

The Link

BULLETIN OF THE NATIONAL CRYPTOLOGIC MUSEUM FOUNDATION, INC.

VOLUME 4, NUMBERS 3/4

Fall/Winter 2002

REMEMBERING PEARL HARBOR THE BANDSMEN - CRYPTOLOGISTS

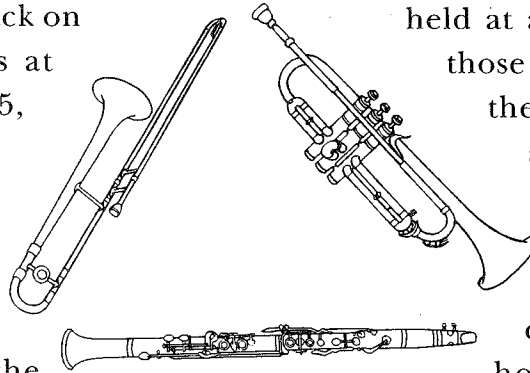
Even with the horror of “9-11” still fresh, the Foundation took time to recall the shock of “7-12,” the 1941 attack on the U.S. Naval Base and ships at anchor in Oahu, Hawaii. At 0755, ships’ bands on all of the major vessels had prepared for their routine Sunday ceremony, the raising of the national flag, after which they anticipated the remainder of the day relieved of duty. Some surprise was expressed at the early activity over on Hickam Field –evidently planes dropping sacks of flour to simulate explosives. Maybe they were making a training film, thought one bandsman. As a torpedo bomber bore in, and a bomb landed on nearby Ford Island, the reality struck. “General Quarters” was sounded and the bandsmen raced for their battle stations. Not a note had been sounded. And life would never again be

the same for those who survived.

In our own program 7 December 2002 – held at an alternative site – three of those bandsmen were honored for their subsequent service. Their ships lost, bandsmen were given assignments assisting the work of LCDR Joe Rochefort and his team of codebreakers. We were honored with their presence.

Two from *USS California* – Pete Panyon (trombone) and Mike Palchefskey (trumpet) participated in a panel with RADM “Mac” Showers (USN Ret), who arrived in February 1942 to begin a distinguished career in Naval

Intelligence. Joining them was Bob Parker (reeds). The NCMF Program Committee Chairman, Julie Wetzel, introduced the panelists, and Committee member Bill Ferguson served as moderator.



I N T H I S I S S U E

REMEMBERING PEARL HARBOR	1
OVERVIEW	2
SPY MUSEUM TO OPEN IN D.C.	2
THE BANDSMEN-CRYPTOLOGISTS OF PEARL HARBOR	3
THE ROLE OF THE “BOMBES” IN EXPLOITING ENIGMA	5
SOLVING THE ENIGMA:	
HISTORY OF THE CRYPTANALYTIC BOMBE	5
AL FRIENDLY, POET-CRYPTOLOGIST	9
BRITISH ACKNOWLEDGE OPERATOR HEARING LOSS	10
GCHQ PLANS TO MOVE	10
NCM VISITS IN 2001	10
“SOLVING THE ENIGMA”	10
FOR THE BOOKSHELF	11

OVERVIEW

Under normal circumstances, our first thought would be to apologize for the disruption of routine in recent months. But these are not routine times, the disruptions were not of our making or choosing, and I am confident that our members and readers appreciate the extraordinary measures necessitated by events since 9 September.

The Foundation has no reason for existence other than to support the National Cryptologic Museum. Furthermore, our office is housed in the NCM. Given the uncertainties at the time and the critical need to subordinate all other considerations to the new priority challenge, it was understandable that the National Security Agency elected to lock down the Museum and turn its attention inwardly as it assessed the threat and adjusted to the reality of a strange war. It has taken time to gain readmission to our files, mailing list, e-mail, and telephone messages. That has now been accomplished. In the interim, our Executive Committee and individual officers seized the time, not only to keep us going, but to accomplish some work that had gone begging. It was a tribute to that spirit that we were able to go ahead with the "Bandsmen-Cryptologists of Peal Harbor" program on 7 December. Adjusted planning for future events will be reflected here and on our Web site.

You'll see that this issue of *The Link* also reflects the ninety-day hiatus.

Renewal reminders have been mailed to all of our members of record. Response thus far has been encouraging, but we do need your renewals, so make sure you have not overlooked the notice or filed it with the "intend-to-do" actions. (We have heard that there were unusual delays in receipt of the mail, perhaps by measures being taken to ensure that the anthrax risk was negated.)

The Museum has been back on its former weekday schedule since early December. The hope is that the popular Saturday opening can be resumed this spring, to accommodate

weekend visitors. Meanwhile, your Foundation has continued with its program planning and identification of alternate meeting sites as a contingency for the future. On 4 April 2002, we plan to present the special program on **Counterintelligence** that was to have been presented last fall, but was cancelled. Details and location will be reaching you by mail. We are also aiming at a one-day **General Membership Meeting** (a make-up for last fall's cancelled annual gathering) on Friday, 14 June 2002, at the Johns Hopkins Advanced Physics facility off US-29. Please note that on your calendar. Although notices and invitations (with map) will come by mail, I urge you to keep posted on the Internet.

John E. Morrison, Jr.
President

P.S. I wish to express the warmest appreciation of the Foundation for the impressive response of our membership to our annual dues solicitation. I would remind those who have not yet responded that your support is critical to our mission success. Your dues are an important element of that support. We'll be looking forward to hearing from you.

J.E.M.

SPY MUSEUM TO OPEN IN D.C.

"The international spy museum, a new museum exploring the craft, practice, history and contemporary role of espionage, will open at 800 F Street in Washington, D.C. in June 2002. It will be the first public museum in the world dedicated solely to the subject of international espionage. In development since 1996, the museum is distinguished by the members of its advisory board of directors and advisory council, which include some of the most respected professionals in the international intelligence community." (AFIO Electronic Bulletin Board, 5 February 2002.)

THE BANDSMEN - CRYPTOLOGISTS OF PEARL HARBOR

Bill Ferguson, Program Committee

As a newly graduated history major in 1957, one of the fascinating aspects of being at NSA was the opportunity to work with a group of active and retired Navy Chiefs and Warrant Officers who had been eyewitnesses to history. One grizzled veteran had served on the USS Panay, the gunboat sunk by Japanese aircraft on the Yangtze River in 1938. Another group had served on Corregidor and were among the last evacuees before it fell in the spring of '42. Yet others began their Navy careers as musicians but were transferred into the SIGINT business when World War II broke out. One story especially fascinated me – the saga of the USS California band which survived the attack on Pearl Harbor with only one loss (as opposed to the USS Arizona band which was totally wiped out) and, thanks to the determination of their band master, was transferred, as a unit, into the SIGINT business. Although I had never knowingly met nor worked with any of that group, the story remained in the back of my mind, and, after retiring and joining the Program Committee of the National Cryptologic Museum Foundation, I found an opportunity to pursue this little known facet of cryptologic history.

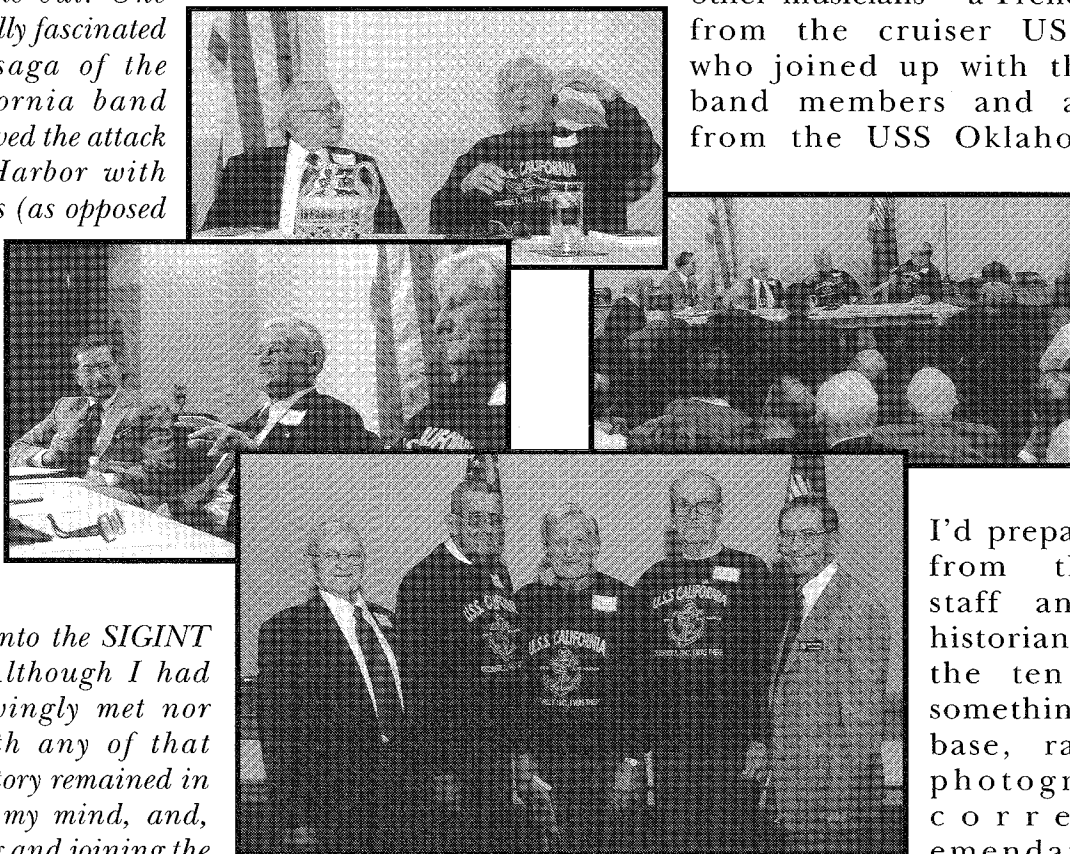
Contacting my first branch chief, Jim Capron, himself a retired Navy Warrant Officer who had had the unenviable job of managing that melange of rough and ready navy types and restless college recruits in the 50's, I learned that one of the USS California bandsmen, Mike

Palchefsky, lived less than two miles away. He and I had actually had a passing acquaintance at the Agency, where Mike had served in both military and civilian capacities. He had kept tabs on his shipmates and provided information on the seven other surviving members from the original group of 20.

I was able to locate and communicate with each of the seven. And as word of the quest spread, I received a number of tips on other possible sources and located two other musicians – a French horn player from the cruiser USS Pensacola, who joined up with the California band members and a trombonist from the USS Oklahoma who was sent off to become a radio intercept operator at Wahiawa. Most were willing, and did, fill out a questionnaire

I'd prepared with help from the Museum staff and the NSA historian, and each of the ten contributed something to our database, ranging from photographs to corrections/emendations to the program write-up.

Interestingly, there was a certain hesitancy among a number of the respondents to document their experiences from reasons that ranged from concern for security compromise, even at this late date, to continued emotional trauma over their experience. Several said that they had only



From left to right: RADM Showers, Bob Parker, Mike Palchefsky, Pete Panyon, Bill Ferguson

Continued on page 4

THE BANDSMEN - CRYPTOLOGISTS OF PEARL HARBOR

Continued from page 3

recently been able to begin telling their experiences to family and friends.

Unfortunately, just as the proposed program was beginning to jell we experienced our 21st Century version of Pearl Harbor and, for a time, it looked as if the program would be shelved for lack of a venue. However, spurred by membership objections to cancellation of an entire slate of Museum-related events, Program Committee Chair Julie Wetzel finally worked out an arrangement with a facility in Colombia, Maryland. Another worrisome aspect was the health and vitality of the potential participants. Our goal was a five member panel however, we had to settle for three. Then one of the three had to drop out for health reasons. In discussing the situation at a NCMF EXCOM meeting one of the members suggested adding RADM "Mac" Showers (USN-Ret) to the panel. Then-Ensign Showers had arrived at Pearl in February '42 and was immediately assigned to the Combat Intelligence unit. Although not a musician himself, he served with the code breakers at Pearl throughout the war and fully appreciated their work from a command context.

The popularity of the event proved another challenge. The capacity of the alternative facility was 90. Over 125 members and guest had indicated that they wanted to attend. As an expedient, technicians successfully piped audio and video to overflow seating in an adjacent room.

Finally, on December 7th, 2001, the NCMF presented its program, "And the Band Played On – But to Punch Cards Vice Sheet Music," to an audience of about 110 including NSA's Deputy Director. Static displays complemented the background music of Glenn Miller's orchestra to help set the stage. Panelists included Mike Palchefsky (trumpet), Pete Panyon (trombone) who flew in from Minnesota, and RADM Showers. I served as moderator. A third band member, Bob Parker (reeds) flew in from California to attend but could not participate because of a severe hearing problem. All three


of the musicians wore matching Pearl Harbor commemorative sweatshirts, as seen in the accompanying photographs.

At the end of the presentation everyone agreed that the outcome was worth all the effort. The audience was treated to eyewitness views of the sneak attack, insiders' views of the cryptanalytic effort which allowed the United States to fend off the invasion of Australia, and inflict the first and major defeat of the Japanese Fleet at Midway, and to eliminate Japan's top military strategist, Admiral Isoroku Yamamoto, architect of the Pearl Harbor attack.

Not without some emotion the two musicians-turned-cryptologists described the circumstances of the attack, their own personal brushes with death on that sunny Sunday, the long hours and primitive conditions working in Combat Intelligence in the basement of the Administration Building at the Pearl Harbor Navy Yard, and colorful descriptions of the talents and foibles of their coworkers and the cryptanalysts they supported. Adm. Showers provided an excellent view from both the command and customer perspective and added an appreciation for the linguistic as well as the cryptanalytic challenge facing the Combat Intelligence group.

Beyond the camaraderie and socialization at the post-event reception the three USS California alumni and their families got together the following evening at a local restaurant and spent long hours reminiscing, philosophizing, rhapsodizing and soliloquizing.

In sum, the NCMF commemoration of the 60th anniversary of the attack on Pearl Harbor provided another reminder that the courage, determination and resilience shown during and after 9/11, while magnificent in its own right, was just a more recent example of characteristics which have been demonstrated throughout our history, especially in times of national emergency. The performance of the Navy Bandsmen is part of the heritage and tradition of American cryptology and a continuing inspiration. It was good to be able to share it with some of the actual participants.



THE ROLE OF THE “BOMBES” IN EXPLOITING ENIGMA

Prominent in the National Cryptologic Museum’s main exhibit area is the sole survivor of the U.S. Navy’s wartime “bombes,” which had been displayed for several years at the Smithsonian in Washington. NCM Deputy Curator, Jennifer E. Wilcox, has compiled a small text, *Solving the Enigma: History of the*

Cryptanalytic Bombe (NSA, Center for Cryptologic History, 2001), which is available gratis at the Museum. Because of general interest in the role of the “bombes,” and for the benefit of those unable to visit the Museum, *The Link* will be serializing that work, starting with this issue.

SOLVING THE ENIGMA: HISTORY OF THE CRYPTANALYTIC BOMBE

Jennifer E. Wilcox

PART 1

About the Enigma

As the German military grew in the late 1920s, it began looking for a better way to secure its communications. It found the answer in a new cryptographic machine called “Enigma.” The Germans believed the encryption generated by the machine to be unbreakable. With a theoretical number of ciphering possibilities of 3×10^{14} , their belief was not unjustified.^① However, they never reached that theoretical level of security. Nor did they count on the cryptanalytic abilities of their adversaries.

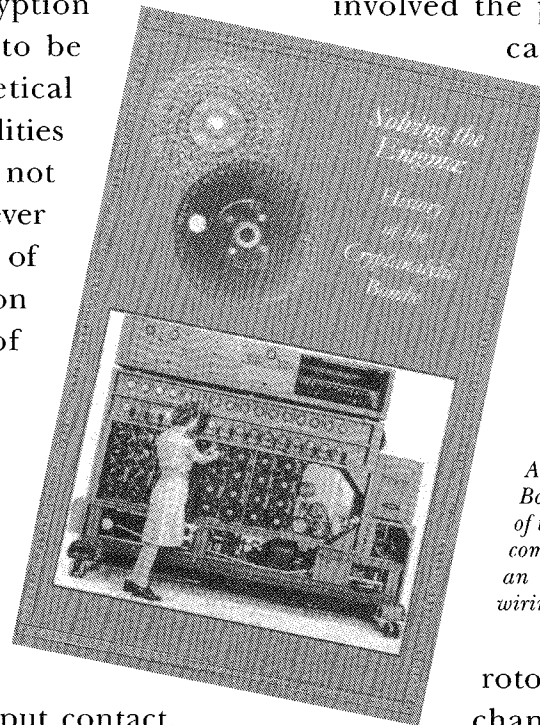
The Enigma machine based its cipher capabilities on a series of wired rotor wheels and a plugboard. Through a web of internal wiring, each of the 26 input contacts on the rotor was connected to a different output contact. The wiring connections of one rotor differed from the connections on any other rotor.

Additionally, each rotor had a moveable placement notch found on an outer ring. The notch forced the rotor to its left to step one place forward. This notch could be moved to a

different point on the rotor by rotating the outer ring. The Germans followed a daily list, known as a key list, to indicate where the notch should be placed each day.

Another complication to the machine involved the plugboard, which the Germans called a *Stecker*. The plugboard simply connected one letter to a different letter. That also meant that the second letter automatically connected back to the first. Again, the key list indicated which letters should be connected for that day.

Each day, the Germans followed the key list to plug the plugboard connections, select the rotors to be placed in the machine, change the rotor notch placement, and place the rotors in the left, center, or right position within the machine. Finally, the code clerk chose which three letters were to appear through three small windows next to the



A Wave operating a Navy Bombe; she is handling one of the commutator wheels. A commutator wheel cover and an inside view of a wheel's wiring.

Continued on page 6

SOLVING THE ENIGMA: HISTORY OF THE CRYPTANALYTIC BOMBE

PART 1

Continued from page 5

rotors. These letters indicated the initial rotor settings for any given message, and the code clerk changed those settings with every message he sent.

The path the electrical current took initiated with the keystroke. The current passed through the plugboard, changing its path if that letter was plugged to a different letter. From there it entered the first, or rightmost, rotor at the input contact. The rotor wiring redirected it to a different output that went directly into the next rotor's input. After passing through, and changing directions in each rotor, the current entered a reflecting plate. This plate not only changed the "letter," but also sent the current back through the rotors, again resulting in three more changes. The current made one last pass through the *Stecker* and finally on to the light panel where the cipher letter lit up.

To decipher an Enigma message, the recipient had to have an Enigma with the same plugboard connections, rotors, notch placement, left/center/right positions, and initial settings. This enabled the current to follow the same pathway in reverse and resulted in the plaintext letter lighting up on the light panel. The Germans, with their published key lists, had the necessary information. The Allies did not. The Enigma eliminated whatever intricacies a language may possess that previous methods of cryptanalysis exploited. One such practice was frequency counts. Certain letters in any language are used more often than others. By counting which cipher letters appeared most often, cryptanalysts could make an assumption about which plaintext letter they represented. Machine encryption like the Enigma destroyed the frequency counts. Cipher letters tended to appear equally often.

Poland Breaks the Unbreakable Machine



In 1928 the Poles, who had actively intercepted German signals since the end of the First World War, realized that the Germans had changed to machine encryption because standard attacks, such as frequency counts, were useless. They purchased a commercial version of the Enigma, but it too was useless. The commercial machine used four rotors to cipher the letters and had no plugboard. The German military had made too many changes to the machine for the Poles to make use of the commercial Enigma.

Determining the exact wiring of each of the three rotors became the Polish cryptanalysts' first task. To accomplish this, Poland's Cipher Bureau tested and hired three mathematicians in 1932. Marian Rejewski, Jerzy Rozycki, and Henryk Zygalski painstakingly analyzed the intercepted encrypted messages searching for clues. Rejewski eventually determined a mathematical equation that could find the wiring connections.

However, the equation had too many unknown variables. He finally made the initial breaks into the wiring sequence only with the aid of a German traitor.

Hans-Thilo Schmidt, an employee of the German cryptographic agency, introduced

Continued on page 7

SOLVING THE ENIGMA: HISTORY OF THE CRYPTANALYTIC BOMBE

PART 1

Continued from page 6

himself to a French intelligence officer and offered to sell German cryptographic information. Captain Gustave Bertrand followed up on the contact, and the initial information Schmidt provided proved authentic. Eventually Schmidt provided the French cryptologic office with documentation on the Enigma machine and some Enigma keys. Unfortunately, the information did not contain wiring diagrams for the rotors.



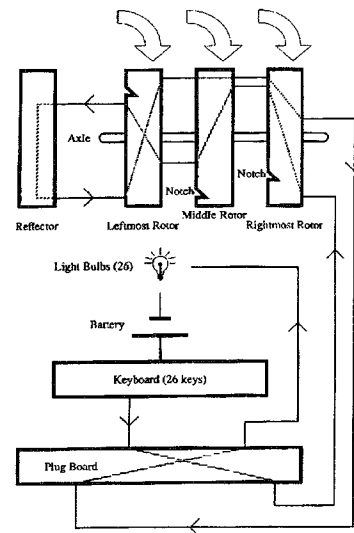
Marian Rejewski (1905-1980) as a second lieutenant (signals) of the Polish Army in Britain in late 1943 or in 1944. (Courtesy Richard Woytak)

With this information in hand, Captain Bertrand arranged a meeting with his counterparts in the Polish cryptologic agency in December 1932. He proposed a cooperative effort to work on the German machine ciphers. They agreed to an arrangement: the French would provide any German intelligence that could further the breaks into the system, while the Poles would work on the actual cryptanalysis. Captain Bertrand left the Enigma documentation with the chief of radio intelligence in the Polish bureau. However, the documents were not passed on to Marian Rejewski until it became obvious no progress would be made without them.

Rejewski determined the necessary complicated mathematical equations to determine the wiring of the Enigma rotors. Initially, there were too many unknown variables. With the information Hans Schmidt sold, Rejewski filled in some of the unknown values. After several months of analysis and work, the Polish mathematician determined the wiring of

each of the rotors. Thus, they completed the first of the difficult tasks in reading the secret Enigma messages.

With some brilliant analytic work and some guesswork, Marian Rejewski also determined the wiring of the machine itself. Originally, he assumed the electrical current coming from the first letter on the plugboard (Q) plugged into the first position on the input drum (A). However, when this repeatedly failed to work, Rejewski



Internal wiring of Enigma showing one connection

tried another easy configuration that proved to be correct. The Germans connected the plugboard to the input rotor alphabetically. Later, when the British learned of this simple connection, they were astonished. They had never tried an alphabetic connection in their early attempts to break the Enigma.

Knowing the wiring of the machine and the rotors, the Poles could now replicate the machine on their own. The Cipher Bureau contracted with AVA Radio Manufacturing Company to build a machine to Rejewski's specifications. Unfortunately, having a copy of the Enigma was not sufficient to read the encrypted messages.

Although the Germans, at this time, had only the three rotors and left them in the same position inside the machine (left, center, or right) for three months, the settings of the rotors changed with each message. Each Enigma rotor had a ring with numbers (1-26) or letters (A-Z) inscribed on it. A number or letter on each of

Continued on page 8

SOLVING THE ENIGMA: HISTORY OF THE CRYPTANALYTIC BOMBE

PART 1

Continued from page 7

the three rotors could be seen through small windows on the Enigma machine. This indicated the initial rotor setting for a message and that setting changed with every message. Discovering a method for rapidly determining the rotor settings became the next task for the cryptanalysts.

At first the mathematicians attempted to solve the problem by using the indicators included in each message. Since the German cipher clerk determined the initial rotor settings, they had to be sent to the intended recipient in the clear, that is, unenciphered. The first three letters of the code group, sent unenciphered, told the receiver where to set the rotors. The following six letters were the ciphered letters (repeated) of the settings for the rest of the message. They were sent twice in order to avoid garbles in transmission. For example, the clerk might send HIT in the clear. The receiver set his Enigma rotors to read HIT through the windows and then typed the next six letters in the message, KOSRLB. These were the indicators. The letters that lit up (LERLER) told him where to reset his rotors. Changing his rotor settings to read LER through the windows, the receiver now decrypted the rest of the message.

Because the clerk made up his own six-letter settings, the Polish cryptanalysts could occasionally guess the settings. The military did not allow an obvious setting such as ABC. However, cipher clerks sometimes chose settings like QWE (the first three letters on the keyboard) or names. In the example above, if the first three letters were HIT, the cryptanalysts could guess that KOS and RLB were the ciphers to LER, spelling out HITLER. BER was usually followed by the ciphers of LIN. One particular German

code clerk continually used his girlfriends's name, Cillie, for his messages, and so these easy-to-guess indicators became known as "Cillies."⁹

The Poles could try these Cillie combinations relatively quickly. However, communication security policy discouraged this type of indicator, and most rotor settings were relatively random. To determine these random settings, the Poles relied on pure analysis and comparison. Henryk Zygalski developed a way to compare the message indicators. It involved stacks of perforated pages cut in exact positions. In our example, KOSRLB, the K and the R are ciphers for L. There are only certain combinations that allowed for that circumstance to occur. Holes in the perforated pages that lined up allowing K and R to correspond were considered as possible rotor settings. Cutting the pages took time, but once completed, they made the comparison quickly. This system worked very well until the Germans changed their indicator system and sets of new pages had to be cut.

As the German military grew, so did the number of messages sent using the Enigma. It began to overwhelm the small staff of cryptanalysts in Poland. They realized that the time-consuming hand-worked method of analysis would not be sufficient. Marian Rejewski developed plans for a machine that could, through brute force, work through the more than 17,000 possible positions.⁹ The machines was called a Bomba.⁹

AVA Radio Manufacturing Company (Wytownia Radiotechniczna AVA), the same company that built the Polish copies of the Enigma, also built the first Bomby (the plural of Bomba) for the Polish cipher bureau. It resembled three pairs of Enigma duplicates linked together. The new Bomby and Zygalski's sheets worked well, finding solutions in two hours or less through 1938. Then the Germans

Continued on page 9

SOLVING THE ENIGMA: HISTORY OF THE CRYPTANALYTIC BOMBE

PART I

Continued from page 8

added two new rotors to the collection. Although the Enigma machines continued to use only three rotors at a time, the Poles had no way of knowing which three out of five had been selected. Rejewski determined the wiring of the new rotors as he had the original three, but the Bomba was not built to work through the combinations available with a choice of five rotors. Instead of having six interlinked Enigmas, the Bomba would need sixty. It was more than the Polish system could handle.

On July 25 and 26, 1939, with the threat of German invasion looming over them, the Poles shared their cryptanalytic secret with the French and British. Despite the French-Polish agreement and the contribution of German information that France provided, Poland had never disclosed the break in the Enigma messages. The French and British representatives were astonished to see not only Enigma replicas, but also a machine that could break the Enigma settings. Returning home with copies of the Enigma, each renewed efforts to break the German encryption. *[continued]*

① - A. Ray Miller, *The Cryptographic Mathematics of Enigma* (Ft. George G. Meade, MD: Center for Cryptologic History, National Security Agency).

② - 6812th Signal Security Detachment (PROV), dated 15 June 1945; (NARA Record Group 457, File #2943, 7.) Hereafter referred to as 6812th.

③ - Each rotor on an Enigma can be set in any one of twenty-six positions (I-26 or A-Z). On a three-rotor machine the number of possible settings is 26^3 or 17,576.

④ - Bomba is Polish for bomb. Wladyslaw Kozaczuk's book *Enigma* (University Press of America, 1984, 63) cites a letter from Col. Tadeusz Lisicki, chief of a Polish signal unit, which claims that Jerzy Rozycki named the machine after an ice cream dessert the mathematicians were eating at the time. The bomba dessert was a round ball of ice cream covered in chocolate and resembled an old-fashioned bomb. However, in an article Rejewski himself says, "For lack of a better name we called them bombs." ("How Polish Mathematicians Deciphered the Enigma," *Annals of the History of Computing*, v.3, n.3 (July 1981): 226.) Finally, a U.S. Army document describing the Polish Bombes claims, "When a possible solution was reached a part would fall off the machine onto the floor with a loud noise. Hence the name 'bombe'." (6812th, 10.)

AL FRIENDLY, POET-CRYPTOLOGIST

The distinguished post-war journalist at the *Washington Post*, Alfred Friendly, was a WWII member of the cryptologic workforce. As was the case with others, he brought talent to bear, and indulged that same talent as a "breather" from the countless serious hours of work. Among the fading papers that survived the war is the following ditty, in which Mr. Friendly displays some of the conventions used to convey uncertainty or corrupt text to the readers of MAGIC and ULTRA translations:

Come live with me in halls of marble

Where we can loaf and love and -G-

We'll spend our days in hugs and kissing

As for our nights, -(15 groups missing).

Forsaking spots where black gloom hovered

Forsaking life that's -U-

Forsaking tumult, noise and rackets

Making love in [(double brackets)]

As when Apollo Thetis marries

They soon produce some ??double queries??

*To cares and sadness were driven**

** Line breaks off; text as given.*

(To those unacquainted with the conventions used, read -G- as "garbled" and -U- as "unrecovered" [code group].)

BRITISH ACKNOWLEDGE OPERATOR HEARING LOSS

According to the Winter 2002 *NCVA Cryptolog*, citing the *London Daily Telegraph*, GCHQ (Government Communications HQ, the British equivalent of NSA) “has settled the hearing loss problem of intercept operators with large cash settlements. Due to the type of earphones used over the years by British intercept operators, loss of hearing has been progressive.” *Cryptolog* quotes the *Telegraph* as reporting that “the problems resulted from the use of headphones without adequate volume controls. Officials say the 4,000 workers turned the volume up to full if foreign transmissions were difficult to understand.” “New and safer headphones were introduced in 1995.”

Traditional models of the SIGINT process start with the intercept operator (now more euphemistically known as “the collector”). Few outside the field can appreciate how important the “ears” and brains of an experienced operator were to the process – the value to traffic analysis of an added “op” comment that, for example, “XYZ on 5050 same man as ABC on 6220.” And it is understandable that, straining to hear faint signals, dedicated ops unwittingly harmed their hearing. (Attention seems to have centered on avoidance of ear infection by trading headphones.) Comparable to this is the casual attitude toward hearing loss when firing a rifle – well into the ‘50s/’60s the practice was to insert a spit-moistened cleaning patch in the right ear. Over time, the degradation of hearing became known as “having an M1 ear.” (There’s probably a lesson here for young people with “boom boxes” glued to their ears, or their cars vibrating from the volume of “rap” music.)

GCHQ PLANS TO MOVE

NCVA Cryptolog (above) also notes plans for a relocation of GCHQ from Cheltenham some four miles away to Gloucestershire, where a new headquarters facility is being built. An unusual design, it is to have a central space, “similar to the Pentagon,” with the building surrounding the central space. (And, needless to say, there are vocal critics of the cost, estimated at “up to a billion £.”)

NCM VISITS IN 2001

Notwithstanding the three-month closure of the Museum, curator Jack Ingram reports a total of 45,059 recorded visitors in 2001, and he concludes that, given the nine month operation, the year’s total would have been equal to, or even surpassed, that of 2000.

Among the visits, there were 841 tours provided (351 scheduled, 445 “walk-ins,” and 45 for VIPs). School visits totaled 55; Media, 22; and Scouts, 22. Thirty-one dinners or social events were hosted during the year.

“SOLVING THE ENIGMA”

“It may well be doubted whether human ingenuity can construct an enigma of the kind which human ingenuity may not, by proper application, resolve.”

Edgar Allan Poe, *The Gold Bug*

FOR THE BOOKSHELF


The Emperor's Codes: the Breaking of Japan's Secret Ciphers, by British historian Michael Smith (New York: Arcade Publishing, 2001, ISBN 1-55970-586-X) was expected to be devoted to proving that, whatever the Yanks did, the Brits had done earlier. (In the words of the song from "Annie Get Your Gun," "Anything you can do/ I can do better.") While there is quite a bit along that line, it turns out to be surprisingly objective and easily readable, a balanced account that will be a reminder for some and a handy guide for others.

Because of the way in which declassified material has been released among the countries involved, it is likely that we will continue to see more claims of "getting there first." Done with fidelity to the facts (as they are known) and good humor, accounts of the rivalry between colleagues certainly has a place, and bring back memories. But Smith's tone is stern in condemning the reticence and lack of cooperation on the part of upper echelons of the U.S. Navy almost to the very end of the war. *"[H]istorians have argued that [code-breaking] shortened" the war "by around two years, saving many lives on both sides of the conflict. Yet it is impossible to make this claim with regard to the war in the Far East without also accepting that the difficulties placed in the way of co-operation, both with the British and their own military, by elements within the US Navy must have cost lives, the majority of them American . . . [T]he effects of the rows over co-operation and the refusal of FRUMEL [LT Rudi Fabian's naval cryptologists in Melbourne] to share their material with Central Bureau were not momentary mistakes. They were the result of a sustained and deliberate policy based only partly on security concerns. It was clearly also motivated by a desire to ensure that the US navy's signals intelligence hierarchy received the credit for any successes. . . . Its architects and proponents were administrators, some*

of whom had little respect for those who achieved the success, as demonstrated most clearly by the appalling treatment meted out to Joe Rochefort" (277).

With the focus on the war with Japan, Smith nevertheless spreads his canvas wide, keeping in touch with the challenges of Engima and the war in Europe to provide context. His descriptions of deployment of Commonwealth signal intelligence resources are concise, even touching on Mountbatten's Southeast Asia command, in which the role of Americans – the China-Burma-India theater – has yet to be well told. Most pleasing is the way in which, through interviews and recollections, he is able to recreate the human aspects of this strange war. He conjures up the atmosphere, the vocabulary, and the work itself, devoting a section to explaining the "stripping" away of superencipherment to enable recovery of the underlying code book.

Most interesting of all, to this reviewer, is that, in his research, Smith discovered a previously concealed bit of history: Using elderly (and legendary) CAPT Eric Nave as his co-author, British writer James Rusbridger had resurrected the conspiracy theory of a crafty Churchill and a naïve or poorly informed Roosevelt in his 1991 *Betrayal at Pearl Harbor: How Churchill Lured Rossevelt into War*. His thesis depended on evidence of superior British code-breaking in the field, and the state of recovery of the main Japanese naval system, JN25, prior to 7 December. Working from a copy of Nave's original memoirs found at the Australian War Memorial, Smith denounces Russbridger for intentional distortions of what Nave wrote, and his damage to Nave's reputation. (Russbridger died as a result of suicide under bizarre circumstances; Nave's WWII service is well appreciated in Smith's book.)



Join the National Cryptologic Museum Foundation

ANNUAL MEMBERSHIP APPLICATION

Please begin/renew my membership in the Foundation

- | | |
|--|--|
| <input type="checkbox"/> \$25 Sustainer | <input type="checkbox"/> \$1,000 Sponsor |
| <input type="checkbox"/> \$100 Contributor | <input type="checkbox"/> \$5,000 Patron |
| <input type="checkbox"/> \$250 Supporter | <input type="checkbox"/> \$10,000 Benefactor |
| <input type="checkbox"/> \$500 Donor | |

The Foundation is certified as a non-profit organization by the I.R.S.

Name _____

Address _____

City _____

State _____ Zip _____

Phone _____ E-Mail _____

Date _____

Please make your check payable to:

The National Cryptologic Museum Foundation

The National Cryptologic Museum Foundation, Inc.

PRESIDENT
Maj. Gen. John E. Morrison, Jr.
USAF (Ret.)

VICE PRESIDENT
Mr. Robert E. Rich

SECRETARY
Mr. John B. Callahan

TREASURER
Mr. William T. Kvetkas, Jr.

GENERAL COUNSEL
Leonard E. Moodispaw, Esq.

S/A PRES/CHMN
Mr. Eugene Becker

BOARD OF DIRECTORS
CHAIRMAN
Maj. Gen. John E. Morrison, Jr.
USAF (Ret.)

MEMBERS
Mr. Joseph Amato
Ms. Ann Z. Caracristi
Mr. Robert J. Fitch
Mr. David W. Gaddy
Ms. Lee Hanna
The Hon. Robert J. Hermann
Mr. Robert M. Huffstutler
Mr. David Kahn
Mr. James W. Pryde
Mr. Robert E. Rich

MEMBERS CONTINUED
ADM William O. Studeman USN (Ret.)

ADMINISTRATIVE STAFF
Ms. Jan Leach
Ms. Sherri Legere

COMMITTEE CHAIRMEN
Mr. William Arrington, *Finance & Audit*
Mr. Rodney B. Sorkin, *Acquisition*
CAPT. Fred R. Demech, *USN (Ret.), PAO*
Mr. Richard S. Finlay, *Membership*
Mr. W. Edwin Kirk, *Facilities*
Maj. Gen. John E. Morrison, Jr.,
USAF (Ret.), Development
Mr. Milton Zaslow, *Recognition*
Mrs. Julie Wetzel, *Program*
Mr. David W. Gaddy, *Bulletin Editor*

FOUNDATION TELEPHONE:
(301) 688-5436 & 5437
Fax (301) 688-5619
email: cryptmf@aol.com
http://www.
nationalcryptologicmuseumfoundation.com

MUSEUM TELEPHONE:
(301) 688-5849

MUSEUM HOURS:
Monday - Friday - 9:00 a.m. - 4:00 p.m.
Saturday - 10:00 a.m. - 2:00 p.m.

RETURN SERVICE REQUESTED

The National Cryptologic
Museum Foundation, Inc.
P. O. Box 1682
Ft. George G. Meade, Maryland 20755-9998

NONPROFIT
U.S. POSTAGE
PAID
FORT MEADE, MD
PERMIT NO. 43