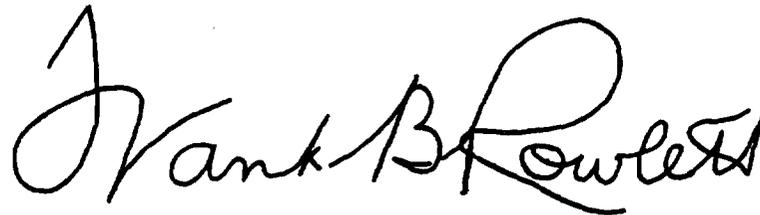




Frank B. Rowlett

Theodore M. Hannah



—A Personal Profile

Finally, Genevieve Grotjan finds the evidence we are looking for. Time is about 2 p.m. Ferner, Small, and I are at table in working area discussing prospects and reviewing work. Grotjan enters room, obviously excited, politely interrupts, asks if she can show us what she has found. She takes us to her desk in next room, lays out worksheets, points to one example, then another, then a third. She stands back, with eyes tranced behind her rimless glasses. Al Small dashes around the room, hands clasped above his head like a victorious prizefighter. "Whoopee!" he yells. Ferner, the quiet one, clasps his hands, shouting "Hooray, Hooray." I jump up and down — "That's it! That's it!" The room gets crowded; everyone in section suddenly in room. Friedman comes in and asks, "What's all the noise about?"

I settle down and say, "Look what Miss Grotjan has just discovered." Gene wipes her eyes, tries to regain her composure. I point to the worksheets — "Gene's found what we've been looking for. Look here, and here, and here." Friedman examines each one and understands what he sees; he looks suddenly tired. We take a break and send out for Cokes. The excitement gradually wears off and we look ahead to the next step.

That next step would soon lead to the solution of Japan's highest level diplomatic cipher system, the so-called Type "B" machine, better known as "Purple." What young, studious Genevieve Grotjan had discovered on that warm Friday afternoon in Septem-

ber 1940 represented the decisive breakthrough into a highly sophisticated machine system that for 18 months had stubbornly resisted the concerted attack by some of the best cryptanalysts in the world. Its solution has been called "the greatest feat of cryptanalysis the world had yet known," one which, in the words of another author, "involved a unique intellectual effort of heroic proportions." With its solution the United States became an unlisted subscriber to the communications network serving the Japanese Foreign Ministry and its major embassies abroad, and thereby gained important insight into Japan's diplomatic and military moves. The decrypts were also a primary source of information on Hitler's intentions in Europe, as reported to Tokyo by the Japanese ambassador in Berlin, Baron Oshima.

Present at the breakthrough into Purple, and indeed largely responsible for it because he was the cryptanalyst in charge of the Army's work on the Japanese diplomatic intercepts, was Frank Byron Rowlett, one of the very early members of the Signal Intelligence Service, the Army predecessor of NSA. This is the story of his early career, beginning more than 50 years ago.

It was a few minutes before eight o'clock in the morning on the first of April—All Fool's Day—1930. I was standing in front of the main entrance to the Munitions Building at 21st and B Streets, N.W., in Washington, D.C. In my hand was a letter telling me

to report at 8 a.m. to Room 3406 in that building. I was to be employed as a Junior Cryptanalyst in the Signal Service at Large, Office of the Chief Signal Officer, War Department. I was not quite 22 years old.

I had passed the Civil Service examination for Junior Mathematician the previous summer and had been hired as a Junior Cryptanalyst at \$2,000 per year, which was about \$500 more than my wife and I together were making as teachers in southern Virginia. I had no idea what a cryptanalyst did; I didn't even know what the word meant—I couldn't find it in the dictionary—but there was a lot of publicity at the time about bringing back the World War dead from Europe, and I naively thought I'd be doing some kind of statistical work on crypts! It wasn't until my first day at work that I learned, from William F. Friedman, Chief of the Signal Intelligence Service, what a cryptanalyst was. "I suspect," he said, "that there are only a very few people who know what the word 'cryptanalyst' means. In fact, the words 'cryptanalyst' and 'cryptanalysis' were officially adopted by the War Department only a few weeks ago, although I started using them several years ago. The first official use of these words was in the description of the duties of the staff of the Signal Intelligence Service, and you have the honor of being the first individual to be employed by the U.S. Government as a Junior Cryptanalyst."

Before my arrival, the Signal Intelligence Service (SIS) consisted of Mr. Friedman; his secretary, Annie Louise Newkirk; and Captain Norman Lee Baldwin, who was setting up the Second Signal Service Company, the collection arm of the SIS. By the end of the month we grew by another 50 percent when two more Junior Cryptanalysts, friends from high school and college, Abraham Sinkov and Solomon Kullback, started work.

Sinkov, Kullback, and I were hired because we had all studied math and foreign languages—Sinkov had taken French; Kullback, Spanish; and I, German. Friedman's efforts to round out the team with a combination mathematician and Japanese linguist had so far failed: the Civil Service Commission, Military Intelligence, and the State Department had all been unable to produce anyone with that rather unusual combination of talents. Soon, however, through the good offices of Congressman Schaeffer of Virginia, Friedman learned of a young man named John Hurt, the congressman's nephew, who, though lacking an extensive math background, was unusually fluent in Japanese. The Army major who interviewed him told Friedman that he had never met an American so proficient in that difficult language. "He is unbeliev-

able," he said. "He is fluent in conversation, he can read both forms of the written language, and his vocabulary is fabulous. He knows Japanese much better than I or, for that matter, anyone else in G-2." We learned later that Hurt had mastered the language mainly by rooming with Japanese students at college, where he had majored in Latin and French. While Hurt was processing for employment, the rest of us continued our cryptologic training under Friedman, using mainly his pamphlets and exercise books. As soon as Hurt arrived, Friedman wanted him to begin teaching us the rudiments of Japanese, for Japan was to be our number one priority.

Two very important things happened to me toward the end of that first month: I got my first paycheck and I rented an apartment. My pay for the first two weeks of work (we were paid twice a month) was the grand sum of \$83.33, only about \$8.00 less than I had received for a full month's work as a schoolteacher in Franklin County, Virginia. The apartment was in the old Boulevard Apartment building at 2121 New York Avenue, N.W., within easy walking distance of the Munitions Building; if I hurried, I could have lunch at home instead of having to eat at the Navy cafeteria, in which I was by now beginning to lose interest. The apartment was the barest minimum offered for living purposes in the area, consisting of a single room (with a so-called Murphy bed which folded up into the wall when not in use) and a small kitchenette and bathroom. It rented for \$50.00 per month furnished, with a free month's rent if it was occupied for a full year. I figured that my wife and I could make do with the one-room apartment for at least a couple of months until we could find something a bit larger, but still within our means.

It was not a good year for the American economy. The Great Depression was deepening, and military budgets, already small during those peacetime years, were shrinking even more. So austere was the Army budget that we sometimes had to supply our own pencils and paper. We bought penny pencils at the dime store, and we brought in scratch paper and tablets from home. We once had to take a temporary reduction in salary; another time, when funds ran out completely, we all had to take a month's leave without pay. My wife and I just closed up our apartment and took a springtime vacation on the farm in southern Virginia, so for us it was no particular hardship.

The Black Chamber Revisited

One hot, humid morning in late June 1930, Friedman came into the vault and asked Kully, Abe, and

me to accompany him to the G-2 area of the Munitions Building. He escorted us down the stairs to the second floor corridor without any explanation of the purpose of our trip. I clearly remember that I was wearing, for the first time, a brand-new summer outfit — a blue serge jacket, white pin-striped trousers, and white suede shoes. I recall that as we walked along the second floor corridor behind Friedman I was feeling very proud of myself for being so well dressed for what, judging by Friedman's attitude, seemed to be a very special mission.

When we arrived at the cross corridor of the seventh wing, Friedman swung to the left without missing a step. We followed closely behind. The cross corridor was deserted. After a few steps he turned abruptly to his right and stopped at Room 2742. He took from his inside coat pocket a small card, and started to operate the combination lock on the front of the steel door. We watched with high curiosity. When he had set the final number, he threw the bolt and swung open the door, exposing the second steel door behind it. He again reached into his pocket, extracted a key, and

unlocked the inner door, which he opened with a flourish. The area behind the second door was pitch dark. He now produced a small box of matches, lit one, and by its light sought out the pull cord of the switch of the nearest ceiling light. When the light came on, it revealed a room about twenty-five feet square, almost completely filled with filing cabinets, arranged back-to-back in double rows with barely enough space between them for the drawers to open. Friedman's next move was to switch on the electric fans to their highest speed and to turn on the remaining three ceiling lights. While he was going through this process, the three of us remained just outside the door, waiting for his instructions. He came back to the vault door, peered up and down the corridor, and then waved us inside the vault. When we were all inside, he set the inner steel panels slightly ajar and turned to us, saying in a solemn and very imposing manner: "Welcome, gentlemen, to the secret archives of the American Black Chamber!"

I was puzzled by the serious manner he assumed as he made the announcement. I had never heard of



The Signal Intelligence Service about 1935.

Seated: Mrs. Louise Newkirk Nelson. *Standing, left to right:* Herrick F. Bearce; Solomon Kullback; Captain Harold G. Miller, USA; William F. Friedman; Abraham Sinkov; Lieutenant L. T. Jones, USCG; Frank B. Rowlett. John B. Hurt was ill when the picture was taken.

anything called the American Black Chamber and the words meant nothing special to me, but I said nothing and neither did Abe or Kully; we just stood, looking as impressed as we could, surveying the dust-covered contents of the room.

Friedman then explained that the room contained the working files of a highly secret cryptanalytic organization that had operated in New York City for several years and which had been closed down during the previous summer. Military Intelligence had had an interest in this operation and had brought its files to the Munitions Building, where they were being held in storage. The files had been turned over to the Chief Signal Officer for the use of the Signal Intelligence Service, and it was our job to organize and catalog them. He suggested that we spend the next couple of hours looking over the files, familiarizing ourselves with their contents. He pointed out that as the first order of business we should try to locate all the information they contained about German Army field ciphers and Japanese diplomatic codes and ciphers. After saying that he would return by lunchtime, he left, carefully setting the steel doors so that the contents of the room were not visible from the outside corridor.

After Friedman left the room, Abe drew his index finger across the top of the nearest file cabinet. When he held up his finger and noted the thick smudge of dust on it, he grimaced.

Besides the file cabinets, the only pieces of furniture in the room were a single oak chair and a small table on which were arranged some pencils and ruled pads. I took off my new blue jacket and hung it on the chair. After Abe and Kully had disposed of their jackets, Kully turned to Abe and, with an impish grin on his face, pointed to my new and immaculate white trousers. Then they both laughed.

We now started to look at the materials in the file cabinets. In a few minutes we forgot all about the thick dust that covered everything in the room, and we forgot about the summer heat and the poor ventilation. We were completely hypnotized by what we were finding. Here were the secret records dealing with the American code-breaking activity sponsored by the State Department and the Director of Military Intelligence; here were copies of the secret codes and ciphers, both purloined and cryptanalytically recovered, of many of the great nations of the world; here were the worksheets used in breaking Japanese diplomatic codes; here were the translations of Japanese messages relating to the negotiations of the Washington Naval Conference, to which were attached letters of appreciation signed by high State Depart-

ment officials; here were the decipherments of the German field ciphers of 1917 and 1918, with descriptions of how they were broken; here were hundreds of copies of unsolved code messages from every important capital of the world; and here was a wealth of other cryptologic material which could be appreciated only after hours and hours of further detailed study. King Solomon's mines could have offered no greater treasures for us.

We were so intrigued by the contents of the vault that we lost all track of time. Friedman's return startled us. He found three sweaty and grimy but nonetheless starry-eyed Junior Cryptanalysts. Kully had a dirty streak across his forehead. Abe's shirt was spotted with smudges of dust and soaked with perspiration. My brand-new white pin-striped trousers were no longer white; they were a dirty mess. Friedman looked us over and, after remarking on "what a dirty business cryptanalysis is," suggested that we clean up and go to lunch. He asked us to spend some time at his desk after we had finished lunch, stating that we would be joined by Hurt for an important discussion about our future duties.

Our Mission Described

Early that afternoon the four of us met with Friedman in his office. He settled us in chairs around his desk and carefully closed the office doors. For me, it was the most electric moment that I had yet experienced, and all sorts of romantic ideas were racing through my mind.

Friedman began by describing the work of what he called "Yardley's bureau," a joint intelligence activity conducted by the State Department and War Department G-2, with the State Department supplying most of the money. Herbert O. Yardley had conducted the activity in New York City under the guise of a legitimate enterprise known as the "Code Compiling Company." In the summer of 1929, when the new Secretary of State, Henry Stimson, learned of the nature of Yardley's activities, he had summarily abolished "Yardley's bureau." He ordered that the organization be closed out in the shortest possible time and said that no such activity would be tolerated inside the Department while he was Secretary. G-2, viewing Stimson's order as a major disaster to the American intelligence effort, had tried to have his order reversed. But Stimson was adamant and G-2 finally had to accept his decision.

When the Director of Military Intelligence realized that Stimson meant what he said, he proposed to the Chief Signal Officer that a code-breaking operation be set up in the War Department. He offered to supply

the funds previously contributed to the State Department in support of Yardley's operation. The money would be used to hire a small group of young men who would be trained in cryptology, and who hopefully would become the cadre of an effective cryptanalytic organization. The Chief Signal Officer had enthusiastically received the proposal and had accepted the responsibility for administering the organization. The funds made available by G-2 to the Chief Signal Officer were barely sufficient to provide for the employment of four Junior Cryptanalysts and one Cryptographic Clerk. The four of us represented the first step in the implementation of the long-range plan to develop a new cryptologic capability in the War Department.

Friedman then went on to explain that the long-term mission of the Signal Intelligence Service was twofold. The first and more important objective was to insure that U.S. military codes and ciphers were the best and most secure that could be devised. The second was to undertake the peacetime interception and analysis of foreign code and cipher communications for the production of intelligence for the country's top planners and policymakers and, in the event of war, to be prepared to intercept and solve enemy messages at all levels. He also disclosed to us that an intercept service was then in the process of being organized and that it was being staffed by the best radio operators in the Signal Corps. Some had already been assigned to the intercept organization and were being trained for intercept work. He added that the first of a worldwide network of intercept stations was then being established at Fort Monmouth, New Jersey.

He impressed on us the need for secrecy, pointing out that both the Director of Military Intelligence and the Chief Signal Officer were afraid that if the State Department became aware that a new cryptanalytic activity was being established, steps might be taken at the highest level of government to have the organization abolished. He explained that the organization had been administratively located in the Office of the Chief Signal Officer rather than G-2, for if its existence did become known to the Secretary of State, its continuation could be justified as being part of the Chief Signal Officer's responsibilities to design, compile, store, and issue all cryptographic materials required by the War Department, and to supervise the use of all cryptographic systems in the Army.

Friedman said that for the next several months the four of us would spend part of our time studying cryptology with the aim of mastering all that was currently known about cryptography and cryptanalysis; the remainder of our time would be devoted to

producing improved codes and ciphers for the War Department. He emphasized his conviction that all currently used U.S. codes and ciphers were "woefully inadequate, outdated, inefficient and, worst of all, insecure." He added that it was imperative that we get started as soon as possible on improving all cryptographic systems used in the War Department, so that at least the Army would have adequate cryptographic security in the event of another war.

Our Codes Are an Open Book

A fortuitous combination of circumstances soon allowed me to see firsthand how insecure the War Department's codes really were. The Signal Corps had recently become responsible for all phases of War Department cryptographic security, which until then had been shared with the Adjutant General's Office. One result of the realignment—and this was my first lucky break—was that there developed a temporary shortage of trained code clerks. It was decided that Kullback, Sinkov, and I would be detailed to work in the code room for a few weeks until new clerks could be trained. The second lucky break was that I could type, and since messages had to be typed before they cleared the code room, I was assigned there more often than the others. What I learned during those long night shifts was both rewarding and discouraging—rewarding because I gained a better understanding of military communications and procedures; discouraging because I learned how woefully weak was the cryptographic security of those communications.

Most messages, regardless of their classification (Restricted, Confidential, or Secret), were encoded from the same codebook, the old War Department Telegraph Code of about 50,000 groups, and this of course was an inherently insecure procedure. The military attaché network used a smaller, more sophisticated code of about 10,000 groups; messages sent in this system were always enciphered. Unclassified messages went out in the clear when transmitted over the War Department radio network. When sent over commercial circuits—RCA or Western Union, for example—they were encoded, not for security but for economy, since the government had to pay by the group, and encoded messages were always shorter, hence cheaper, than the plain-language originals.

Friedman assured me that as soon as appropriations came through, he intended to produce new codes and eventually to develop automatic cipher machines for use in Washington and the overseas departments. "In the next few years, Mr. Rowlett," he said, "we are going to revolutionize the security of governmental

*Frank Rowlett on. . .***What's Important in Cryptology**

In my experience most people have assumed that the production of intelligence is the primary purpose of the cryptologic effort. I disagree. It's important but it's not paramount. The most important goal of the cryptanalyst is to use his knowledge of foreign cryptography to improve our own cryptographic security.

The Effect of The American Black Chamber

I think Yardley's book was a good thing for U.S. cryptology because it forced the Japanese to replace their cryptosystems with better, more secure systems and that in turn forced us to improve our cryptanalytic capability. Moreover, were it not for Yardley's book, the Japanese might not have introduced their new systems in time for us to master them before

war came. I don't condone disclosures of sensitive information, but in this case it had a beneficial effect.

Personnel Security

The rules on security clearances were pretty loose in the early days. As long as you were a second-generation American you were assumed to be loyal and you were cleared. If you were first-generation, you might be cleared. If you weren't born in America, you couldn't be cleared. In my own case, I guess it was assumed that a mountain boy from the heart of southwest Virginia would be unlikely to have any allegiances except to the United States. I didn't get formally investigated and cleared until the war was half over, or some 12 or 13 years after coming to work.

communications, and you and the other young men you are associated with are going to be deeply involved in these developments."

Growth and Training

By the end of 1930, the staff of the Signal Intelligence Service had grown to eight. The two newcomers were Lieutenant Mark Rhoads of the Signal Corps, the first Regular Army officer to be assigned full time to the SIS, and Larry Clark, a chemistry major attending evening classes at George Washington University, who was hired, as an Assistant Cryptographic Clerk, to work on secret inks, one of our several responsibilities at the time.

Meanwhile, Sinkov, Kullback, Hurt, and I continued our cryptologic training under Friedman. Early in 1931 we began studying machine cipher systems, starting with a modified version of the Wheatstone cipher device. That led us to the Bazeries multiplex alphabet system, which we solved with relative ease. Next was the German Kryha machine, said to be indecipherable because of the enormous number of possibilities— $17 \times 26! \times 26!$, as I recall—that would have to be tested before text could be recovered. According to the manufacturer's brochure, it was humanly impossible to make all these tests, thus the cipher could not be

broken. Nothing daunted, we pressed on and solved the system in fairly short order.

Next on our list was the B-211, an electromechanical device invented by the Swedish engineer Arvid Gerhard Damm. It was a beautifully made machine, about the size of a portable typewriter. Cryptographically, however, it wasn't particularly formidable, being nothing more than a fractionating system easily duplicated on paper. To satisfy ourselves that we fully understood the functioning of the device, we enciphered a short message using both the machine and our paper analog. We were delighted to find that the cipher texts were identical.

Our training in machine cipher systems continued with the study of the Vernam device, a sophisticated machine developed by AT&T. Probably the first fully automatic cryptographic device actually constructed, it had been successfully tested by the Signal Corps on wireline circuits. But it had one great weakness, which Friedman had earlier exploited and which he now wanted us to discover. As I recall, once that weakness was found and the underlying principle understood, solving the machine was much like completing a word puzzle, and the solution came fairly easily.

The most difficult machine we studied was the Hebern cipher machine, developed in the early twenties for the Navy. Friedman had found it to be cryptographically weak, and it was redesigned. Our

job was to duplicate his original analysis, using the same test messages provided him by the Navy. Although we mastered the cryptographic principles involved, we were unable to solve the system until Friedman explained the underlying statistical concepts, whereupon we recovered the message texts and the wiring of the electrical commutating elements—loosely called cipher wheels—used in the encipherment.

Open for Business

In 1932, Friedman announced that we were ready to begin our intelligence mission, with Japanese diplomatic communications being our first priority. But it was not to be a full-time effort, for we were still responsible for producing codes for the War Department, and this took precedence over signals intelligence.

We began by reviewing the Japanese material inherited from Yardley's Black Chamber operation in New York. Considerable amounts of live traffic soon began to arrive from the Army's nascent intercept service. This was augmented by the do-it-yourself intercept activity of Colonel Joseph Mauborgne, Signal Officer for the Ninth Corps area. Mauborgne (later General Mauborgne, head of the Army Signal Corps)

set up an unofficial intercept station in the basement of his quarters in the Presidio of San Francisco, from which he copied Japanese diplomatic traffic on the San Francisco-Tokyo circuit. He mailed us his undulator tapes and Kullback and I transcribed them. Since I knew Morse code, I read the characters to Kully, who, in order to save paper, wrote out the messages on the backs of old Signal Corps weather reports.

Our approach was to sort incoming intercepts into homogeneous groups—an easy matter since the Japanese used a unique identifier on each message, evidently for the convenience of the code clerk—and then test each code against the Black Chamber's solutions. With the help of John Hurt's linguistic talents, we soon produced our first current translation of a Japanese diplomatic message, this one in a modified form of the so-called LA code. While at the time not holding much significance for us, the achievement did cause the Chief Signal Officer and the Director of Military Intelligence to take renewed interest in our work. It also lent new stimulus to the effort to enlarge the staff of the Signal Intelligence Service, since Friedman very convincingly made the point that we could either compile codes or solve Japanese diplomatic systems, but we could not be expected to do both.



Frank Rowlett at Arlington Hall Station in 1948.

In September 1932, Sinkov, Kullback, and I began spending a few hours each week studying Japanese under John Hurt. We used the Rose-Innes text for our study of conversational Japanese and the standard national Japanese elementary language textbooks (Kokugo Tokuhon) for the written language. The latter were in written Japanese (kana and Chinese characters), and so far as I was concerned were much more useful for our cryptanalytic purposes than was the Rose-Innes text. Our lessons continued until the following May, when Hurt was stricken with tuberculosis and had to be hospitalized. His replacement was a Mr. Ayvoztoglou, a former colonel in the Imperial Russian Army who had studied Japanese at the Oriental Institute in Moscow. Unfortunately for us, his knowledge of spoken English was so poor and his pronunciation so atrocious that he sometimes had to resort to using the French or German equivalent of the English term to enable us to understand him. He had to leave after three months because of a lack of funds to pay him, but by that time we were learning more from code recovery than from the language classes, for the messages gave us the vocabulary actually used by Japanese diplomats.

When Hurt returned to work, Friedman urged that he concentrate on Japanese, leaving the strictly cryptologic work to the rest of us; this pleased Hurt, for he much preferred spending his time on language.

Kully's Discovery

One afternoon the three of us, Kully, Hurt, and I, were quietly working at our places in the vault when, with no warning whatsoever, Kully started to beat the top of the table at which he was working and loudly exclaimed, "That's it! That's what they have done! It's an English monoalphabet!"

I had no idea what he was so excited about. I hurriedly got out of my chair and went to look over his shoulder. He started to wave a worksheet wildly through the air. "That's what they are doing," he exclaimed. "They're enciphering English texts with a monoalphabetic substitution. And all along we were looking for something else."

"Show me," I said, as Hurt joined us.

Kully slammed the worksheet down on the table. "Look at that," he said, pointing to three of the cipher groups he had underlined in red. "Look at the letter patterns for those three words. Can they be anything but a monoalphabetic substitution of the English words 'The Japanese Government'?"

"Now look at the next words," he continued. "Decipher them by using the equivalents from the other three words, and see what you get."

"I'll tell you what it is," he said. "The rest of the line of text will decipher to give 'requests that the Government of the United States.'"

"Why don't you write in the equivalents on the worksheet?" I asked. "Then you can check out the remainder of the message."

Kully rapidly filled in the assumed plain text while Hurt and I looked on. Every letter he entered fitted accurately. It was indeed a monoalphabetic substitution, with vowels replacing vowels and consonants replacing consonants. He continued his decipherment of the remaining groups and in a short time had finished the entire message. There was no doubt about it—the Japanese were using the most insecure type of cipher possible for enciphering this message.

"I can't understand it," Kully remarked. "Why would they do anything so stupid?"

"Why don't you test another message?" Hurt asked.

Kully soon located another intercept with the same indicator. As Hurt and I looked on, he deciphered a couple of groups using the substitution alphabet recovered from the message he had just deciphered.

"That's not English," I observed.

"But it's perfect Japanese!" Hurt exclaimed. "Decipher some more groups so that I can translate it."

Kully continued his decipherment of the message until Hurt interrupted him. He took the worksheet from Kully and studied it for a few seconds.

"Except for a couple of garbled letters, this is perfect Japanese. It's apparently a news release which the Japanese Foreign Office is transmitting to its installations abroad for the information of Japanese nationals in foreign countries. I've seen similar examples in the plain-language messages we've been intercepting."

Kully sought out some more messages with the same indicator. All could be deciphered and all were in Japanese. It was really a stroke of luck that Kully had spotted the only intercept with English plain text. Otherwise, it might have been weeks before we realized that this particular category of traffic was indeed a monoalphabetic substitution, for we were looking for something much more sophisticated.

"Let's see what Mr. Friedman has to say," suggested Hurt.

I stepped to the vault door and opened it. "Excuse me," I said. "Kully has discovered something that you will find most interesting. Would you mind stepping into the vault to look at it?"



Arlington Hall Station, 1942 or 1943.

Seated: A. J. McGrail, W. Preston Corderman, William F. Friedman. *Standing:* Mark W. Rhoads, Solomon Kullback, John B. Hurt, Edward J. Vogel, Frank B. Rowlett, Abraham Sinkov.

Friedman pushed his work aside and followed me into the vault. "What have you found?" he asked Kully.

"The Japanese are using a monoalphabet for enciphering some of their diplomatic messages," Kully answered.

Friedman looked doubtful. "Why do you think that?" he asked.

"I just solved one," Kully answered gleefully.

"Well, that's a rather convincing argument," Friedman replied. "But there must be something wrong. No government with any competence whatever in cryptography would intentionally use such a patently insecure system. A code clerk must have made a mistake, or they are using a cipher machine in which a mechanical failure occurred, thereby producing a

monoalphabetic substitution encipherment which was transmitted by mistake."

"But there are several messages on different dates which use the same substitution," Kully answered. He then spread out his worksheets and demonstrated the decipherments. Friedman picked up the worksheet of the message in English and read it carefully.

"This message seems to be a note which the Japanese ambassador has been instructed to deliver to the State Department," he said. "It is possible that they used a simple encipherment merely to disguise the contents of the message from the communications personnel who would be handling it. If the Japanese were planning to provide the exact text of one of their messages to another government, they certainly wouldn't want to encipher it in one of their secret

codes. To do so might result in their code being compromised, for it would take an exceptionally secure cryptographic system to resist analysis when such a long message together with its exact decipherment were available for study."

Friedman was obviously pleased with Kully's discovery. "Well done, Mr. Kullback," he said as he left the vault.

The Red Machine

The mid-1930s saw us continuing our efforts to solve Japanese diplomatic cryptosystems, particularly any that might be carrying traffic relating to a suspected secret codicil to an Axis pact then under discussion. Our search led us to a system used on two important networks—the Far Eastern diplomatic network and a net linking Tokyo with major world capitals, including Berlin and Rome.

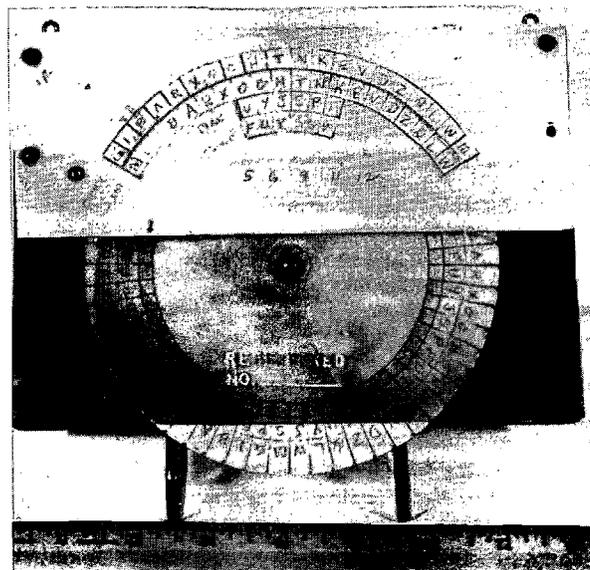
The system was characterized by five-letter text preceded by a five-digit group. Friedman, who by now was taking a strong interest in our examination of the unsolved intercepts, thought the Japanese might be using a cipher machine, and suggested that the five-digit group served not only to identify the system but also to indicate the specific keys employed for enciphering the message. With the help of our IBM accounting machines we tested the texts for repetitions. We found none we considered significant, but in the process we discovered that six of the cipher letters displayed a significantly higher or lower frequency count than the other 20, that the frequency pattern changed at 10-day intervals, and that some messages used the same initial five-digit group. Our statistical tests also showed that when two messages in the same 10-day period used the same five-digit groups, the messages were enciphered with the same keys.

The job of breaking the system fell to Kully and me, for in 1936 Sinkov, the only bachelor among us, was assigned to the Panama Canal Zone, the site of the first Army intercept station outside the United States. While Kully and I studied the traffic from the various 10-day periods, Friedman told his opposite number in the Navy, Commander Joseph N. Wenger, about our work on the system and the progress we had made so far. Wenger said that the Navy had recently broken into a Japanese naval system which used an electromechanical cipher machine and the kana alphabet, but beyond that he would not go.

I should explain that, while there was a complete exchange of intercepted Japanese diplomatic traffic between ourselves and the Navy, there was at that time no direct contact between us except for an

occasional meeting between Friedman and Wenger. Though he didn't say so, I sensed that Friedman felt he was being unfairly treated by the Navy by being denied technical information, whereas the Army, through Friedman, had always shared information fully with the Navy. He made an appointment with Wenger for the next day with the intention of requesting complete details about the machine the Navy had solved. Despite Friedman's argument that the cryptographic principles employed in the Japanese naval machine could well be similar to those used in the diplomatic machine, Wenger still declined to divulge any more information, or even to confirm or deny that there *were* similarities. He would say only that the kana sequence had been broken into two subsets, but we already knew that. When pressed, he suggested that we search for a basic cycle of "more than 40 but less than 50" elements, and that was all Friedman could get out of him.

Our test for a cycle of the length suggested by Wenger yielded nothing. Somewhat dejected, we admitted that for the time being we had run out of useful ideas, and we decided to consolidate our materials and organize the files while considering how best to attack the system. Later, after an exhaustive examination of the best intercepts, Kully and I succeeded in deciphering certain parts of an exceptionally long message in which the vowel and consonant patterns corresponded to those expected in romanized Japanese plain text. When we found a recurrence of



Analog of the Japanese Red Machine, made by Frank Rowlett sometime around 1936.

the plaintext word *oyo-i* in two of the passages we had tentatively deciphered, we knew we were into the system, for *oyobi* is the Japanese word for "and." That led us to review what we knew about the system. There were two sequences, one for vowels, the other for consonants. These sequences apparently provided for independent encipherment of the vowels and consonants: a vowel would always be enciphered by a vowel and a consonant by a consonant. Evidently the two sequences operated synchronously, both advancing with the encipherment of each letter of the message, whether consonant or vowel. There was a motor key involved, which controlled the advancement of the two sequences, introducing additional steps at certain points in conformity with an overall pattern. Armed with that knowledge and some educated assumptions of the underlying plain language, we soon recovered enough text to know that we were well on our way to breaking the "Code Machine, Type A," the most important Japanese cryptographic system then in use.

Friedman, of course, was elated, particularly so because we had succeeded in recovering an unknown cipher machine by reconstructing the principles solely from intercepted messages, without help from any outside source. As he congratulated us on our success, he added, "You know, gentlemen, I am glad that Wenger did not disclose to me the details of the Japanese naval cipher machine and how it was solved. You have clearly demonstrated that the Signal Intelligence Service does not need cryptanalytic assistance from anyone."

The next problem was how to process the large volume of messages which now lay open to us. We were still a very small group, and even with part-time help from Larry Clark and Louise Newkirk Nelson, Friedman's secretary, we could not cope with the processing and translating of the intercepts, even if we were relieved of all other duties. What we needed was an analog of the Japanese machine, but that was out of the question for at least two years because of a lack of funds. In the meantime, we devised a 60-point disc with the two sequences continuously inscribed around the edge. The first models, made of heavy drawing paper, didn't hold up well; a later version, made of plastic, was more durable and served until, more than two years later, the Navy Yard model shop built us an electromechanical analog.

Our success in exploiting high-level Japanese diplomatic communications brought us a new measure of respect in the War Department. Almost overnight we assumed a different status in the eyes of the officers with whom we dealt, and their attitude of polite

tolerance turned to one of open respect. The Chief Signal Officer liked to refer to us as "magicians," and it was probably from his use of this appellation that the cover name "Magic" was later applied to intelligence produced by cryptanalysis. Needless to say, Friedman's requests for more people now received full support.

Another result was that as soon as Hurt began producing translations of current intercept, the Chief Signal Officer and G-2 became concerned about the lack of formal regulations governing the dissemination of information about our work on Japanese diplomatic communications. The resulting rules provided, among other things, that G-2 would get all translations but no technical information and that translations had to be kept in a designated secure area protected by a combination lock.

Finally, there was the question of what to call the Japanese diplomatic cipher machine. Our usual term, "Japanese cipher machine," seemed too explicit, too likely to result in a compromise. Friedman therefore asked Kully, Hurt, and me to suggest something else, not only for this machine but also for others we would solve in the future. We recommended using colors of the spectrum; and for the first machine we solved, what better choice than *red*, the first of the primary colors?

Purple

By 1938 we were all back together in Washington, Sinkov having completed his two years in Panama and Kullback his year in Hawaii, and by the end of the year we were in the enviable position of being able to read every Japanese diplomatic cryptosystem then in use. Clearly, this couldn't last, and it didn't. Decrypts of messages from the Red machine revealed that a communications expert named Okamoto was being sent from Toyko to install a new kind of cipher machine in the major Japanese embassies, including the one in Washington. The new machine, called the Type B, was to replace the Type A (Red) machine for high-level Foreign Ministry communications, but we didn't know when.

We weren't surprised to learn that the Red machine was to be replaced. It had, after all, been in use since at least 1932, and it was becoming increasingly unreliable, so much so that we estimated that in half of the embassies holding the machine only one of the two machines was still working properly. In at least one embassy both machines were faulty, and both we and the Japanese cipher operators had to exercise special care when deciphering messages from that city.

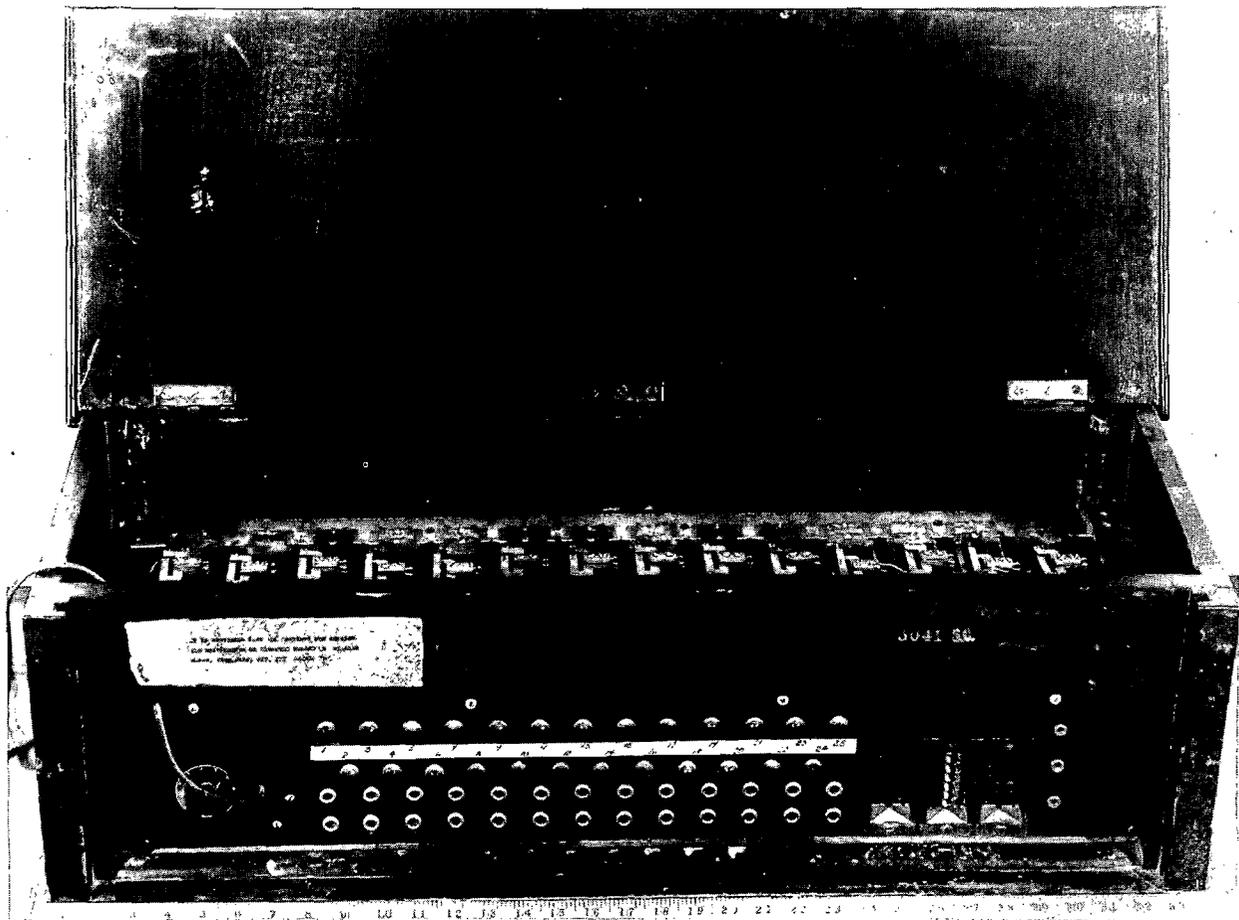
When we received three unreadable messages sent from Warsaw to Tokyo on 20 March 1939, we knew that the new system was in use. The volume of messages in the new system gradually increased until, in mid-April, it was clear that the new machine had virtually replaced the old on the major diplomatic circuits.

In the group working on the Japanese diplomatic traffic, the excitement was intense. Everyone, whether typist, translator, cryptanalyst, traffic sorter, stenographer, or clerk, was anxious to see a break into the new system, which we had named "Purple." The Chief Signal Officer and the Officer-in-Charge, War Plans and Training Division, under whose aegis we operated, visited our area almost every day. The liaison officers from G-2 and the Office of Naval Intelligence who regularly picked up our translations of Japanese diplomatic messages never failed to inquire about progress on the new system. It was the same in the Navy cryptanalytic group. We consulted with the Navy

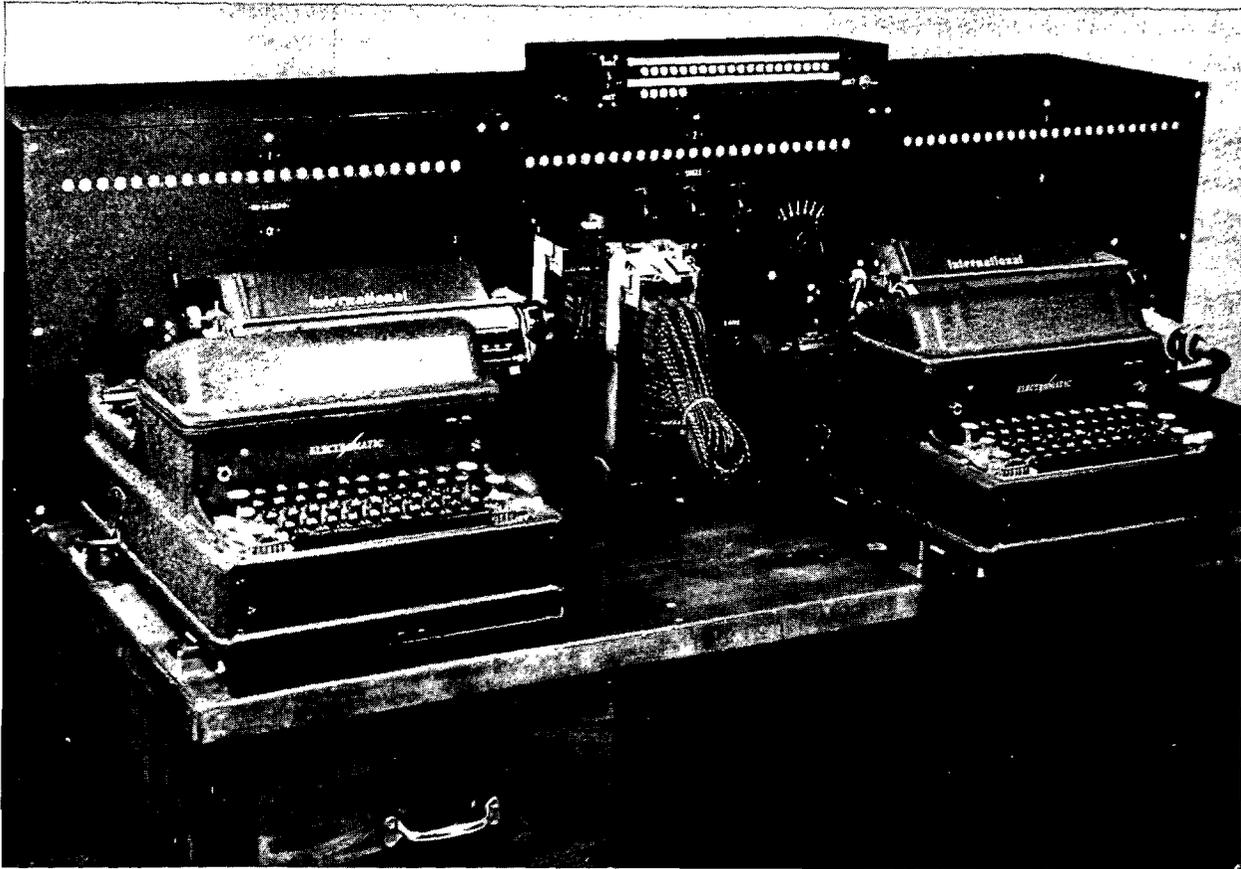
cryptanalysts daily and exchanged ideas on methods of attack on the new system. Both the Army and Navy groups organized their files and technical records so that both units could be kept current on technical progress, and we set up procedures designed to insure that any significant information on the new system developed by one unit was immediately made available to the other.

Though the new machine was based on a different, and much more complex, cryptographic principle, it had one feature in common with the older one: its cryptographic mechanism was designed to treat the 26 letters of the alphabet as two subsets, one of six elements and the other of 20.

It took only a few weeks for us to discover how the "sixes" were enciphered, and this allowed us to recover the plaintext equivalents of the letters making up the "sixes" wherever they appeared in the intercepts. But it was a slow, laborious, pencil-and-paper process, not made easier by the fact that we were receiving



The first operational analog of Japanese Purple Machine, from 1940, built under the direction of Leo Rosen.



A later analog of Japanese Purple Machine, possibly from March 1944.

hundreds of intercepts each month. We obviously needed some means of doing this time-consuming task automatically. Fortunately, an MIT graduate electrical engineer, Leo Rosen, had recently joined the SIS, and he was given the job of designing a device for deciphering the "sixes." He hit upon the idea of using standard, six-level, 25-point telephone selector switches for this purpose. Colonel Spencer B. Akin, at that time the Officer-in-Charge, War Plans and Training Division, of which the SIS was a part, called a friend of his in Chicago who worked for a company that manufactured telephone equipment, and had a supply of switches airmailed to us. Rosen obtained the other parts through local purchase or by cannibalizing some of our unused cipher machines. In about two weeks, he had completed a working model of the "six-buster," as we called it. It saved so much time and effort that we decided to build two more. For the input keyboards, we turned to the Washington IBM office, whose chief,

Mr. Lamont, gave us—no questions asked—two boards from their new alphabetic keypunch machines.

The details of how Purple was solved have been described elsewhere and I'll not repeat them here. But it should be said, again, that probably the most important factor in our success was the determination of the team to break the system—never during those 18 months did any of us doubt that we would ultimately succeed. There was pressure, great pressure, so much that it contributed to Friedman's emotional collapse and hospitalization. There were untold amounts of night and weekend work—for example, the many 14-hour days the wiring team worked, voluntarily, building and testing the banks of stepping switches, each of which required over 500 separate soldered connections. But if there was pressure, long hours, and hard work, there was also a pervasive spirit of cooperation and seriousness of purpose. No task was too menial or too onerous to be undertaken by any

member of the team, regardless of rank or position. Our feelings were summed up in the section's watchword: "Make no mistakes; record all findings; identify source of data for each recovery; keep the team informed."

We handed in our first two translations on 27 September 1940, just one week after Gene Grotjan's discovery of the crucial key to unlocking the system. (Ironically, that was also the day on which Japan announced that it had joined with Germany and Italy to form the Tripartite Pact, which was aimed directly at the United States.) We had, however, recovered the machine settings for only one of the indicators, and we had made no headway whatever in exploiting the thousand or so diplomatic messages which had accumulated during the year and a half we had been working on the system.

Recovering the machine settings for the remaining indicators, while straightforward, was a slow, mainly manual, process, requiring the identification of the initial relative positions of the banks of stepping switches and the order in which they operated. Through plain hard work we established the machine settings for over a third of the indicators within the next two and a half weeks. While these were being recovered, Leo Rosen pushed ahead on the construction of two fully automatic Purple machine analogs. Each had three major components: the cryptographic mechanism, an input keyboard, and a solenoid-operated typewriter. The cost of the parts for the cryptographic mechanism was \$290.97, and for the keyboard and the typewriter another \$393.68, for a total of \$684.65, surely one of the government's better bargains. Rosen then used some of the leftover switches to build a Red



Leo Rosen, who directed the construction of the first Purple analog, receiving the NSA Exceptional Civilian Service Award in December 1967 shortly before he retired as head of the Agency's R&E organization. NSA Director Marshall S. Carter and Deputy Director Louis W. Tordella shared in the presentation.

machine analog, at a cost of \$174.17. The ultimate tribute to the quality of his work came in intercepted messages which showed that the Japanese were having much more trouble with their machines than we were with ours. In other words, our machines, built entirely by cryptanalytically duplicating the functions of the originals, were considerably more reliable than the Japanese models.¹

With the solving of Purple came pressure from G-2 to fully exploit traffic on the Tokyo-Berlin and Tokyo-Rome circuits as well as to process the backlog of Purple messages in general. What followed is well known. A machine for deciphering Purple was given to the Navy, another was sent to the Philippines and one was given to the British. Translated diplomatic traffic, known as "Magic," soon began to reach the highest levels of the government, including the President, who later insisted on seeing the unedited English translations. Magic provided some of the best intelligence available on Japanese plans during that fateful year before Pearl Harbor. If we were not warned of the attack in time to prepare for it—and the reasons for this are still debated—the fact remains that Magic did tell us that war was imminent, and throughout the war it continued to give us a unique look at the diplomatic background of Japanese strategy and plans.

And not just Japanese. By reading messages from Baron Oshima, the Japanese ambassador in Berlin, we obtained a detailed description of German fortifications along the Normandy coast. So valuable was this information to Allied invasion planning that when General Eisenhower later visited Arlington Hall Station he asked to meet the people who had produced the intelligence so that he could thank them personally.

In these and other ways, the Magic intercepts were of immense value to the Allied cause. A joint congressional committee summed it up this way: Magic "contributed enormously to the defeat of the enemy, greatly shortened the war, and saved many thousands of lives." It was one of American cryptology's proudest achievements.

Epilogue

Frank Rowlett served in the Army from 1942 to 1946, rising to the rank of colonel. After the war, he

¹ When, after the end of the war in Europe, we had an opportunity to compare our analog to an actual Japanese Purple machine, we found that, of the several hundred connections we had recovered, only two were incorrect, and their effect on decipherment was negligible.



Genevieve Grotjan Feinstein receiving award from Brigadier General P. E. Peabody, May 1946.

became Chief of the Intelligence Division of the Army Security Agency, where he played a leading role in formulating policies establishing the Armed Forces Security Agency, the predecessor of NSA. He served as Technical Director for Operations in AFSA, and in 1952 he transferred to CIA, where for five years he was a senior staff officer and advisor to the DCI. In 1958, he became Special Assistant to the Director of NSA, a position he held under four directors. He led a study group which prepared the way for the founding of the National Cryptologic School, and in 1965 he became the School's first Commandant. He retired at the end of 1965 and now makes his home in Florida. His awards and honors include NSA's Exceptional Civilian Service Award, the National Intelligence Distinguished Service Medal, the President's Award for Distinguished Federal Civilian Service, the National



President Johnson presents the President's Award for Distinguished Federal Civilian Service to Mr. Rowlett, 2 June 1965. Vice-President Humphrey looks on.

Security Medal, the Legion of Merit, and the Order of the British Empire. In 1964, Congress awarded him \$100,000 as partial compensation for cryptographic inventions held secret by the government.

William Friedman served with the Army Security Agency and the Armed Forces Security Agency before becoming a research consultant and then Special Assistant to the Director of NSA. He retired in 1955. The following year Congress awarded him \$100,000 for cryptographic inventions held secret by the government. He died in 1969. In 1975, in his honor, the NSA auditorium was dedicated as the Friedman Auditorium. His wife, Elizebeth, herself a gifted cryptanalyst, died in 1980.

Solomon Kullback, Abraham Sinkov, and Leo Rosen saw commissioned service in the Army during World War II, and all held senior positions with NSA before retiring during the 1960s. John Hurt continued in linguistic work until his retirement in 1963; he died in 1966.

Finally, what of Genevieve Grotjan, the quiet young Junior Cryptanalyst with whom we began this story? Only this much is known: after the breakthrough into Purple, she continued to work on Japanese and other cipher systems; she was for a while an instructor in machine cryptanalysis; and she was a mainstay of the small cryptanalytic research section, where she worked

on a variety of machine cipher systems. Sometime in late 1942 or early 1943 she married a man named Feinstein, who may have worked at the National Bureau of Standards. In May 1946 she received the Exceptional Civilian Service Award. She is thought to have left government service later that year or perhaps early the next year.

And there the trail ends. . .

This profile of Mr. Rowlett (accent on the first syllable) is based on material copyrighted 1980 by Frank B. Rowlett, Sr., and Frank B. Rowlett, Jr.

Ted Hannah, a frequent contributor to *Cryptologic Spectrum*, is on a year's fellowship in cryptologic history.

Additional Reading

Open Sources

Farago, Ladislas. *The Broken Seal: "Operation Magic" and the Secret Road to Pearl Harbor*. New York: Random House, 1967.

Kahn, David. *The Codebreakers*. New York: The Macmillan Company, 1967.

U.S., Congress, Senate, Joint Committee on the Investigation of the Pearl Harbor Attack, *Investigation of the Pearl Harbor Attack*, 79th Cong., 2d sess., 1946. A one-volume summary of the congressional hearings on the Pearl Harbor attack. Useful for its documentation of the value of communications intelligence in anticipating Japanese diplomatic and military moves.

Classified Sources

Callimahos, Lambros D. "The Legendary William F. Friedman." *Cryptologic Spectrum*, Winter 1974, pp. 8-17.

Hannah, Theodore M. "In the Beginning...." *Cryptologic Spectrum*, Spring 1976, pp. 19-21. A view of the Army intercept service, 1939-1942.

Snyder, Samuel S. "A Translator Extraordinaire." *Cryptologic Spectrum*, Fall 1976, pp. 16-19. A sensitively written tribute to John Hurt by one who was there.

The definitive account of the breaking of the Japanese Purple cipher machine was submitted to the Chief Signal Officer by William F. Friedman on 14 October 1940. It appears, in slightly different forms, in two issues of the *NSA Technical Journal*: Vol. IX, No. 2, May 1964, pp. 1-9, and Vol. XIX, No. 1, Winter 1974, pp. 1-12. The latter version includes a credits section rich in praise of those who contributed to the solution of Purple.