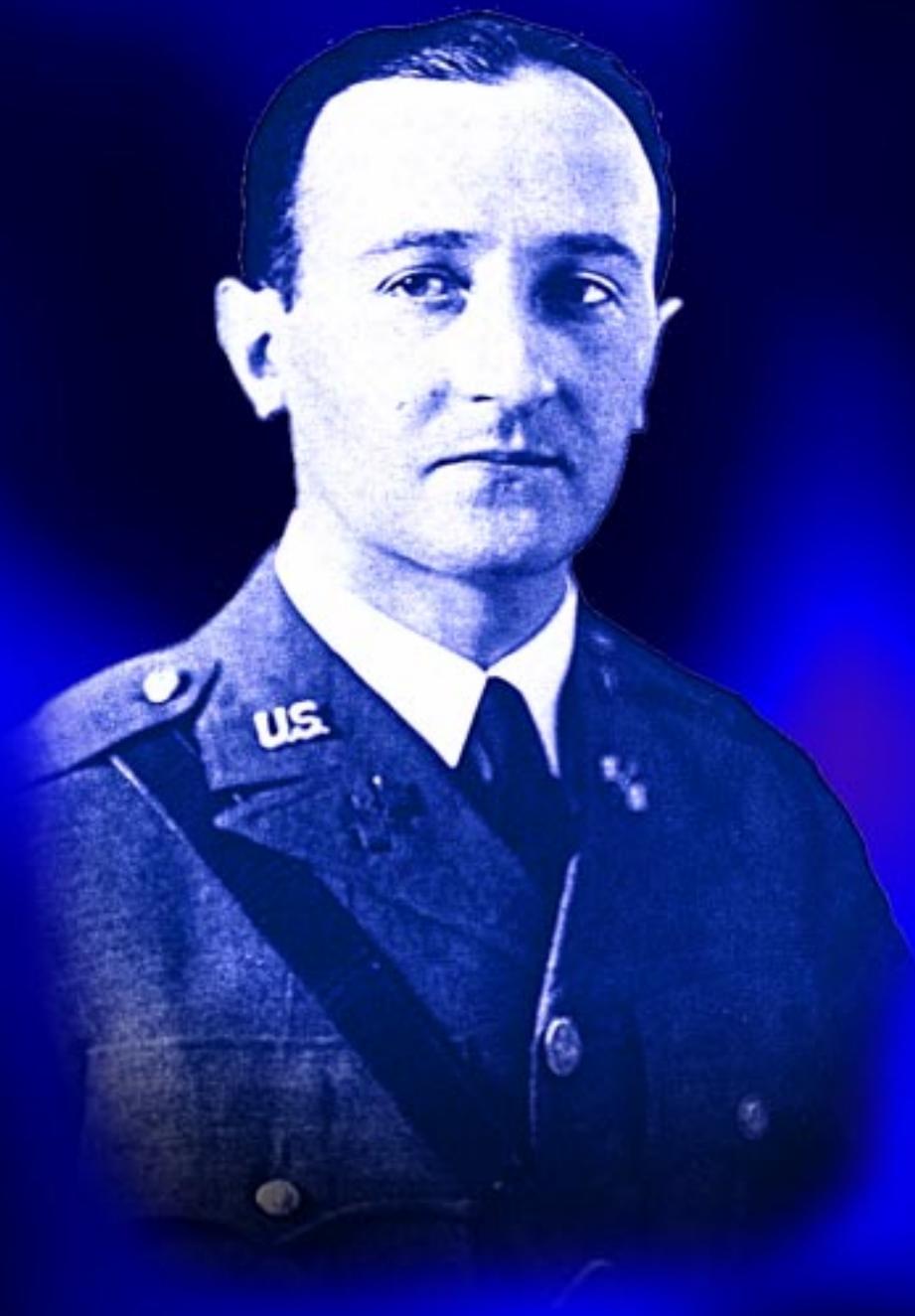


*William W. Friedman*



Principal Cryptologist

## WFF: Cryptanalyst

William Friedman is remembered by history for an act of towering intellect. By force of his mind alone, he saved the lives of countless combatants in World War II. When asked by Congress after the war about the contributions of the Signal Corps cryptanalysts, an admiral enthused, “Hell, they won the war!” Hyperbole aside, the work of Friedman’s Signal Intelligence Service had a profound effect upon the outcome of the war. The story of the breaking of the Japanese highly secret, superenciphered codes by reinventing their “B” cipher machine has been told in the fascinating books *The Man Who Broke Purple* by Ronald W. Clark and David Kahn’s *The Codebreakers*.

But it is not that single accomplishment that I wish to discuss here, but rather Friedman as a leader responsible for recognizing the value of a science of cryptanalysis, organizing and training a pool of men and women to meet the military need, and managing the resultant Signal Intelligence Service in the time of crisis. The reading of Japanese military secrets did not simply come about at a single stroke of genius. It was the culmination of groundwork laid in the 1920s, good training offered in the 1930s despite the absence of funding, and smart organization on the eve of war.

Soon after solving the “Purple” system, Friedman wrote *Preliminary Historical Report on the Solution of the “B” Machine* on 14 October 1940. In that document Friedman showed his characteristic modesty and declined to accept the credit for this important breakthrough. He said, “The successful solution of the B-machine is the culmination of 18 months of intensive study by a group of Cryptanalysts and assistants working as a harmonious, well-coordinated and cooperative team. Only by such cooperation and close collaboration of all concerned could the solution possibly have been reached, and the name of no one person can be selected as deserving of the major portion of credit for this achievement. He went on to credit Frank B. Rowlett and 23 other cryptanalysts, specialists and translators. He did not forget the supporting agencies outside his team. “The vigilance and excellent work done by our various monitor stations in intercepting and copying the necessary traffic also deserves special mention. The assistance rendered by G2 in obtaining certain data has already been mentioned.”<sup>1</sup>

William Frederick Friedman was born in 1891 in Kishinev, Moldavia. His father, a Rumanian Jew from Bucharest, was a linguist and a translator for the Russian Postal Service and his mother was the daughter of a prosperous wine merchant. Fleeing widespread Russian anti-Semitism, the father immigrated to Pittsburgh in 1892 and found work selling Singer sewing machines door to door. His mother followed him to the United States in 1893 with William and his sister. A pogrom in 1902 would kill hundreds of Jews in their former home town and destroy their communities. The news of this atrocity would remain with Friedman for his lifetime, leaving him with a fear of persecution.

A youthful idealism led him to admire a Jewish back-to-the-soil movement and he planned a career in genetics, one that would allow him to develop more productive strains of vegetables. After a six-month stint at Michigan Agricultural College in Lansing, he entered Cornell University in 1911 to study genetics. He graduated in 1914, but stayed on for two years of graduate studies. It was a professor and mentor at Cornell who got him together with George Fabyan, a millionaire cotton merchant and honorary colonel<sup>2</sup> who was undertaking genetic research to find a stronger cotton plant at his Riverbank Laboratories in Geneva, Illinois, outside Chicago.

Friedman wrote about his decision to join Colonel Fabyan. “I had

notions of scratching a living out of the soil when the “back to the farm” movement hit this country in 1910. A few weeks of preparation for the ‘return’ showed me that Mother Nature got the wrong number when I answered that call. But I was impecunious and could not afford to pay for the kind of training that I really was cut out for, electrical engineering, so I specialized in what seemed to offer great possibilities for research and ingenuity, genetics. After graduation and almost two years of work in the graduate school, it seemed advisable to start in to see how hard making a living really is, so I quit and went to Chicago where a certain rich man set me up with a laboratory on his estate, paid me to experiment, and generally had a good time and lots of publicity to the chagrin of the few ‘curiosities’ like myself who lived on the place.”<sup>3</sup>

It was one of history’s coincidences that would bring Friedman together with an aging English teacher named Elizabeth Wells Gallup, who had devoted her life to find evidence in Shakespeare’s plays that Sir Francis Bacon was their real author, research that was sponsored by the eccentric Fabyan at Riverbank Labs. Her theory was based on a reference in Bacon’s writings to a bilateral cipher, one that she thought would prove her thesis if she could find the cipher at work in Shakespeare’s plays. She enlisted Friedman’s help, at first as a photographer, and then as a cryptographer as his mathematical facility and intuition drew him to the mysteries of breaking ciphers and codes.

At Riverbank he met his wife, Elizabeth Smith, a newly recruited English major from an old Pennsylvania family, who was similarly drawn to cryptology and who would later make a name for herself in the field. They were married in May 1917.

When war with Germany was declared, the U.S. Army had no communications intelligence capabilities. Their own attempts at coded, secure communications were laughable and they could not intercept or decode enemy transmissions. The job of rectifying that situation fell upon three Signal Corps officers who constituted the Army’s entire pool of expertise. They were Capt. Parker Hitt, author of *Manual for the Solution of Military Ciphers*, Capt. J. O. Mauborgne, and Maj. Frank Moorman. Mauborgne would become a general officer heading up the Signal Corps.

Realizing the Army would need help in the area of cryptography, Mauborgne readily responded to an offer by Fabyan to put his cryptographers and laboratory at the disposal of the government. Riverbank became the unofficial cipher bureau until Major Herbert O. Yardley established MI-8, the section of the Military Information Division responsible for ciphers and codes.

Friedman taught the first class of four men from the Intelligence Corps and the following class of 80, assisted by four assistants including his wife Elizabeth. They were housed in the Aurora Hotel in Aurora, Illinois. A photograph of the graduates standing on the steps of the hotel face the camera or present their profiles, and in this way use the bilateral Baconian cipher to spell out Bacon’s dictum “Knowledge is power.”

Friedman was commissioned and joined Pershing’s headquarters at Chaumont, France, in July 1918. He was assigned to the German Code and Cipher Solving Section of the General Staff, or as it was better known under its code name, the Radio Intelligence Section led by Colonel Frank Moorman. Having had experience in cipher work, he chose to be assigned to the code-solving unit rather than the cipher unit “in order to broaden my professional knowledge and practice in cryptology.”<sup>4</sup> By the time of the armistice in November, he had five month’s experience and enough knowledge about the subject to write a technical paper for Colonel Moorman entitled “Field Codes Used by the German Army During the World War.” He then turned to writing a history of the Army’s Code and Cipher Solving Branch, the

first of several histories he would record of Army cryptological efforts. He was demobilized on 5 April 1919.

While in France, he learned of Fabyan's interception of the Army offer of a commission in 1917 and was disappointed that his employer's double-dealing denied him a chance to get to work sooner in military cryptology and, according to Yardley, "make a name for himself." But oddly, he went back to work at Riverbank for his old boss and spent time testing cipher devices for the Army. Shortly after being demobilized, Yardley offered him a commission as a first lieutenant in the regular Army or a civilian position at \$3,000 per year. Friedman refused, holding out for a captaincy. Shortly thereafter, he reported for a physical before an Army medical board and was turned down because of evidence of a heart condition. Brig. Gen. Joseph O. Mauborgne, now the chief Signal Officer, then gave both Friedmans six-months contracts as civilian cryptographers beginning 1 January 1921. For William it was the beginning of a 34-year career as the Army's principal cryptographer. At the end of the year he was officially named the Cryptanalyst, Signal Service, at the annual salary of \$4,500, a position he would hold until becoming in 1947 the director of Communications Research in the newly organized Army Security Agency.

In his first year he went right to work compiling a "War Department Staff Code." In July he travelled to Camp Alfred Vail, New Jersey, where he lectured and prepared monographs on basic military cryptology. His classes would become an annual training event. He began his time as an Army Reserve officer in 1922.<sup>5</sup>

At home, after a busy day in Washington's Munitions Building, he wrote *Elements of Cryptanalysis*, a work that became the bible for Army cryptanalysis. It became a training pamphlet in 1923.

At the Signal Corps School at Camp Alfred Vail in New Jersey, he taught a course every year on "The Solution of Military Codes." The two-week course continued until 1930 when it was replaced by a correspondence course in Military Cryptography and Military Cryptanalysis.

Another project that occupied his attention in 1926 was the Enigma machine. He obtained a report on the machine from a Dutch Army cryptologist and even bought at least one Enigma from European sources. He tried without success to devise ways to decipher its output without knowledge of the letter rings and keys.

In May 1929 Yardley's "Black Chamber, the code and cipher section of the Military Intelligence Division, ceased to exist at the orders of Secretary of State Henry Stimson for whose department most of the work was done. The Military Intelligence Division had long recognized that the bureau should combine cryptology and training in the arcane science and recommended it be so organized as the Signal Intelligence Service under the Chief Signal Officer.

Friedman was the key player in the formation of the Signal Intelligence Service, and, along with Major O.S. Albright, the G2's cryptographic officer, drafted its charter. It placed upon the Chief Signal Officer the responsibilities for "Code and cipher compilation, code and cipher solution, interception of enemy radio and wire traffic, location of enemy radio transmitting stations by goniometric means, and laboratory arrangements for the employment and detection of secret inks." For the sake of efficiency, the business of secret communications which was formerly spread over G2, the Signal Corps, and the Adjutant General, was now organized "into a single coordinated service" called the Signal Intelligence Service.

William F. Friedman was to head the new organization which still received most of its funding from the Military Intelligence Division. In 1930 he began to develop the service, hiring a core of cryptanalysts who would agree to make this their life's work. They were Frank Rowlett, Abraham Sinkov and Solomon Kullback, young math majors who would be joined by two other men who were selected for

their “peculiar talents for mathematics, oriental and classical languages, statistics, mechanics or philology.”<sup>6</sup> Friedman personally trained Lieutenant Mark Rhoades for two years before putting him in charge of future training in scientific cryptanalysis at the Signal Intelligence School

The decade of the 1930s was a period of frustration as Friedman tirelessly sought to add personnel and training to his small organization, efforts that he would characterize as fruitless.

In a farseeing move, the SIS under Friedman’s leadership set up radio intercept stations at a few locations around the world. In 1936 a Philippine station was established by Lieutenant Rhoades and a small radio detachment. Sinkov went to Quarry Heights in the Panama Canal Zone in 1936 to set up a station, and Kullback traveled to Hawaii for that purpose. Other stations cropped up in San Francisco, Fort Sam Houston, Texas, and Fort McKinley in the Philippines. The First Radio Intelligence Company also became active at Fort Monmouth, New Jersey.

In 1934 the Signal Intelligence Service took advantage of some IBM tabulating machines that were not being used by the Office of the Quartermaster General. Friedman found them so useful for code compilation that he asked for their lease to be continued. He wrote to his boss, Major Spencer Akin:

In many years service here I have never once “set my heart on” getting something I felt desirable. But in this case I have set my heart on the matter because of the tremendous load it would lift off all our backs. The basic idea of using machinery for code compilation is mine and is of several years standing. The details of the proposed system were developed in collaboration with Mr. Case, of the International Business Machines Corporation. I regard this as one of my most important and most valuable contributions to the promotion of the work for which we are responsible. Please do your utmost for me. If you do we can really begin to do worthwhile cryptanalytic work.<sup>7</sup>

The lease was picked up by the Signal Intelligence Service in February 1935. The machines were rented from International Business Machines Corporation at \$600 per year. Each unit consisted of a punch, sorter, and tabulator.

These machines could also be useful for cryptography, that is, producing codes for the U.S. Army. In 1936 the SIS turned out three editions of the field code for use at division level, a separate military intelligence code and a code for the staff.

In 1939 Friedman made an inspection tour of the intercept stations in Panama and Honolulu, part of a plan of General Mauborgne to reorganize the signal detachments, taking them out of the control of the signal officers in the areas where they were located and placing them all under the centralized command of the Second Signal Service Company located first at Fort Monmouth and then in Washington, D.C.

When H. O. Yardley’s *The American Black Chamber* appeared in 1931, it not only embarrassed the U.S. government which was shown to be reading the allies mail, but alerted the Japanese to the fact that we could read their codes. They scrapped their old systems and adopted new, more secure cryptosystems that would force Friedman and his team to start from scratch. The Navy would help, taking on all of the Japanese codes except Purple, freeing up some time for Friedman and his associates to tackle one of the most complex diplomatic codes to be devised in the days before computers. He was told in February 1939 to drop all other projects and concentrate on Purple.

On 23 December Friedman was promoted to full colonel, given a full medical exam, and placed on active duty in preparation for a trip to England. But he would not make the trip. Instead he was taken to the neuropsychiatric ward of Walter Reed General Hospital suffering

from extreme nervous fatigue “marked stress due to prolonged overwork on a top secret project.”<sup>8</sup> He was released on 22 March and back at work by 1 April 1941. It was the end, however, of his career in the U.S. Army reserve. He received a letter from the Adjutant General telling him that he was being honorably discharged “by reason of physical disqualification.” He continued with the Signal Intelligence Service in his civilian capacity, spending the war in mufti, his characteristic bow tie and black and white wingtips marking him as fastidious in his dress as well as his code work. After the war a medical board would conclude that he was fit for full active duty so he was retired in the rank of colonel that he had held in 1941.

In 1947 when he began working as the Director of Communications Research for the Army Security Agency, it was discovered that the man at the heart of the most secret work in the U.S. Army had never been given a security clearance since his demobilization after World War I. He was also being carried on the books, after 25 years of service, as a “temporary” employee.

A colleague at this time described his approach to cryptologic work. “Mr. Friedman was meticulous in his work habits, whether on staff policy papers or in technical exposition. He would first think out the problem or situation in broad outlines, and then would map out points a, b, c, ...n in logical progression, with clarity of exposition and the greatest attention to detail. He wasted but little time or motion, and especially on technical matters he knew instinctively when he was on the wrong track—a splendid attribute for any cryptanalyst. He had immense drive, and knew how to organize his colleagues for the most effective teamwork to achieve the maximum efficiency of effort.”<sup>9</sup>

After the war Friedman applied for the declassification of a patent he held for a ciphering machine known as the M-228. He was told it was necessary to keep the patent secret, denying him any chance at making money from commercial rights. He would enter into a long legal wrangle with the government and could not even tell the lawyers he hired about the patent he was suing to get back. His financial losses were estimated to be in the millions of dollars. He would obtain a victory of sorts, the courts granting him \$100,000 in lieu of the profits he could not get because of the secrecy involved. But it was again a strain on his health. In the winter and spring of 1949-50, he had another breakdown, suffering from depression.

He was struck by heart attacks in 1955, but his services were so valuable to the NSA, in both writing training lectures and consulting, that he was allowed to work at home with a secretary assigned to him. He retired from the agency in August 1955 and received the National Security Medal from Allen Dulles, then Director of Central Intelligence. In 1957 he was again called upon to undertake a secret liaison trip to England to consult in matters of NATO cryptography. In 1958 he undertook two more such trips.

Friedman did receive public recognition for his three decades of service. In 1944 he became one of the first to receive the newly created Commendation for Exceptional Civilian Service. In 1946 President Truman gave him the Medal for Merit, the civilian equivalent of the Distinguished Service Medal. It cited him “for exceptional technical ingenuity which ranks him among the world’s foremost authorities.” He added the National Security Medal in 1955, making him and J. Edgar Hoover the only persons to hold both the National Security Medal and the Medal of Merit.

He began to be a critic of the NSA in the late 1950s for what he thought was the agency’s obsession with secrecy. He wrote that overclassification had become “a handicap rather than a help in National Defense.”<sup>10</sup> In the mid-1960s he was writing, “I am hampered by restrictions which are at these times so intolerable and nonsensical that it is a wonder that I have been able to retain my san-

ity.”<sup>11</sup> That his sanity was a tenuous thing was a medical fact. In February 1963 he was back in the hospital with deep depression.

About one chief of staff at the NSA, a major general, he had this to say: [his] only claim to fame was that his occupational specialty was that of ‘mule specialist’ (honestly) and the Army by then had very few mules indeed—but a major general of course had to have a job commensurate with his rank. And in such cases soldiers of his rank are more or less automatically shoved into ‘Intelligence’—which the guiding lights of the Army and of the War Department thought (and still think) very little of professionally.”<sup>12</sup>

Friedman had good reason to think his superiors had gone too far. He was being shadowed when he made public lectures to make sure that he was not deviating from the agencies rules. His home library was raided by Army agents and 48 of his personal writings were confiscated, books or papers that dated from the first world war, had long been declassified, and were on the shelves of the Library of Congress. They took his published paper of the Zimmerman telegram which had been declassified in 1953 and reclassified it “Confidential.” He wrote a friend that “the secrecy virus [had] reached its height of virulence and the NSA took away from me everything that some nitwit regarded as being of a classified nature.”<sup>13</sup>

The man who broke Purple died on 2 November 1969 of a heart attack, after suffering an attack earlier in the year. He was buried in Arlington National Cemetery with full military honors a few days later. An academic building at Fort Huachuca is named for him.

His brilliance as a cryptographer is unquestioned. It was said of Friedman that he had the Midas touch. “Everything he touched turned to plaintext.”<sup>14</sup> But in addition to his technical contributions, he was the shaper of the Signal Intelligence Service. He built the staff, guided the policy, and most importantly trained the cadre of cryptographers and cryptanalysts that would play such an important role in wartime.

In the mid-1930s, he introduced electric tabulating machines to compile and card codes that would provide a the data base for future solution. This groundwork enabled one man to crack a code in two days that would have previously taken four men six weeks.

He single-handedly accomplished research, development, testing and, in some cases, fielding of new cipher machines that would become mainstays in the Army’s inventory for many years to come.

The dozens of men he trained before the outbreak of World War II would become the backbone of wartime communications intelligence and propel the U.S. Army COMINT effort over the decades to come.

Summarizing the impact that he made on military cryptography and cryptanalysis, it can be seen that his contributions reached far beyond the solving of the complex Japanese diplomatic ciphers. He was an unquestionable leader, employing vision, energy and genius in the cause of U.S. Army intelligence.

#### Notes

1. Friedman, William F., *Preliminary Historical Report on the Solution of the “B” Machine*, Special Research History-159, 14 October 1940.
2. Fabyan had been awarded the honorary rank of colonel by the Governor of Illinois for his work on the peace commission that drafted the Treaty of Portsmouth which ended the 1905 Russo-Japanese War.
3. Clark, Ronald, *The Man Who Broke Purple: The Life of Colonel William F. Friedman Who Deciphered the Japanese Code in World War II*, Little, Brown and Company, Boston, 1977.
4. *Ibid.*, p. 64.

5. *Historical Background of the Signal Security Agency*, Volume III, Prepared Under the Direction of the Assistant Chief of Staff, G-2, 12 April 1946. (Also known as Special Research History 001.), p.26.
6. Clark, p. 120.
7. *Historical Background of the Signal Security Agency*, pp. 233-4.
8. Clark, p. 158.
9. Callimahos, Lambros D., "The Legendary William F. Friedman," Signal Research History 058, 25 October 1974, declassified 16 June 1980, pp. 4-5.
10. Clark, p. 248.
11. *Ibid.*, p. 249.
12. *Ibid.*, p. 249.
13. *Ibid.*, p. 252.
14. Callimahos, p. 6.