Center for Cryptologic History

The SIGABA/ECM II Cipher Machine: "A Beautiful Idea"

This publication is distributed *free* by the National Security Agency.

If you would like additional copies, please e-mail cchpubs@nsa.gov or write to:

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

Timothy Mucklow was a senior historian on the staff of the Center for Cryptologic History following a long career in information assurance at NSA and with the Air Force. After a decade in academia, he served as a military historian at the wing, division, and major command levels and produced a series of monographs and articles on such topics as information assurance, telecommunications and computers, and national defense issues, and has offered IA seminars at military facilities around the world. He received his Ph.D. in 1982. He retired from the CCH in 2013.

Acknowledgments. The Center for Cryptologic History is grateful to Dr. Craig Bauer, professor of mathematics at York College of Pennsylvania and editor-in-chief of the journal *Cryptologia*, for his assistance with this project, and to LeeAnn Tallman for earlier research.

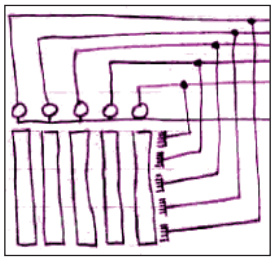
The SIGABA/ECM II Cipher Machine: "A Beautiful Idea"

Timothy J. Mucklow

National Security Agency
Center for Cryptologic History

2015

Contents

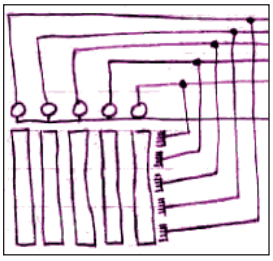


Introduction

During World War I, both the Americans and the Europeans had used manual code and cipher systems to secure their critical information. With the advent of the machine age, however, it was only a matter of time before cryptography became mechanized. Two decades later, as the world embroiled itself in another major conflict, the use of cipher machines became commonplace, and the old craft of cryptology at long last became mathematically based. With the dawn of this new cryptologic age, a worldwide scramble for even stronger encryption began.

Well before the First World War, much work had been done to formalize the cryptographic discipline. One of those who made a major contribution to this process was the 19th-century polyglot Auguste Kerckhoffs, who, besides teaching languages, dabbled in cryptography. In 1883 he penned a two-essay series, *La Cryptographie Militaire*, for the *Journal des Sciences Militaire*, which earned him a niche in cryptographic history. Kerckhoffs in his writings had articulated six basic principles of cryptography, but he is most commonly remembered for his second, which states that the "design of the system should not require secrecy, and compromise of the system should not inconvenience the correspondents."[1] His argument was that neither the elements of an encryption algorithm nor the workings of an encryption machine should constitute the basis of a cipher's security. Instead, an easily changeable key should be the critical component.

In the 1930s, the U.S. Army cryptologist William Friedman and his assistant Frank Rowlett drew on this simple precept to conceive a cipher machine that was easy to use, simple to rekey, and ostensibly impossible to break. Then, in a fit of collaboration with the Navy, as unprecedented as it was peculiar, the two services went on to perfect and jointly field their device. To the Army it was known as SIGABA, to the Navy, ECM (Electric Cipher Machine) II. (The technical aspects of SIGABA's operation can be found in Appendixes A and B.) Not only was SIGABA the most secure cipher machine of World War II, but it went on to provide yeoman service for decades thereafter. The story of its development is improbable. Its impact was incalculable.



And Hebern Saw the Wheel

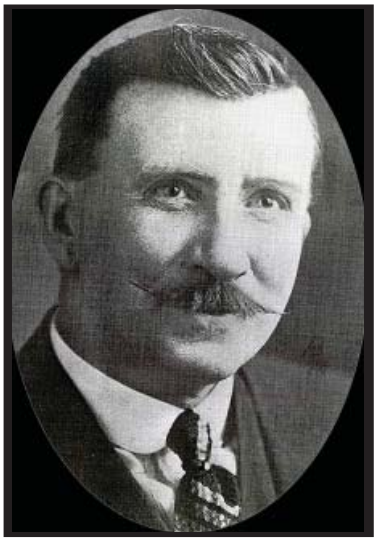
Mr. Edward Hebern of Madera, California, is generally credited with inventing the first American electromechanical rotor cipher machine.[2] According to lore, he came up with the idea around 1912 while serving a term in the state penitentiary for horse thievery. If there were any connection between breaking rocks and his cryptographic epiphany, Hebern never offered one. By the end of 1915 he had built a working model, filed a patent, and was knocking on the doors of potential buyers.[3] It was not long before the U.S. Navy began showing interest in Hebern's device, and in the years that followed the Navy would buy and test a number of his successive machines. As something of a historical twist, one of Hebern's early employees, Agnes (Meyer) Driscoll, went on to become a luminary of American cryptology in her own right.

Half a century after Hebern set out to peddle his original device, the Army cryptologist Frank Rowlett acknowledged in his memoirs that the Hebern cipher machine was an important invention in pre-World War II American cryptography. Rowlett, nevertheless, went on to add,

> Navy cryptographers asked [William] Friedman for his assessment of the security it afforded … [T]he Navy [supplied] a set of messages prepared exactly in accordance with the procedures which they had proposed, but using a set of cipher wheels whose wiring was to be unknown to Friedman … Friedman was successful in his attack on the system.[4]

With little effort, Friedman was able to decipher every Hebern-enciphered message sent his way. To do this, Friedman, who had already married cryptanalysis and mathematics, used a statistical approach along with a "divide-and-conquer" strategy to break the Hebern machine. As Friedman saw it, there were only two unknowns, the cipher wheel (with twenty-six characters) and the rest of the machine. Since the cipher wheel stepped regularly and predictably, the rest of the machine could be considered a constant. It was then a simple matter of sequentially analyzing the individual components.

Friedman realized from experience that the regular advancement of the Hebern cipher rotors, like all machines of that era, posed an intrinsic cryptologic vulnerability that was mathematically exploitable. He conjectured that to make a cryptographically sound machine, one would need a countermeasure to address predictable rotor movements. But just how such pseudorandom movement could be achieved consumed Friedman's thoughts for years. Friedman's solution, when it finally came to him around 1926, was conceptually simple and the technology proven.[5] It occurred to him that paper tape similar to that used by telegraphers



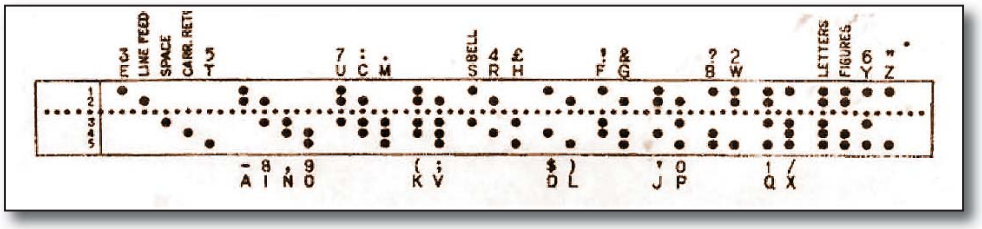
Edward Hebern and his electromechanical rotor cipher machine
(courtesy of Ralph Simpson, CipherMachines.com)

could also be used to dictate the movements of the cipher wheels. Friedman reasoned that it would be relatively easy to generate long sequences of random five-unit keys and that the tape itself was easily replaceable and relatively inexpensive. Holes punched in a tape would permit feeler contacts to turn an electrical current on or off, causing a cipher machine's rotors to step. Thus, with each key stroke, randomly placed holes in a five-group tape would produce an apparent random stepping for one or more of the cipher rotors. The cipher text is printed on a small tape. The decryption process simply works in reverse. Key tape could be manufactured in secure facilities, distributed to the appropriate recipients, and inserted into the machine according to rigidly imposed, pre-established schedules.[6]

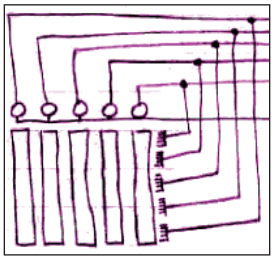
William Friedman with AT&T printing telegraph, 1920 (courtesy of the George C. Marshall Foundation, Lexington, Virginia)

The crypto rotor wheels William Friedman envisioned for his device were flattened cylinders with an alphabet around the circumference. One face of the cylinder had twenty-six spring-loaded copper pins protruding from it; the other face had twenty-six flush copper contacts. Inside each cylinder was a wire maze connecting the electrical contacts on one side to the pins on the other.

Thus, an electrical impulse beginning with, say, the letter *A* on one side might connect to *H* on the other side and so on around the wheel in random fashion. Several cylinders serially juxtaposed on a spindle side-by-side could further scramble impulses. (Image courtesy the online Crypto Museum, www.cryptomuseum.com)



Five-group punched hole paper telegraphic tape

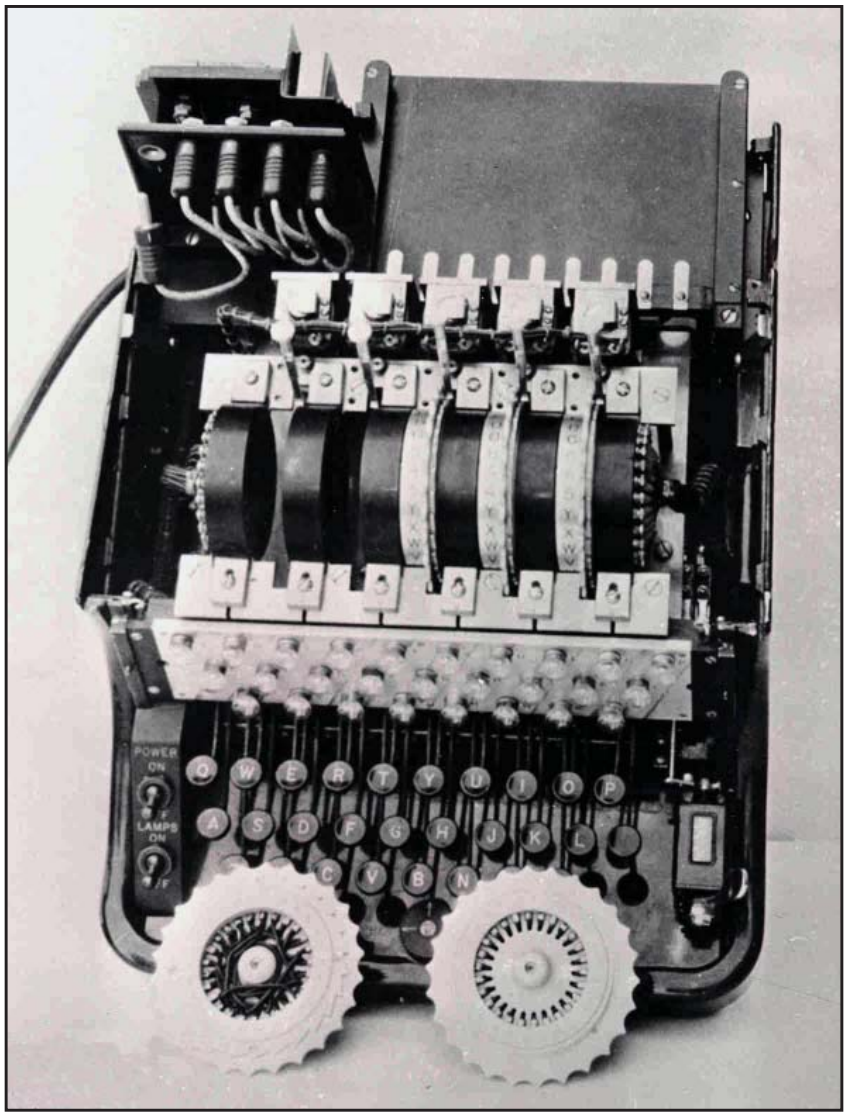


Deus ex Machine

On April 23, 1932, Friedman revealed his idea of randomly stepping rotors to his three junior cryptanalysts: Frank Rowlett, Solomon Kullback, and Abraham Sinkov.[7] This foursome at the time constituted the bulk of the U.S. Army's cryptanalytic organization, the Signal Intelligence Service (SIS). At the meeting Friedman enthusiastically explained that "the inherent weakness of all such devices" (where the devices were cipher machines that determined their own rotor stepping pattern) is that "the keying mechanism is a part of the device itself."[8] He then went on to draw for them several rough sketches of a cipher machine with a "key tape transmitter" that, in conformity with Kerckhoffs' second principle, would separate keying material from the cipher machine. His colleagues were duly impressed with his visionary countermeasure; certainly Friedman had good reason to be pleased with his own inventiveness.

William Friedman, over the course of his life, demonstrated a penchant for collecting cryptographically related patents. Ultimately he was granted thirty of them.[9] Like inventors before and since, he discovered that dealing with the U.S. Patent Office was neither a pleasant nor an alacritous proposition. In fact Friedman's own experiences with government red tape proved to be an ongoing source of exasperation that consumed his time and sapped his energies. As many times as he explained it to them, patent office officials simply could not—or would not—recognize the unique contribution to cryptology presented by randomly stepping rotors. There remain today bundles of letters between Friedman and the patent office, often in duplicate and triplicate copies, meticulously detailing the merits of his respective patents years after the initial patent applications were filed.[10] In spite of his repeated petitions, patent office officials sitting only blocks away from Friedman obdurately continued to presume that any cipher rotor machine was just an unimaginative derivation of the Hebern machine.

In a letter from Friedman to the U.S. Patent Office dated December 5, 1934, regarding Patent Serial No. 682,096, he stated, "the cipher key here serves as the physical embodiment of the 'keying principle' … and that its sole purpose is to serve as the controlling element in effecting the displacements of the cipher wheels in a variable manner. Contrast this situation with that in Hebern."[11] In the Hebern cipher machine, the complexity is the machine's wiring, not the initial setting of the cipher wheels or the placement of the rotors. Friedman continued, "Referring now only to the mechanism for displacing the cipher wheels, in Hebern there is embodied no such thing as a cipher key which corresponds to a 'keying principle which is variable in character' because the mechanism for displacing the cipher wheels is absolutely fixed."[12] In the Hebern cipher machine, the cipher wheels advanced in the



Friedman's M-134 converter. Note plugboard at upper left.

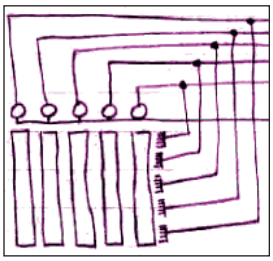
same regular manner for every message. Friedman's complaint was in response to a letter from the Patent Office, posted June 6, 1934, which states that Friedman's claims were "rejected on Heburn [*sic*]."[13]

In still another letter from Friedman to the Patent Office, dated April 3, 1934, he again contended,

> In Hebern the movements or displacements of the code wheels are purely mechanical; these movements are regular or periodic in character, and controlled by ratchet mechanisms internal to the device itself. In the present invention [Friedman's], these movements are controlled by the cipher key transmitter in an aperiodic manner … It will be recognized that the Hebern structure has the inherent weakness of all such devices where the keying mechanism is a part of the device itself. Periodical recurrence of movements is a natural characteristic of all such mechanisms and the predictable factor thus introduced defeats the essential purpose.[14]

As the months turned into years, it probably occurred to Friedman that his purposes might have better served by addressing his letters to Santa Claus.

From the time Friedman had identified the weakness in contemporary rotor cipher machines and had conceptualized an effective countermeasure, the subsequent refinements to his pseudorandom stepping rotors were entirely evolutionary. As Friedman's design for his new devices became more sophisticated, they manifested themselves under a succession of names, including M-134, M-134A, M-134-T1, and M-134-T2. When Friedman's M-134 Converter went into production, it "consisted of the chassis, the machine itself, an assembly of wheels," a plugboard, and a punched tape transmitter (reader).[15] Drawing on a pool of ten different rotor wheels, the M-134 used five wheels at a time, but it was the paper key tape that provided movement to the respective rotors and gave it cryptographic strength.

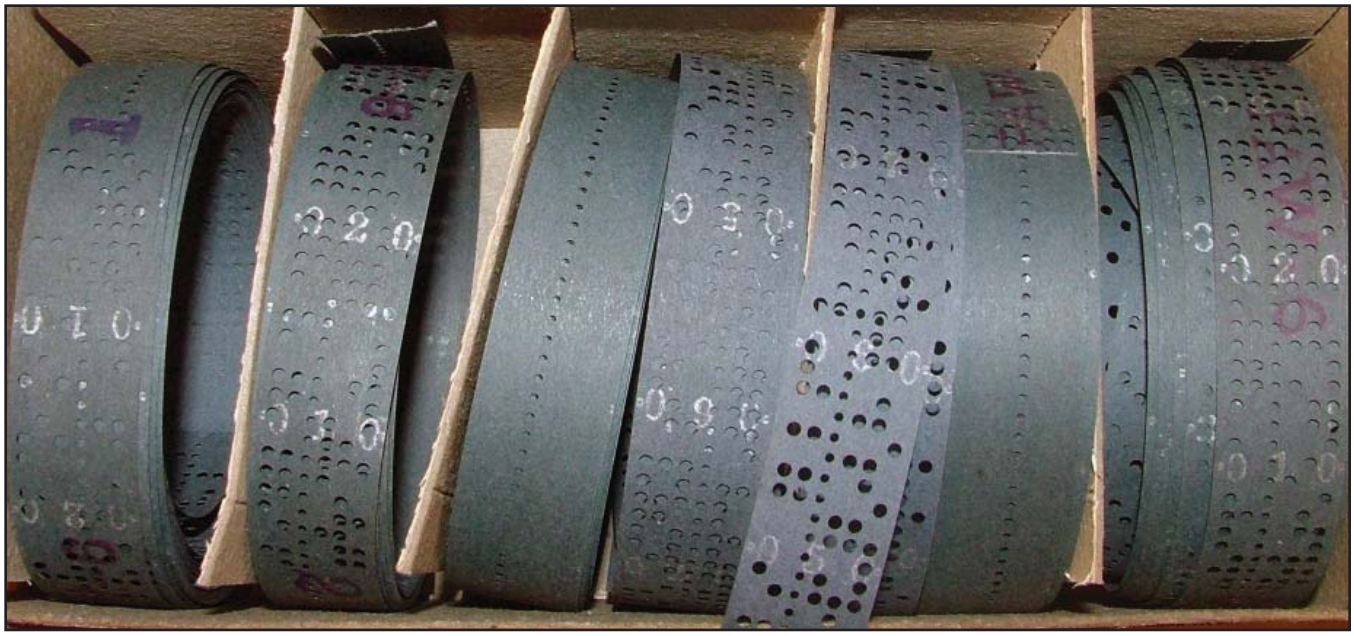


Rowlett's Epiphany

Frank Rowlett, who had received several years of cryptanalytic training under Friedman, was given the unenviable task of creating the quantities of key tape necessary to drive Friedman's electric cipher machines. Rowlett recorded why and how in 1934 he had been assigned the job of making key tape. He said, "Now Friedman's thought was that we ought to get cracking on the construction of these tapes so that when the machines came off the assembly line" they could be sent out to field stations right away. Unfortunately, the machine Friedman had designed for the process of generating key tapes was beset with problems, and Rowlett spent much of his time trying to make it work properly. Rowlett continued with a touch of irony: "I got stuck with the job of making the tapes because I had a little bit more practice in mechanical things than the rest of the group and I think they were smarter than I because they didn't let it be known."[16] Being the dedicated mathematician that he was, Rowlett set out to make the key as random as possible. Since theory and practice are frequently at odds with one another, he discovered that producing key tape proved to be a more difficult undertaking than Friedman had envisioned.

Rowlett struggled with the problem of key generation until he became completely frustrated. It was obvious to him that producing loops of paper tape with holes randomly punched throughout their lengths was too labor intensive and probably rife with vulnerabilities. Too, Rowlett really doubted the overall practicality of Friedman's key tape transmitter. He surmised that in stressful environments operators might easily tear or misuse key tapes. Just as disturbing to him was the prospect of their succumbing to the temptation to reuse the key tapes and their starting places. Rowlett was also concerned about numerous issues associated with Friedman's machine. Not only were Friedman's key tapes lengthy, but they required all parties on a particular network to maintain the same large inventories of keying material. The distribution of and the accountability for tape alone would entail untold manpower and resources, not to mention acquiring secure facilities for its storage.

Besides his reservations about Friedman's key tape transmitter mechanism, Rowlett just didn't like making the paper key tapes for the M-134 and would do almost anything to return to the more exciting work of breaking into Japanese ciphers. Given Rowlett's affinity for machine solutions, he sought a means of automating this impossible assignment. With a burst of inspiration, he decided that it might be possible to use one set of rotor wheels to generate the random stepping movement for the M-134 cipher rotor wheels. If he could find a way to do that, the entire process would become much easier and undoubtedly more secure. He would later admit in an interview,



Key tape for the M-134 converter

> I don't know that I ever was confronted with a more hopeless task than making these [Friedman's] devices work and do what was needed and I soon became desperate. It didn't take more than a month for me to realize that I was fighting a real losing battle here, and as you are apt to do in the case of where necessity becomes very evident you try to figure out some better way of doing things and I was dreaming about how rotors could be made to do other [things] and decipher [messages].[17]

As the drudgery of developing key tapes became more tedious, the solution came to him.

> I thought it would be a helluva good idea if we replaced these key tapes with a second set of rotors which in effect would generate five screens of impulses equivalent to the holes and no holes in the five levels of the tape and use this assembly of five additional rotors instead of the tapes. Well, I thought this was a pretty powerful thing and I just was so enthusiastic about it because it looked like I was getting out of this impossible task, I went to tell Friedman about it.[18]

Armed with enthusiastic conviction, Rowlett approached his boss about scrapping the whole key tape transmitter concept and moving on to something more cryptographically sound. After permitting Rowlett only briefly to present his discovery, Friedman would hear no more. He categorically refused to believe it possible to create a machine capable of generating its own random stepping.[19] Friedman, who was every bit as hard-headed as his nemeses over at the Patent Office, remained wedded to using replaceable paper key tape. After all, his salient argument for pursuing a patent for his key tape transmitter—which caused the cipher rotors to advance irregularly—was that any machine that determined its own stepping would be in violation of Kerckhoffs' second principle and, therefore, vul-

nerable to cryptanalysis. To what degree the loss of a potential patent clouded the respectable Friedman's thinking is not known.

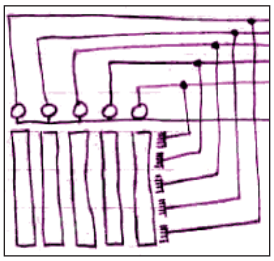
Frank Rowlett, besides being intellectually brilliant, was a tenacious man and not the sort to abandon a cause in which he genuinely believed. Time and again, he requested of his employer the opportunity to fully explain his concept. Each attempt made Friedman all the more formal—to the point of being brusque—and their strained working relationship slowly approached a breaking point. Years later, Rowlett recounted,

> This went on for, oh, I guess six, eight, ten months, I confronted Friedman … Friedman was still reluctant and finally out of a real fit of desperation I said, either Mr. Friedman I don't know what I'm talking about or I know what I'm talking about and you don't understand me … I think we've got to clear this up because I'm going to have to quit that job. I just can't meet your requirements.[20]

Then being on something of a roll, Rowlett went on to inform the unsmiling Friedman that he would have to go above Friedman's head to the Army's chief signal officer if Friedman did not give his proposal a fair hearing. This of course was a risky gamble for a family man in the depths of the Great Depression. Friedman was now faced with an ultimatum and had to weigh the respective merits of retaining a capable and loyal assistant or losing face to his subordinate. Reluctantly, he offered Rowlett an opportunity to fully lay out his concept.[21]

Frank Rowlett, besides being intellectually brilliant, was a tenacious man and not the sort to abandon a cause in which he genuinely believed.

Frank Rowlett



Iacta Alea Est.*

Rowlett knew this would be his sole opportunity to sell his stepping maze concept and came to the meeting well prepared. One after the next he responded to Friedman's sometimes insightful, sometimes petty questions with rock-solid, unambiguous answers. At the end of the tension-filled session, Friedman was forced to pause and reconsider some of his own cherished cryptographic perceptions. Not only did Rowlett's invention run counter to Friedman's previously published opinions against the incorporation of keying logic into a cipher machine, but it made Friedman's beloved pet project, the M-134, obsolete. Following Rowlett's presentation, there was a long and pregnant silence, after which Rowlett was coolly dismissed from the room. Ominously, Rowlett heard nothing from his boss for the rest of the day. As the afternoon slowly wore on, Rowlett mentally cleaned out his desk and began to consider his prospects for future employment.[22]

Years later Rowlett recalled the incident: "Well, next morning he [Friedman] came in, eyes shining, just all excited and he says, we're going to do this." He called it a "beautiful idea … and he went up to see the Chief Signal Officer with stars in his eyes to try to sell this new idea."[23] A night of due reflection had forced Friedman to recognize that Rowlett's concept marked a gigantic step in cryptography, and his prudent acquiescence to Rowlett changed the course of history.

Surprisingly, once Friedman fully accepted that he had been wrong, his attitude toward his junior changed entirely, almost. Rowlett went on to recollect,

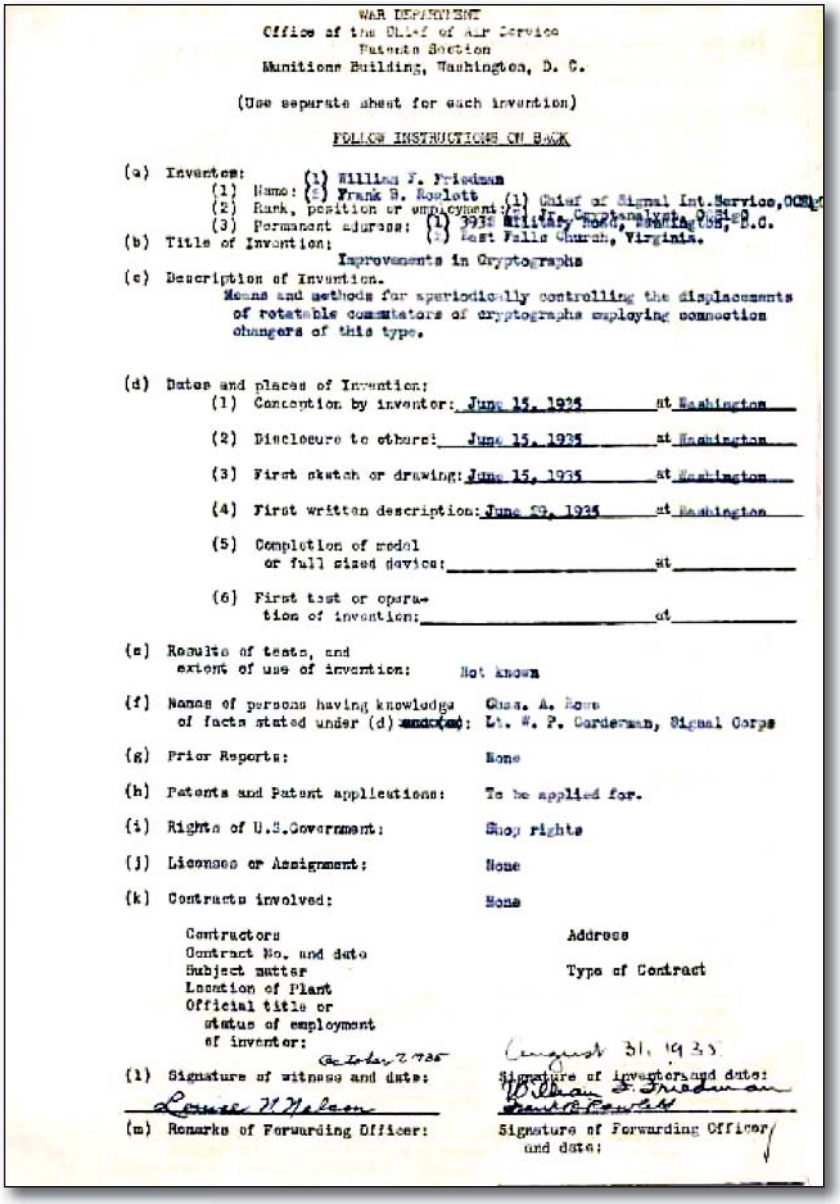
> . . . I had never before found him so friendly and so agreeable to work with. He still retained his "boss-employee" attitude, but I could see that as he reached a more comprehensive grasp of the principles I had discovered, he was accepting me as a professional cryptanalyst rather than as a student.

Before the day was out, Friedman told Rowlett, "I want you to start immediately on drafting patent specifications, and I will work directly with you in developing these new principles into their most advantageous form." The odious work of key tape generation was put on hold for the time being.[24] Patents come. Patents go. Patents come again.

By summer's end in 1935 Friedman and Rowlett had refined the details for a wholly new cipher machine, the M-134-C, which synthesized the principles of Rowlett's stepping maze and Friedman's earlier M-134s. They also managed to complete a draft patent (shown opposite) for what was to

* The die is cast.

become SIGABA. (Army cryptographic equipment of that period was given code names beginning with *SIG* [for *signals*] followed by randomly chosen letters.) Unfortunately for the cryptographers, the nadir of the Depression had been reached, and the Army's budget for cryptographic research and development had been entirely depleted by Friedman's M-134 device. Thus, any fielding of SIGABA was out of the question. Still, the Army did have a small sum which could be allocated for retrofitting Friedman's existing M-134s. This they used to construct a number of "add-on" devices to be used with the existing M-134s.[25] The so-called SIGGOO (M-229) component replaced Friedman's "key tape transmitter" with a less robust version of Rowlett's stepping maze.



WAR DEPARTMENT
Office of the Chief of Air Service
Patents Section
Munitions Building, Washington, D. C.

(Use separate sheet for each invention)

FOLLOW INSTRUCTIONS ON BACK

(a) Inventor: (1) William F. Friedman
(1) Name: (2) Frank B. Rowlett
(2) Rank, position or employment: (1) Chief of Signal Int.Service,OCSig
(3) Permanent address: (1) 3937 Military Road, Washington, D.C.
(2) East Falls Church, Virginia.

(b) Title of Invention: Improvements in Cryptographs

(c) Description of Invention.
Means and methods for aperiodically controlling the displacements of rotatable commutators of cryptographs employing connection changers of this type.

(d) Dates and places of Invention:
(1) Conception by inventor: June 15, 1935 at Washington
(2) Disclosure to others: June 15, 1935 at Washington
(3) First sketch or drawing: June 15, 1935 at Washington
(4) First written description: June 29, 1935 at Washington
(5) Completion of model or full sized device: _____ at _____
(6) First test or operation of invention: _____ at _____

(e) Results of tests, and extent of use of invention: Not known

(f) Names of persons having knowledge of facts stated under (d): Chas. A. Rowe
Lt. W. P. Corderman, Signal Corps

(g) Prior Reports: None

(h) Patents and Patent applications: To be applied for.

(i) Rights of U.S.Government: Shop rights

(j) Licenses or Assignment: None

(k) Contracts involved: None

Contractors — Address
Contract No. and date
Subject matter — Type of Contract
Location of Plant
Official title or status of employment of inventor:

(l) Signature of witness and date: October 2 1935
Louise W. Nelson

Signature of inventor and date: August 31, 1935
William F. Friedman
Frank B. Rowlett

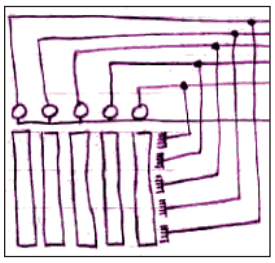
(m) Remarks of Forwarding Officer:

Signature of Forwarding Officer and date:

William Friedman and Frank Rowlett's draft patent of August 1935 for what was to become SIGABA

The SIGGOO assembly consisted of a three-rotor setup in which five of the keyboard inputs were live, as if someone had pressed five keys at the same time on an ENIGMA. These outputs were "gathered up" into five groups as though all the letters from "A" to "E" were wired together. In that way the five signals on the input side would be randomized through the rotors and come out the far side, ensuring power in one of five lines. The SIGGOO rotors, therefore, could be controlled with a day code, or key, eliminating the need for paper tape keying material. Because of cost constraints, though, not all of the model M-134s could be retrofitted with SIGGOOs, and large numbers of them continued to rely on Friedman's original paper tape transmitters.[26]

The M-134 Converter modification with its five rotor cipher wheels, the three rotor wheel SIGGOO add-on, and a 26-wire plugboard was hardly elegant in appearance and resembled a comic-strip Rube Goldberg device. It was, nonetheless, the strongest device in the shadowy world of cryptology and easily surpassed anything the British or the Axis Powers had at their command. Since one cannot know what he doesn't know, neither Friedman nor Rowlett at the time truly appreciated just how advanced their new cipher machine really was.



Enter the Navy

As the torrid summer in 1935 lost its grip on pre-air conditioned Washington, DC, it was apparent to no one that the sister services were on a cryptographic collision course. While Friedman and Rowlett occupied themselves with fine tuning a patent request for SIGABA, the Navy's OP-20-G organization was considering the acquisition of new cipher machines. The Navy cryptographers for several years had relied on Hebern machines to meet their communication security needs, but by the mid-1930s they began to doubt the machines' integrity and balked at a contract to procure more of them. Quietly, Lieutenant Joseph N. Wenger, acting chief of the Navy's cryptologic organization, OP-20-G, and his colleagues began looking farther afield for something more secure.[27]

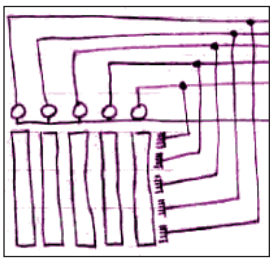
Early in October Wenger made the fateful decision to seek out Friedman's advice and walked over the little-used pedestrian bridge that linked the Navy and Munitions buildings on the Mall in Washington. Clearly, the Navy was in dire straits if it admitted to needing any advice from the Army. As Frank Rowlett remembered it, "in one of the rare periods of consultation between [the] navy organization and the army organization I think it was Joe [Wenger]… [who] told Friedman that the navy would been [*sic*] real disappointed with the [existing] contract."[28] Lieutenant Wenger went on to tell Friedman that the new machine Hebern was trying to sell the Navy "had been unsatisfactory [as well and] they now had a lot of development money but didn't have any ideas to invest the money in and for goodness sakes did the Army have something … any good ideas at all."[29] Friedman, who was initially taken aback by this admission, sat up in his chair and brightly suggested that he might indeed have something to share. But first he would have to gain permission from his senior leadership.

Later that month on the 21st, Lieutenant Wenger and a colleague, John W. McClaran, met with Friedman and Rowlett at the Munitions Building. There, the Army proudly shared its plans for SIGABA with the Navy. Lieutenant Wenger, who among his colleagues was hardly known for animated expression, remained true to form and demonstrated little indication that he was impressed. Ten days later, on Halloween, another OP-20-G complement composed of Wenger, McClaran, and John Harper ambled across the bridge for another meeting with Friedman. Again, Friedman explained Rowlett's plan for the stepping maze and how it could control cipher rotor movements.[30] The following day a still larger contingent of naval officers assembled in Friedman's office for a briefing on the SIGABA concept. Throughout this last presentation, Friedman's guests exhibited an uneasy institutional politeness and left with Wenger's same general lack of enthusiasm.

Lieutenant Joseph N. Wenger, acting chief of the Navy's cryptologic organization OP-20-G (pictured later in his career)

> Wenger told Friedman that "they now had a lot of development money but didn't have any ideas to invest the money in and for goodness sakes did the Army have something … any good ideas at all."

Rowlett, after several anxious months, had received no feedback from OP-20-G and began to pester Friedman for word about the Navy's plans for SIGABA. Friedman finally tired of these queries and confessed that Wenger had reported that "there were certain … operational difficulties and that they just weren't sure the idea would work." To this, Rowlett mused, "well, I thought the doggone thing would work and maybe they weren't as smart as they thought they were."[31] Rowlett had reason to be irritated. He knew it was a good idea, a very good idea, and became all the more convinced not only that it would work but that it offered secure communications beyond anything thought possible at the time. With SIGABA's future on indefinite hold, Friedman and his colleagues returned to solving Japanese ciphers and producing paper key tapes for those M-134s not fitted with SIGGOOs (since the standard M-134s and those with SIGGOOs were not compatable, they were used on separate networks).



A Disagreeable but Rewarding Surprise

Four years later, in 1939, with one war spreading across Europe, another was looming on the Pacific horizon. In anticipation of the latter conflict, Rowlett and Navy Lieutenant Commander Wesley (Ham) A. Wright were working on the Japanese PURPLE analog cipher machine (used to decrypt the Japanese diplomatic cipher designated as PURPLE) when a shocking revelation came to light. Rowlett recounted this incident in his memoirs:

> … we were speculating about what type of cryptographic mechanism the Japanese might have used to produce such an unconventional substitution system. "Maybe they're using something like what we're planning to use in our new Navy cipher machine", Wright remarked. "Let me explain it to you, and you can give me your opinion of it". He then started to sketch out for me the cryptographic circuitry of for [*sic*] the new Navy cipher machine.[32]

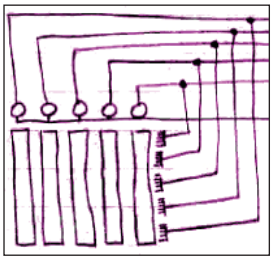
Rowlett with an increasingly sickening realization recognized the new Navy cipher machine as his own invention. He was particularly stunned since back in 1935 he had learned through Friedman that the Navy had rejected the idea as being impractical. Without revealing that he had conceived of the cryptographic principles involved, Rowlett asked Wright whose idea the cipher machine was. Wright responded that he believed it was Wenger.[33]

Frank Rowlett was no little upset by this news. Not only had he been excluded from SIGABA's development, but he saw the credit for his invention going to another man. At best Ham Wright had been misinformed, and at worst Wenger was hoping to pass off the rotor maze as his own idea. In either case, Rowlett decided to get to the bottom of the matter as quickly as possible. As soon as Wright left, Rowlett hurried down the hall to tell Major William Reeder what had just occurred.[34] Reeder, who, as Friedman's superior, was the head of the Signal Intelligence Service, needed to be informed of this turn of events. That Reeder already seemed to be aware of the Navy's work on SIGABA came as the second disagreeable surprise of the day. Just how long Reeder had been keeping this to himself is unclear. While he had not gone to Rowlett with the news, Reeder was perfectly straightforward about it when asked. In spite of this omission, Rowlett still considered Reeder to be a good supervisor and a friend. Several months later, Major Reeder, in trying to make amends, went to Rowlett with something that he wanted to hear. The Navy would soon be taking delivery of a working model of their new cipher machine and Rowlett was invited to help test it.[35]

On 3 February 1940 the Army's primary SIS cryptologists—Friedman, Rowlett, Sinkov, and Kullback—trooped over to the Navy Building to see the prototype of the Electric Cipher Machine Mark II (SIGABA). Following an informal demonstration of the device, during which Friedman and Rowlett could hardly contain their excitement, they were finally given the opportunity to put it through its paces. It was a case of love at first sight. Rowlett later said, "… it was the most beautiful thing to look at from where I stood and I couldn't keep my hands off it and of course the Navy was delighted to find somebody as enthusiastic about it as I appeared to be."[36] The Navy had exceeded any expectations Rowlett had entertained, and he wanted to explore every facet of the Navy's engineering triumph. He and Friedman were all the more heartened by the Navy's willing acknowledgment of the Army's visionary role behind SIGABA. (The Army designated the combination of machines as the M-134-C, which was also applied to the later, more mature SIGABAs. For the purpose of this paper, the M-134-C machine will be referred to by its more popularly used Army short title, SIGABA, whenever possible.) [37]

Rowlett, besides being taken with the purely mechanical aspects of the machine, was also quite interested in SIGABA's wiring scheme. He later said, "I was very curious about the circuitry that they'd decided on in terms of the association of the contacts on the in-plates of the control maze with the stepping magnets of both mazes."[38] He was also fascinated by the additional set of rotor wheels that the Navy had included. When he and Friedman shared the stepping maze concept with the Navy, the design incorporated a plugboard similar to that on the German ENIGMA machine. At first the Army cryptographers did not perceive "… the advantage of the extra set of rotors that the Navy had introduced … We [Friedman and Rowlett] preferred the plugboard. The Navy for some reason didn't like plugboards but this was not a point … to quibble about."[39] With either the plugboard or the index rotors, SIGABA represented the pinnacle of cryptography, and both the Army and Navy were confident in its ability to resist all assaults.[40]

Those who attended the demonstration at the Navy Building had every reason to bask in the warmth of self-congratulation. It had been a long and unlikely path from Friedman's and Rowlett's collaboration to the Navy's manifestation of their concept, and Rowlett couldn't help but reflect with a little nostalgia on the old ways of doing business: "… before, you had to have a different set of codebooks and these became onerous, but with the new secure cipher machines, all the cipher clerk needed was a box of rotors and a little pamphlet that told him how to use the rotors, which made the concept … very practical."[41] As elated as all of them were, none present could then conceive the extent to which their accomplishment would alter the future.



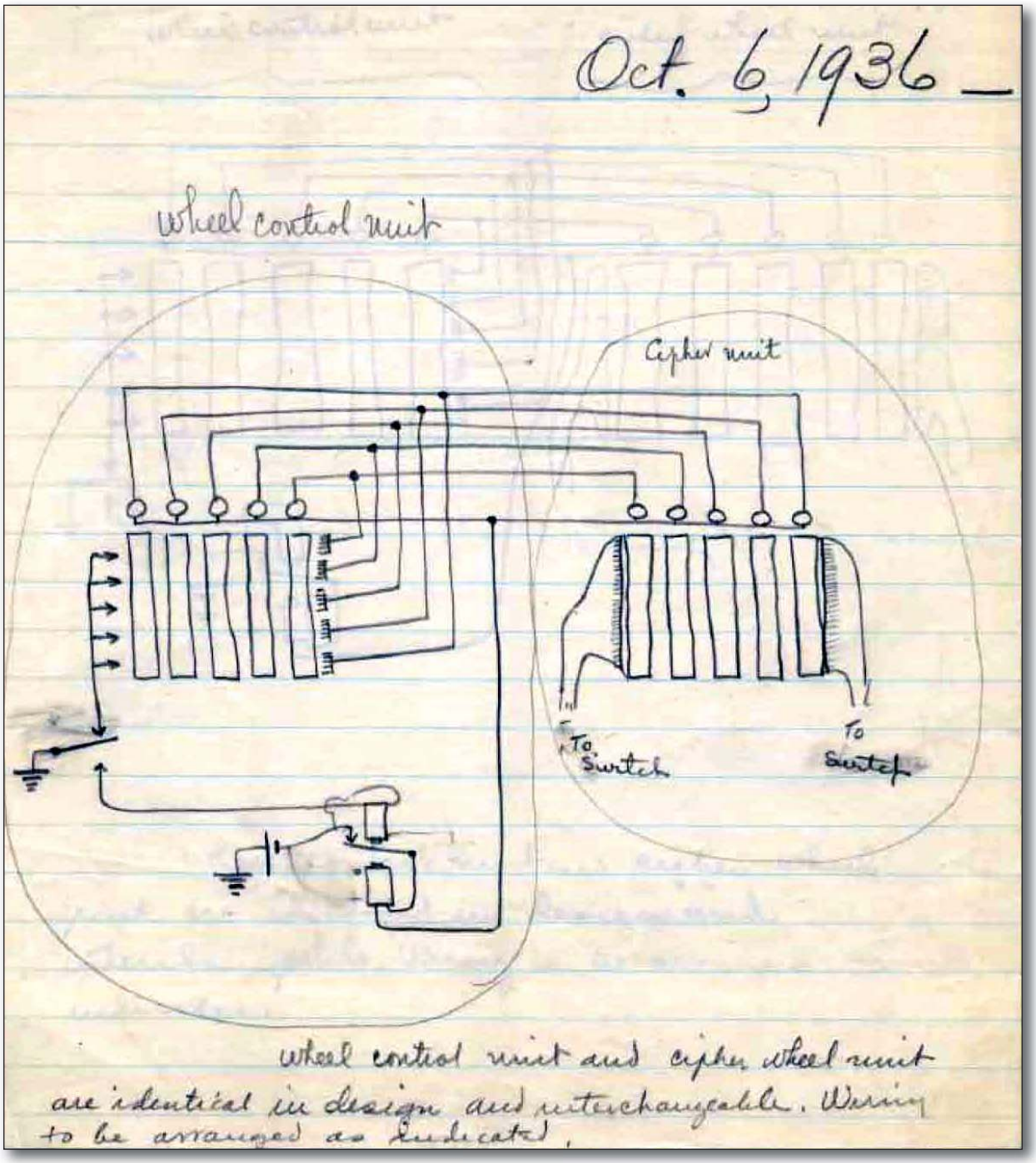
SIGABA Is Built

Friedman and Rowlett's idea behind SIGABA had been elegantly simple, but engineering it into practical reality proved to be a formidable undertaking for the Navy. From late 1936 until January 1941, Navy cryptographers and their prime contractor, the Teletype Corporation, developed a series of prototype machines, each building on the lessons gleaned from its predecessor. Early prototypes were prone to failure due to environmental conditions such as heat, humidity, and vibration, but as the SIGABA design matured, these problems and others were resolved. Successive models were smaller, lighter, faster, and more reliable.

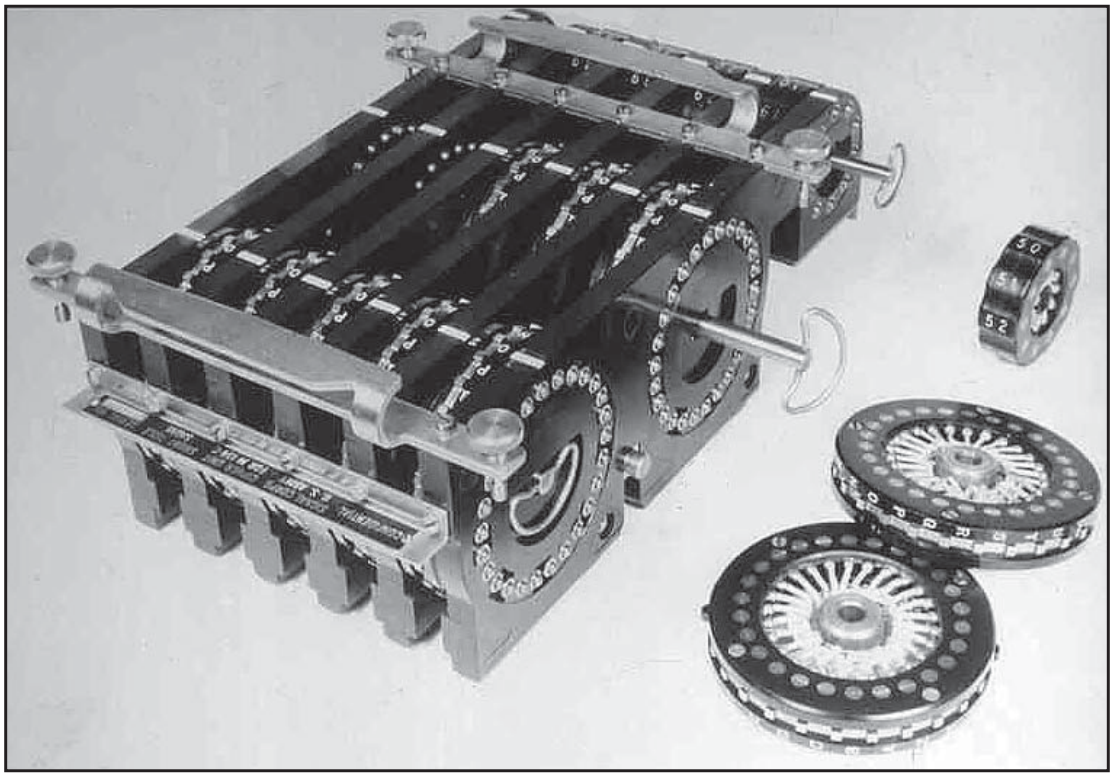
By the time the ECM Mark II (SIGABA) neared its birthing stage, the resulting device proved to be both electromechanically robust and cryptographically strong. Variant models could operate on 115-volt alternating electricity or 24-volt direct current/battery power to suit the respective needs of the sister services. Production-run SIGABAs achieved an impressive 60 words per minute capability. To allay any Army reservations about SIGABA's reliability under austere conditions, Navy engineers offered emergency, manually cranked attachments. These saw almost no actual use in field operations. Another option was a forty-pound thermite bomb for SIGABAs destined to go into harm's way. While the Navy steadfastly prohibited these emergency destruction devices aboard ships, the Army mandated their inclusion for SIGABAs deployed outside of the continental United States.[42]

The quest to further enhance ECM/SIGABA would likely have continued for some time had not the Battle for France, then raging in Europe, convinced Navy officials that the time to field their new cipher machine had arrived.[43] As the Navy prepared to let contracts for full-scale production of SIGABA, the cryptologists at OP-20-G and their counterparts in the War Department were fully confident that SIGABA/ECM II could deliver the degree of security they sought. This optimism was founded in the combination of six factors identified by Navy cryptographer Lieutenant Laurance Safford and paraphrased below:

> 1. SIGABA/ECM II included a sufficient number of cipher wheels in the maze to generate an astronomical number of "alphabets" and starting points. The five-wheel cipher maze of the ECM and Combined Cipher Machine (CCM) provided 11,881,376 alphabets for each arrangement of code wheels. (The ENIGMA, by contrast, offered only 17,576.)[44] [CCM was a specially modified, less sophisticated SIGABA that was interoperable with the British mainstay TYPEX machine.]
>
> 2. The SIGABA/ECM II included ten reversible cipher wheels in a set. This pro-



A sketch of the wheel control unit, the "control rotor bank," separate from the cipher unit, called the "cipher rotor bank." Note at bottom reads, "Wheel control unit and cipher wheel unit are identical in design and interchangeable. Wiring to be arranged as indicated." It is similar to the diagrams Friedman showed the Navy during 1935. (Friedman Collection, NSA/CSS accession #47270, box 10, folder 5)



SIGABA rotor maze. Note the five small ten-pin wheels that replaced the Army's original plugboard.

vided 9,667,680 possible wheel orders, making an adversary's "trial and error" solutions impractical, if not impossible.[45] (The CCM also offered ten reversible cipher wheels per set.) [There is a common misconception that SIGABA rotors could **rotate** either forward or backward. While the direction of travel for SIGABA rotors was forward only, all fifteen rotors could be flipped in either direction to maximize their cryptographic potential.]

3. The use of aperiodic stepping of cipher wheels, instead of regular or modified-regular stepping motion, precluded all known analytical solutions and prevented "short-cut" solutions with captured cipher wheels.[46]

4. The stepping of the alphabet maze was controlled by an independent source—in this case by both the five index rotor set and the five control rotor set.[47]

5. The use of a multiplicity of stepping actions (5,855), *dependent solely on the key*, instead of only one in other cipher machines.[48]

6. The replication of code wheel sets—both "effective" and "reserve"—with prompt change of code wheels in case of known compromise, and a periodic change as an added security measure. The inclusion of a back-up set of fifteen wheels (five index rotors, five control rotors, and five cipher rotors) was taken to dispel any lingering doubts as to the *absolute security* of SIGABA.[49]

Women assembling SIGABA crypto rotor wheels

With America's involvement in the war a near certainty, the Army identified the necessary funds to assist the Navy in procuring SIGABAs in numbers. The Army's first lot of 459 machines was fielded in June 1941. With a due sense of urgency, it distributed these SIGABAs to upper echelon headquarters in the CONUS and to selected organizations in American possessions in the Far East. Naval units in the Atlantic theater were given priority because forces in the Pacific had already been equipped with the older ECM Is.[50] Of course some sensitive sites like Corregidor, Guam, and Pearl Harbor necessitated the highest degree of security for the signals intelligence information they processed and thus received the new cipher machines as well. The Navy was in the process of outfitting its capital ships of the Pacific fleet with ECM Mark IIs (SIGABAs) when Pearl Harbor was bombed. Ninety-six had been issued to ships of the 14th Fleet, with another 100 in storage awaiting distribution to capital ships and other units. Twenty-five more were ashore undergoing depot-level maintenance. Fortunately, the machines destined for the doomed vessels were still in the warehouse on 7 December 1941 and thus escaped destruction. A hundred of these Pearl Harbor-surplus machines were hastily transferred to the Army and later used in North Africa. To meet the demand of producing more than fifty devices per month, contracts were let with additional manufacturers. By 1943 5,730 ECM Mark II/SIGABAs were in service and more than 300 per month were being delivered. The only feature distinguishing the Army and the Navy machines was the service-unique designation on the name plates. For the first time in the nation's history, the Army and Navy enjoyed cryptographic interoperability.[51]

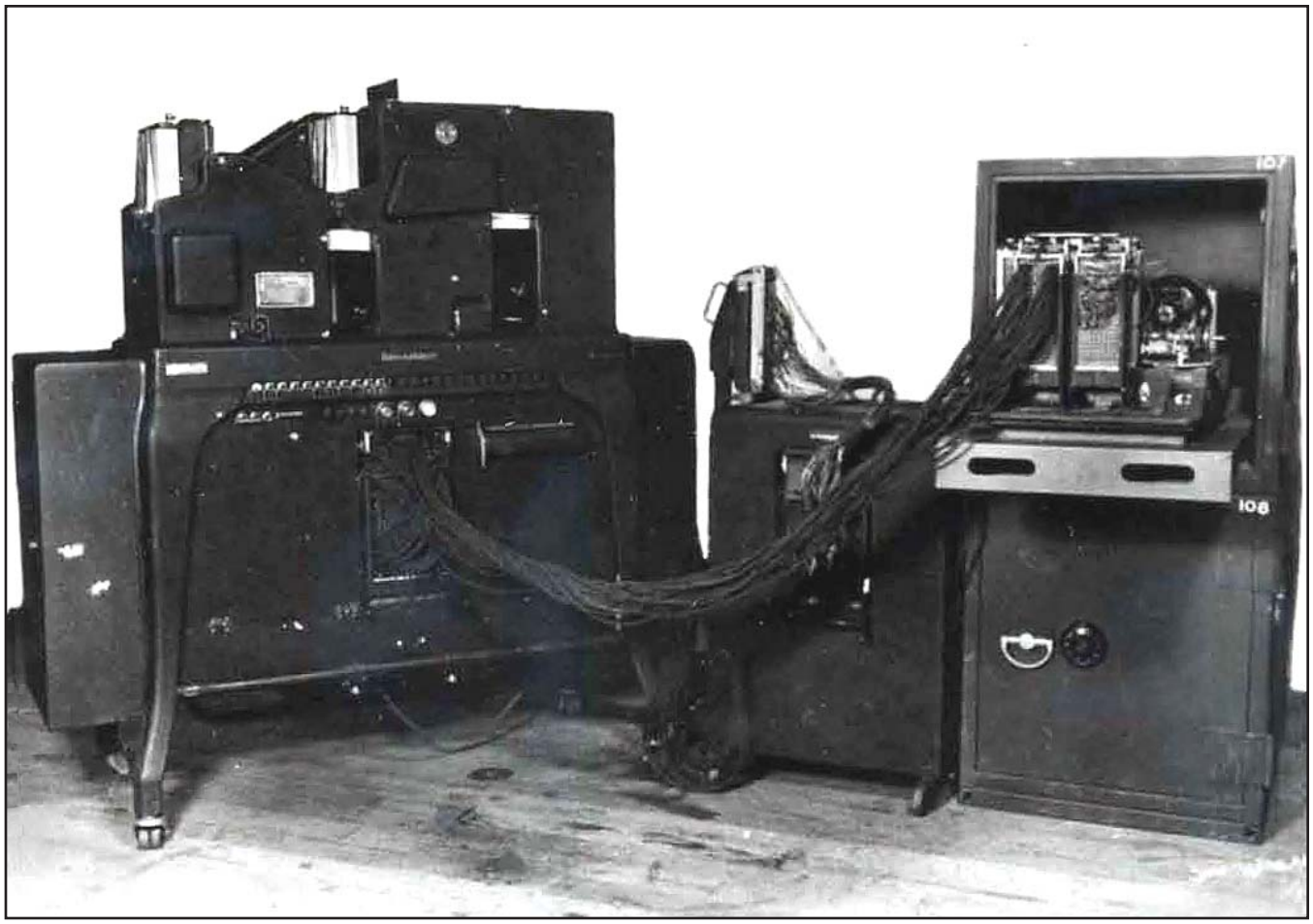
The most security-sensitive work of wiring the rotors was performed by more than 200 WAVES (Women Accepted for Volunteer Emergency Service). WACs (members of the Women Army Corps) ... performed the same task for the Army.

While trusted civilian contractors such as the Teletype Corporation manufactured and assembled the SIGABA chassis, the all-important crypto rotor wheels remained a military in-house activity. Uniformed Navy personnel and civilian workers fabricated rotors from stock materials at the Washington (DC) Navy Yard (later at the Nebraska Avenue Naval Station). The most security-sensitive work of actually wiring the rotors was performed by more than 200 WAVES (Women Accepted for Volunteer Emergency Service). WACs (members of the Women Army Corps) at Arlington Hall performed the same task for the Army. Since each cipher machine required a minimum of two complete sets of fifteen cryptographic rotors, these military women were pressed to meet growing production quotas. On occasion when the Army's requirements overwhelmed its capacity to produce them, the Navy lent a willing hand in providing additional rotors. Because SIGABA/ECM IIs saw heavy use, the life expectancy of a rotor was between six months and two years. In 1943 the average WAVE managed to solder the connections for fourteen wheels per day. One actually assembled a record twenty-two wheels on her shift. The average for male shipyard electricians had been seven wheels per day before the decision was made to assign them to other duties. Midway through the war, the Navy women alone had wired more than 150,000 rotor wheels. Remarkably, there was not a single configuration error and only one instance where a wheel had been mislabeled![52] Before the rotors were shipped to the field, each one underwent more than 2,800 operations before they were certified for use. When SIGABA production ceased after World War II, some 10,060 machines were in the inventory along with over 450,000 crypto wheels to support them.

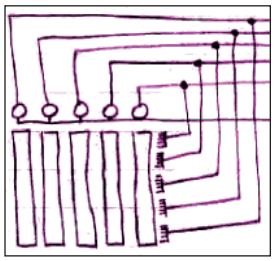
According to the U.S. Army's account of the SIGABA's development, *History of Converter M-134-C*, "each of these experimental and adopted models is in the direct line of cryptographic development which culminated in Converter M-134C."[53] In keeping with Army procedures, the major constituent subcomponents of the SIGABA encryption system were given their own alphanumeric designations.[54] Below are examples of SIGABA crypto-nomenclature.

SIGABA	Converter M-134-C chassis, less the rotors
SIGKKK	Maintenance instructions for converter M-134-C
SIGQZF	Crypto-operating instructions for converter M-134-C
SIGBRE	General instructions for converter M-134-C
SIGIVI	Cipher basket unit for converter M-134-C Set of 10 rotors as designated in the current key list Keying data in the current key list

As though SIGABA were not already sufficiently sound cryptographically, the Army and Navy took additional measures to ensure the system's robustness. Unlike the cipher systems used by the British and the Axis Powers, SIGABA's daily settings were generated by yet another rotor-based cipher machine rather than humans. Army and Navy key generators produced each month's daily settings printed on a single sheet of paper. Thus, the key was easy to transport, easy to use, easy to destroy, and, if necessary, easy to replace.



IBM SIGABA key generator used at headquarters to produce daily key settings[55]



An Impenetrable Machine

Throughout World War II, SIGABA offered America an inestimable advantage. While decrypted Axis communications channeled a continual flood of actionable intelligence to U.S. decision makers, SIGABA denied the enemy a similar resource. The collaborative nature of SIGABA's design enabled Army and Navy forces to coordinate their complex, joint operations in complete secrecy. That the services were operating identical machines turned out to be particularly important in the early hours of the war when the distribution of machines and rotors was not yet complete. During critical engagements in the Philippines, Java, Australia, and North Africa, Army and Navy crypto-maintenance personnel shared components back and forth as necessity demanded. There were also emergency situations when the Navy and Army used each other's equipment to ensure the unimpeded flow of secure wartime communications.[56]

The need for Anglo-American interoperability similarly hastened Allied cooperation in fielding cryptographic solutions. Later modifications permitted specialized, less sophisticated ECM Mark IIs [SIGABAs] to interoperate with British Typex cipher machines in support of joint U.S./British/Canadian operations. This functionality was achieved through three different means. The first of these, the ECM Adapter (CSP 1600), was produced at the Washington Naval Yard ECM Repair Shop where 3,500 were made available for retrofit. The second was the CCM, a SIGABA variant made at the ECM Repair Shop exclusively for joint Allied communications. Because of cost, only 631 of these models were made. The third, most common and most cost-effective, was the "X" Adapter manufactured by the Teletype Corporation in Chicago. Forty-five hundred of these were sent to depot-level maintenance facilities for installation. All three of these options used Typex-configured cipher rotors. By the war's end, nearly all U.S. military communications facilities could process joint-Allied secure communications traffic.[57]

In spite of SIGABA's enormous cryptographic strength, the sister services harbored a slight but healthy anxiety about the enemy's cryptanalytic capabilities and continued to upgrade SIGABA. What if the Japanese or Germans were enjoying success against SIGABA similar to the Allied success against ENIGMA? The notion could not be blithely dismissed. Thus, during the latter part of the war, the Allies sought means to validate the integrity of their cryptographic efforts. Intercepted enemy messages were closely scrutinized, and prisoners of war were examined for any hint that U.S. cryptography had been compromised. Even before Berlin fell, it had become clear to the Allies that the Nazis had exploited some lower-level U.S. cipher systems when there had been lapses in COMSEC discipline. On the other hand, no evidence emerged

that the Germans had made any headway against SIGABA.[58]

Deciphered Japanese traffic also indicated that they had not broken into Allied ciphers. An intercepted JN-A-20 message, dated 24 January 1942, from the naval attaché in Berlin to the Vice Chief of Naval General Staff Tokyo afforded a comforting revelation. In it the naval attaché said he considered "joint Jap[anese]-German cryptanalytical efforts" to be "highly satisfactory," since the "German[s] have exhibited commendable ingenuity and recently experienced some success on English Navy systems," but are "encountering difficulty in establishing successful techniques of attack on 'enemy' code setup."[59] In another decrypted JN-A-20 message, the naval attaché wrote home that he had "…discovered that Heine [German] CI [Cryptographic] organization totals 800 persons and is … receiving unsatisfactory results on American Communications." He went on to report, "Since last year when Italy capitulated, English and American countermeasures have become more vigilant due to interpreting the CI situation."[60] The Japanese in their own internal communications confessed that they had made no real progress against American cipher systems and that the Americans were becoming even savvier about the security of their cryptographic operations.

Following V-E Day, Friedman and his associates were anxious to discover just what the Axis cryptanalysts had known. According to Rowlett, [61]

> We also were very much interested in what results … have been achieved by the Germans on the ECM or the SIGABA. And we got the answer to that. … they talked to the fellow who was in charge of what they called the American Big Machine.[62] See, they'd identified the Big Machine as the one jointly used by the Army and Navy, and they couldn't tell we were using different rotors or other things because their cryptanalytic understanding was just not at that level; and that was an interesting item in itself. They did have some success with the Hagelin.

Rowlett continued,

> …we had truckload after truckload of German cryptographic equipment. … We had some of the technical reports right up to the solution of code books and ciphers of other countries, photographic copies of second story jobs that they had performed on safes and embassy code rooms …This was gone over, carefully evaluated and assessed and a series of reports produced which you might find under the term TICOM [Target Intelligence Committee] Reports.[63]

With the return of peace in late 1945, the victorious Allies began compiling exhaustive studies on Axis technologies and capabilities. One of these, the Seabourne Report, was a series of technical treatises drafted by German subject matter experts. Volume XIII of this report detailed the Nazis' successes against Allied cryptographic systems. According to interviews with senior officials of the Luftwaffe Signal Intelligence Service contained in the report, the Germans revealed they had made no headway against the British Typex cipher machine, which was greatly inferior to SIGABA. The Luftwaffe cryptologists interestingly did not address SIGABA specifically, and their American counterparts were reluctant to press for answers lest they raise unwanted questions from their former enemies. Considering the immense disparity between SIGABA and Typex, it is a certainty that the Nazis made no inroads into the "American Big Machine."[64]

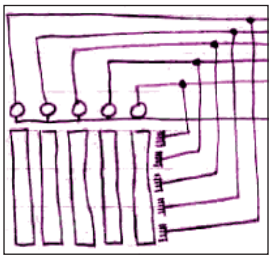
The official *War Diary of the German Signal Intelligence Group* again seems to validate the findings of the other inquiries. Entries made between February and November 1944 again strongly suggest that the Axis made no inroads into SIGABA. While their cryptologists were reading "un-Steckered" Croatian ENIGMA machines (early commercial model ENIGMA machines without a plug-

board or *Steckerbrett*), British transposition ciphers, Yugoslavian ciphers, and a variety of others, they undertook efforts against an American five-letter system. A translated notation in March 1944 reads, "A study was begun of a group of 5-letter messages from U.S.A. links presumably were enciphered with a machine of unknown type."[65] These doubtlessly were SIGABA messages. With each successive month the War Diary reflected that no progress was made on the five-letter American cipher system. Then in September 1944, with the Allied forces steadily advancing against the Germans, the War Diary includes, "U.S. 5-letter traffic: Work discontinued as unprofitable at this time." The Third Reich's cryptologists ostensibly decided to focus on ciphers they could exploit.[66]

During his detention by the Allies, the German cryptographic mathematician and POW Dr. Erich Huettenhain was asked what work was done on British and American ciphers. He answered that most of the successes were diplomatic and "Most of the American strip cipher was read."[67] When he was asked what type of cipher machines were broken, he responded, "The main machine broken was the American Hagelin which was broken only when [an] error occurred." He continued, "[c]ommon and regular solutions [were] impossible" against the Hagelin machine. Only when a soldier or sailor grew lazy and neglected to change the daily key were the Germans able to leverage their way into a Hagelin-based cipher.[68] If the Germans could exploit only a lower-level Hagelin machine on occasion, there was no possibility that they could even begin to unravel SIGABA. Dr. Huettenhain, when pressed about other Allied cipher machines, said, "I know of no other type of American machine, but the British Typex is known. It was not broken, and so far as we know cannot be solved unless the wheel positions are known."[69] Dr. Huettenhain continued,

> We have the ENIGMA [*sic*] which is similar to the Typex, and as we believe that the ENIGMA cannot be solved, no great effort was made to solve Typex. Typex has seven wheels and we therefore believe it to be more secure than our ENIGMA. ENIGMA when used according to instruction is unbreakable. It might be broken if a vast Hollerith complex is used but this is only slightly possible.[70]

After months of interviews, none of the cryptologic POWs could offer any information about SIGABA. They spoke candidly, even proudly, about their successes against British and American ciphers, and why not? Had they broken SIGABA, surely they would have been all the more delighted to regale their captors with their cryptanalytic prowess. Little did they suspect that their own cherished ENIGMA machines had been entirely compromised. Extensive evidence gleaned from the Japanese after the war indicated that they had made even less progress against SIGABA than the Germans had.[71]



The Big Machine That Did

SIGABA, besides merely securing critical information, made possible a major shift in the way America's intelligence organizations conducted their business. Before the summer of 1941, the flow of information from far-flung radio collections sites back to Washington took days to several weeks. The sensitive nature of intercepted data, analysis, and reports necessitated that stringent methods be employed to ensure their confidentiality during transit. Since the United States in the 1920s and 1930s did not have absolute faith in its own cryptographic devices, the services had to rely on physical security to coordinate their classified communications. This meant that messages had to be laboriously typed onto onion-skin paper and then forwarded via costly registered air mail to their destinations.[72] Given the paucity of air service in those days, however, most mail was couriered to awaiting naval ships which carried it back stateside. Army elements stationed in the continental United States relied on couriers as well as the postal system. For those abroad in such places as China, the Philippines, and Panama, the Army process mirrored that of the Navy. As war became imminent, the demand for a rapid, secure means of transmission became paramount, and SIGABAs were distributed to higher priority customers as quickly as they could be produced.

One of the concomitant benefits of secure radio and telegraph communications was the centralization of intelligence activities, which enabled economies of scale and a synergy of efforts. Thus, by late 1942 the sister services were able to streamline the production and dissemination of processed intelligence information. Whether Safford and Wenger had envisioned the new, centralized operational model when they championed the development of SIGABA back in 1935 is not known, but it is consistent with Wenger's overall grand designs for the Navy's radio intelligence function. The Army similarly benefitted from SIGABA's implementation at its central cryptologic facility at Arlington Hall Station near Washington, DC.

SIGABA also supported Allied intelligence and military operations. The most striking example of this was its role in the Battle of the Atlantic. From collection platforms in Britain and at sea, radio signals collected from German U-boats were enciphered by American-operated SIGABAs and routed chiefly by undersea cable to Washington. There, the Navy processed the four-rotor ENIGMA traffic on the cryptoanalytic "bombes" at the Nebraska Avenue station. Hours later, critical, actionable wartime intelligence relating to U-boat operations was again encrypted on SIGABAs and sent back across the Atlantic to Allied forces. While the United States and the United Kingdom enthusiastically shared most of their cryptologic secrets with one another, this did not apply to SIGABA.[73]

The United States for various reasons regarded any information about the SIGABA machine as so sensitive that it did not share any of its principles or details with the British. SIGABAs deployed to British military facilities were operated and stored in secure enclaves to which host-nation personnel were not permitted. Joint U.S.-UK tactical communications in the Pacific Theater were passed along circuits using the Enigma-like British Typex machine; during the latter part of the war the Allies used the CCM to coordinate joint activities. Throughout World War II high-level communications to and from Roosevelt and Churchill passed through SIGABA-based circuits. Messages from Downing Street were forwarded to the American embassy in London where they were encrypted and sent to Washington, DC, where they were rendered into plaintext and directed to the White House.

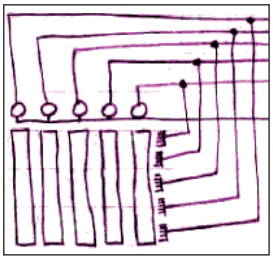
When peace returned in the summer of 1945, more than 16 million Americans were wearing the uniform of their country; two years later those numbers had dwindled to slightly more than 1.5 million, and the nation was awash in surplus military materiel. Cryptographic equipment such as M-209 cipher machines and M-90 devices could be purchased for a nominal sum. Not for sale, however, were the 10,060 SIGABAs which had successfully defied the best efforts of the Axis Powers. Postwar technical analysis of German and Japanese cryptologic capabilities put SIGABA's principles in a perspective that the Americans themselves were only just then coming to appreciate. Studies suggested that SIGABA was so much more technologically advanced than had been thought that its principles needed even more protection after the war than during it.[74] Army and Navy cryptologists were not so much concerned that an adversary might be able to exploit SIGABA if he were privy to its design; rather, their chief concern was that an enemy could use its cryptographic principles to protect his own communications. To this end the sister services promulgated policies that mandated that all SIGABAs be guarded twenty-four hours a day by armed military personnel.[75] This had been the usual practice during the war in overseas locations, and the services did not want a relaxation of security with the return of peace.

Army and Navy cryptographers, still concerned that SIGABA's principles might be compromised, undertook to remove SIGABAs from geographical areas where they might be compromised and replaced them with SIGRODs.[76] SIGROD was a transportable, electromechanical, keyboard-operated cryptographic machine capable of enciphering and deciphering message traffic at the rate of forty to fifty words per minute. It was nearly identical cryptographically to the joint U.S./UK CCM as well as the British Typex machine. Smaller, lighter, and much cheaper to maintain than SIGABA, the five-rotor SIGRODs were capable of processing top secret information and, importantly, if compromised would not disclose the sensitive cryptographic principles embodied in SIGABA.[77] SIGABAs were phased out incrementally and replaced with the less powerful machines. Nevertheless, SIGABAs continued to be used at higher level headquarters for processing the nation's most closely held secrets and were stockpiled in heavily secured facilities against emergency situations when they might be needed again. When the Korean War broke out, SIGABAs were used extensively at higher echelons because of their dependability and high degree of security. For the remainder of the 1950s, the brainchild of Friedman and Rowlett could be found in military higher headquarters and critical message centers around the world.[78] During the course of twenty years, SIGABA had processed millions of classified messages, contributed to the saving of countless lives, shortened the agony of war, and helped to advance the cause of freedom. That it altered the course of history goes unquestioned.

In 1956 a grateful Congress awarded $100,000 to William Friedman for his contribution to SIGABA and for other cryptologic achievements. Two

The SIGABA/ECM II

years later a similar sum was granted to Laurance Safford for his World War II cryptographic work; it would be another eight years before Frank Rowlett received his reward. Then, in something of a bureaucratic parody of itself, the Patent Office on 16 January 2001 granted a patent for SIGABA—some sixty-six years after its conception and thirty-two years after William Friedman's death.



Appendix A: Technical Analysis of SIGABA's Key Space

The SIGABA machine (U.S. Patent 6175625) had five cipher rotors, five control rotors, and five index rotors for a total of fifteen rotors. All fifteen rotors, in banks of five, were encased in a removable module or rotor maze on top of the 100-pound machine. The cipher and control rotors were interchangeable and greatly added to the overall security against a brute force attack. Each rotor had twenty-six contacts on one side wired to twenty-six contacts on the other side. These cipher rotors could be placed in any order in the five slots. They could also be inserted forward facing or reverse. The initial settings for the rotor placement were dictated by a code book, and changed daily.

Adjacent to the bank of five cipher rotors were the five control rotors. Not only were the cipher and control rotors interchangeable, but it took only seconds to rearrange them in a new configuration. In Friedman's own words, "Wheel control unit and cipher wheel unit were identical in design and interchangeable." Even if the enemy had captured the rotors and knew the wirings of each rotor, they still had to exhaust over 10! = 3,628,800 different combinations of cipher/control rotor locations. Furthermore, the enemy would have to determine if each rotor was placed forward or backward. This increased the key space by a factor of 2^{10}, since there were two choices for each of the ten rotors. Also, any of the 26 letters/numbers on the rotors could be "on top" for each of the 10 wheels, giving another 26^{10} possibilities. Configuring the control and cipher rotors in the machine in their correct forward/reverse orientations and the correct letter "on top" positions would take an exhaust of $(2^{10})(10!)(26^{10}) \approx 5.2 \times 10^{23}$ for their initial settings. SIGABA code clerks and operators used key charts published monthly to determine the wheels' forward/reverse orientation, placement position in the rotor maze, and the "on top" settings of each rotor for each message.

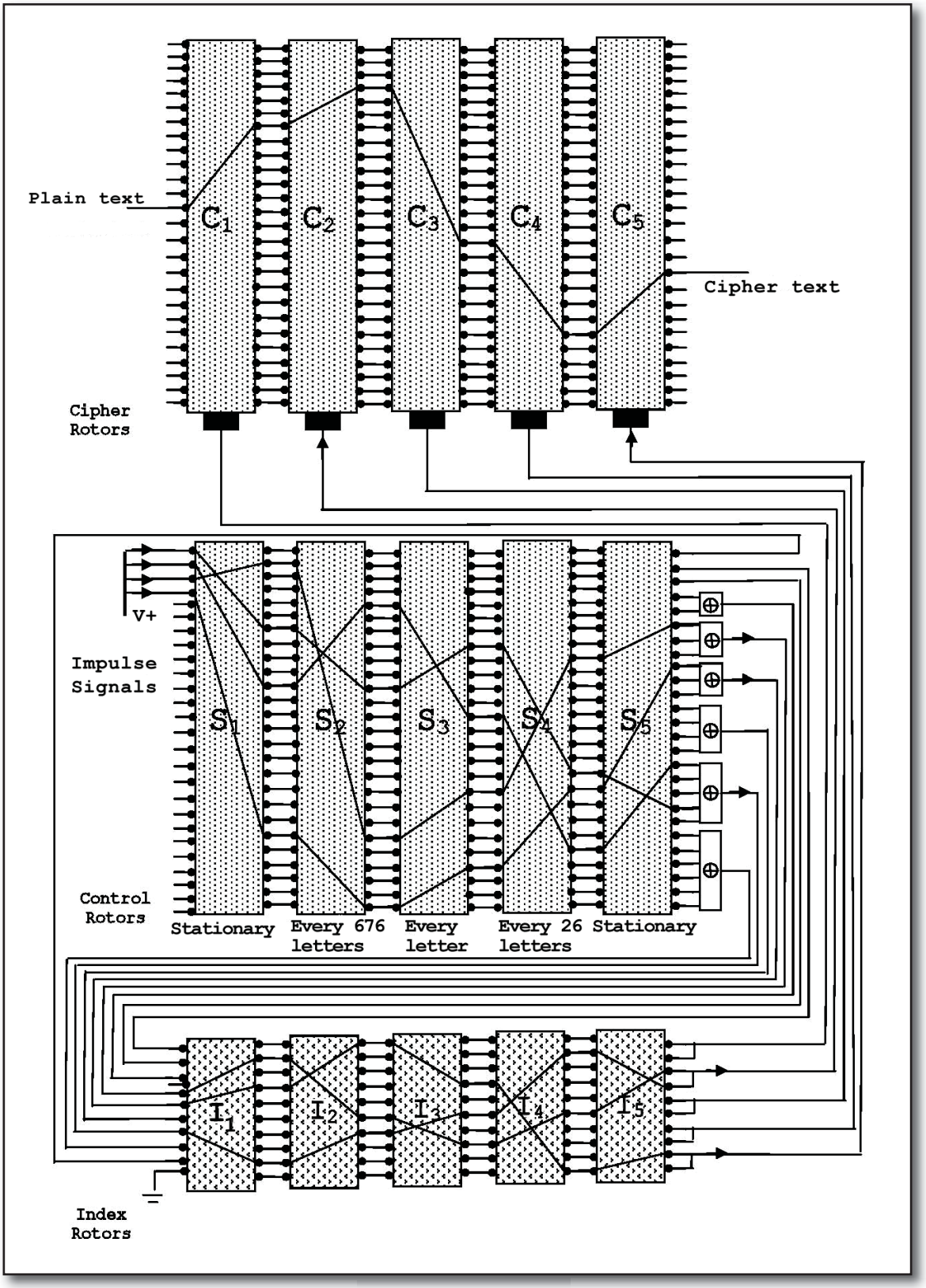
The third bank of cryptographic wheels contained in the rotor maze was the five index rotors which sat next to the control rotors and was the closest to the keyboard. The index rotors were smaller than the other rotors and had only ten contacts on each side. Unlike the other ten rotors, the index rotors did not "rotate/advance" during operation but were set daily to initial values dictated by the published key chart. While it was physically possible to insert these rotors in either the forward or reverse position, the index rotors were placed forward throughout World War II. Like the other rotors, each index rotor could be placed in any of the five slots in the index rotor bank. This capability afforded an exhaust of 5! = 120 to find the correct index rotor permutation. From June 1945 onward, however, the index rotor configuration did not change, and the setting for

each index rotor was provided by the daily key list. An enemy without knowledge of how it was implemented would have to consider reversals (another factor of 2^5) and which value was "on top" (another factor of 10^5). Therefore, finding the correct setting for each of the fifteen rotors would take $(2^{10})(10!)(26^{10})(5!)(2^5)(10^5) \approx 2.0 \times 10^{32}$ attempts, which is approximately $2^{107.3}$ possible key combinations. Once the index rotors were no longer permuted daily in 1945, this dropped to $(2^{10})(10!)(26^{10})(2^5)(10^5) \approx 1.7 \times 10^{30}$, which is $2^{100.4}$ trial decryptions. This was surprisingly good by the modern Advanced Encryption Standard (2^{128}, 2^{192}, or 2^{256}) and Data Encryption Standard (2^{56}) key sizes.

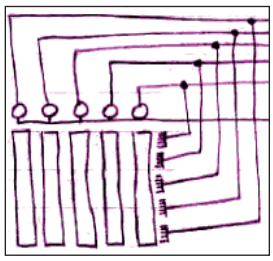
Of course, as long as the enemy did not recover the machine, the wirings in each rotor added to the security. For each of the ten cipher and control rotors there were 26! theoretical ways for them to be wired. A large number of these wirings would have been avoided since it does not seem random to have rotors that mapped A → B, B → C, C → D, etc. But these "nonrandom" wirings should be included in the theoretical possibilities, since they are valid wiring combinations. If an enemy did not know any of the rotors' wiring, there would be 26! possibilities for each of the 10 and 10! possibilities for each of the 5. So the total number of configurations for the system would be $(26!)^{10}(10!)^5 \approx 2^{992.8}$. One need not count rotor reversed orientation settings or consider which value is "on top," because such changes are already represented by one of the wirings considered. Some wirings would produce identical encryptions, but the effect on the already massive key space is minimal.

Even with this enormous theoretical key space, the Army and Navy took no chances when they suspected (later proved false) a physical compromise of SIGABA in the last months of the war in Europe. In a surge effort, the services produced an entirely new set of fifteen rotors for each of the 10,060 machines in the inventory. In retrospect, given the state of Axis cryptologic prowess, this was not warranted. All the same, General Eisenhower, who personally ordered the fielding of the new rotors, was not willing to imperil the success of military operations or the lives of his troops. Thus, at the war's end, each SIGABA was equipped with two sets of rotors.

The SIGABA's wiring scheme is provided on the next page.



SIGABA wiring scheme



Appendix B: The Mechanics of SIGABA

Refer to the wiring diagram in Appendix A for more information about SIGABA's cryptographic wiring.

The SIGABA machine works in a relatively simple manner. Four input signals are activated with each keystroke. These four signals go through the five control rotors. These rotors (see SIGABA wiring scheme on previous page) are designated as S_1 through S_5 in the diagram. After each keystroke, the center, or third, control rotor (S_3) will step forward one letter. After every twenty-six keystrokes, both the third (S_3) and the fourth (S_4) control rotor will step. After every 676 keystrokes, the second (S_2), third (S_3), and fourth (S_4) rotors will step. The first (S_1) and fifth (S_5) rotors are stationary. This ensures that the impulse signals from every keystroke are scrambled in a different fashion. Rotors S_3, S_4, and S_2 comprise a 17,576-long counter. That is, after S_3 does a full cycle, rotor S_4 steps. Then, after S_4 finishes a full cycle (and S_3 has completed twenty-six full cycles), rotor S_2 will step. By the time S_2 has gone through its full cycle, the whole machine has enciphered 17,576 letters, which is only $2^{14.1}$, making this the "cycle length" for the control rotor scrambling maze. After 17,576 enciphered letters, the machine will start over, essentially reusing the same scrambling system. This was why the rotor placements had to be changed daily.

The fact that each message used a different message indicator (initial setting) meant that each message for that day would start in a different place along the scrambling maze. While reusing the scrambling maze does not mean the enemy could immediately read the messages, it did weaken the cipher system. Certainly, overuse of the high-level SIGABA system could have led to German or Japanese cryptanalytic capabilities against SIGABA, but the Americans avoided this by relying on the tactical Hagelin machines to conduct much of their chatter. Furthermore, to conduct an exhaustive attack against the SIGABA machine would take $2^{48.4}$ trial decryptions to get the rotors in the right order. Overuse would weaken the encryption system, not break it.

The twenty-six outputs from the control rotors are bundled together into nine different input signals that are then connected to the index rotor bank. At most, there could be four live wires going into the index rotors. At the minimum, there could be a single live wire. In the diagram pictured in Appendix A, there are three live wires going from the control rotor bank to the index rotor bank.

The index rotors, denoted I_1 through I_5, further scramble the inputs from the control rotors. Once the signals travel through the five index rotors, they are bundled by adjacent pairs into five wires that connect to each one of the five cipher rotors. If the wire com-

ing from the index rotor bank is live, then the cipher rotor it is connected to will step forward one letter. Otherwise, it will not move. For each keystroke, there can be between one and four live wires coming from the index rotor bank and going into the cipher rotor bank. In the diagram, there are exactly two wires that are active: wire number two and wire number five. This means that both the second (C_2) and fifth (C_5) cipher rotor will step, but the other three will remain stationary for this particular keystroke.

Each letter of the message travels through only the five cipher rotors, C_1 through C_5 in the diagram. The control rotors and index rotors exist only to dictate the stepping of the five cipher rotors. The plaintext letter from the keyboard travels via wire to the left-hand side of the cipher rotor bank. The signal wire is then scrambled through the five cipher rotors and emerges on the other side of the cipher rotor bank as an encrypted letter. The cipher text is then printed on a small tape. The decryption process simply works in reverse.

Five pages from the SIGABA user's manual *Crypto-Operating Instructions for Converter M-134-C*

SECTION II

GENERAL DESCRIPTION

5. Description and Use.—Converter M–134–C is an electromechanical, transportable, cipher machine to be used in permanent and mobile cryptocenters (code rooms)* for the purpose of automatically enciphering and deciphering messages, both tactical and administrative, with speed, accuracy, and security.

6. Component Parts.

a. Keyboard.—The keyboard resembles a typewriter keyboard and should be operated at a maximum speed of 45 to 50 words per minute (40 words per minute if operated in tandem); if this speed is exceeded, characters may fail to print.

b. Cipher Unit.

(1) The cipher unit (short title: SIGIVI) consists of six bakelite separators which form a support for three rotor shafts. The unit supports the index, stepping control (control), and alphabet (cipher) rotors in such relative positions that electrical circuits are formed through each row of rotors.

(2) The five small rotors in the front row are called the index rotors. The index rotors can be moved manually only.

(3) The five rotors in the middle row are known as the stepping control (control) rotors. The two end stepping control rotors remain stationary during encipherment and decipherment.

(4) The five rotors in the rear row are known as the alphabet (cipher) rotors. All five alphabet rotors step in an irregular manner during encipherment and decipherment.

c. Printer Unit.—The printer unit is a tape printer which automatically spaces the cipher text into groups of five letters in enciphering and in the deciphering process, it spaces the deciphered text into word lengths. There is also provision for printing plain text directly by keyboard operation.

d. Controller.—The positions of the controller and their effect on the operation of the converter are as follows:

(1) *Off Position* ("O").—The power supply line is open and no current is supplied to the converter.

*Certain new terms are used throughout this document. In each instance where a new term is used for the first time, it is followed by the old term in parentheses.

5

(2) *Plain-text Position* ("P").—All keys of the keyboard and the space bar can be operated, and the converter will print plain, unenciphered text exactly as typed. The rotors remain motionless during typing.

(3) *Reset Position* ("R").—Only the numeral keys 1 to 5, inclusive, and the "Blank" and "Repeat" keys can be operated. The rotors may be zeroized with the controller in this position and the zeroize-operate key in the "Zeroize" position. (See paragraph 10*b*.) The tape will not feed while the controller is at "R." When the controller is moved to or through the "R" position, the tape may advance as many as five spaces. This is caused by the tape feed ratchet resetting so that printing will begin on the first letter of a five-letter cipher group.

(4) *Encipher Position* ("E").—The alphabet, "Blank," and "Repeat" keys and the space bar can be operated. Numeral and "Dash" keys cannot be operated. The converter enciphers the letters struck on the keyboard and prints the resulting cipher text.

(5) *Decipher Position* ("D").—The alphabet, "Blank," and "Repeat" keys can be operated. Numeral and "Dash" keys and the space bar cannot be operated. The converter deciphers the letters struck on the keyboard and prints the resulting plain text.

e. For a more detailed explanation of component parts of the converter, consult the maintenance instructions for Converter M–134–C.

7. Classification of Parts.

a. The converter, exclusive of rotors, is classified CONFIDENTIAL.

b. The cipher unit, exclusive of rotors, is classified CONFIDENTIAL.

c. The index rotors are classified CONFIDENTIAL.

d. The alphabet and stepping control rotors are classified SECRET.

SECTION III

KEYING INSTRUCTIONS

8. Keying Elements.—Converter M–134–C employs two keying elements:

a. The *daily keying element* consists of the daily rotor arrangement (assembly) and the alignment of the index rotors. The alignment of the index rotors is different for each security classification.

b. The *message keying element* consists of the alignment of the stepping control and alphabet rotors used at the beginning of the encipherment or decipherment of a message.

9. Rotor Arrangement and Alignment of Index Rotors.

a. Each converter is provided with five small rotors to be used in the index (front) position and ten large rotors to be used in the stepping control (middle) and alphabet (rear) positions.

(1) *Index Rotors.*—Each of the index rotors bears a sequence of 2-digit numbers: one rotor is marked with the sequence 10 to 19 inclusive; another, the sequence 20 to 29 inclusive, etc. The complete set of five index rotors is numbered from 10 to 59 inclusive. The index rotors are always used in a fixed order in the five rotor positions (10–19, 20–29, 30–39, etc.).

(2) *Stepping Control or Alphabet Rotors.*—Each of the stepping control or alphabet rotors bears an identifying number, usually opposite the letter "O." Most sets of rotors will, in addition to the numbers, bear an identifying letter or letters, usually associated with the identifying number. A set of ten rotors is numbered from 1 to 10 inclusive, 11 to 20 inclusive, or 21 to 30, etc. These rotors are all interchangeable and reversible within any set of ten.

b. Rotors are inserted and aligned according to instructions published in a key list which is included in each edition of a Converter M–134–C system.* A sample extract from a key list is shown below.

DAY OF MONTH	ROTOR ARRANGEMENT (FOR ALL CLASSIFICATIONS)		SECRET	
	STEPPING CONTROL (MIDDLE)	ALPHABET (REAR)	INDEX (FRONT) ALIGNMENT	26–30 CHECK GROUP
1	ØR 4 6 2R 7	1 8 5 9 3R	1Ø 23 31 49 5Ø	R N H V C
2	2 3R 9R 1 5	6 4R 8 7 Ø	14 25 33 46 59	S E M N O

*If old-style key lists are still effective after the effective date of this document, ignore the columns headed "INITIAL ALIGNMENT (CONTROL AND CIPHER)."

DAY OF MONTH	CONFIDENTIAL										RESTRICTED									
	INDEX (FRONT) ALIGNMENT					26–30 CHECK GROUP					INDEX (FRONT) ALIGNMENT					26–30 CHECK GROUP				
1	12	28	31	44	53	P	W	V	M	T	17	25	36	43	58	M	C	S	D	T
2	15	2Ø	32	48	56	E	H	E	W	B	1Ø	27	34	42	56	R	S	T	H	H

c. The Key List.—The key list contains the arrangement of the stepping control and alphabet rotors for each day of the month and the alignments of the index rotors for each of the several security classifications for every day of the month. The arrangement of the stepping control and alphabet rotors remains the same throughout the cryptographic period for all security classifications. The alignment of the index rotors differs for each security classification.

(1) *Arrangement of Rotors.*—Figures in the column marked ROTOR ARRANGEMENT (FOR ALL CLASSIFICATIONS) specify which stepping control and alphabet rotors are to be used on a specific day of the month and the positions of these rotors in the converter. Numbers in the table refer to the second digit of the rotor number. A set of rotors bearing the numbers 21 to 30 inclusive, for example, will be regarded as being marked 1, 2, 3, ... 0. "R" in the table indicates that the rotor so designated is to be inserted in the reversed position, i. e., the characters on the periphery will appear upside down to the operator. The rotors will be inserted in their respective positions in order, from left to right as the operator faces the converter. Example: On the second day of the month, the sample extract from a key list in paragraph 9*b* designates 2–3R–9R–1–5 for the stepping control rotors and 6–4R–8–7–Ø for the alphabet rotors. Rotors marked 2, 3, 9, 1 and 5 (disregarding the tens digits) will be inserted in the control position in that order, from left to right as the operator faces the converter, with rotors number 3 and 9 reversed. The remaining five rotors marked 6, 4, 8, 7 and Ø, will be inserted in the alphabet position in that order from left to right with rotor number 4 reversed.

CAUTION: Do not touch rotor contacts when arranging the rotors.

(2) *Alignment of Index Rotors.*—The sets of numbers under INDEX (FRONT) ALIGNMENT designate the alignment of the index rotors used for enciphering and deciphering messages on a specific day of the month. In three separate columns, each headed INDEX (FRONT) ALIGNMENT, the key list gives the daily alignment of the index rotors for each classification. The alignment of the index rotors is determined by the classification of the message and the day of the month. Example: According to the key list above, on the first day of the month the numbers of the index rotors should be aligned from left to right on the white reference mark at 1Ø 23 31 49 5Ø for SECRET messages; at 12 28 31 44 53 for CONFIDENTIAL messages; and at 17 25 36 43 58 for RESTRICTED messages.

10. Alignment of Stepping Control and Alphabet Rotors.—The alignment of the stepping control and alphabet rotors at the beginning of encipherment or decipherment of a message constitutes the message keying element. The letters to which the stepping

control and alphabet rotors are aligned constitute the message rotor alignment (internal message indicator). The message rotor alignment is derived and aligned on the stepping control and alphabet rotors in the following manner:

a. Select a group of any five letters *at random* (message indicator). All 26 letters of the alphabet, including the letters "O" and "Z," may be selected. Letters of the alphabet in proximity to the letter "O," i. e., P, Q, R, or L, M, N, will not be *deliberately or consistently* selected in the message indicator merely to reduce the number of steps required to align the letters of the message indicator on the stepping control rotors as explained below. Bona-fide words must not be used except as they occur by chance.

b. Zeroize the converter. This is accomplished by switching the zeroize-operate key to "zeroize," turning the controller to "R," and then pressing down the "Blank" and "Repeat" keys simultaneously until the letter "O" on the stepping control and alphabet rotors comes to rest at the reference mark.

c. Leave the controller at "R" and switch the zeroize-operate key to "Operate."

d. Strike the numeral "1" key the number of times required to align the first stepping control rotor (next to the left end plate) to the first letter of the message indicator. The first stepping control rotor will step one letter each time the "1" key is depressed.

e. Align the second stepping control rotor by striking the numeral "2" key, the third by striking the numeral "3" key, etc., until all five stepping control rotors are aligned to the five letters of the message indicator. With each step of the stepping control rotors, the alphabet rotors will step in an irregular manner.

NOTE: If the letter "O" is to be aligned on any of the five stepping control rotors, it will be necessary to step that rotor *26 times* when setting up the message indicator.

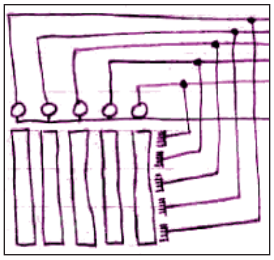
f. If any rotor is stepped past the correct letter or if the rotors are not aligned in proper sequence, the entire process must be repeated from the zeroize position (subparagraph 10*b*). Do not use the "Repeat" key with the numeral keys in aligning the message indicator and avoid a sharp, quick touch of the numeral keys. It is possible to press the numeral keys and release them too quickly so that the stepping control rotors will step but the alphabet rotors will not, thus resulting in an incorrect alignment.

g. After the stepping control rotors have been aligned, check the alignment of the alphabet rotors to insure that *all* five are not aligned to the letter "O." The alphabet rotors should step in an irregular manner while the stepping control rotors are being aligned. If for any reason all of the alphabet rotors do not step, they will remain aligned to the letter "O." This is an indication that the converter is not functioning properly or that the procedure outlined herein has not been followed correctly.

11. The 26–30 Check.

a. The 26–30 check groups provided in the key list are used to check the correctness of the daily rotor arrangement and index alignment and the stepping of the stepping control and alphabet rotors. The 26–30 check is performed as follows:

(1) Arrange the stepping control and alphabet rotors and align the index rotors in accordance with the key list and security classification to be checked.



Notes

1. David Kahn, *The Codebreakers: The Story of Secret Writing*. New York: MacMillan, 1967, 235.
2. Kahn, *Codebreakers*, 415.
3. Jack Levine, *United States Cryptographic Patents, 1861-1989* (Terre Haute, IN: *Cryptologia*, 1991), 85.
4. Frank B. Rowlett, *The Story of Magic: Memoirs of an American Cryptologic Pioneer* (Laguna Hills, CA: Aegean Park Press, 1998), 69. Also Captain Laurance Safford, United States Navy OP-20-S-5, *History of Invention and Development of the Mark II ECM,* SRH-360, 19-21 (National Archives and Records Administration [NARA]: RG 457, box 1124).
5. Army Security Agency, *History of Converter M-134-C*, Vol. 1, or *SRH-359* (Washington, DC: Army Security Agency, n.d.), 18.
6. Ibid., 51-60.
7. Friedman Collection, NSA/CSS Archives accession #47270, box 14, folder 1.
8. Ibid.
9. Levine, *United States Cryptographic Patents,* 115.
10. Friedman Collection, 1920-1960, NSA/CSS Archives accession #47270, box 14, folders 1-2.
11. Ibid., folder 1.
12. Ibid.
13. Ibid.
14. Ibid.
15. Frank B. Rowlett, Oral History Interview 1974, OH-1974-01, Part B, 45c, Ft. Meade, MD: Center for Cryptologic History (CCH).
16. Ibid., 45c-45d.
17. Ibid., 38.
18. Ibid., 39.
19. Ibid., 39j.
20. Ibid., 40.
21. Ibid., 39-40.
22. Ibid., 40; Rowlett, *Story of Magic*, 97.
23. Rowlett, Oral History Interview 1974, OH-1974-01, 40, Ft. Meade, MD: Center for Cryptologic History.
24. Ibid.; Rowlett, *Story of Magic*, 97-98.
25. Heather Ellie Kwong, thesis: *Cryptanalysis of the SIGABA Cipher*, San Jose State University, 2008.
26. http://www.sccs.swarthmore.edu/users/08/ajb/tmve/wiki100k/docs/SIGABA.html.
27. Laurance Safford, *History of Invention and Development of the Mark II ECM*, SRH-360, NARA RG 457, Box 1124. The ECM Mark I was the Navy's primary cipher machine from May 1936 to January 1942. It was also the Navy's first attempt at an "in-house" cipher machine. In spite of ECM Mark I's formidable cryptographic strength, the Navy remained uneasy about its vulnerability to exploitation. The Mark I arguably was the most powerful cryptologic device extant, but at the time the cryptographers at OP-20-G had little appreciation of this fact. The ECM Mark I embodied elements of contemporary Hebern machines and then was heavily modified by Donald Seiler and Laurance Safford. These novel cryptographic enhancements placed the Mark I in a league of its own, well above the Hebern machine. Seiler also went on to perform much valuable engineering work on the ECM Mark II's development. According to Safford, the Mark I was beset with

numerous mechanical deficiencies that required almost constant maintenance to keep it operational. This fact alone was probably the largest, immediate driving factor in the Navy's quest for a new machine. When he returned from sea duty and was briefed by Wenger on his interview with Friedman and Rowlett, Safford readily embraced the SIGABA principles and pressed for its development.

28. Rowlett, Oral History Interview, 1974, OH-1974-01, 41, Ft. Meade, MD: Center for Cryptologic History.
29. Ibid.
30. Safford, *History of Invention and Development of the Mark II ECM,* 24-25, 29.
31. Rowlett, Oral History Interview 1974, OH-1974-01, 45n, Ft. Meade, MD: Center for Cryptologic History; Army Security Agency, *History of Converter M-134-C*, vol. 1, SRH-359, Washington, DC: Army Security Agency, n.d., 139.
32. Rowlett, *Story of Magic*, 143.
33. Army Security Agency, *History of Converter M-134-C*, 138-139; Rowlett, *Story of Magic*, 143.
34. Rowlett, *Story of Magic*, 143-144.
35. Ibid., 144.
36. Rowlett, Oral History Interview 1974, OH-1974-01, 46, Ft. Meade, MD: Center for Cryptologic History.
37. On 1 August 1941 the sister services formally adopted the SIGABA/ECM II as their joint cipher machine. Each agreed not to share any information whatever about the machine to any outside person or organization.
38. Rowlett, Oral History Interview 1974, OH-1974-01, 46, Ft. Meade, MD: Center for Cryptologic History.
39. Ibid., 47. The Navy's Donald Seiler had given due consideration to plugboards and rejected them in favor of the index rotor wheels even before the first ECM Mark II had reached the blueprint stage. Safford, *History of Invention and Development of the Mark II ECM,* 39. Safford, Chief OP-20-G, relates that besides being inconvenient to the user, plugboards in the past had not prevented the initial solutions of six different cipher machines the Navy had tested. He also eschewed them because user errors in plugging had directly led to compromise of the key, not to mention the effect on the reliability of communications. The Navy's greatest argument in favor of rotors over plugboards was that rotors offered 49 times more stepping combinations than the latter (SRH 360, 28). German and American cryptographers independently of each other conceived of using plugboards as enhancements to their respective cipher machines.
40. Rowlett, Oral History Interview 1974, OH-1974-01, 45, Center for Cryptologic History, Ft. Meade, MD.
41. Ibid., 46.
42. Safford, *History of Invention and Development of the Mark II ECM,* 40; The Navy deemed the thermite emergency destruction devices too dangerous to use aboard ships where fire is the greatest threat. Navy tests of thermite bombs reduced the ECM's critical components to molten metal in 97 seconds. Safford, *History of Invention and Development of the Mark II ECM,* 61. This notwithstanding, the Army had few qualms about fielding both thermite and TNT charges atop SIGABA's 800 lb. security cabinets aboard tactical communications vehicles. There is no record of an unintended mishap associated with these devices; even so, the Navy's concerns were partly vindicated by more than one Army incident of a near discharge.
43. Safford, *History of Invention and Development of the Mark II ECM*, 42; 37-52 passim.
44. Ibid., 6; the ECM Mark I, despite the Navy's reservations about it, was still more powerful than any cipher device fielded by either the British or the Axis Powers.
45. Ibid., 6-8.
46. Ibid.
47. Ibid.
48. Ibid.
49. Ibid.
50. Safford, *History of Invention and Development of the Mark II ECM*, 54.
51. Ibid., 55-56.
52. R. A. Ratcliff, *Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers* (New York:

Cambridge University Press, 2006), 81. Also Safford, *History of Invention and Development of the Mark II ECM*, 52.

53. Army Security Agency, *History of Converter M-134-C*, 7.
54. Ibid., 147-158, 247-248.
55. The Navy generated its SIGABA key at the Nebraska Avenue Naval Station where it operated its ECM Mark II maintenance facility. Army cryptographers produced SIGABA keys at Arlington Hall. Later in the war, the Army moved its SIGABA maintenance and training functions to Vint Hill Farms near Warrenton, VA.
56. Safford, *History of Invention and Development of the Mark II ECM*, 31.
57. Ratcliff, *Delusions of Intelligence*, 105, 164, 168, 177. By the war's end, more than 8,000 SIGABAs had the capability to interoperate with the British Typex machine.
58. J. G. Seabourne, *The Signal Intelligence Service of the German Luftwaffe*, vol. 13. November 24, 1945 (National Archives and Records Administration: RG 457, box 976). The Navy's anxiety about its own ECM Mark I led Wenger to approach Friedman about the Army's cryptographic research—Rowlett, Oral History Interview 1974, OH-1974-01, 45m—in the first place. The sister services' continued development of, and their absolutely rigorous application of, COMSEC doctrine demonstrate their concern over enemy attempts to break into U.S. crypto systems.
59. JN-A-20 messages, 1942 (National Archives and Records Administration: RG 457, box 1006, temporary folder).
60. Ibid.; Ratcliff, *Delusions of Intelligence*, 201-203.
61. Rowlett, Oral History Interview 1974, OH-1974-01, 105.
62. Ratcliff, *Delusions of Intelligence*, 202. Several different German cryptologic organizations named SIGABA as the "Big Machine."
63. Rowlett, Oral History Interview 1974, OH-1974-01, 158-159.
64. Seabourne, *Signal Intelligence Service*. Also see report: *European Axis Signal Intelligence in World War II as Revealed by "TICOM" Investigations and Other Prisoner of War Interrogations and Captured Material, Principally German*, vol. 5, The German Air Force Signal Intelligence Service. Army Security Agency, 10 October 1946.
65. *War Diary of the Signal Intelligence Group*, February–November 1944 (NSA/CSS Archives, accession #5411, box G22-0303-3), 64.
66. Ibid.
67. Erich Huttenhain, interview, 10 July 1945 (NARA: RG 457, box 1006).
68. Ibid.
69. Ibid.
70. Ibid.
71. Ibid. *The Japanese Signal Intelligence Service*, 17 October 1952 (NARA: RG 457, box 1129).
72. Ratcliff, *Delusions of Intelligence*, 178; Pre-War Radio Intelligence Activities in the Philippines, 63, CCH Files; Timothy Mucklow, *Federal History Journal*, 2011, 59.
73. *Army-Navy Joint Policy Concerning Distribution and Disclosure of Cryptographic Design of the ECM-M134C*, 26 June 1942; Safford, *History of Invention and Development of the Mark II ECM*, 57-58.
74. Safford, *History of Invention and Development of the Mark II ECM*, 110-111, 115-116; Ratcliff, *Delusions of Intelligence*, 168.
75. Letter, Col. George A. Bircher, SC, to CG, AAF, Washington, DC, Attn: Ch, Sec, Air Communications Office, 9 May 46, sub: Policy on Storage of Converter M-134-C:

    . . . 2. This Agency does not consider that the cessation of hostilities justifies any relaxation in security regulations pertaining to cryptographic material and has noted with alarm a tendency towards such relaxation during recent months as has been evidenced by an increase in the number of physical and cryptographic compromises.

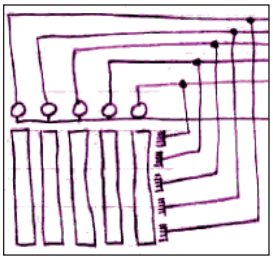
    3. Since the cryptographic principle and design of Converter M-134-C is in the sole possession of the United States and it is considered to be the best cryptographic device of its type, it is not advisable to jeopardize its use or storage under unsatisfac-

> tory security conditions. It is considered that eliminating the necessity for a 24-hour armed guard, regardless of geographical location, even if the converter were stored in a CH-76 in a locked code room, would result in such a condition, and that no justification exists for undergoing such a risk. . . .

Ratcliff, *Delusions of Intelligence*, 168.

76. *History of Converter M-134-C*, 5 May 1950, included in the CCH copy of SRH 360, 1-10.
77. Ibid., 7; Extracts: Annual Report, Security Division, CSAS-80, Fiscal Year 1948 (included in CCH copy of SRH 360), 1-5; Excerpt: Tab A10, "Staff Study Concerning the Issue of SIGROD Machines to all Military Attachés," Annual Report, Sec Div, Tech Staff, FY 48 (23 April 1947) 1948 (included in CCH copy of SRH 360), 1-4; Extract: Tab A7, "Staff Study on the Introduction of the SIGROD," Annual Report, Security Division, Technical Staff, FY 48 (3 February 1950), 19 (included in CCH copy of SRH 360).
78. Until recently, cryptologic historians were under the impression that the end for SIGABA came not because of any cryptographic weakness but because it simply could not keep pace with modern high-speed telecommunications. Research based on newly acquired information suggests that SIGABA was taken out of the inventory to keep the advanced technology out of the hands of the Soviets. Because every SIGABA and rotor had been accounted for and because Army and Navy cryptologists had much confidence in the integrity of SIGABA principles, they were confident that SIGABA's secrets could be retained; *History of Converter M-134-C*, 5 May 1950 included in CCH copy of SRH 360, 7-10 (included in CCH copy of SRH 360).

SIGABA and its temporary successor SIGROD were slowly replaced in the 1950s by the TSEC/KL-7 (ADONIS/POLLUX). The new cipher machine was an electronic-mechanical hybrid that employed a programmable cipher rotors/bezel assembly (eight rotors/thirty-six pins), cams, and vacuum tube technology along with a novel re-flexing principle. It was phased out of the U.S. military inventory in the early 1980s.



Selected Bibliography

Published

Budiansky, Stephen. *Battle of Wits: The Complete Story of Codebreaking in World War II*. New York: The Free Press, 2000.

Chan, Wing On. "Cryptanalysis of SIGABA." Master's thesis, San Jose State University, 2007. http://cs.sjsu.edu/faculty/stamp/students/Sigaba298report.pdf.

Clark, Ronald William. *The Man Who Broke PURPLE: The Life of the World's Greatest Cryptologist, Colonel William F. Friedman*. Boston: Little, Brown, 1977.

Kahn, David. *The Codebreakers: The Story of Secret Writing*. New York: MacMillan, 1967.

Kwong, Heather Ellie. "Cryptanalysis of the SIGABA Cipher." Master's thesis: San Jose State University, 2008.

Lee, Michael. "Cryptanalysis of the SIGABA." Master's thesis, University of California, Santa Barbara, 2003. http://ucsb.curby.net/broadcast/thesis/thesis.pdf.

Levine, Jack. *United States Cryptographic Patents, 1861-1989*. Terre Haute, IN: *Cryptologia*, 1991.

Mucklow, Timothy and LeeAnn Tallman. "SIGABA/ECM II: A Beautiful Idea." *Cryptologic Quarterly*, 30 (2011): 3-25.

Pekelney, Rich. "Electronic Cipher Machine (ECM) Mark II," San Francisco: USS *Pampanito*, San Francisco Maritime National Park Association, July 2008. http://www.maritime.org/ecm2.htm.

Ratcliff, R. A. *Delusions of Intelligence: ENIGMA, Ultra, and the End of Secure Ciphers*. New York: Cambridge University Press, 2006.

Rowlett, Frank B. *The Story of Magic: Memoirs of an American Cryptologic Pioneer.* Laguna Hills, CA: Aegean Park Press, 1998.

Savard, J.J.G. and R. S. Pekelney. "The ECM Mark II: Design, History and Cryptology." *Cryptologia*, 23, no. 3 (1999): 211-228.

Stinson, Douglas R. *Cryptography: Theory and Practice*, 3rd ed. Boca Raton, FL: Taylor & Francis Group, 2006.

Tucker, Alan. *Applied Combinatorics*, 4th ed. Singapore: Wiley, n.d.

Werner, Herbert A. *Iron Coffins: A Personal Account of the German U-Boat Battles of World War II*. New York: Holt, Rinehart and Winston, 1969.

From the Center for Cryptologic History and National Security Agency/ Central Security Service Archives

SRH = Special Research Histories

SRMN = U.S. Navy Discrete Records of Historical Cryptologic Import

Army Security Agency. *History of Converter M-134-C*, vol. 1, *SRH-359*. Washington, DC: Army Security Agency, n.d.

Cryptographic Security Section. *HCM (Hebern Cipher Machine) Cipher No. 21*, SRMN-063. Washington, DC: Navy Department, Office of Chief of Naval Operations, 25 August 1935.

"Crypto-Operating Instructions for M-134-C," or "SIGQZF-3," November 1946. NSA/CSS Archives, accession #13943, box H18-0506-6.

Friedman Collection, 1920-1960, NSA/CSS Archives, accession #47270, boxes 1-15.

Friedman, Elizebeth. Oral History Interview #OH-1973, Center for Cryptologic History, May 16-17, 1973.

The Friedman Legacy: A Tribute to William and Elizebeth Friedman, 3rd ed. Ft. Meade, MD: Center for Cryptologic History, National Security Agency, 2006.

Friedman, William. *Elementary Course in Cryptanalysis,* SRH-214. Washington, DC: Army Security Agency, 1930.

———. *Elementary Course in Cryptanalysis*, SRH-216. Washington, DC: Army Security Agency, 1940.

———. *Elementary Course in Cryptanalysis*, SRH-218. Washington DC: Army Security Agency, 1946.

———. *Expansion of the Signal Intelligence Service from 1930 to 7 December 1941*, SRH-134. Washington, DC: Army Security Agency, 4 December 1945.

Friedman, William and Lambros Callimahos. *Military Cryptanalytics*, Part I & II. Washington, DC: National Security Agency, 1956.

Hurt, John B. *A Version of the Japanese Problem in the Signal Intelligence Service (Later Signal Security Agency) 1930-1945*, SRH-252. Washington, DC: Army Security Agency, n.d.

Miller, A. Ray. *The Cryptographic Mathematics of ENIGMA*. Ft. Meade, MD: Center for Cryptologic History, National Security Agency, 2006.

Mowry, David. "William F. Friedman" (Ft. Meade, MD: Center for Cryptologic History, National Security Agency, 2002).

Photographic Equipment – IBM Sigaba Unit manual, n.d. (NSA/CSS Archives Accession #41220, Box G03-0701-6).

Reeder, William. Center for Cryptologic History, biography files.

Rowlett, Frank B. Oral history interviews #OH-1974-01 through OH-1974-12. Center for Cryptologic History, 1974.

Safford, Captain Laurance. Officer Biographies, n.d. (NSA/CSS Archives Accession #47403, Box H16-0203-3).

———. *History of Invention and Development of the Mark II ECM*, SRH-360. Washington, DC: United States Navy OP-20-S-5, Office of the Chief of Naval Operations, 30 October 1943.

———. Center for Cryptologic History, biography files.

Small, Albert W. Arlington Hall Station, "Letter to Lieutenant Colonel Charles G. Renfre, Armed Forces Security Agency," 12 October 1950. NSA/CSS Archives accession #5515, box #G22-0303-3, folder #19.

War Department. "Converter M-209, M-209-A, M-209-B, Technical Manual." Washington, DC, 17 March 1944. Reprint. Washington, DC: National Cryptologic Museum.

"War Diary of the Signal Intelligence Group," February–November 1944. NSA/CSS Archives, accession #5411, box G22-0303-3.

Wilcox, Jennifer. *Sharing the Burden: Women in Cryptology during World War II*. Ft. Meade, MD: Center for Cryptologic History, National Security Agency, 1998.

———. *Solving the ENIGMA: History of the Cryptanalytic Bombe.* Ft. Meade, MD: Center for Cryptologic History, National Security Agency, 2006.

From the National Archives and Records Administration, College Park, MD

"CRYPTOSYSTEMS 742 (SIGFKE) & 604 (SIGFHK)," April 12, 1948. NSA/CSS Archives accession #13943, box H18-0506-5.

Friedman, William F. "Analysis of a Mechanico-Electrical Cryptograph," 1934-1935. RG 457, box 745.

Huttenhain, Erich. Interview, 10 July 1945. RG 457, box 1006.

"The Japanese Signal Intelligence Service," 17 October 1952. RG 457, box 1129.

JN-A-20 messages, January 24, 1942. RG 457, box 1006, temporary folder.

Muentz, Lieutenant D. R. Interview, 10 July 1945. RG 457, box 1006.

Rentschler, R. R. Interview, 10 July 1945. RG 457, box 1006.

Rosen, Leo. *M-134-C*. RG 457, box 1124.

Safford, Laurance. United States Navy OP-20-S-5, *History of Invention and Development of the Mark II ECM*, SRH-360. RG 457, box 1124.

Seabourne, J. G. "The Signal Intelligence Service of the German Luftwaffe," vol. 13. November 24, 1945. RG 457, box 976. The Seabourne Report is named after Colonel J. G. Seabourne, the project leader.

Related Publications

The Cryptographic Mathematics of ENIGMA

The Friedman Legacy: A Tribute to William and Elizebeth Friedman

German Cipher Machines of World War II

Solving the Enigma: History of the Cryptanalytic Bombe