely using an inverter. This system protected only against casual eavesdropping and could be easily inverted back by determined amateurs. There was no key as such, and inverters are not hard to build.

In some cases, the devices were not even needed. With practice it is possible to understand much inverted speech, even if it isn't that old professor of yours speaking.

AT&T and RCA companies offered a slightly more sophisticated scheme in 1937. Known as the A-3 Scrambler, this system split the speech into five channels (a.k.a. subbands), each of which could be inverted, and shuffled them before transmitting. However, this was still weak, and it was implemented in an especially weak manner. Since there are only 5! = 120 ways to reorder the 5 subbands and 2^5 = 32 ways to decide which (if any) of the subbands will be inverted, we have a total of (120)(32) = 3,840 ways to scramble the speech. Thus, the key space is way too small. If the attacker knows how the system works, he could simply try all of the possibilities. Even worse, many of these keys failed to garble the speech sufficiently to prevent portions of it from remaining understandable. Worst of all, of the 11 keys deemed suitable for use, only 6 keys were used! They were applied in a cycle of 36 steps, each lasting 20 seconds, for a full period of 12 minutes.[1]

Hence, like the inverters of the 1920s, the A-3 Scrambler was understood to offer "privacy, not security." A good analogy is the privacy locks on interior doors of homes. If someone walks up to a home bathroom that is in use, and the lock prevents the doorknob from turning, he'll think, "Oh, someone's in there," and walk away. Privacy is protected. However, there is no real security. Someone intent on entering that bathroom will not be stopped by the lock. In the same manner, a scrambler would protect someone on a party line,[2] but could not be expected to protect national secrets against foreign adversaries.

When President Franklin D. Roosevelt and Prime Minister Winston Churchill spoke on the phone, they needed real security, not just privacy, yet they initially used the A-3 Scrambler! It was solved by the Germans by September 1941, after only a few months' work.[3]

As the following quotes show, allies on both sides of the Atlantic were aware of the problem.

> The security device has not yet been invented which is of any protection whatever against the skilled engineers who are employed by the enemy to record every word of every conversation made. (British Foreign Office Memorandum, June 1942)[4]

> In addition, this equipment furnishes a very low degree of security, and we know definitely that the enemy can break the system with almost no effort. (Colonel Frank McCarthy, Secretary to the Army General Staff, October 1943)[5]

Given that the Americans and the British knew that the system they were using for voice encryption offered no security, it's natural to ask why they didn't use something better. The answer is that securing speech with encryption is much more difficult than encrypting text. There are several reasons why this is so, but one of the most important is redundancy. Redundancy in speech allows us to comprehend it through music, background noise, bad connections, mumbling, other people speaking, etc. Text is about 50 percent redundant (in other words, removing half of the letters from a given paragraph does not prevent it from being reconstructed), but speech is much more redundant and it is hard to disguise because of this.

Speech that is scrambled in the manner of the A-3 Scrambler can be reconstructed using a sound spectrograph, which simply involves plotting the tones and reassembling them like a jigsaw puzzle. So, although splitting the voice into more channels would increase the number of possible keys, the attacker could simply reassemble what amounts to a jigsaw puzzle with more pieces. A successful voice encryption system

would have to operate in a fundamentally different manner than inverting and shuffling.

The Cost of Insecurity

There was a very high cost associated with the lack of a secure voice system. Shortly before the Japanese attack on Pearl Harbor, American cryptanalysts broke a message sent in the Japanese diplomatic cipher known as Purple. It revealed that Japan would be breaking off diplomatic relations with the United States. In the context of the times, this meant war. General Marshall knew he needed to alert forces at Pearl Harbor to be prepared for a possible attack, but, not trusting the A-3 Scrambler, he refused to use the telephone. If the Japanese were listening in, they would learn that their diplomatic cipher had been broken, and would likely change it. The United States would thus lose the benefit of the intelligence those messages provided. The result was that the message was sent by slower means and didn't arrive until after the attack.

A Solution from the Past

Fortunately, the simpler problem of enciphering text had been mastered—a perfect system had been found—and it was possible to create an analog of it for voice.[6]

The perfect system for text is known as the one-time pad. The key for a one-time pad can be presented in various ways, but for our purposes here it is simplest to show it as a random string of integers between 0 and 25, inclusive—for example, 7, 4, 13, 2, 18, 21, etc. If we wish to send the message ATTACK, we simply shift each letter forward as many positions as is indicated by the number in the same position as that letter in our key. We have A+7, T+4, T+13, A+2, C+18, K+21, which turns into HXGCUF. Observe that T+13 and K+21 both took us past the end of the alphabet. When this happens, we simply start again at the beginning (imagining Z to be followed by A, and the rest of the alphabet again).

This system is referred to as the one-time pad because a given key should be used only once. If it is reused, there are attacks that allow both messages to be recovered. This has happened.[7]

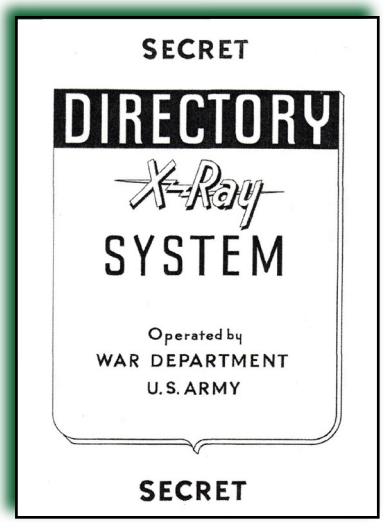


Fig. 2. Is this how we should market texts?

The voice analog of one-time pad encryption would have to add random values to the sound wave. It's a method completely different from inverting and reordering subbands. It's the story of SIGSALY.

SIGSALY

The following are equivalent:

1. SIGSALY
2. RC-220-T-1
3. The Green Hornet
4. Project X-61753
5. Project X (the atomic bomb was Project Y)
6. X-Ray
7. Special Customer

Proof—see the literature.

As indicated above, SIGSALY, the ciphony system that would replace the A-3 Scrambler for Roosevelt and Churchill (and others), had many different names. This is an indication of its importance.

The sixth name may be seen on the cover of a formerly classified directory for the system (Figure 2). The cover is certainly attention grabbing, but the contents are quite dry by comparison.

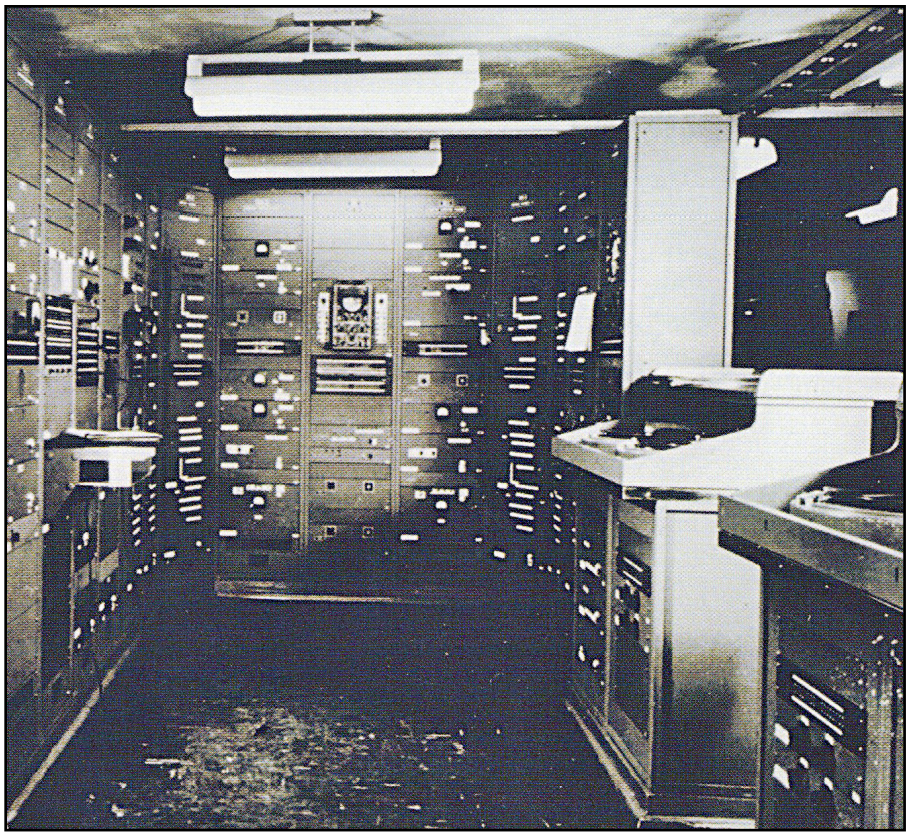


Fig. 3. A view of SIGSALY[8]

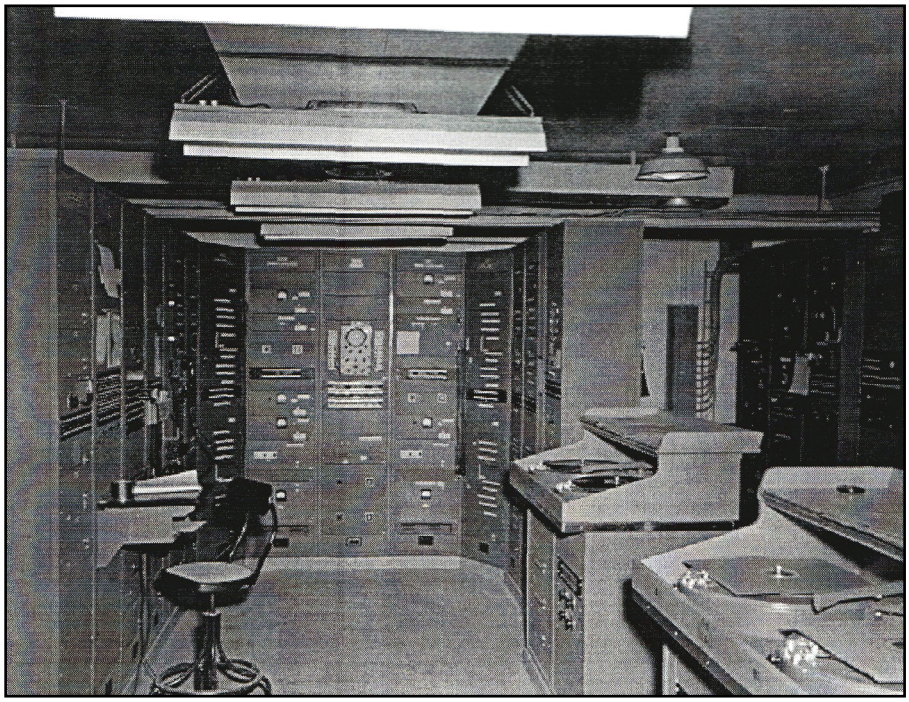


Fig. 4. Another view of SIGSALY[9]

Before getting into the details of how SIGSALY worked, a few pictures are presented (Figures 3 and 4).

Upon first seeing images like Figures 3 and 4, I asked, "So where in the room is SIGSALY?" I wasn't sure which item I should be looking at. The answer was, "It *is* the room!" The result of the quest for secure voice communication led to a fifty-five-ton system that took up 2,500 square feet. In fact, the images show only *part* of SIGSALY. It literally filled a house. Some reflection makes sense of why the project didn't turn out a more compact device.

Necessity is the mother of invention, so it's not surprising that the need to keep voice communications secure from Nazi cryptanalysts is what finally motivated the design of a secure system. But this impetus also meant that no time could be wasted. The designers didn't have the luxury of taking a decade to make a system of utmost elegance. Instead, they based it on earlier technology that could be readily obtained, saving much time. The heart of the system was a *vocoder*, which is a contraction of *voice coder*. The original intent of such devices was to digitize speech so that it might be sent on undersea phone cables using less bandwidth, thus reducing costs. Due to the aforementioned high redundancy of human speech, compression down to 10 percent of the original was found to be possible, while still

allowing the original meaning to be recovered.[10] For SIGSALY, the compression was a bonus. The important thing was to digitize the voice, so that a random digital key could be added to it in the manner of the one-time pad. Off-the-shelf vocoder technology took up much space!

For those interested in hearing how early vocoders transformed speech, a recording of a Bell Labs vocoder from 1936 may be heard at http://www.complex.com/music/2010/08/the-50-greatest-vocoder-songs/bell-telephone-laboratory.

Middle-aged readers of this paper might find the sound reminds them of the Cylons in the original (1970s) *Battlestar Galactica* TV series. Indeed, this sound effect was produced using a vocoder.[11] Decades earlier, Secretary of War Henry Stimson had remarked of a vocoder, "It made a curious kind of robot voice."[12]

This brings us to an interesting point. Vocoders sound cool. For this reason, many musicians have used them. Dave Tompkins, a hip-hop journalist, aware of the use of vocoders in voice encryption and music, wrote a very entertaining book that examines both applications. The front cover of this book appears in Figure 5.

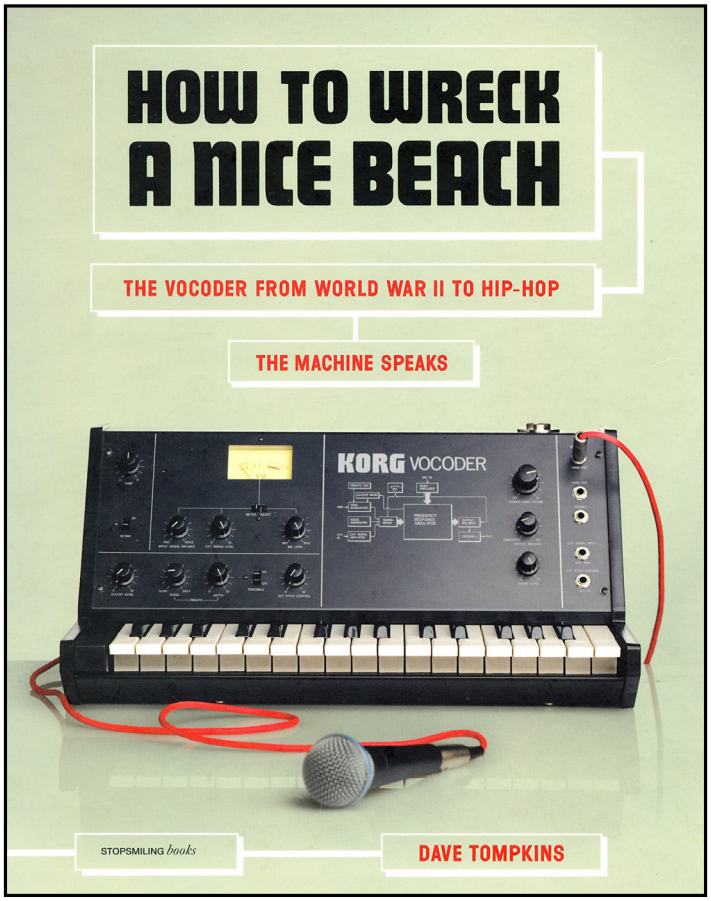


Fig. 5. For a book with cryptologic content, Tompkins's work contains a record-shattering amount of profanity.

The title of Tompkins's book arose from the manner in which vocoders were tested. Various phrases would be passed through the vocoders, and listeners, ignorant of what they were supposed to hear, would try to determine the messages. In one instance, the phrase "How to recognize speech" was misheard as "How to wreck a nice beach." Clearly that vocoder was not suitable to military applications in which a slight misunderstanding could have a calamitous effect.

The diverse applications of the vocoder, detailed in Tompkins's book, are represented below by Figures 6 and 7.

The vocoder used by SIGSALY broke the speech into ten channels (from 150 Hz to 2950 Hz), and another channel represented pitch. Some sources describe the pitch as being represented by a pair of channels. Both points of view can be considered accurate, as will be made clear in the next paragraph. Each channel was 25 Hz, so the total bandwidth (with two pitch channels) was (12)(25) = 300 Hz. Ultimately, the communications were sent at VHF.

The digitization of each channel was done on a senary scale; that is, the amplitude of each signal was represented on a scale from 0 to 5, inclusive. A binary scale was tried initially, but such rough approximation of amplitudes didn't allow for an understandable reconstruction of the voice on the receiving end.[13] For some reason the pitch had to be measured even more precisely, on a scale from 0 to 35. Since such a scale can be represented by a pair of numbers between 0 and 5, pitch may be regarded as consisting of two channels.

Fig. 6. These men knew nothing about the future use of vocoders by musicians.[14]

Before we get to modular arithmetic, the mathematical star of this tale, we examine how logarithms contributed to winning the war. When discretizing sound, it seems reasonable to represent the amplitude using a linear scale, but the human ear doesn't work in this fashion. Instead, the ear distinguishes amplitudes at lower amplitudes more finely. Thus, if we wish to ease the ability of the ear to reconstruct the sound from a compressed form, measuring the amplitude on a logarithmic scale is a wiser choice. This allows for greater discernment at lower amplitudes. Thus, the difference in amplitude between signals represented by 0 and 1 (in our senary scale) is much smaller than the difference in amplitude between signals represented by 4 and 5.

This technique goes by the technical name *logarithmic companding*, where *companding* is itself a compression of *compressing* and *expanding*.[15]

The concept described above will already have been familiar to all readers. When presenting logarithms to students, who hasn't used the decibel scale as an example?

Having discretized the signal, we're ready to add the random key. With both the speech and the key taking values between 0 and 5, the sum will always fall

Fig. 7. Musicians, represented here by Michael Jonzun (and a Roland SVC vocoder), knew nothing of the use of vocoders by the military.[16]

between 0 and 10. SIGSALY, however, performed the addition modulo 6, so that the final result remained between 0 and 5, as represented in Figure 8.

Why was the addition of the key done in this complicated manner? Why not just add without the mod 6 step? Three reasons are given below.

1. The mod 6 step was Harry Nyquist's idea.[17] Students of information theory will recognize this name and, for them, it certainly lends a stamp of authority to support the inclusion of this step. But an argument from authority is not a proof! Fortunately, we have two more reasons.

2. If we don't perform the mod 6 step, then a cipher level of 0 can arise only from both message and key being 0. So, whenever a 0 is the output, an interceptor will know a portion of the signal. Similarly, a

cipher level of 10 can only arise from both message and key being 5.

Hence, without the mod 6 step, an interceptor would be able to immediately identify 2/36 ≈ 5.5% of the signal from the simple analysis above.

3. Simply adding the key without the mod step would result in random increases in amplitude, which may be described as hearing the message over the background noise of the key. Are you able to understand a friend talking despite the white noise produced by an air-conditioner or chainsaw in the background?

SIGSALY enciphered every channel in this manner using a separate random key for each. A simplified schematic for the overall encryption process is provided below (Figure 9).

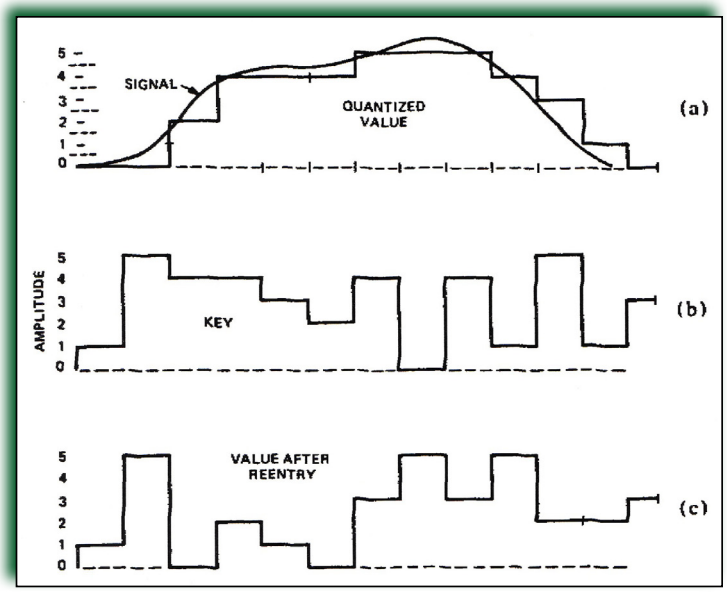


Fig. 8. The mod 6 addition of the key was referred to as "reentry" by the creators of SIGSALY.[18]

Figure 9 shows the speech entering the system on the left-hand side and getting broken down into a pitch channel (pitch detector) and ten voice channels (spectrum 1 through spectrum 10). There are steps, not discussed here, both before and after the mod 6 (reentry) takes place. The "missing steps" are of great-

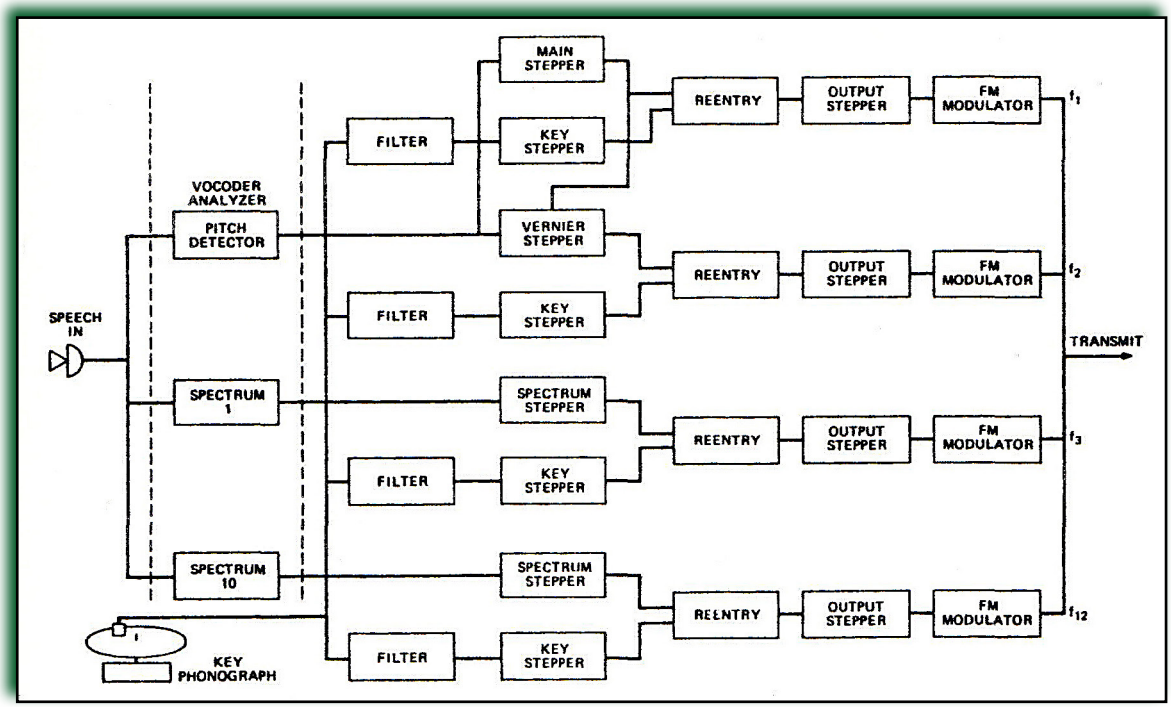


Fig. 9. An incredibly simplified schematic of a SIGSALY transmit terminal[19]

er interest to engineers than mathematicians, and can be found in Donald E. Mehl's book (Mehl 1997).

At this point I'd like to draw your attention to the lower left-hand corner of Figure 9. The "key phonograph" is exactly what it sounds and looks like. The source of the keys that needed to be combined with each channel was simply a record.

The one-time key for voice encryption was codenamed SIGGRUV. As with text, the key was added to encipher and subtracted to decipher. Taking the form of a record, a built-in safety mechanism caused communication to cease if the key stopped. Otherwise, the speaker would suddenly be broadcasting in the clear.

The digitized speech was sampled fifty times per second, so to separately encipher all of the channels, the record had to be simultaneously playing twelve tones at different frequencies, and these tones had to change every fiftieth of a second.

It's natural to ask why the sampling rate was fifty times per second and not higher or lower. The fundamental unit of speech, known as a phoneme, has a duration of about a fiftieth of a second, so the sampling rate is just high enough to allow it to be captured. A higher sampling rate is not needed to make the digitized voice comprehensible and would worsen the synchronization problem—the record at the receiving terminal, used to subtract the key, must be synchronized with the incoming message, if there is to be any hope of recovering it! While we're on the topic of synchronization, it should be mentioned that the records contained tones for purposes other than encryption. For example, a tone at one particular frequency was used for fine-tuning the synchronization.

Ideally the keys would be random, a condition simulated for SIGGRUV by recording thermal noise backward. None of these records would become classic tunes, but the military was content with one-hit wonders. Indeed, the system would become vulner-

Fig. 10. A SIGSALY turntable and record, with a modern CD for scale[20]

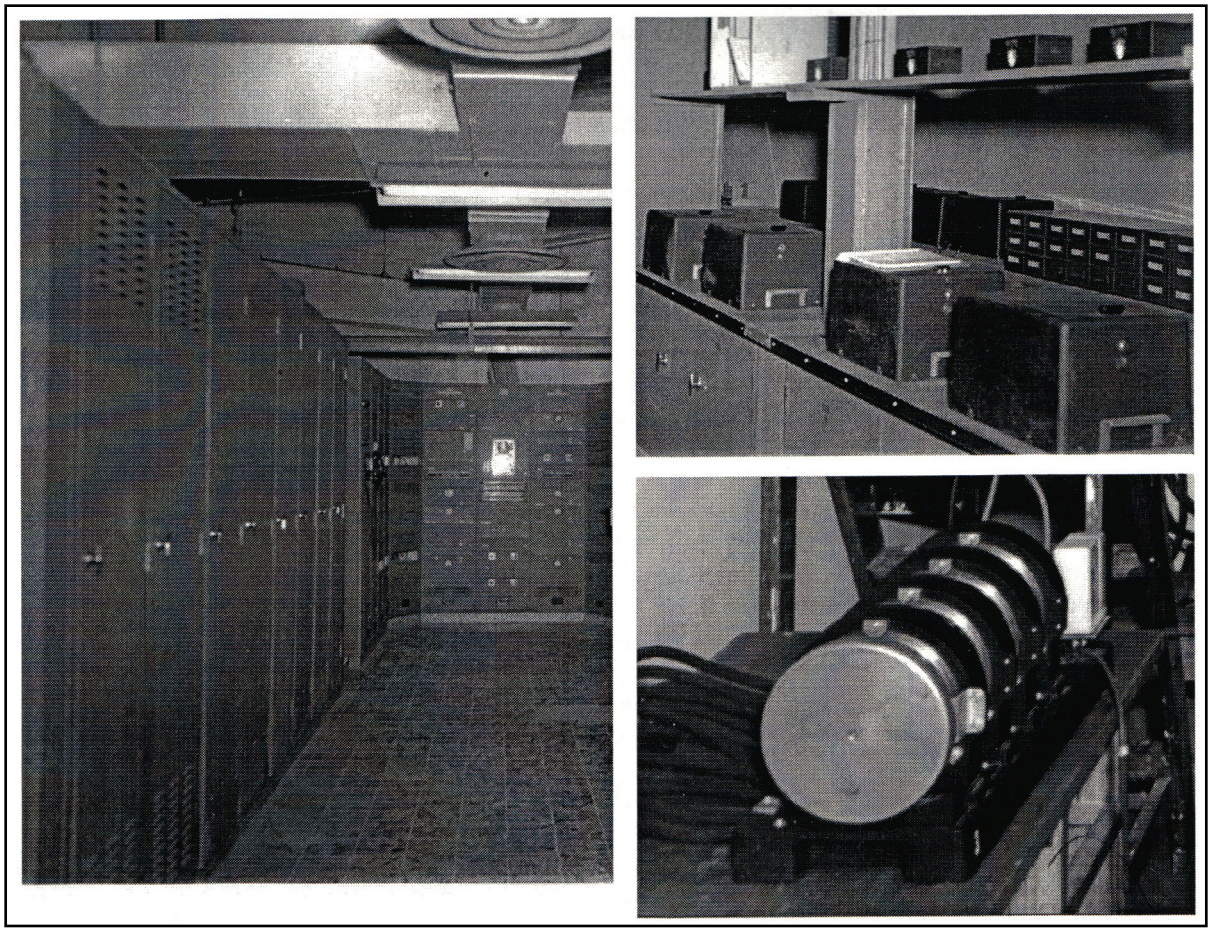


Fig. 11. SIGSALY's back-up key SIGBUSE[21]

able if the same record were ever replayed. Although not labeled as such, the implicit warning was "Don't Play it Again, Uncle Sam!," and the records were destroyed after use.

Vinyl aficionados may have noticed that the record in Figure 10 is unexpectedly large in comparison to the CD. SIGSALY's records measured sixteen inches and could be played from start to finish in twelve minutes. Over 1,500 of these key sets were made.[22]

Plan B

Once the SIGSALY installations were in place, all that was necessary for communication was that each location have the same record. Initially spares were made, but as confidence was gained, only two copies of each record were made. Still, there was a Plan B.

Figure 11 looks like a locker room, but it is simply SIGSALY's back-up key, codenamed SIGBUSE. If for some reason the records couldn't be used for keying purposes, SIGBUSE could generate a pseudo-random key mechanically.

Since SIGSALY would link Roosevelt and Churchill, the Americans and the British needed to be satisfied that it was secure. The British had the added concern that the operating teams, which would consist of Americans, even in London, would hear everything.

Thus, in January 1943, the British sent their top cryptanalyst, Alan Turing, to America to evaluate the

Fig. 12. SIGSALY's air conditioning system[23]

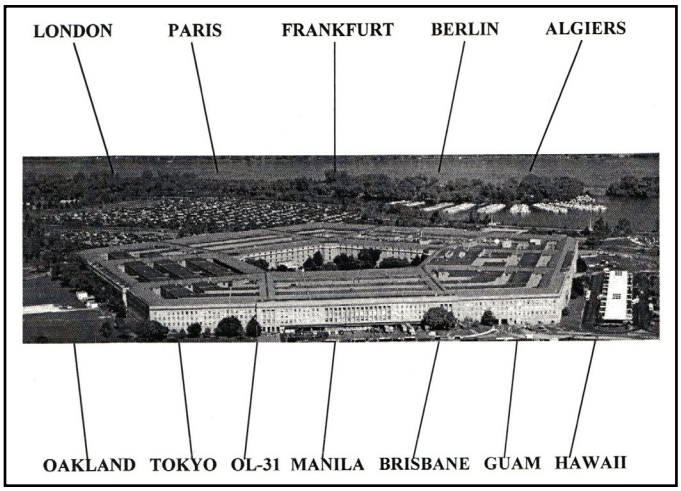


Fig. 13. The SIGSALY installations: OL-31 was on a barge.[24]

system. After much debate, probably reaching President Roosevelt,[25] Turing was allowed access to details of the closely guarded secret project.

Turing helped by suggesting improvements to the SIGBUSE key, and he reported to the British, "If the equipment is to be operated solely by U.S. personnel it will be impossible to prevent them listening in if they so desire." In reality, the Americans were often so focused on their jobs they had no idea what was actually said.

Turing's examination of SIGSALY inspired him to create his own (completely different) system, Delilah. Turing's report on Delilah appeared publicly for the first time in the October 2012 issue of *Cryptologia*.[26]

Ultimately, SIGBUSE turned out to be wasted space. The records never failed, so the alternate key was never used.

A more critical part of SIGSALY was the air-conditioning system. It is shown in Figure 12. A voice encryption system that fills a house requires a cooling system on the same scale!

SIGSALY in Action

In November 1942 an experimental station was installed in New York, and in July 1943 a final version was activated linking Washington, DC, and London. This marked the first transmission of digital speech and the first practical "Pulse Code Modulation."[27]

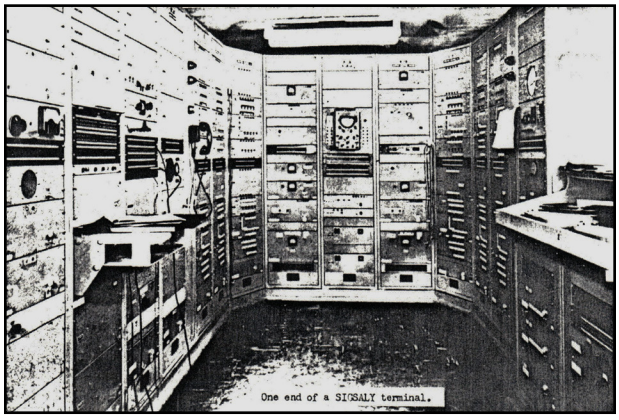


Fig. 14. Yet another view of SIGSALY[28]

Although the bandwidth-compressing vocoder was described earlier in this article as preexisting technology (which it was), it had not become practical enough for use.

Figure 14 provides yet another view of a SIGSALY installation. In this one, the phone is clearly visible, but this is not what the caller would be using. The phone you see was used by a member of the operating team to make sure synchronization was being maintained.

A separate room existed to allow the user(s) to converse in a more comfortable condition (Figure 15).

Although technology rapidly diminished the space needed for secure voice encryption, JFK's system (Figure 16) looked decidedly less cool. It looked like something Maxwell Smart of the TV series *Get Smart* might have used. What would the next step be, three phones?

SIGSALY Retires

SIGSALY received an honorable discharge, having never been broken. The Germans didn't even recognize it as enciphered speech. They thought it was just noise or perhaps a teletype signal. The sound they heard was similar to the music played at the start of the *Green Hornet* TV show of that era. Although they might not have been familiar with the program, Americans certainly were, and this is why the system was sometimes referred to as the Green Hornet.

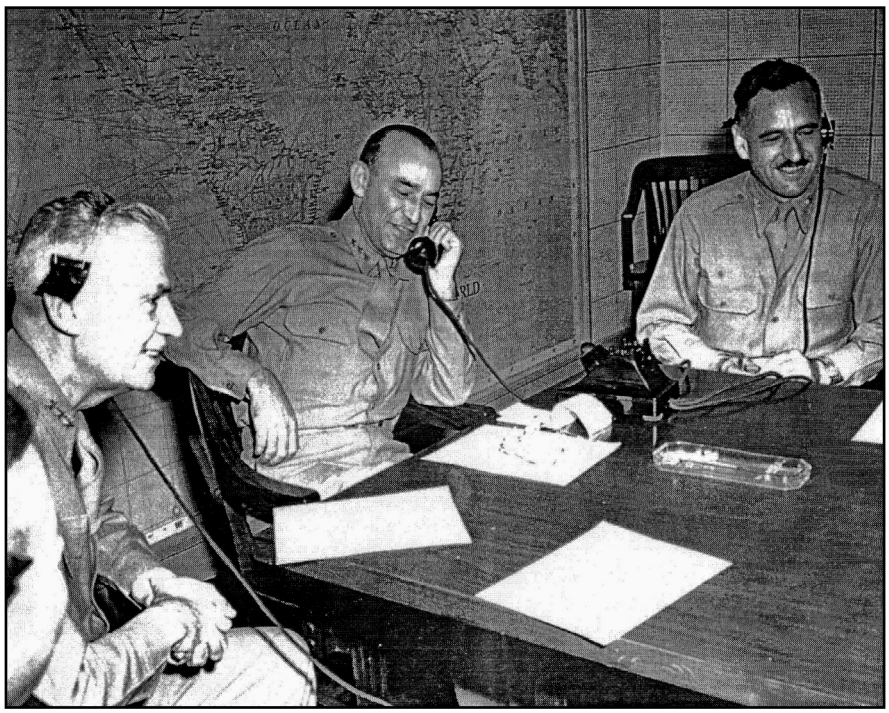


Fig. 15. SIGSALY users—fighting the Germans and Japanese … and loving it![29]

Fig. 16. President Kennedy's voice encryption system

NEW YORK TIMES, PAGE 27

JULY 3, 1976

From WWII era

'Green Hornet' patent awarded

Franklin D. Roosevelt

Winston Churchill

By STACY V. JONES
New York Times Service

WASHINGTON — A historic note was struck in the inventors' world this week when basic patents were granted for a secret method of speech transmission used by President Franklin D. Roosevelt, Prime Minister Winston Churchill and other Allied leaders in World War II.

Bell Telephone Laboratories Inc., as assignee of the inventors, received the two patents, both entitled "secret telephony." They had been applied for almost 35 years ago, but were, until recently, classified secret by the government.

The patents were awarded to Robert C. Nathes and Ralph K. Potter. P. W. Blye was project manager in charge. All three engineers have long since retired from the Bell staff.

THE X System, as it was called, was developed in the early 1940s for the government and was the first speech encoding technique that could not be deciphered by anyone but the intended recipient. The user spoke into a specially designed handset. The speech was encoded with electronic pulses called "key signals" and transmitted by shortwave radio. At the receiving end, the key signals were subtracted and the listener heard only the clear message.

A person receiving the message had to have a phonograph record of the identical key-signal pattern being transmitted. The recordings had to be started simultaneously at both ends, and new pairs were made every day.

The X System, which was nicknamed "The Green Hornet," after a popular radio show of the 1940s, was the precursor of digital speech encoding and a forerunner of the present-day "pulse code modulation" which is used in the Bell System to transmit encoded conversations over telephone channels.

Fig. 17. A 1976 *New York Times* article on SIGSALY[30]

Although SIGSALY was never broken, General Douglas MacArthur didn't trust it! Happily, others did, and the rewards of the instant communication it provided were reaped. Given its success, it's natural to ask why it wasn't kept in use longer. There were several reasons:

1. It weighed fifty-five tons and had a seventy-ton shipping weight.

2. It took up 2,500 square feet.

3. It cost $250,000–$1,000,000+ per installation.

4. It converted 30 kilowatts of power into 1 milliwatt of low-quality speech.[31]

5. The deciphered speech sounded like Donald Duck.[32]

SIGSALY was finally declassified in 1976. This allowed a slew of patents, applied for decades earlier, to finally be granted.

A mock-up of a portion of SIGSALY may be seen today at the National Cryptologic Museum adjacent to Ft. Meade, Maryland (Figure 18). This museum also has an excellent library that includes the David Kahn Collection.[33] Kahn is widely regarded as cryptology's greatest historian and, prior to his donation, his collection was the largest in private hands.

Early in this paper we saw the consequences that may be faced when a nation is without a secure voice encryption system. We close with a look at the advantage gained when a nation does possess such a system.

Voice vs. Text

Text systems take longer to encipher and decipher than voice systems. The situation was far worse during the precomputer era of World War II. Then, an enciphered message might take an hour to reach readable form. Sometimes this was too long to wait! The instant communication voice encryption allows can make a tremendous difference when speed is of the essence. The best example of this is provided by another voice system—the Navajo codetalkers. The rapid communication made possible by these men allowed for equally rapid and coordinated movement of troops, in response to changing conditions. This was an advantage the Japanese did not possess.

> Were it not for the Navajos, the marines would never have taken Iwo Jima! (Major Howard M. Conner)[34]

Like SIGSALY, this was a "voice system" that was never broken. But codetalkers couldn't be used for-

ever, while digital voice encryption has been continuously improved up to the present day.

Acknowledgments

Many thanks are due to the National Security Agency for making it possible for me to pursue my passion full-time as a scholar-in-residence at the Center for Cryptologic History. Rene Stein, National Cryptologic Museum librarian, was invaluable in helping me locate all of the materials I needed. Wayne Blanding showed great patience as I asked many questions that showed my complete ignorance of engineering. Dave Tompkins clued me in to applications of vocoders in music, enlivening presentations I give on this topic. Thank you all!

Fig. 18. The National Cryptologic Museum's SIGSALY mock-up

References

Boone, J. V., and R. R. Peterson. *The Start of the Digital Revolution: SIGSALY Secure Digital Voice Communications in World War II*. Fort George G. Meade, MD: Center for Cryptologic History, National Security Agency, July 2000. http://www.nsa.gov/about/cryptologic_heritage/center_crypt_history/publications/sigsaly_start_digital.shtml.

Hodges, Andrew. *Alan Turing: The Enigma*. New York: Simon & Schuster, 1983.

Kahn, David. *The Codebreakers*. 2nd ed. New York: Scribner, 1996.

Mehl, Donald E. *The Green Hornet*, self-published, 1997.

Tompkins, Dave. *How to Wreck a Nice Beach*. Chicago: Stopsmiling Books, 2010.

Turing, Alan, and Donald Bayley. 2012. Government Code and Cypher School: Cryptographic Studies, HW 25/36, "Report on speech secrecy system DELILAH," a technical description compiled by A. M. Turing and Lieutenant D. Bayley REME, 1945-1946, British National Archives, released in 2009. *Cryptologia* 36 (October): 295-340.

Weadon, Patrick, D. *Sigsaly Story*, 2009. Available online at http://www.nsa.gov/about/cryptologic_heritage/center_crypt_history/publications/sigsaly_story.shtml.

Notes

1. David Kahn, *The Codebreakers*, 2nd ed. (New York: Scribner, 1996), 554.
2. Younger readers will likely require an explanation of the term "party line." As a first step, imagine a house with phones that actually connect to jacks in the walls (i.e., land lines). A boy upstairs might pick up the phone in his room and hear his dad talking to someone. He'd realize his dad was using the downstairs phone and hang up. All of the phones in the house were wired via a common line. This would be convenient for conference calls, but inconvenient the rest of the time. A family member would sometimes have to wait his turn, when wanting to make a call. "Party lines" worked on the same principle, but the phones were in different homes. That is, in the old days, you might be on a party line with one or more neighbors. You could listen in on their calls, if you desired, but would hopefully respect their privacy and hang up when you discovered the line was in use.
3. Kahn, *Codebreakers*, 555-556.

Fig. 19. A comparison between SIGSALY and a secure telephone from the year 2000[35]

4. British Foreign Office memorandum FO/371/32346. Taken here from Andrew Hodges, *Alan Turing: The Enigma* (New York: Simon & Schuster, 1983), 236.
5. From a letter to Harry Hopkins, assistant to President Roosevelt. Taken here from Donald E. Mehl, *The Green Hornet*, self-published, 1997, 5.
6. This system was published in 1882 but ignored or forgotten, and finally reinvented in 1917-1918. The original discovery was only recently recognized. For details see Steven M. Bellovin, "Frank Miller: Inventor of the One-Time Pad," *Cryptologia*, 35, no. 3 (July 2011): 203-222.
7. See Jan Bury, "From the Archives: Breaking OTP Ciphers," *Cryptologia*, 35, no. 2 (April 2011): 176-188. Also see Jan Bury, "Breaking UnbreakableCiphers: The Asen Georgiyev Spy Case," *Cryptologia*, 33, no. 1 (2009): 74-88.
8. Image from http://www.cryptologicfoundation.org/content/A-Museum-Like-No-Other/COMSEC.shtml.
9. Image from http://homepage.mac.com/oldtownman/WW2Timeline/espionage.html.
10. Dave Tompkins, *How to Wreck a Nice Beach* (Chicago: Stopsmiling Books, 2010), 23.
11. A Cylon from a 1977 episode of *Battlestar Galactica* may be heard at http://www.youtube.com/watch?v=0ccKPSVQcFk&feature=endscreen&NR=1.
12. Tompkins, *How to Wreck a Nice Beach*, 63.
13. Andrew Hodges, *Alan Turing: The Enigma* (New York: Simon & Schuster, 1983), 246.
14. Mehl, Donald E., *The Green Hornet*, self-published, 1997, 45.
15. The pitch channel, however, wasn't companded.
16. Image from http://www.amazon.com/gp/customer-media/product-gallery/1933633883?ie=UTF8&index=3&isremote=0.
17. Mehl, *Green Hornet*, 38.
18. Image from Mehl, *Green Hornet*, 40, and J. V. Boone and R. R. Peterson, *The Start of the Digital Revolution: SIGSALY Secure Digital Voice Communications in World War II* (Fort George G. Meade, MD: Center for Cryptologic History, National Security Agency, July 2000), 19.
19. Mehl, *Green Hornet*, 26.
20. Ibid., 31.
21. Mehl, *Green Hornet*, 34.

22. Tompkins, *How to Wreck a Nice Beach*, 68.
23. Mehl, *Green Hornet*, 50. Mehl appears on the right in this photo.
24. Mehl, *Green Hornet*, 86.
25. We have no proof, but Mehl, p. 69; Hodges, p. 245; and Tompkins, p. 59, all believe the matter reached Roosevelt. In any case, Secretary of War Stimson resolved it.
26. "Report on speech secrecy system DELILAH, a technical description compiled by A. M. Turing and Lieutenant D. Bayley REME, 1945-1946," *Cryptologia* 36, no. 4 (October 2012): 295-340.
27. This refers to the digitization process.
28. Image courtesy of the National Cryptologic Museum, David Kahn Collection, Folder 12-7.
29. Mehl, *Green Hornet*, 103. An alternate caption for this image is "SIGSALY: Your digital pal who's fun to be with!"
30. Image courtesy of the National Cryptologic Museum, David Kahn Collection, Folder 12-7.
31. Hodges, *Turing*, 247.
32. General Eisenhower complained that it made his wife sound like an old woman. The system was optimized for male voices, and as a result, deciphered female voices sounded worse.
33. David Hamer, "The David Kahn Collection at NSA's National Cryptologic Museum," *Cryptologia* 35, no. 2 (April 2011): 110-113.
34. Doris A. Paul, *The Navajo Code Talkers* (Pittsburgh, PA: Dorrance Publishing, 1973), 73.
35. Image from Reunion 2000, 805th Signal Service Company, Washington, DC, October 2000, p. 4, courtesy of National Cryptologic Museum, VF 60-38.

Craig Bauer wrote this paper while serving as the scholar-in-residence at the National Security Agency's Center for Cryptologic History. He was the ninth to hold this position and the first mathematician. He is the author of *Secret History: The Story of Cryptology*, a comprehensive look at both the history and mathematics of cryptology, presented with absolute minimal prerequisites. He is also the editor-in-chief of *Cryptologia*, a quarterly journal devoted to all aspects of cryptology.

Two Cryptologic Nights at the Cinema: *The Red Machine* and *The Imitation Game*

David A. Hatch

I have long been a movie buff and have always been a sucker for movies based on history. Films that take care in re-creating a historical event or show something about an important person are a joy to watch. For the historian, films that botch the events are also a source of joy, although for different reasons.

A scene from *The Red Machine*

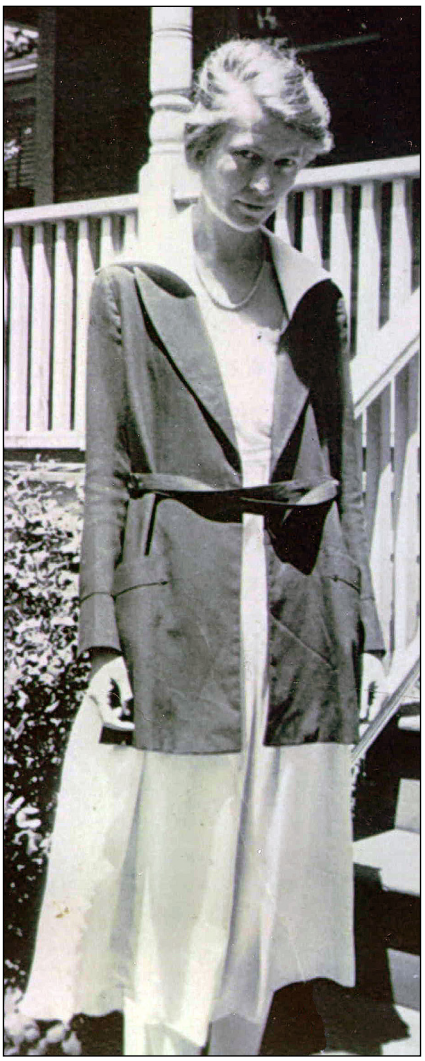
No motion picture can be absolutely accurate in showing historical events. No historian, least of all me, expects that. But painstaking efforts to show the past can do important things for people in the present. For example, *The Longest Day*, a 1962 movie that is relatively bloodless compared even to today's television programs, still helps viewers understand the vast scope of the D-Day operation and its complexity, as well as the sacrifice of their future by thousands of young men so that our future could be secure.

The Red Machine

This brings us to movies that are less scrupulous in showing the past, and, specifically, to the 2009 production *The Red Machine*. In a generally favorable review, the magazine *Wired* said, "How faithful is the movie's Red Machine to the real thing? [The writer and director] strove for historical accuracy in every respect."

As a historian writing about this film, my dilemma is where to begin? The film has historical inaccuracies beginning about thirty seconds into the story, and the mistakes just keep on coming.

Set in the late 1930s, the film opens in a large but sparsely furnished room where half a dozen civilian codebreakers working for the U.S. Navy are scanning and rapidly solving encrypted messages sent by the Japanese Navy. One of them finds an anomalous message and, after consulting reference material and one of his colleagues, decides to show it to "Miss Aggie."



Agnes Meyer Driscoll in the 1920s
(Photo courtesy Meyer family,
CCH holdings)

Later scenes, by the way, show this building to be a stand-alone, wooden, barracks-style structure in the middle of a Navy base.

Pause, for a reality check. The Navy in the 1930s required that its cryptanalysts be active duty officers (the Army did hire civilians). Until World War II began, the cryptologic work was done in cramped quarters in the Navy Building. This was a large office complex located in the District of Columbia on the site of what is now the Vietnam Veterans Memorial.

"Miss Aggie" was a real person, Agnes Meyer Driscoll, a civilian exception to the Navy's requirement about active duty officers as cryptologists. She had been involved in cryptology since World War I, and was acknowledged by the uniformed cryptanalysts around her as the most talented of them all. While she was an important person in Navy cryptology in the 1930s, the film depicts her as supervising the effort, which is untrue; in real life she acted in a capacity that we would today call "technical director."

Back to the film: The anomalous message turns out to have been enciphered on a cryptomachine, quickly given the nickname "Red." Admitting that it would take years to solve through pure analysis, the Navy springs a talented young safecracker from a Washington, DC, jail and offers him his freedom if he will help them break undetected into Japanese facilities to photograph the Red Machine and related keying documents.

The Red Machine is in a locked and guarded room in an apartment rented by the Japanese naval attaché, while keying documents are in an office safe in the Japanese embassy. The balance of the movie shows the preparation and execution of the two capers.

When we finally see the Red Machine itself, it greatly resembles a rubicund ENIGMA. In a thrilling scene, the burglar and the lieutenant minding him fully disassemble it, down seemingly to the dust in the open spaces, for photographing.

There was a Red Machine in real life. However, it was used by the Japanese Foreign Ministry, not the Navy, and it was solved by the U.S. Army, not the Navy. Just to complicate the real life story, the U.S. Navy had pinched a copy of an earlier Japanese Navy codebook, which the Americans called the "Red Code" because of the binder in which it was kept. (Prewar codebreaking was nothing if not colorful!)

Before World War II, there were a few occasions in which the U.S. Navy conducted "black bag jobs" against Japanese targets. This is not well documented, but appears to have been done against Japanese ships in American ports and, perhaps, consular buildings. A former NSA senior used to refer to this as "second-story cryptanalysis."

Although the documentation is sparse, there was at least one "black-bag job" against a Japanese consular residence. It was not, of course, in search of a Red Machine, since such a thing did not exist.

Most of the Navy's cryptanalytic work, like the Army's, was done by pure analysis. This is important and even exciting, but, unfortunately, is not very cinematic.

One other problem: I'm not into militaria, but something else looks wrong in the film. All the Navy officers wear their medals on their work uniforms—not a ribbon in a row of ribbons, but the actual medal hanging from a strip of cloth. My understanding is that such medals are worn only with the highest level of dress uniforms.

The Navy's pre-World War II cryptanalytic work was vitally important; in fact, we would have been much less well prepared for the wartime effort if we had not had the COMINT information the Navy produced in the 1930s.

I like a thriller as much as anybody, but *The Red Machine* does a real disservice to cryptology today by misportraying how the work was done. It certainly is disrespectful to the small and skilled group of professionals who actually solved Japanese codes and ciphers in the 1930s and war years.

The Imitation Game

The Imitation Game, a major motion picture released in 2014, pays tribute to the accomplishments of Dr. Alan Turing. He was the mathematics genius—a word used carefully, not just as an enthusiastic tribute—who made important contributions at Bletchley Park toward exploiting German cryptosystems in World War II, and whose theoretical work led to development of the modern computer. Turing was homosexual, was forced into hormonal treatments as the result of a court case, and committed suicide in 1954.

Alastair Denniston,
director of Bletchley Park

The movie is richly filmed, with good acting and a riveting story. Benedict Cumberbatch as the adult Alan Turing is especially memorable and may only have been out-acted by the young man who played the teenaged Turing as he wrestled with questions of his self-identity.

The story, however, is riddled with inaccuracies. Most of them don't matter much if one looks at the story as a parable that people today need to internalize about misunderstood genius and the tribulations a gay man had to pass through in a hostile society.

A few of the inaccuracies do matter, however.

My personal opinion is that the filmmakers owe an apology to the families of Alastair Denniston and Hugh Alexander. Denniston, the director of Bletchley Park, though he held reserve rank in the Royal Navy, had been a civilian cryptanalyst since World War I. The film portrays him as a military martinet who opposed Turing because Turing lacked discipline and ignored the chain of com-

NSA/CSS hosted a screening of *The Imitation Game* in November 2014. In attendance were (l to r) actor Allen Leech, who played John Cairncross; Patrick Weadon of the National Cryptologic Museum; the film's director Morten Tyldum; and executive producer and screenwriter Graham Moore. The photo was taken at the museum's Enigma exhibit.

mand. Denniston was replaced as director early in the war because his management skills were not equal to an industrial-scale enterprise; he did not harass Turing for failing to conform to expected norms of wartime behavior.

Hugh O'Donel Alexander, once chess champion of the British Empire, went on to a long career at GCHQ after the war. The film portrays him as a bragging womanizer; this portrayal runs contrary to all we know about him.

These two characters are likely in the film to show how the bureaucracy reacted to Turing, and to contrast his homosexuality with the actions of an aggressive heterosexual. This doesn't bother my historical sensibilities; on the contrary, these characters help put Turing's life and contribution into perspective. I just wish the film makers had used fictional names for the characters.

The film shows Alan Turing as the center of all the successful cryptanalytic activity at Bletchley Park, including the purchase of parts and assembly of the cryptanalytic bombe, which exploited ENIGMA-based messages. In actuality, the bombe was designed by Turing but built elsewhere; and Turing's bombe was made faster and more efficient by Gordon Welchman, also a Cambridge mathematician.

Turing was really important, but he wasn't Superman. In this aspect, *The Imitation Game* reminds me of those classic biopics of the 1930s: young Tom Edison knows, despite all opposition, that he will grow up to invent the light bulb.

One other significant inaccuracy should be noted. In the film, once Turing and a few colleagues have solved the Naval ENIGMA machine and have shown that the bombe can solve messages on a recurring basis, Turing and these colleagues decide how the resulting intelligence, called ULTRA, will be distributed. The source is secret; even the Bletchley Park hierarchy is not to know the ENIGMA has been solved, and the Turing team calculates statistically which decrypts will be released to the military, thus determining who will live or die in battle. This is necessary, they say, to prevent the Germans from realizing that the ENIGMA is vulnerable.

This is not true. The ULTRA decrypts were distributed by the military to a select group of cleared readers, mostly senior commanders and their intelligence officers. The commanders were required to come up with a cover plan to disguise the source of their information before they could

act on it. In real life, for example, Allied commanders, who were remarkably well informed about their enemy, would order unnecessary reconnaissance or patrolling to fool the Germans about their intelligence. Despite a number of myths, no one's life was sacrificed to protect the ULTRA secret.

Let me mention two small but interesting miscues among many inaccuracies in the movie. After Turing's arrest, a newspaper article sports the headline, "Cambridge Professor Convicted of Indecent Acts." Actually, Turing was a professor at the University of Manchester.

There was a Soviet spy at Bletchley Park, and the movie references him (John Cairncross). However, the film shows the spy unmasked because he used an insecure "Beale cipher" when passing secrets to the Soviets. In reality, the Beale cipher refers to a specific encrypted message from early 18th-century Virginia that is reputed to hide the location of a fabulous buried treasure; it is not a particular kind of cipher.

Lest you think I didn't like *The Imitation Game*, let me say that I did enjoy it as a movie. It is well written, has good performances, and raises social and political issues that still must be settled today. It is good to see Turing getting the public recognition that he deserves, and it is good to remind us all of the unjust and tragic consequences of acting on society's prejudices. But these inaccuracies affect the intelligence community, especially the cryptologic community, in several negative ways. Both films give the public a false concept of what cryptology is and how cryptologists protect the country. *The Red Machine* reinforces the idea that intelligence agencies will do anything, including outright criminal acts, to achieve their goals. *The Imitation Game* shows members of the intelligence community playing God with people's lives.

If the public accepts these portrayals as true, and they will—most of us have encountered people who think James Bond movies are documentaries—how long before these false beliefs about cryptologic work are reflected in the actions of their government representation?

Not the least of the negative effects of these false images will be their influence on recruiting the next generation of cryptologists.

It may be impossible to show the drama and excitement of real-life cryptologic work on the screen in any popular way. If this is true, we can only hope that in the future, film makers will avoid showing it in ways that have a negative impact on the community.

David A. Hatch is currently technical director of the Center for Cryptologic History (CCH) and is also the NSA Historian. He has worked in the CCH since 1990. From October 1988 to February 1990, he was a legislative staff officer in the NSA Legislative Affairs Office. Previously, Dr. Hatch served as a Congressional Fellow. He earned a B.A. degree in East Asian languages and literature and an M.A. in East Asian studies, both from Indiana University at Bloomington. Dr. Hatch holds a Ph.D. in international relations from American University.

Family Album

Field Trip: Famous Visitors to NSA Maryland

David A. Hatch, NSA Historian

The NSA campus at Fort Meade has had many high-level visitors over the years. The visitors have not been only members of the executive branch of the government, as might be expected.

This album displays a few of the better known Fort Meade visitors.

Vice President Hubert H. Humphrey (center) came to NSA in September 1967. The then-director, LTG Marshall Carter, had been Humphrey's military aide and invited him to address the workforce. Humphrey, one of the great stump speakers of his generation, gave a barn-burner of a speech. In this photograph, HHH is about to shake hands with Oliver Kirby, then the director of Production, predecessor of the Signals Intelligence Directorate. General Carter can be seen to Humphrey's left.

Maryland Governor Marvin Mandel visited NSA in 1972. Since he didn't have a security clearance, he was shown some "gee whiz" computer technology and had a courtesy call with the director.

Maryland governor Martin O'Malley (third from left) visited NSA in 2010. At left are NSA Director GEN Keith Alexander and Deputy Director John C. "Chris" Inglis.

Ronald Reagan was the first president to visit NSA, in September 1986. In addition to his wife Nancy, he was accompanied by senior members of his administration. At this invocation, on the far left is William Casey, director of central intelligence; next to Nancy Reagan on the far right is Caspar Weinberger, secretary of defense.

(Above, l to r) Vice President Dick Cheney, NSA Director GEN Keith Alexander, and President George W. Bush at NSA, 23 October 2008

Both Presidents Bush visited NSA multiple times. George Herbert Walker Bush (above), shown in 1991, visited NSA both as director of central intelligence and vice president.

U.S. senator from Maryland Barbara Mikulski has visited NSA numerous times. In November 2013 she visited the Memorial Wall in OPS 2B with NSA Director GEN Keith Alexander.


CENTER for
CRYPTOLOGIC
HISTORY