Return to N.C. Gerson
- ONLY COPY -

THE LEGENDARY WILLIAM F. FRIEDMAN

By Lambros D. Callimahos

February 1974

"To my disciple, colleague, and friend, Lambros Demetrios Callimahos--
who, having at an early age become one of the great flautists of the world,
deserted the profession of musician, in favor of another in which he is
making noteworthy contributions--

From

William F. Friedman--

who, having at an early age aspired to become noted in the field of biology,
deserted the profession of geneticist, in favor of another, upon which he
hopes he has left some impression by his contributions.

In short: From deserter to deserter, with affectionate greetings!

W.F.F.

Washington, 21 November 1958"

(Facing page 1)

THE LEGENDARY WILLIAM F. FRIEDMAN

By Lambros D. Callimahos

Unclassified

PROLOGUE

When I joined the U.S. Army to enter the cryptologic service of my adopted country on February 11, 1941, William F. Friedman was already a legendary figure in my eyes. I had read two early papers of his, "L'indice de coïncidence et ses applications en cryptographie" and "Application des méthodes de la statistique à la cryptographie," when I was living in Paris in 1934, concertizing as a flute soloist throughout Europe while privately pursuing an active hobby of cryptology, which I felt would be my niche when the time came for me to enter the army. (Besides the U.S. Army, I was also liable for service in the Greek, Egyptian, and Turkish armies, and barely missed being in one of the latter.) As a member of the original group of 28 students in the Cryptographic School at Fort Monmouth, N. J., I was overjoyed when I found that Mr. Friedman's texts on Military Cryptanalysis were to be our Old and New Testaments combined.[1]

I did not meet William Friedman until after our school moved in October of 1942 to Vint Hill Farms Station, Warrenton, Va. The previous summer I had been promised a direct commission by the Headquarters staff of Fort Monmouth. At that time I was, as a senior private first class--I had the rank that went with the job--head of the language department and taught Italian and cryptanalysis and, since I was presumably indispensable on weekdays, pulled KP only on Saturdays and Sundays. Tired of waiting, I went to Officer Candidate School and graduated with my class in August 1942.

It was at Vint Hill that Mr. Friedman first paid us a visit, and we were all properly impressed at the dapper figure with the Adolph Menjou moustache, the characteristic bow tie, and the two-tone black-and-white shoes--the cryptologic giant who asked the most searching questions and understood our answers even before we had finished our explanations. Having been at Vint Hill for 14 months and, thinking that I might be stuck there for the duration of the war (I was Chief Instructor in cryptanalytics, with several hundred students in the school), I seized the opportunity, when Mr. Friedman again visited us, to ask him to get me out of there. In two weeks I was transferred to Arlington Hall Station where I was to have been assigned to Mr. Friedman for four months to

[1] The way I got into the Cryptographic School was no accident. I paid a courtesy call on my New York City draft board complete with waxed mustache, goatee, big black hat, Chesterfield coat, spats, gloves, and cane, like something out of a Dumas novel. When I showed them the list of 40-some works on cryptology I had read in preparation for eventual military service, the board sent me to Army Headquarters in Church Street, and they in turn sent me to Governor's Island, where G-2 arranged for what I thought was to be Army service of one year in the Cryptographic School.

write a course in operational cryptanalysis and then to have been sent to Europe. The Army, though, has a wonderful way of working. The officer to whom I was to have reported was on leave; I reported to the wrong officer, was sent to the wrong building, found myself two weeks later enrolled in a Japanese course, and it was made perfectly clear that my destiny was eventual service in the Far East. Mr. Friedman discovered my predicament too late to do anything about it, so after a year at Arlington Hall I went to New Delhi as an Assistant Signal Intelligence Officer for the China-Burma-India Theater. When the war was over I was sent as a junior captain to Leavenworth (to the Command and General Staff College--not to that other place). When I graduated in February 1946, Mr. Friedman requested my assignment to ASA, and I was detailed as his Technical Assistant.

FRIEDMAN THE MAN

My respect and admiration for the man for whom I worked increased with every contact and discussion. At first, our relationship was most formal--"Captain C." and "Mr. Friedman." Later on it became "Cal" and finally "Lambros," but it was always "Mr. Friedman." It took Mark Rhoads, his administrative assistant and colleague of long standing, a dozen years to call him "Bill"; and Mr. Friedman was "Bill" only to his friend and respected colleague Brigadier John H. Tiltman, to the Chief, ASA, and to a handul of senior military officers. To the rest, including his closest associates of the early 30's--Solomon Kullback, Frank Rowlett, and Abraham Sinkov--he was <u>always</u> "Mr. Friedman" even when they were not in his presence.

I used to speak of him affectionately as "Uncle Willie"--when not within earshot; the sobriquet caught on and became widespread at Arlington Hall, and when he learned of the appellation he was amused. But once, at an Agency party when the two of us were by ourselves at the canape table and I called him "Uncle Willie," I was made aware of my impertinence. One simply did not take liberties with WFF.

Mr. Friedman's desk in his private office in Headquarters Building at Arlington Hall was about 15 feet from mine in the outer office, but much of our daily contact was in the form of written notes. I would screen incoming technical papers and pass on to him those meriting his personal attention, with a buck slip. He would buck notes back and forth to me, sometimes exchanging six or seven notes: Mr. Friedman was fond of written records. Since he did superior work himself, he expected that all those around him would also do the same, without question. Compliments were hard to come by. Once, when I did something evidently worthy of particular notice, he wrote on a note, "Capt. C.--Good!" I poked my head into his door and inquired solicitously "Are you ill, Mr. Friedman?" "No, why?", he replied. I answered "You wrote 'Good!' on your note." He laughed, and from then on he allowed himself an occasional complimentary adjective that greatly added to the psychic income that was already mine in having the privilege of working with him. On another occasion when I outlined what I thought was an especially good idea, he listened patiently and, when I had finished, said: "That's fine. I have a patent on that." At another time I received his compliments on an original procedure, until I found out a couple of weeks later that he had already written about it and had forgotten about it, so I embarrassedly brought it to his attention. Homerus nutat.

As an Army captain, I was very proud to work for Mr. Friedman, in view of what he had done and was doing for his country. Always a stickler for le mot juste, he abhorred imprecise or inelegant language. Once, when I did not use the term "repetition" when he felt that I should have, he said: "Don't ever use 'repeat' as a noun again!" When I found that the dictionary recognized the use of "repeat" as a noun, I was a bit miffed, but I swallowed my pride and was very careful in the future how I expressed myself to the Great One. On another occasion, when he came across the cover name ICKY in a technical report he blew his top, exclaiming that this word made him puke /sic/.

Mr. Friedman had complete faith in his subordinates--otherwise, he felt, they wouldn't be working for him. He took for granted that I knew all that was necessary to know about cryptanalysis--a most flattering compliment, but unrealistic. One day a paper came through on a most complicated and abstruse phase of a technical matter about which I comprehended not even the title. I shrugged my shoulders and bucked the paper to him, feeling that this certainly was one matter with which I should have absolutely nothing to do, especially since three leading technicians of the Agency differed among themselves as to the merits of technical points. To my horror, Mr. Friedman bucked the paper back to me with a note, "Captain C.: please study and prepare comments for me." I was frantic. But I spent the next three days working 18 hours a day, did some historical research on the problem, spoke with technicians on the project, fortunately came up with a refutation of points held by the author of the paper, discovered a new approach, and drafted a substantive reply worthy of William Friedman. It wasn't until many years later that I told Mr. Friedman how that one paper made me sweat blood--he of course had blithely assumed that I was versed in all matters of cryptanalysis, including that one.

When I was first assigned to Mr. Friedman's office I was living in a room on the third floor of Headquarters Building: my family was still in New Jersey, where they had been while I was overseas, as apartments were almost impossible to obtain in the immediate post-war years in Washington. I was working two shifts: the day shift for Mr. Friedman, the swing shift for me. With Mr. Friedman's knowledge and permission, I went systematically through all his files, reading hundreds of technical reports over a period of many months, trying to remember all I could in this unparalleled opportunity for acquiring a comprehensive technical education. The effort paid off when my boss asked me about things I had already digested and on which I was now knowledgeable: my ready answers strengthened his conviction of the extent of my cryptanalytic knowledge.
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.

In his technical writings, Mr. Friedman was a man of punctilio. In the first book that he wrote for the U.S. Government, "Elements of Cryptanalysis," a little gem of 157 pages published in May 1923 by the Office of the Chief Signal Officer, he brought order into the chaos of cryptologic exposition of previous authors in the public domain. This work he expanded in the late 1930's into his classic textbooks, *Military Cryptanalysis*, Parts I-IV. He had a flair for the dramatic, as witnessed by the following extract from one of his technical papers[2] in which he not only had two successive sentences ending with exclamation marks, but with some italics thrown in for good measure:

> "A set of fifty test messages, each 25 letters in length and beginning at the same initial enciphering juxtaposition, was submitted by Mr. Burdick. By superimposing the messages the writer solved them and completely reconstructed both basic alphabets, *by applying and extending the principles of indirect symmetry of position that were first discovered by Mr. Burdick himself!* It is not often that a cryptanalyst unknowingly discovers the very weapon that deals the deathblow to his own brain-child!"

It's too bad that not many tellers of cryptologic tales emulate the patterns set by the Master.

On a couple of occasions in the early 1950's I received brief handwritten notes from Mr. Friedman asking me to do something or other which I felt really wasn't necessary. So I just let the notes go by, hoping he would forget about them. Several weeks later, he asked me what I had done about the items, and I lost no time in doing what he asked me to do in the first place, marvelling at his memory. Much later I found out his secret: he kept *carbon copies* of everything he wrote in longhand, no matter how brief! I was shocked: I never really got over what I considered to be a very unethical and underhanded way of doing business. After he retired in 1955 I was bold enough to tell him of my feelings, and he got a kick out of my reaction to his craftiness.

Mr. Friedman had a fine sense of humor, but his was a passive one, enjoying others' overt actions. He was particularly fond of me and enjoyed my company, considering me a character (this proves that Mr. Friedman was not always infallible in his judgment), and after he retired and we became fast friends I was able to pull his leg (in private, of course!) and treat him more irreverently than anyone else dared. Only once, however, did I overstep my bounds. He never like to think of eventual death, and I had the temerity to suggest to him that after he passed on to the Great Beyond he should will his body to NSA so we could stuff him and prop him up in a corner of the Cafteria. Needless to say, *that* went over like a lead balloon.

[2] "The Principles of Indirect Symmetry of Position in Secondary Alphabets and their Application in the Solution of Polyalphabetic Substitution Ciphers," Office of the Chief Signal Officer, Washington 1935.

I used to smoke Roi Tan Golfers, little cigars about $3\frac{1}{2}$" long. Once in the late '50s when I was visiting Mr. Friedman at his home, he asked "Why do you smoke those little cigars?" I replied that I liked their taste and convenient size. "You know, somebody might think that's an affectation," he said, as he dipped into his engraved silver snuff box. I asked him if I might try some of his snuff, gingerly placed some in each nostril, sneezed, blew my nose (into a handkerchief), and found that it was a pleasant sensation. So for the next dozen years I gave up smoking in favor of snuff, and I collected over 170 varieties from all over the world. What bothered me, though, was that as soon as I had gotten hooked on snuff, he quit. Now that's no way for a pusher to act, I thought. (I myself quit in 1971, one less vice in my repertoire.)

In the years after his retirement, Mr. Friedman used to call me several times a week. The phone would ring, I'd pick up the receiver, and a voice would say "Cal?" I would reply, "Yes, Mr. Friedman." At other times the voice would say, "Professor?", and again I would reply, "Yes, Mr. Friedman." Once, however, when I picked up the phone and all I heard was someone clearing his throat, I said, "Yes, Mr. Friedman," and he was too startled for words: he never got over it. How could I explain to him that a musician's ear could recognize the "harrumph" of a particular speaker? This is closely correlated with linguistic talent, and Mr. Friedman was not conversant with any language other than English; but that did not prevent him from achieving significant successes with cipher messages in Japanese and other languages.

Mr. Friedman often relived his earlier years, and he found mine a willing ear as he recounted his early triumphs and successes. His career was rich in experiences, richer perhaps than anyone in the cryptologic world has had, before or since. I would ask him about technical points, and he would outline for me a particular solution that he had accomplished years before. I sincerely regret not taking notes of our discussions, for somebody should have been a Boswell to his Johnson.

During the last several years of his life, I was Mr. Friedman's close confidant. There were times when he felt depressed, that the world was no damned good, and that he really hadn't done anything to make it a better place to live in. Of course I vehemently disagreed, pointing out all he had done for his country (as if he didn't know!). He often asked my advice on various matters, technical and nontechnical, so I proposed that he retain me as an advisor for a dollar a year: after all, he didn't have to take my advice, but if he paid me he would respect me more. Several months ago Mrs. Friedman found among her husband's effects a note reading "Pay Cal a dollar a year."

Mr. Friedman always had a very inquiring and discerning mind. He was a bibliophile, a gentleman, and a true scholar. He was astute in judging character, and he could read his adversaries like a book. He was, as I have indicated before, very sensitive on interpersonal relationships, and he relished the friendship and acquaintance with high persons in the government and in industry, both here and abroad. He was an elegant dresser, prided himself on his ability as a ballroom dancer, and was a golfer of no mean stature.

FRIEDMAN THE CRYPTOLOGIST

William Friedman was blessed by phenomenal luck throughout his entire career as a cryptanalyst--everything he touched turned to plain text, a sort of latter-day Midas. But since this luck was so consistent it couldn't have been just luck; on the other hand, it *must* have been luck. He was a young man when he started, and therefore had the courage of his convictions and the boldness of youth. He started young enough not to be scared of the magnitude of the problems facing him: had he been a Ph.D. with three or four years' post-graduate training, he could have been ruined. His definition of a cryptogram was simply a secret message that was meant to be solved, just that. Time and again he *shouldn't* have been able to solve a particular message or a cryptosystem, but *he did*: the odds were against him, but luck was for him. That is, luck tempered by logical insight and remarkable intuition. Some of his early solutions may seem almost childish by present-day standards, but William Friedman was the first child of any age to arrive at those solutions.

He wasn't disturbed by the apparent odds against him: after all, even a simple substitution cipher in a literal system involves $26!$ ($= 4.03 \times 10^{26}$) possible alphabets, and it can be demonstrated that, if there existed a computer capable of testing 1,000,000 alphabets per second, even if we had 1000 of these computers it would take over 1 billion years to run the gamut of all the alphabets. He might have countered that, since there is a .5 probability of success halfway through, he would expect results after only 500,000,000 years.

There is no least common denominator of what makes a brilliant cryptanalyst: he *can* be a mathematician, but he may just as likely be an archeologist, a chemist, a biologist, a musician, a gambler, a painter, or a cook--in short, just about anything. Now Mr. Friedman's background in mathematics was slight: college freshman mathematics. Even if he computed odds incorrectly, it didn't make any difference because he would forge ahead in his blissful ignorance and solve the problem anyway. On several occasions he told me that if he had had more of a mathematical background, he might not have been able to solve some of the things he did. Mr. Friedman may not have been a mathematician, but he had superb mathematical feeling and insight, inventing techniques that were missed by mathematicians working on the problem. A classic example of his innovative abilities was in his solution of the Hebern machine in 1923, the first solution in history of a wired-rotor cipher machine. He postulated that there were 91,000,000,000 alphabets involved when there were really only 45,000,000,000 and--in spite of his modest mathematical background--originated an important theory of coincidence and, with only ten messages, arrived at a solution of the machine.

I told Mr. Friedman of an ancedote I used to relate to the students in my classes as an example of his lack of mathematical profundity, but stressing to them that this had absolutely no bearing on his prowess as a cryptologist. In his 1923 work, "Elements of Cryptanalysis," he gave on p. 105 three 72-letter transposition messages with the following footnote:

> "As an example of a most remarkable coincidence, note the appearance of the word CIPHER in the cipher text of the third message. Theoretically, such an event will happen, as a result of chance, once in 26^6 (=308,916,776) times. The word CIPHER does not appear in the plaintext message at all!"

What Mr. Friedman did not note was (1) that the cipher texts did not approach the appearance of random text but were composed of a good assortment of letters as found in English plain text; (2) that in calculating probabilities, he did not take into account in which message, nor at what position in that message, the word should be; and (3) that he was not even looking for that particular word in the first place. Mr. Friedman always got a charge when I related this anecdote. To offset this mathematical lapse, though, it must be remembered that his paper written in 1922, "The Index of coincidence and its applications in cryptography," was the pioneer paper in cryptomathematics.

As a simple example of the perpetual luck which plagued him, a case may be cited of a 443-letter cryptogram submitted to the War Department for solution[3]. The cipher text factored to 10 alphabets, and Mr. Friedman unerringly selected equivalents for plaintext E in some of the alphabets when the next highest cipher values were only 1 or 2 tallies less than the supposed E plain, and he derived five other values scattered sporadically in the cipher message. At this point he focussed his attention on the beginning of the text, which he had thus far deciphered as - - T T H - - - - - -. It must begin, said Friedman, with the words BUT THOUGH--and it did. Well, I assure you, dear reader, that this will be the first and last time you will ever encounter a message beginning with the words BUT THOUGH: the Friedman luck paid off again.

Another unbelievable piece of luck occurred in 1917 when Mr. Friedman was at Riverbank Laboratories in Geneva, Illinois, where he was employed as a geneticist mating fruit flies (or rather, helping them to mate). The British knew of a geared disk cipher device invented much earlier by Sir Charles Wheatstone which was regarded as absolutely indecipherable if the sequences for both plain and cipher components were unknown. The British did not dare use it earlier in World War I, because if the Germans captured it they too would have the indecipherable cipher. But now, since the United States had entered the war, the British decided to use this device for joint U.S.-British communications since its indecipherability was acknowledged by both London and Washington. But somebody in Washington suggested that perhaps it might be wise to have the device tested by William Friedman at the Riverbank Laboratories which were operated by

[3] Cf. L. D. Callimahos and W. F. Friedman, Military Cryptanalytics, Part II, pp. 108-113.

a wealthy eccentric named Colonel George Fabyan, who had a quasi-official relationship with the Government.[4] Accordingly, five very short test messages--a most unrealistic test--were sent to Friedman, and by a process that remains a mystery to this day he was able to scrounge out from the cipher texts the sequence for the cipher component, a numerical-key columnar transposition-mixed sequence based on the word CIPHER. But now he was stumped, since he didn't quite know what to do next (it wasn't until 1923 that he discovered the principle of reduction to monoalphabetic terms, which would have made the problem a very simple one). But he called in one member of his staff, his wife Elizebeth, told her he was going to give her a certain word, and asked her to give him the first word that occurred to her. He said "cipher," and she replied "machine." Sure enough, the plain component was a numerical-key columnar transposition-mixed sequence based on MACHINE. And one of the messages read "This cipher is absolutely undecipherable." The solution went back to the British and, although 11,000 of the devices had been manufactured, they were never used.

Mr. Friedman returned to Riverbank Laboratories after the war: he had been in France as a member of the Code and Cipher Solving Section, G2 GHQ AEF. At Riverbank occurred a third example of how he was hounded by incredible luck. The AT&T Corporation had devised a very complicated cipher teleprinter, adjudged to be beyond the realm of solvability. But though (there, I did it!) the system was good indeed, there was still a Friedman to be reckoned with. Accordingly, a set of 150 cipher tapes was dispatched to Riverbank, and for six weeks, sometimes working 12 hours a day, Friedman and his staff of six studied the traffic. His staff was disheartened: this was the first time they spent such a length of time on a system without solving it, and they wanted to quit. Friedman, though, was sure that his methods were correct--therefore was it not possible that either he or one of his assistants had made an error in transcribing the punched tapes into characters on paper? He asked them to hang on for one more week to review their work. Sure enough, in checking, he discovered that one character had indeed been omitted accidentally in transcribing one of the tapes--but that character was at a very crucial point. Within minutes, he made an entry into the plain text, and the system was solved.[5] To make the solution even more convincing, a punched tape was laboriously prepared by hand and sent to Washington with the proper indicators: when the tape was set on their machine and the message read, it gave the proof of the solution.

[4] Fabyan's title was an honorary colonelcy conferred by the Governor of Illinois for Fabyan's participation as a member of the Peace Commission that negotiated the Treaty of Portsmouth, which terminated the Russo-Japanese War in 1905. One of Fabyan's fields of interest was cryptography, and in the latter part of 1916 he established a Department of Ciphers at Riverbank, first headed by Miss Elizebeth Smith and later by Mr. Friedman, who took over both the Department and Miss Smith. The Department of Ciphers conducted cryptanalytic work for the State, War, Navy, and Justice Departments, since at the time none of these organizations had any cryptanalytic units whatsoever until the Army established a unit (under Herbert O. Yardley) in the latter part of 1917.

[5] For Mr. Friedman's own account of this solution, see "Can Cryptologic History Repeat Itself?", NSA Technical Journal, Vol. XVIII, No. 3, Summer 1973.

All of these wonders William Friedman accomplished without the benefit of any machine aids whatsoever. In fact, during Riverbank days he invented the very first mechanical cryptanalytic aid made in the U.S. It was called the poly-alphabet wheel" and consisted of the 26 letters A through Z on a rubber-faced wheel which, when inked, could be used for running down the alphabet from a predesignated initial letter. The device was improved by assembling ten such wheels together so that the plain-component sequences could be completed on ten letters at a time, but this required the services of a muscular cryptanalyst to bear down on the roller.

On January 1, 1921, Mr. Friedman began a six-month's contract with the U.S. Army Signal Corps to prepare cryptographic systems, and the contract was renewed for another six months. In 1922 he was hired as the sole cryptanalyst in the Signal Corps, with a cauliflower-eared ex-professional boxer as a secretary. Until April 1, 1930, the entire cryptologic organization of the U.S. Army still consisted only of Mr. Friedman and one clerk-typist. During that first week in April, the Signal Intelligence Section was expanded by the addition of three young high school mathematics teachers recruited by Mr. Friedman as junior cryptanalysts: Solomon Kullback, Frank Rowlett, and Abraham Sinkov, who were to remain in cryptologic work, making notable contributions for over three decades and rising to high positions in NSA and its predecessor organizations.[6]

An amusing story is connected with a challenge message submitted to the Signal Corps in 1933 by a New York lawyer representing his client, a poor devil who had bought, for $100,000, the North American rights to a cipher machine invented in 1924 by Alexander von Kryha of Germany. The machine was touted by the inventor as absolutely indecipherable, and a German mathematician had demonstrated that the number of ways in which a message could be enciphered was $2.29x10^{82}$, a figure 100 million times as large as the number of atoms in the universe. Friedman had studied the machine earlier, and had demolished it along with everything else he studied. After an exchange of correspondence with the lawyer, Friedman told his superior that it might be a profitable training exercise for his subordinates if the 200-word challenge were accepted. Accordingly, the lawyer prepared a message enciphered on the machine, the alphabets and initial setting being secret. The message, in triplicate as requested, was received on February 24, and was date-stamped "Feb 24 AM 11:12," with the notation in Friedman's handwriting, "Commenced work. W.F.F." On another part of the message was the pixie-ish observation, "Time out during lunch period, 50 minutes. W.F.F." And then over the date-time stamp "Feb 24 PM 2:43," was the cryptic notation, "Solved. W.F.F." Elapsed time: 3 hours and 31 minutes, less 50 minutes for lunch--2 hours and 41 minutes! A letter with the decipherment and the keys was sent to the lawyer that afternoon. This solution in 2 hours and 41 minutes is remarkable not only because of the absence of any machine aids at that time,[7] but

[6] In selecting his personnel, Mr. Friedman picked the three persons from the civil service list who had made the highest scores on the mathematics examination.

[7] It was not until 1936, after Mr. Friedman's continued insistence, that the Army obtained its first IBM data processing machines for cryptologic purposes.

particularly so for the light it throws on Mr. Friedman's direction and organization of the cryptologic effort of his three assistants. As a result of this solution the Signal Intelligence Section gained renewed respect and--far more important--recognition at the highest Army levels and increased fiscal support.[8]

Cryptologic literature in the 1930s was woefully inadequate.[9] Mr. Friedman therefore embarked on a program of translating foreign works in the public domain, and of publishing technical reports of the solution of cryptosystems studied, in order to begin collecting a body of literature for training cryptanalysts in the years to come. As a consequence, during an eight-year period in the 1930s the members of the Signal Intelligence Section (numbering not more than eight at any one tine, including student officers) wrote over 16 books of expository technical works in cryptanalysis.[10] Friedman systematized the art, and unfolded the science in his classic four volumes, *Military Cryptanalysis, Parts I-IV*. When Kullback, Rowlett, and Sinkov were recruited, they spent their first two years with Mr. Friedman in a course of study, consisting of a series of cryptanalytic problems prepared by the latter; the textbook was "Elements of Cryptanalysis," then the finest work extant. In 1931 1st Lt. Mark Rhoads was assigned to Mr. Friedman for one year, to learn all there was to know about cryptography and cryptanalysis. Towards the end of his year, Lt. Rhoads wrote a memo to the Chief Signal Officer saying that one year was insufficient to learn all there was to know about cryptology: it would take two years. Consequently, Lt. Rhoads was kept on for a second year and became the instructor for 1st Lt. W. Preston Corderman, who was assigned for a two-year tour. The Signal Intelligence School was formally established, and Lt. Corderman (later to become Chief, Army Security Agency) was the instructor for the next student, and so on for a number of student bodies consisting of two each. Thus was established the groundwork of scientific cryptanalytic training.

Friedman studied many proposals for cryptographic systems, embracing both manual and machine methods, demolishing everything that came his way. Good cryptographic ideas were hard to come by, as requirements were stiff and standards set were high. One machine that was studied, the IT&T cipher machine with ten large cam wheels for teleprinter encipherment, had a period of 8.65x10^{14}: the inventor and his sponsors claimed that cryptograms produced by the machine were practically, if not absolutely, indecipherable without the key. It took almost four years to construct the machine, at a cost of approximately $100,000--but it took Friedman and his staff less than three hours to break it. In another case, an ingenious machine fractionated a plaintext letter into two parts, subjected these fractional parts to a complex substitution, and finally recombined the parts

[8] For the story of this solution in detail, see L. D. Callimahos, "Q.E.D.--2 Hours, 41 Minutes," *NSA Technical Journal*, Vol. XVIII, No. 4, Fall 1973.

[9] Cryptologic literature in the 1970s is woefully inadequate.

[10] In a memorandum which I sent on June 14, 1960, to the Director of Training, NSA, I pointed out that by comparison, NSA should have published approximately 3200 books in the last 8 years, but that the true figure was less that 16, or one-half of one percent of the productivity of the early Army effort.

to produce a single cipher letter: this was a brilliant idea that did not long withstand Friedman's scrutiny. In addition to his ability to destroy everyone else's ciphers, Friedman was able to invent a number of cryptographic systems for his country that would withstand sophisticated attack by enemy cryptanalysts. For his inventions Congress in 1956 awarded him $100,000 in compensation for profits he might have realized if the patents had not been held secret by the Government.

Because of Mr. Friedman's foresight and pioneering efforts in cryptanalysis, cryptanalytic training, data-processing machine utilization, and cryptanalytic organization, the U.S. Army was fully prepared to meet the cryptologic challenges of World War II. Friedman took part in all these aspects during the war and continued to make notable contributions. After the war a most spectacular role of cryptanalysis was revealed in the hearings held by the joint congressional committee on the investigation of the Pearl Harbor attack. At that time it was made public that, shortly before the war, the U.S. in a brilliant stroke of cryptanalysis had been able to reconstruct the Japanese cipher machine which was used for the highest-level diplomatic communications, enabling this traffic to be read throughout the war. The successful solution of this machine, known by its cover name as the PURPLE machine, represented 18 months of intensive study by a group of U.S. Army cryptanalysts under the direction of William F. Friedman.

Mr. Friedman continued after the war as Director, Communications Research, under whom I was privileged to work as an Army officer. With the establishment of the Armed Forces Security Agency in 1949, he became Chief of the Technical Division and I was once again working for him, but this time in civilian clothes. In 1952 the National Security Agency was created; he was now Technical Consultant to the Director, and two years later was named Special Assistant to the Director, the post he held until his retirement in 1955, after over 35 years of service with United States cryptologic activities.

EPILOGUE

His inventions and many achievements won for Mr. Friedman the nation's highest awards and a reputation as one of the world's leading cryptologists. In 1944, he was presented the War Department's highest decoration, the Exceptional Civilian Service Award; in 1946, he was awarded the Presidential Medal for Merit; and in 1955, Mr. Allen Dulles, then Director of Central Intelligence, presented him the National Security Medal, the country's highest award for contributions to the national security. He was the author of many classified publications and training texts, of articles in scholarly journals, and of the articles on cryptology in the 1927 and 1954 editions of the Encyclopaedia Britannica. With his wife (who was for years a cryptologist with the Treasury Department), he wrote the book, The Shakespearean Ciphers Examined, for which they were were awarded the Folger Shakespearean Literary Prize and the Fifth Annual Award of the American Shakespearean Festival Theater and Academy.

On Sunday, November 2, 1969, William Frederick Friedman died quietly at his home in Washington, D.C., and was buried with full military honors in Arlington Cemetery. The legendary figure is with us still--in the works he left behind, in the science he created, and in the inspiration he bequeathed to his colleagues and friends.

Curriculum vitae

WILLIAM F. FRIEDMAN (1891-1969), dean of modern American cryptologists, the most eminent pioneer in the application of scientific principles to cryptology who laid the foundation for present-day concepts. Born in Kishinev, Russia, on September 24, 1891, he came to the United States in 1892; he retired from the National Security Agency in 1955, after 35 years of service with U.S. cryptologic activities, and died at his home in Washington, D.C., on November 2, 1969.

B.S. (Genetics), Cornell University, 1914; Research Fellow, New York State Experiment Station, Geneva, N.Y., 1914; Graduate Student and Instructor in Genetics, Cornell University, 1914-1915; Director, Department of Genetics, Riverbank Laboratories, Geneva, Ill., 1915-1916; Director, Departments of Ciphers and Genetics, Riverbank Laboratories, 1916-1918; 1st Lt., N.A., serving in Code and Cipher Solving Section, G2, GHQ AEF, Chaumont, France, 1918-1919 (retired as Lt. Col., USAR, 1951); Director, Department of Ciphers, Riverbank Laboratories, 1919-1920; Cryptographer, Office of the Chief Signal Officer, Washington, D.C., 1921; Cryptanalyst, War Department, 1922-1947; Director, Communications Research, Army Security Agency, 1947-1949; Cryptologic Consultant, Armed Forces Security Agency, 1949-1951; Research Consultant, National Security Agency, 1951-1954; Special Assistant to the Director, NSA, 1954-1955 (retirement); Member, NSA Scientific Advisory Board, 1954-1969; Special Consultant, NSA, 1955-1969.

For his many contributions to the security of his country, he received the War Department Medal for Exceptional Civilian Service (1944), the Presidential Medal for Merit (1946), the Presidential National Security Medal (1955), and a special congressional award of $100,000 for inventions and patents in the field of cryptology held secret by the Government (1956). For their contributions to literature, he and Mrs. Friedman received the Fifth Annual Shakespeare Award in 1958 from the American Shakespeare Festival Theater and Academy for their book The Shakespearear Ciphers Examined.

Mr. Friedman was a member of Sigma Xi, the Cosmos Club, the U.S. Naval Institute, and The Shakespeare Association of America. He was listed in Who's Who in America and in American Men of Science.

Author of many classified books and brochures, technical treatises, and articles on cryptologic subjects; articles in the Signal Corps Bulletin (1925-1940); Riverbank Publications on Cryptology (1918-1922), the more important of which are "Several Machine Ciphers and Methods for Their Solution," "The Index of Coincidence and Its Applications in Cryptography," and "An Application of the Science of Statistics to Cryptography." Technical papers and reports published by the Office of the Chief Signal Officer and by the Signal Intelligence Service (1935-1945), among which may be mentioned "The Principles of Indirect Symmetry of Position in Secondary Alphabets and Their Application in the Solution of Polyalphabetic Substitution Ciphers," "American Army Field Codes in the American Expeditionary Forces During the First World War," "Analysis of a Mechanico-Electrical Cryptograph," and "Military Cryptanalysis" (revised and enlarged in the late 1950's by Lambros D. Callimahos in the "Military Cryptanalytics" series). Encyclopaedia Britannica article on "Codes and Ciphers (Cryptology)," 1927 (revised 1954). "Jacques Casanova, Cryptologist," in Casanova Gleanings, Nice, France, 1961. Co-author with his wife Elizebeth Smith Friedman, of The Shakespearean Ciphers Examined, 1957; "Acrostics, Anagrams and Chaucer," Philological Quarterly, 1959; "The Cryptologist Looks at Shakespeare" (Folger Literary Prize), 1955.