>>Solving the Enigma

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^{114}, 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 were 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 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 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.

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 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 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 girlfriend's name, Cillie, for his messages, and so these easy-to-guess indicators became known as "Cillies."[2]

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 comparisons 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.[3] The machine was called a Bomba.[4]

AVA Radio Manufacturing Company (Wytwornia 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 added two new rotors to the collection. Although the Enigma machine 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.

Britain Builds the Bombe

Britain, like Poland, began hiring mathematicians to work in their Government Code and Cipher School (GC&CS). Alan Turing and Gordon Welchman, both mathematicians from Cambridge University, joined the GC&CS at the outbreak of hostilities with Germany. In early September 1939, the mathematicians reported to the new home of GC&CS, a Victorian manor in Bletchley, England, known as Bletchley Park (BP). They received a briefing on the work of the Polish Cipher Bureau and the Polish mathematicians. Turing and Welchman individually began thinking of ways to more quickly solve the German Enigma messages. They would both play a crucial role in the development of the cryptanalytic machine.

Alan Turing realized that the solution did not lie in creating a machine that replicated sixty Enigmas. The Polish Bomba searched for matches in indicators. Once already the Germans had changed how indicators were used, throwing the Poles back into the darkness until new Zygalski sheets could be cut. The Germans could easily change the indicators again. Turing began thinking about a machine that worked, not with the indicators, but with assumed text. By using text that cryptanalysts assumed appeared in the message, the machine would not be dependent on the indicators.

Like the Polish Bomba, the machine Turing conceived would also run through all the possible settings. Rotors and wires would simulate a series of Enigma rotors and pass an electrical current from one rotor to the next. However, rather than looking for the one correct rotor setting based on the indicators, as the Bomba did, Turing's would look for all the rotor settings that allowed the cipher to match the assumed plain text. Or, more correctly, it searched all the settings and disregarded those that were incorrect. For example, if the assumed letter was "G" and the corresponding cipher letter was "L," Turing's test register ignored any results that did not allow the electrical current to pass from "G" to "L." By disproving thousands of rotor settings, those left were possible correct settings.

While Turing developed plans for his cryptanalytic machine, Gordon Welchman also thought about the Enigma problem. Though GC&CS assigned him to work in traffic analysis, a field that involves the externals of a message and not the message itself,[5] he contemplated ways to break Enigma messages more easily. On his own, he reinvented the series of perforated sheets that Henryk Zygalski had developed for the Poles. Poland had turned this achievement over to Britain at the same time as the Bomba, and BP was already creating new sheets for five rotors.[6]

Undeterred, Welchman began working on another complication on the Enigma, the plugboard. Because the plugboard uses a cable to connect one letter to another, it automatically connects the second letter back with the first. If A is plugged into E, E is plugged into A. Knowing this, Welchman designed a board that connected each letter with every other letter. The wires created a pattern of diagonal lines. He created a "diagonal board."

Gordon Welchman showed his design to Alan Turing, who agreed it would greatly enhance his machine. Although simple in design, combined with Turing's test registers, the number of possible rotor settings decreased from thousands to only a few. Analysts could easily test these few solutions on an Enigma duplicate or analog.

Turing and Welchman took the design to Harold "Doc" Keen, an engineer at British Tabulating Machines (BTM), who was in charge of actually building the machines the mathematicians conceived. Work had already begun on Turing's machine, but upon seeing Welchman's diagonal board and realizing its implications, Doc re-engineered the cryptanalytic machine. Turning the mathematicians' conceptions into working machines took extensive engineering experience. Fortunately, "Doc" was able to combine both men's thoughts into an integrated, workable machine.

It took months to design and build the cryptanalytic machines. It wasn't until August 1940 that the first operational machines arrived at Bletchley Park. Initially, each Bombe took six weeks to construct, but later BTM completed one Bombe each week. The completely redesigned Polish machine also received a slight name change from the Polish "Bomba" to the French spelling, bombe.[7]

The British manufacturing company BTM built most of the approximately 210 Bombes used in England throughout the war. Although the machines changed and improved during the five years of production, the basic Bombes weighed one ton and stood six and a half feet high, seven feet long, and two feet wide. Each of the basic machines had thirty-six sets of three rotors. Within each set, the top drum represented the leftmost, or slowest, rotor on the German Enigma; the middle corresponded to the German's center rotor; and the bottom Bombe drum represented the Enigma's rightmost, or fastest, rotor.

The British Bombes worked through rotor settings in the opposite direction of the Enigma. Since the Bombe needed to try every combination of rotor settings, it didn't matter from which direction this was accomplished. Even though it represented the slowest moving Enigma rotor, the top Bombe drum spun the fastest at 50.4 rpm.[8] In the instant that each position made contact, an electrical current tried to complete a path through each of the test registers and the diagonal board. Most could not complete the path correctly and were discarded. Those that did complete the path caused the machine to stop.

Members of the Women's Royal Naval Service, Wrens, operated the machines, and when the machine found a "stop" the operator wrote down the rotor settings. She then reactivated the Bombe enabling it to search for any other possible solutions within that wheel order. Another Wren tested the stop on a checking machine and passed the result to a cryptanalyst in another building. When the cryptanalysts found the one correct setting, they notified the Wrens to stop work on that message and move on to the next. It took ten minutes for the Wrens to change the wheel order for the next run and an additional thirty-five to fifty minutes to set up the connections and rotor positions.[9]

By the time the British Bombes arrived at Bletchley Park, cryptanalysts had already made breaks into the German Air Force and Army Enigma systems, allowing the Bombes to routinely find the message's settings. The German Navy Enigma was much more difficult to read. The German Air Force and, to a lesser degree, the German Army, were so sure of the imbedded security of the Enigma itself that they were lax in their communication security measures. The German Navy, however, complicated their system with strict enforcement of communication security practices and the addition of three more rotors to the collection. The Navy now had eight rotors from which to select the three used in the Enigma each day. Without knowing the wiring of the Navy's additional rotors, Britain could read very few German naval messages.

Because the Polish cryptanalysts had briefly been in occupied France, the British considered them suspect. Therefore, GC&CS did not turn to Marian Rejewski for help concerning the new rotors' wiring. The equation he developed in the 1930s could have retrieved the wiring as it had the originals. But without his assistance, Bletchley Park could have made no significant breaks into their enemy's secret naval messages. Due in part to the Allies' lack of knowledge of German naval intentions, the Kriegsmarine submarines ruled the Atlantic shipping lanes.

Britain depended heavily on U.S. supplies crossing the Atlantic. Although the U.S. claimed neutrality, it sold materiel and supplies to Britain and provided escorts for their convoys. Germany planned to destroy this supply line and cripple Great Britain. Their most destructive weapons in the Battle of the Atlantic were the German submarines, known as U-boats. For twenty-one months, as the cryptanalysts at Bletchley Park desperately tried to make breaks into the naval Enigma messages, the U-boat wolf packs decimated Allied shipping convoys.

Admiral Doenitz, commander of the U-boat fleet, operated his submarines in a coordinated strategic plan. The U-boats patrolled the ocean in search of their prey. Once they spotted a convoy, the subs alerted their forces by way of Enigma-enciphered radio messages. Other U-boats were sent to assist in the assault. Like a pack of wolves, the U-boats attacked the supply ships sending many of them to the bottom of the ocean. Had Bletchley Park been able to read the messages sent to and from the U-boats, they could have alerted the convoys. But without prior knowledge of the attacks, the ships were all but helpless. A German victory in the Atlantic loomed over the Allies before Britain finally got the break it needed.

The inability to read the Navy Enigma messages finally ended in May 1941 when Britain captured the German submarine U-110 with its encryption equipment intact. U-boat commander Fritz-Julius Lemp, fearing that the sub was sinking rapidly and that it was about to be rammed, ordered his crew to abandon ship. The radioroom crew, believing they were in great peril of drowning and obeying the order to abandon, did not destroy the Enigma or codebooks before donning their life vests and jumping overboard.

With the German submarine crew treading water in the cold Atlantic, the British ship *Bulldog* sent a boarding party to the U-110. They found a treasure trove of secrets. The boarding party collected all books, charts, logs, and other important documents and equipment. Among the captured material were codebooks, instructions, and key lists for several different German Navy and submarine codes. It also included an Enigma machine with the daily settings in place and each of the eight rotors.

Representatives arriving from Bletchley were astonished at the find. They photographed the most important documents and boxed everything up for shipment to BP. Within days BP would be reading the German Navy messages again.

Britain had at last acquired the missing rotors. With the rotors and the keys through June, Bletchley didn't even need the Bombes in order to read the messages. But those two months would pass quickly, and the Bombes needed to be ready when the keys ran out. BP began wiring drums for the Bombes to match the wiring of the three new rotors.

Fortunately, Admiral Doenitz did not realize that the U-110's Enigma rotors and other vital communications information were now in the hands of the Allies. Had he known, he certainly would have changed the system. The U-110 was boarded in sight of some of the survivors, so Britain went to great lengths to convince them that the submarine sank before it could be boarded. Word got back to Admiral Doenitz that the code was safe.

From June 1941 through the summer, BP read the U-boats' "Heimisch" or home waters coded messages at the same time as the Germans themselves. Admiral Doenitz used the home waters code to command his forces. With foreknowledge of a U-boat's location, the Allies could take steps to avoid the wolf packs or send bombers for an Allied attack.

Admiral Doenitz noticed this change in his submarine forces' ability to sink the supply convoys. Before the spring of 1941, German attacks sank a majority of Allied shipping tonnage. Then, almost suddenly, it was the attacker who became the prey. Despite the assurances he received concerning the U-110, Admiral Doenitz suspected the Allies could read his fleet's Enigma messages. When he asked German High Command of this possibility, they assured him that the Enigma could not be broken. They proposed other reasons as to why his U-boats were less effective, including Allied direction finding capabilities (called Huff Duff by the British), aerial reconnaissance, or even a German traitor. In truth, even when the Navy Enigma messages could not be read, British direction finding combined with traffic analysis did have substantial successes.

Certainly the Germans' faith in the Enigma was not unfounded because of the astronomical mathematical possibilities. However, to encourage this unquestioned confidence, Britain went to great lengths to disguise how Enigma information, known as Ultra, had been obtained. The British took no action based on Ultra without first providing the Germans with a deceptive reason for the actions taken. Most commonly, British aircraft flew a reconnaissance mission over an area that Ultra had shown to be significant. When the Allies subsequently attacked that area, the Germans believed their forces had been spotted by the aircraft, not given away by Enigma.

Admiral Doenitz, however, was not satisfied. He intended to change the U-boat Enigma machines. He could not radically alter the machine itself as it had to continue to work with the rest of the German Navy. His change added a thin fourth rotor between the leftmost rotor and the reflecting plate. When necessary, the rotor could be set in a straight-through position, enabling it to act as a three-rotor machine.

Bletchley Park learned of the impending change from decrypts and captured material, but until it was actually implemented there was little they could do to prepare. Fortunately, the Germans made an error. In December 1941, before the change had been made official, a U-boat sent a message using the four-rotor machine. To compound the mistake, the same message was retransmitted using only three rotors. From this seemingly innocuous error, the cryptanalysts at BP determined the wiring of the fourth rotor.

In February 1942 Admiral Doenitz officially changed the Enigma machines on his U-boats. Despite recovering the wiring to the fourth rotor, Bletchley Park had a lot of work ahead of them. In addition to changing the machine, the Kriegsmarine also instituted a new code, which Britain referred to as "Shark." BP now had two obstacles: break Shark and redesign the Bombe. The cryptanalytic Bombe developed by Alan Turing, Gordon Welchman, and "Doc" Keen found the rotor settings for a three-rotor machine. It could not find the settings for four rotors. Once again German submarine messages were indecipherable. Admiral Doenitz' U-boats began again to successfully prowl the waters of the Atlantic.

America Joins the Secret Battle

The complete cessation of Ultra intelligence concerning U-boats in the Atlantic coincided with the devastating attacks on shipping by U-boats off [U.S.] coasts. In fact, the outlook during the summer of 1942 was rather gloomy.[10]

Despite its involvement with the British convoys, the United States took none of the precautions learned by its allies. Merchant ships came up the east coast of the United States without the benefit of convoys or escorts. Sailing alone, there were no other ships to come to their defense when attacked by the U-boats. To make matters worse, ships were in plain sight even at night. The United States did not initially require its citizens to black out their homes and businesses at night as the British did. Hence, ships coming up the coast were silhouetted against the bright lights of the cities they passed. The U-boats had no trouble seeing them and sinking them. Add to this the fact that the German cryptologic service, B-Dienst, could read the Allied Naval Cipher No. 3 used for convoy communications. By reading the convoy messages, the Germans learned of changes and movements in Allied shipping. This enabled them to easily respond and continue to follow and attack the ships. The Germans referred to the spring of 1942 as the "Happy Time." Between January and March they sank 216 ships off the East Coast.

The United States didn't begin sending its ships in convoys or require blackouts on the East Coast until May 1942. Unfortunately, even these measures made only a small improvement. The Allies still could not read the U-boat four-rotor machine's messages, so there were few ways of knowing where the U-boats were located.

The Allies did make use of direction-finding and other reconnaissance measures. This provided limited information, but was no substitute for the valuable Ultra messages.

Bletchley Park and BTM began work to redesign the Bombe for a fourth rotor and promised the United States that a solution would be available by August or September. The U.S. waited, somewhat impatiently, for assistance. Neither the U.S. Army nor Navy had made any breaks into the Enigma problem. Prior to entering the war, the United States was not intercepting large volumes of Enigma messages and had not seriously worked to break it. Assistance from the British would be required if the United States hoped to combat the U-boat attacks off America's coast.

Representatives of both the U.S. Army and Navy visited Bletchley Park prior to the United States' entrance into World War II and knew of Britain's success against the Enigma messages. GC&CS agreed to share information concerning the Enigma, but it was not completely forthcoming in 1941. This may have been due to security concerns. GC&CS was not confident that the United States services would be able to keep the Enigma secret. However, the adaptations to the British three-rotor Bombe were not pro-gressing satisfactorily, and members of the U.S. cryptologic services continued to press Britain for further information.

In March 1942 the U.S. Navy contracted with the National Cash Register Company (NCR) in Dayton, Ohio, to work on the development and construction of other specialized machines. This contract established the Naval Computing Machine Laboratory (NCML). Lieutenant Commander Ralph Meader acted as the liaison between the Navy and NCR. National Cash Register's engineer, Joseph Desch, became the NCML's research director. The public knew of some of the work conducted by NCML including the production of bomb fuses, shell casings, and aircraft carburetors. However, it would be decades before the people of Dayton, or even his family, learned of the work Joseph Desch did for the Navy. The Navy did an extensive background investigation on him because of his German heritage and relatives still in Germany. He even "jokingly claimed that the Navy had found relatives that he had never heard of."[11] With his background in radio and computing machinery, Joe was indispensable to the Navy's

research in building its own Bombe. Because of the secret nature of the work the Navy needed Joe Desch to do, he was forced to disassociate from all his Dayton relatives, except his mother. "The war demanded immediate, unrelenting research in areas for which Joe Desch was qualified, and he had no choicebut to accept the responsibility that the Navy asked of him."

Meanwhile, in Washington, communication continued with Britain. In April 1942, Colonel John Tiltman from GC&CS visited OP-20-G, the U.S. Navy's cryptanalytic office, and sent a message back to England: "In view of the fact that [the U.S. is] now at war and have a vital interest in submarine traffic, they are entitled to results. . . ." [13] He also stressed, "Unless a rapid and satisfactory solution is found . . . the high command will insist on their Naval cryptanalysts attempting to duplicate our work on 'E'." [14]

In July 1942 two U.S. naval officers went to Bletchley Park with the intention of studying BP's research organization. They had additional orders to acquire more details about the Enigma solution. They learned much about the British Bombe and returned with wiring diagrams. After studying the information, the Navy decided that the development of a high-speed four-rotor Bombe should be designed differently than the British plans indicated. The fact that the British weren't making much progress with their own design supported this decision.

As the summer of 1942 progressed, it became apparent to Navy officials that the British would not be able to meet the August/September deadline for a four-rotor Bombe. Joseph Desch and other NCR engineers, working with the Navy and Lieutenant Commander Meader, looked for alternative designs to the British plan. They investigated the possibility of both an electromechanical design and an electronic design. They were forced to use the electromechanical plans because of the power requirements of the electronic design and material shortages brought on by the war. By the end of August, the Navy concluded that their design showed sufficient promise to continue and inaugurated their own Bombe program.

Captain Hastings of GC&CS protested. He argued that Britain had lived up to the agreement arranged by Colonel Tiltman in April that stated the U.S. would be given results "or a detailed statement as to why this traffic cannot be read. . . ." [15] Since the British had provided a detailed statement, Captain Hastings felt they had met their obligations.

The situation in the Atlantic, however, was of such importance that the U.S. Navy decided they could not accept Captain Hastings' answer. The German U-boats continued to attack Allied shipping throughout the Atlantic. It was imperative that either Britain or the United States make a break into the four-rotor Enigma machine. With that in mind, Commander Wenger, deputy chief of OP-20-G, officially requested funding for the Bombe project on September 3, 1942. With the consent of the chief of OP-20-G, Admiral Redman, the Bombe project proposal was approved the following day.

Once they learned of the Navy's intentions, GC&CS sent Commander Travis to the United States for a visit with the Navy. They drew up another formal agreement. This one proposed that the United States take the dominant position in the Pacific Theater, while Britain continued to conduct most of the work in the European/Atlantic Theater. They did agree, however, to share full collaboration on the German submarine problem. Britain did analyze Japanese codes, and the U.S. worked against German and Italian codes despite the agreement. However, the separation of emphasis worked effectively for the remainder of the war.

Just as the Navy drew up the contract with the National Cash Register Company to work on the production of the Bombe, Britain found a way into the four-rotor Enigma messages.

On October 30, 1942, two men from the HMS *Petard* gave their lives retrieving an Enigma and documents from a captured U-boat, U-559.

Several British ships located U-559 in the Mediterranean near Port Said. They tracked, followed, and depth-charged the submarine for hours. The last of more than 100 depth charges caused significant damage to the sub, and the U-boat commander, Hans Heidtmann, ordered the sub to surface. As the German crew abandoned the U-boat, the *Petard* ceased firing and pulled within sixty feet of the floundering craft. They prepared a boarding party. Lieutenant Anthony Fasson and Able Seaman Colin Grazier removed their uniforms and dove into the choppy waters. As they swam towards the conning tower, another young man, Tommy Brown (who had lied about his age to join the Royal Navy), followed.

When Fasson and Grazier reached the sub, they saw it was riddled with holes and taking on water. Quickly they climbed into the control room. Fasson broke into the captain's room and opened a locked drawer. He removed the documents inside and passed them to Tommy Brown, who had followed them down the conning tower. Brown climbed back up to deliver the secret documents to a waiting whaler that had rowed over from the *Petard*. He made the trip again to retrieve more materials Fasson and Grazier had found. The water rapidly filling the sub, he returned for a third trip even as those on deck called for the men to come out. Fasson refused to leave without the box he desperately tried to pry free. It contained what appeared to be important equipment. Tommy Brown carried out one last batch of papers, but did not go down again. Fasson and Grazier finally released the box and tied it to a line to be hauled out of the sub. Brown called down to them twice, "You'd better come up." Just as the men began to climb up the conning tower, the sub suddenly sank. Brown and the others on deck jumped off and were picked up by the whaler. However, Anthony Fasson and Colin Grazier did not make it out of the sub. Their loss was not in vain, for the material they collected in turn saved the lives of many Allied and German men.

The documents Tommy Brown transferred from U-559 proved vital to the cryptanalysts at Bletchley. They included codes for the Short Weather Cipher and the Short Signal Book. The books, combined with a German communications security error, allowed the British to find a break in the four-rotor messages. The Germans' shore weather stations could read only a three-rotor message. On December 13, 1942, the British team discovered that when the U-boats sent weather messages, they set the fourth rotor into a neutral position. This caused the machine to mimic a three-rotor Enigma. BP needed only to find the three-rotor settings in the usual manner. To find the daily setting of the fourth rotor for nonweather "Shark" messages, they then tested each of the twenty-six places on the fourth rotor.

Suddenly, BP could read "Shark" messages with a slight delay. The actual results were usually delayed thirty-six hours on 70 percent of the days,[16] but were occasionally delayed as long as ten days.[17] Nonetheless, GC&CS was quite pleased with its accomplishment. Once again, the Allies could track the German U-boats with a fair degree of accuracy. For the next several months, the Allied ships played a cat and mouse game with the German U-boats. As BP learned of the subs' locations, ships were rerouted to avoid them. The B-Dienst, reading the Allies' convoy cipher, then rerouted their subs. And again, the Allies altered their shipping route. Across the Atlantic, ships and submarines moved and countermoved, interspersed with attacks.

However, delays in reading Enigma messages resulted in Allied losses. The U.S. Navy, convinced the Bombe designed by Joseph Desch would dramatically reduce the delay, continued its plans to build a high-speed four-rotor Bombe.

Bletchley Park sent Alan Turing to OP-20-G as an advisor in December 1942. Turing viewed the facilities in Washington, D.C., and the Bombe production building in Dayton, Ohio. He was not overly impressed with the American design. "The British didn't believe I would be successful," Joseph Desch later mentioned in an interview. "After the war, [the Navy] showed me the [British] reports and they weren't very complimentary." [18] In Turing's report on his visit he says, "It seems a pity for them to go out of their way to build a machine to do all this stopping if it is not necessary." [19]

Despite Turing's opinion, the Navy moved forward with its plans. In April 1943 Navy personnel began arriving at the National Cash Register Company in Dayton. Eventually 200 sailors and 600 Waves[20] worked with the NCR civilians to build the Bombes. To explain the sudden influx of sailors and Waves, the official story claimed personnel came for training on tabulating machines. One sailor, Robert Shade, recalls that "Our standard explanation was we were looking for submarines on the Miami River in a rowboat."[21] In truth, even the sailors and Waves didn't know what they were working on. Bob Atha, a sailor in Dayton, said, "The exact function of the Bombe equipment was not explained to me. Because of the strict need-to-know practice imposed, this total knowledge was probably known to only a few analysts and design engineers." [22]

The work Joseph Desch did was so secret Navy security personnel followed him to and from work. He wasn't supposed to know about the extra protection, but he realized he was being followed. On one occasion, Mr. Desch took his guards on a roundabout route, only to return home without making any other stops. On another occasion he cheerfully waved to the secret men in the car outside his home. They never acknowledged his greeting.[23]

Because of the secrecy of the work, Waves had to show their identification to the Marine standing guard. Marines guarded the different rooms inside the building as well. Waves were not allowed to see any other rooms unless they could prove to the Marine they had a reason to go inside. "We only knew what was being done in our assigned work area, but we never were told the implications or the importance of our work. We had no knowledge that the Bombe was being conceived and built directly over our heads on floor two. There were always armed Marine guards who saw to it that no one strayed from their assigned work space," recalled a former Wave, Sue Eskey.[24]

Waves were also not allowed to discuss their work with anyone outside their specific assignment and never outside of the building. Even the women working together rarely speculated about the purpose of the job. Sue Eskey suspected that the twenty-six wires she soldered corresponded to the alphabet. Later she remembered, "If you had any intuition or deep thoughts about it you could sort of figure it out. I knew nothing about codes or anything, but I had that thought. And, of course, I didn't share it with anyone because we were not allowed to talk about anything." [25]

The war did not stand still while the engineers, sailors, and Waves worked to build a machine to break the U-boat Enigma settings. The U-boats continued to stalk the Atlantic. Losses mounted, but the tide began to change in favor of the Allies. As the United States grew stronger, it began to extend its reach beyond simply defending and escorting the convoys of ships. It began to actively seek and attack the German fleet.

May 1943 proved to be a significant time in the Battle of the Atlantic. During May, the Allies inflicted more damage to the U-boats than any time previously in the war. Germany had more submarines prowling the ocean than ever before, but because the tide had turned, they sank only fifty Allied ships.[26] This was fewer than the previous month and significantly fewer than their victories in March. By the end of May, Allied forces sank 25 percent of the German submarines, totaling forty-one U-boats.[27] Admiral Doenitz conceded the North Atlantic to the Allies and began withdrawing his subs from the area on May 22.

This Allied victory did not put an end to the Bombe project, however. Admiral Doenitz concentrated his forces elsewhere in the Atlantic and continued to be a threat. The need to know where the submarines operated and in what strength was still imperative to U.S. and Allied plans. This had been proven on March 10 when the Germans began using a new edition of the weather short signal code. The new code made the second edition, captured from U-559, useless. In this case, the cryptanalysts were fortunate, for only nine days later they were able to make use of another U-559 captured codebook, the Kurzsignalheft, as cribs.[28] However, the incident emphasized how important it was to build a machine that was not dependent on captured material.

In fact, by the end of June, the only way to break into the "Shark" messages was by machine. The British, by this time, managed to modify their three-rotor Bombe to accommodate the fourth rotor. However, it required the use of an existing three-rotor machine, thus depriving BP of Bombes needed for Army and Air Force messages. The U.S. Navy Bombe was needed.

Construction of the Bombes proceeded in National Cash Register's Building 26 in Dayton. Newly arriving Waves learned soldering, how to read electrical graphs, and the general aspects of an electrical education. After that the Waves' daily routine included eight hours of soldering wires. Three shifts of women worked throughout the day: 8:00 A.M. to 4:00 P.M., 4:00 P.M. to midnight, and midnight to 8:00 A.M. Each woman was given a graph to follow and several different pieces of colored wire. They didn't know it at the time, but the Waves were wiring rotors to match those on the Enigma machines.

National Cash Register's assistant engineer, Robert Mumma, played a role in helping to keep the wiring secret. He designed the graphs the women followed and selected the colors of the wires. To make it more difficult for a woman to recall the wiring system, he selected colors from a choice of twenty-eight, not twenty-six. He also labeled the commutators and graphs zero through twenty-five rather than one through twenty-six.

The work was tedious and the hours tiring. For her eight-hour shift, a woman wired rotors. When she finished one rotor, another was immediately placed before her. Over 6,000 rotors had to be wired to meet the necessary initial requirements for the Bombes. Also, additional rotors would be needed as replacements. Wave Ronnie Mackey Hulick believed she had failed the battery of tests she had taken when she first entered the service. Surely this was why she had been relegated to such a monotonous task. The importance of the work became apparent only when the Navy transferred her to Washington, D.C., to operate the Bombes.[29] Wave Jimmie Lee Long agreed: "The work at NCR was tiring and there was no room for the slightest mistake. Now I understand why." [30]

Other Waves and the sailors sent to Dayton constructed the rest of the Bombe. They completed the prototypes, named Adam and Eve, around May 1. Members of the maintenance crew, Radio Technician Phil Bochicchio and Radioman K.P. Cook, began working on the machines. They checked the wiring and fixed the oil leaks. After three weeks of inspections, the Bombes were finally ready for operational test runs.

Cryptanalysts in Washington forwarded set-up instructions to Dayton. Like the British Bombes, the American machines required assumed text for

cribs. The assumed message corresponded to the cipher and created the settings for the Bombe.[31] These menus gave Phil and K.P. instructions for setting the dials and rotors on the machines.

On May 28, 1943, on the second floor of NCR's Building 26, Phil made a run on Adam. He set the dials and rotors following his assigned menu. Then he flipped the switch that set the Bombe in motion. The rows of black Bakelite rotors began to spin through each of the twenty-six positions of each commutator. A loud, rapid clicking noise emanated from the huge, gray machine. Then the machine slowed, stopped, slowly reversed, stopped again, and printed out some results before returning to its original forward motion. After only twenty minutes the two-ton "gray elephant" came to a complete stop.

Radio Technician Bochicchio didn't know what the numbers on the printout represented. He ran the settings again to double-check it. Adam repeated its actions, printing out exactly the same results. Calling over to his buddy, K.P., Phil showed him what the Bombe had done. K.P. didn't know what the results were either, but they agreed to try the run on Eve. K.P. reset his machine's wheels and dials to match the settings on Phil's menu. Eve duplicated Adam's actions, stopping and printing the same results. If nothing else, the two machines were performing identically.[32]

The men took the printout to Lieutenant Commander Meader. The commander also did not understand the meaning of the printout, but instructed the sailors to send it to Washington.

A secure communications line had been set up between National Cash Register and Naval Communications in Washington, D.C. The results of Adam's run were sent to Commander Engstrom, head of the OP-20-GM, a technical branch of Naval Communications. A few days passed before Engstrom replied: "That one hit paid for the entire project." [33] At that time he couldn't explain why, but the sailors learned the importance of the printout a few months later when they returned to Washington. Engstrom told them that based on the rotor settings Adam provided, the cryptanalysts in Washington broke a German U-boat message. The message revealed the location of submarines refueling at sea. As a result, the Allies attacked the "milk cow" and sank three subs.

Which subs the resulting message actually referred to cannot be verified, but beginning with the sinking of the supply sub U-118 on June 12, the U.S. Navy waged an all-out assault on German submarines refueling. During the summer of 1943, the Allies sank nine of twelve U-tankers. By removing the supply subs from action, the combat U-boats could no longer roam as far or as long as Admiral Doenitz had originally planned. How large a role radio intelligence played in these sinkings is debated; certainly it contributed.

It was, then, the offensive use of radio intelligence, the increased number and perfected technique and teamwork of carrier task groups, and the greater effectiveness through the improved radar and extended ranges of land-based [aircraft] that accounted for the destruction of the German refueling fleet in the year beginning in June 1943.[34]

Since Adam and Eve successfully proved that the American-designed Bombes could rapidly find the four-rotor Enigma settings, construction on the Bombes continued in Dayton throughout the summer. Initially there had been some discussion about where the Bombes should be permanently located. If the Bombes stayed in Dayton, they would be near the engineers. Design changes caused by German upgrades to the Enigma, as well as routine maintenance, could be more easily implemented in Dayton. However, it was felt that Dayton was too far from those needing the information the Bombes produced. The vice-chief of Naval Operations ruled that the Bombes must be operated in Washington.[35]

By the summer of 1943, construction on the new buildings to house the Bombes in Washington had not been completed. But in Dayton there would be no delay in Bombe construction or use. The machines began to line the hallways and stairwells of NCR's Building 26.[36] In one small room, on a few operational Bombes, some of the Waves learned to operate the machines based on the cryptanalysts' menus. Although the machines were not fully operational, menus and results crossed the secure communication lines between Dayton and Washington throughout the summer. Finally, at a rate of four per week, U.S. Navy cryptanalytic Bombes began arriving at the Naval Communications Annex on Nebraska Avenue in Washington, D.C. Building 4 was still incomplete when Radio Technician Phil Bochicchio arrived to install the machines. The roof on the second floor, where he set up the first of the Bombes, was just a tarp. It was enough, though, and only temporary.[37]

Other naval personnel transferred from Dayton to Washington with the machines, leaving only a handful in Dayton.

Originally a girls' school, the Naval Communications Annex on Nebraska Avenue in Washington, D.C., once again saw women cross its grounds. Waves returned from Dayton to newly built quarters. Other Waves just coming into the service joined them, and together they spent untold hours secretly fighting the Germans.

When the women arrived at their new station, they were taken to the chapel on the grounds of the Annex. An officer impressed upon them the importance of their work and the seriousness of dealing with classified material. This was followed by another officer many women thought to be the chaplain. Expecting to receive a benediction, the Waves were surprised to be told, "If you ever tell what you are doing, you are committing treason. And don't think that just because you are young ladies you will be treated any differently than the men who commit treason. If you ever tell, we will shoot you!" [38]

Having received their security briefing and greatly impressed with the need for secrecy, the Waves then went to work. Rows and rows of Bombes filled the newly constructed Building 4. Eventually, 121 Bombes would be built in Dayton and housed in this facility on two floors. Divided into bays of four Bombes, each bay required four operators and a supervisor. All of the Bombe operators were Waves. Operators conducted tests on the Bombe before each run, set the Bombes according to the menu, and passed the results back to supervisors for checking. The supervisors assigned each menu, helped with the set-up, checked results, and covered during meals and breaks. Three different shifts worked throughout the day and night to keep the Bombes in constant use.

The American Navy Bombes stood seven feet high, two feet wide and ten feet long. Each weighed 5,000 pounds. The front and back of the Bombes each had eight columns of four rotors. The top wheel mimicked the Enigma's new fourth rotor while the bottom commutator represented the rightmost, or fastest, rotor of the Enigma. The bottom rotor spun at a speed of 1,725 revolutions per minute,[39] which allowed the machine to complete its run in only twenty minutes.[40]

Like the British Bombes, the rotors spun through each of the possible rotor settings. At each contact point an electrical current tried to complete the path required in the menu. Those that could not were discarded. When the machine did locate a complete circuit, it was moving too quickly to stop at

the correct location. It took three and a half to four more rotations before the machine could bring itself to a stop.[41] In order to remember where the hit occurred, the U.S. Navy Bombes had "memory" in a unit called the Thyratron chassis, invented by Joseph Desch. After braking, the Bombe automatically reversed itself and returned to the correct position of the hit.

Unlike the British Bombes, the American Navy Bombes printed out the strikes automatically. They then returned to the forward motion to continue scanning for other workable circuits. Like the British version, the American Bombes usually found two or three possible correct solutions.

After twenty minutes, the machine came to a complete stop, and the Wave operator gave the printout to her supervisor. Each bay had a small machine officially called an M-9, but better known as a "checker" to the Waves. It didn't resemble an actual Enigma in appearance, but when hand-stepped, did repeat the results of an Enigma. Because the menus used on the Bombes consisted of only fourteen letters, the Bombe could not find all the Stecker combinations. The supervisors used the M-9 not only to verify the results, but also to find the remaining plugboard connections. The supervisors then took the valid, complete results to an open room at the back of the Bombe deck where three loggers and the watch officer worked. After being logged, the results were sent back to the cryptanalysts.

Cryptanalysts received the Bombe results via a pneumatic tube system. Some of the Waves used the same M-9 machines to actually decrypt short German messages. They transferred longer messages to paper tape and ran them through an M-8. The M-8 was actually a converted U.S. encryption machine known in the Navy as an E.C.M.[42] The M-8 used rotors wired to match those on the Enigma. When cryptanalysts fed the paper tape into the machine, it automatically decrypted the message and printed it out in German. Linguists in another office translated the messages into English for use by the military commanders.

In some cases the Germans double-enciphered messages. They altered the message using a specific codebook before they actually enciphered it on the Enigma. This required additional cryptanalysis by the Allies before a message could be read. To break these messages, cryptanalysts used a captured or reconstructed codebook to strip off one layer of encryption. They could then proceed in the normal routine to retrieve the actual communication.

By the close of 1943, seventy-seven of the requested ninety-six Bombes ran continuously at the Naval Communications Annex. More machines continued to arrive throughout 1944. Improvements made to the standard N-530 resulted in the N-1530. Dayton personnel also built and sent other variations of the Bombe to Washington. These machines worked on other specialized Enigma-type problems. Throughout the remainder of the war, as the Germans altered their Enigmas, the U.S. Navy and National Cash Register kept pace.

With only eighteen four-rotor machines built, and only three of those running routinely, Britain's four-rotor Bombe project never met expectations. In fact, the U.S. Navy cryptanalytic Bombes proved so successful that Britain gave up production of its four-rotor Bombes. In a dispatch to the U.S. Navy, Britain admitted, "Performance of our machine is still poor and likely to remain so. In view of your 4-wheel capacity being more than adequate, priority is being given here to the production of new 3-wheel machines." [43] The U-boat problem fell exclusively to the United States Navy.[44]

By the spring of 1944, ninety-six operational Bombes routinely broke the U-boat messages. The average delay in breaking the daily key settings was only twelve hours. As a result, the Navy could read all the Atlantic U-boat messages sent in the latter half of the day at the same time as the Germans. "In fact, during these hours the translation of every message sent by a U-boat is at hand about twenty minutes after it was originally transmitted." [45]

Once the Bombes retrieved the daily U-boat keys, the machines were then set to search for non-naval settings. So many messages came out of Europe that even Britain's highly effective three-rotor Bombes couldn't keep up. Approximately 55 percent of the opera-tional time on an American Bombe was dedicated to naval keys, the remaining 45 percent on non-naval, under the direction of the British.[46]

To further improve the system, the British requested that the U.S. Navy manufacture fifty additional four-rotor Bombes. Their request was more to further the work done on German Army and Air Force messages than to increase the efficiency of the German naval problem. However, in early September 1944 NCR had completed only twenty-five Bombes, and the Navy determined that "Current rapid developments in the prosecution of the war have made it unnecessary to complete the remainder of the fifty (50) additional Bombes." [47]

Certainly, one of the developments that aided in the "prosecution of the war" was the advance knowledge of U-boat locations and activities. Because of the information learned from Enigma messages, the Navy's ability to destroy the submarines increased significantly. By the end of the war, the United States sank or captured ninety-five German U-boats.

Dedicated to Keeping the Secret

Because the U.S. Navy, like the British, went to great lengths to disguise the source of their information, very few ever knew of the cryptologic contribution. The dedicated men and women working in OP-20-G played an important role in maintaining one of the best-kept secrets of World War II. Threatened with death if they spoke of their activities, and reminded of their oath when they were discharged from the service, these Americans did not reveal their war work to anyone.

In 1974 F. W. Winterbotham, a former group captain in the Royal Air Force, wrote about the work done at Bletchley Park. This was well before the United States planned to declassify the Enigma secret, but the story was out. Slowly, the United States began to reveal its information and role in the Allies' cryptanalytic successes. However, notifying the thousands of men and women involved in the project more than thirty years later was impossible.

Nearly fifty years after the war, during a vacation to Washington, D.C., former Wave Sue Eskey learned the Bombe had been declassified. As many tourists do, she walked into the Smithsonian's National Museum of American History. Upon finding an exhibit that included an actual Bombe and picture of a Wave, she blurted out, "My God! That's me! I'm on the wall of the Smithsonian Institution!" [48] Later that day she called one of her Wave friends with whom she'd remained in contact. Feeling almost guilty for speaking of it over the phone, she told her friend what she'd seen.

Unfortunately, many of those involved passed away before they were able to tell their stories. Joseph Desch never explained to his family what a major role he played in winning the war against the Germans by designing the American Bombe. Alan Turing, designer of the British Bombe, died before the secret had been disclosed. Jerzy Rozycki, one of the first three Polish mathematicians hired to work against the Enigma in 1932, drowned when the ship he was on sank in a storm, possibly after hitting a mine, in 1942. The loss of their experiences is great. But through the memories of

those who survive, the story of the Bombe and the people involved with it is now told.

Some historians claim that World War II could have gone on for as much as two more years, with an untold loss of life, had it not been for the Allies' ability to read Enigma messages. Those messages could not have been read without the Bombes and the men and women who built and operated them.

Jennifer E. Wilcox
January 2001

Notes

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 6812^{th}.

3. Each rotor on an Enigma can be set in any one of twenty-six positions (1-26 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'." (6812^{th},10.)

5. Traffic analysts look at information outside of the actual message text such as the unenciphered headers prior to the message, time of transmission, and the frequency used. With this type of information, traffic analysts can reconstruct an enemy's communication network and hierarchy.

6. Britain called their sheets "Jeffreys sheets" after John Jeffrey, who was in charge of manufacturing the stacks of perforated papers.

7. Some people, not knowing the Bombe's Polish history, suggested that the name for the British Bombe came from the sound the machines made as they ticked their way through the possible rotor settings, like an old time-bomb ticking. However, Gordon Welchman, in his book *The Hut Six Story* (McGraw-Hill, 1982, 77), says, "Our bombes [the British versions] were said to make a noise like a battery of knitting needles." U.S. Navy Wave Veronica Mackey Hulick, who operated the American crypt-analytic Bombes, agreed that "the noise from the Bombe was like thousands of clacking knitting needles." However, CDR McDonald, a Bombe watch officer, doesn't recall a clicking sound, but remembers it made a lot of loud noise.

8. Because there were several different models used throughout the war, the speed of the machine varied depending on the model. This speed (50.4 rpm) refers to the British 39-point machine. (Correspondence to the author from John Harper, Bombe Rebuild Project Manager, Bletchley Park Trust. 12 February 2000.)

9. Leo Rosen and William Friedman, "Cryptanalysis of German Army & German Air Force ENIGMA Traffic" SSA (report on) "E" Operations of the GCCS At Bletchley Park, 1945, 59. (NARA Record Group 457; File #3620.)

10. Memorandum from OP-20-G, "Brief Resume of Op-20-G and British Activities vis-à-vis German Machine Ciphers," July 15, 1944, 1.

11. Anderson, Deborah, "Joseph Desch and Magic," *Miami Valley History* (1993), 11.

12. Ibid.

13. J.N. Wenger, H.T. Engstrom, and R.I. Meader, "History of the Bombe Project," OP-20-G Memorandum dated 30 May 1944, 2 (NARA Record Group 457, File #4584.) Hereafter referred to as *Bombe History*.

14. "E" refers to the Enigma problem. (Ibid., 6.)

15. *Bombe History*, 2.

16. Memorandum from OP-20-G, "Brief Resume of Op-20-G and British Activities vis-à-vis German Machine Ciphers," July 15, 1944, 2.

17. Beesly, Patrick, "Ultra and the Battle of the Atlantic: The British View," *Cryptologic Spectrum*, v.8 n.1 (Winter 1978), 7.

18. American Federation of Information Processing Societies, *Computer Oral History Collection, 1969-1973*, 1977. Interview with Joseph Desch and Robert Mumma. (Washington D.C.: Archives Center, National Museum of American History), 116.

19. *Bombe History*, 7.

20. Waves were women in the U.S. Navy. The acronym WAVES stood for Women Accepted for Volunteer Emergency Service.

21. Correspondence to the author from Robert Shade, February 11, 2000.

22. Atha, Bob, "The Electro-Mechanical Marvel," *U.S. Naval Cryptologic Veterans Association* (Paducah, KY: Turner Publishing Co., 1996), 60.

23. Anderson, Deborah, "Joseph Desch and Magic."

24. Correspondence to the author from Sue (Sadie) Unger Eskey, December 20, 1999.

25. Dalton, Curt, *Keeping the Secret: The WAVES & NCR* (Dayton, OH: self-published, 1997), 21.

26. Winton, John, *Ultra at Sea* (New York: William Morrow and Co. Inc., 1988), 146.

27. Helgason, Gudmunder, editor, *U-boat Fates: The Guide to all U-boat Losses*, http://www.uboat.net/fates/may43.htm 1999.

28. Erskine, Ralph, "Naval Enigma: The Breaking of Heimisch and Triton," *Intelligence and National Security*, v.3 n.1 (January 1988), 171-172.

29. Conversation between Veronica Mackey Hulick and the author, March 28, 2000.

30. Dalton, Curt, *Keeping the Secret*, 22.

31. For an explanation of cribs, menus, and Bombe set-up, see Appendix I.

32. Conversation between Phil Bochicchio and the author, March 20, 2000.

33. Ibid.

34. *Battle of the Atlantic: Vol. II U-boat Operations*, National Security Agency SRH-008, 1945, 127.

35. *Bombe History*, 6-7.

36. Conversation between Phil Bochicchio and the author, March 20, 2000.

37. Ibid.

38. Correspondence to the author from Sue (Sadie) Unger Eskey, December 20, 1999.

39. Conversation between Phil Bochicchio and the author, November 26, 1999.

40. M-7, M-8, M-9 Devices and CSP-890 (A) "*The Standard #530 Bombe*," (NARA Record Group 457, File #1738.)

41. Notes on the chassis of the Bombe by Phil Bochicchio, undated, "Bombe" files of the National Cryptologic Museum.

42. E.C.M. expands to Electromechanical Cipher Machine. An identical machine was used in the U.S. Army and was known as SIGABA (which doesn't expand to anything).

43. *Bombe History*, 10.

44. The U.S. Army also had a Bombe project, but it was not built to deal with the U-boats' four-rotor messages. For a brief description of the Army machine, see Appendix II.

45. Memorandum from OP-20-G, "Brief Resume of Op-20-G and British Activities vis-à-vis German Machine Ciphers," July 15, 1944, 3.

46. *Bombe History*, 9. However, the memo "Brief Resume of Op-20-G and British Activities vis-à-vis German Machine Ciphers," 3, cites the figure as 40 percent naval and the remaining 60 percent on German Army and Air Force. The memo is dated only six weeks after the *Bombe History*, so it is possible the efficiency improved.

47. Memorandum from OP-20-G, "Contract NXs-7892 - Curtailment of," September 8, 1944.

48. Cummings, James, "A Salute to the Waves," *Dayton Daily News,* September 10, 1995, City p.1E.

Appendix I

Cribs, Menus, and Bombe Set-Up[1]

In order to set up the U.S. Navy Bombe, cryptanalysts first had to determine a "crib." A crib is the unenciphered text that is assumed, or known, to appear in the message.

Cribs could come through a variety of methods. Some of the best cribs came from errors made by the Germans themselves. On more than one occasion, a German signal clerk sent the same message twice in two different codes. If the code for one was known, it provided a crib for the unknown system.

Another frequent German mistake came in standardized messages. For example, a shore weather station in the Bay of Biscay sent out a message every day at 7:00 A.M. which began, "The weather in the Bay of Biscay will be. . . ." [2] Knowing the exact wording of a message made a perfect crib for the Allies, so it became a high priority to intercept the daily message from this weather station.

A final example of a common German error involved the practice of submerged U-boats. When the submarines resurfaced after extended periods of time under water, they requested all the important messages they had missed while below the waves. The transmissions that followed inevitably involved communications previously sent and deciphered. Cryptanalysts merely checked the back files for messages with the same number of letter groups and used them as cribs for the new message.[3] Since the resulting message would be identical to the previous one, it helped reveal the Enigma setting for the current day. With the daily setting, all the current day's messages could be read.

Other cribs came from knowing the current activities of the enemy. If, for example, a battle occurred, it could be assumed that messages following the attack reported on the battle. It was more difficult for the cryptanalysts to build cribs for these types of messages since it involved guesswork.

Cryptanalysts also needed to know

- how the Enigma worked,
- what was not possible on the machine, and
- the Germans' standard practices.

Because the Enigma rotors moved with each keystroke, a letter typed twice usually enciphered to two different letters. Also, the Enigma could not encrypt a letter to itself. Finally, the Germans indicated a space between words with the letter X and spelled out numbers.

Knowing these details played an important role in ultimately breaking the Enigma's daily settings.

To better understand the process of developing a crib and a Bombe menu, we'll use an example. The cryptanalyst knows that two Allied pursuit planes attacked U-boat 66, commanded by Kapitanleutnant Friedrich Markworth, at 2130 hours. Shortly afterwards, Markworth sent an encrypted message. The cryptanalyst assumes the message includes the following:

Assumed text: MARKWORTHXATTACKEDXBYXTWOXPURSUITXPLANESX

(To make it easier to follow the example, the assumed plain text will be in English. Cryptanalysts during World War II would have used cribs in German.)

Part of the intercepted message includes the following cipher text:

VWHCD IUGHL UVFAO BNEWN AGZWY ZUXNN PYZWN LKMUO FRIIL OJPAE

The cryptanalyst begins by lining the assumed text beneath the cipher and looking for links that violate what is known about the Enigma.

Cipher:	V	W	H	C	D	I	U	G	H	L	U	V	F	A	O	B	N	E	W	N	A	G	Z	W	Y	Z
Crib:	M	A	R	K	W	O	R	T	H	X	A	T	T	A	C	K	E	D	X	B	Y	X	T	W	O	X

Lining up the assumed text with the beginning of the cipher results in several incorrect links. The first is the *H* in Markworth which ciphers to an *H*. Since the Enigma cannot encipher a letter to itself, this is not a valid comparison.

In this example, the cryptanalyst finds only one possible position for the alignment without a letter encrypting to itself.

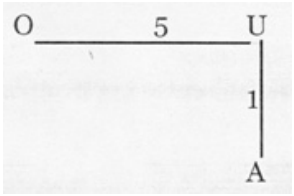
Position:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Cipher:	I	U	G	H	L	U	V	F	A	O	B	N	E	W	N	A	G	Z	W
Crib:	M	A	R	K	W	O	R	T	H	X	A	T	T	A	C	K	E	D	X

The next step in developing a menu to set up the Bombe is to diagram the links. The diagram shows the relationship of letters and their position in the message to other letters.

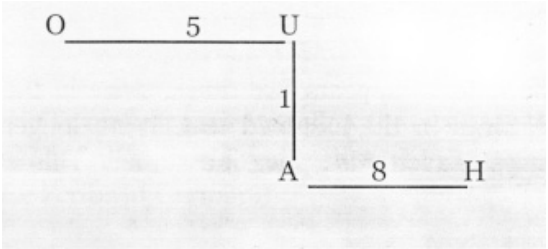
In our example the letter *A* appears five times, twice in the cipher text and three times in the assumed text. It no longer matters to the cryptanalyst if a letter is cipher or assumed. This is because an *A* enciphering to a *U* at a specific rotor position deciphers a *U* to an *A* at that same rotor position. The letters are linked at that position. What becomes important is the link between a cipher and its plaintext letter. From now on the two remain associated, and their position within the message is noted.

For example, in position 1 the *A* is linked to the *U*. This link is diagrammed.

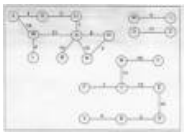
Next, the cryptanalyst looks for other links that contain either *A* or *U*. At position 5 the *U* is linked to the *O*. Working off the A/1/U link, the U/5/O link is added to the diagram.



A has another link at position 8 to an *H*. A/8/H can be added to the diagram.



This process continues until all links and connections have been diagrammed. Our example results in the following diagrams:



The purpose of diagramming the message is to determine if it contains any "closures." Even though the crib may be correctly aligned, without these "closures" the Bombe will find too many hits, making it difficult to determine the Enigma's settings.

A closure occurs when links circle back. The loops become obvious when diagrammed. In our example, A-H-K-A is one closure and A-U-O-X-W-A is another. The Bombe required two such closures in order to disprove thousands of possible settings. It also required a total of thirteen or fourteen links.

Having determined that our example has the two required closures, the cryptanalyst moved on to the next step: number transposition.

Changing the letters into numbers was primarily a security measure. Numbers and their associated letter were harder to recall, especially since the A equated to zero instead of one.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

The example message transposes to

Position:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Cipher:	8	20	6	7	11	20	21	5	0	14	2	13	4	22	13	0	6	25	22
Crib:	12	0	17	10	22	14	17	19	7	23	0	19	19	0	2	10	4	3	23

The final step transfers everything onto the appropriate form. The form tells the Bombe operator how to set the Bombe's dials and rotors. Since there are only sixteen sets of dials and rotors on the Bombe, the menu cannot include all nineteen links in our example. However, it must include the links involved in both closures.

According to our diagram, there are two sets of links that have no other connections. The link M-I at position 0 and D-Z at position 17. Leaving these two off the menu still gives us seventeen links. At least one more must be eliminated to fit the Bombe's sixteen sets of rotors. Another link that can be discarded is located at position 4, L-W. Since the L links only to the W and nothing else, it is unnecessary in our menu. All of the other links can be transferred to the form, although only thirteen or fourteen links are required.

The menu form referred to cipher and assumed letters, now transposed into numbers, as "Switch In" and "Switch Out." There are four wheels to mimic the four-rotor Enigma. However, the first three wheels were normally set to zero to begin a run. The last wheel, the bottom rotor on the Bombe, was placed at the position the accompanying link appeared in the message with respect to the previous link. The first switch bank's wheel settings are always 0-0-0-0, regardless of that link's position in the message. The wheel settings for switch bank 2, in this example, are set to 0-0-0-1. Link 6-17 is only one position away from Link 20-0. However, switch bank 4 has a wheel setting of 0-0-0-4 (instead of 0-0-0-3) because Link 14-20 is two positions away from the previous Link 10-7.

The transposed message portion would not appear on the form, but for clarification it is shown here.

Position:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Cipher:	8	20	6	7	11	20	21	5	0	14	2	13	4	22	13	0	6	25	22
Crib:	12	0	17	10	22	14	17	19	7	23	0	19	19	0	2	10	4	3	23

Switch Bank	Switch In	Switch Out	Wheel Settings 1	2	3	4
1	20	0	0	0	0	0
2	6	17	0	0	0	1
3	10	7	0	0	0	2
4	14	20	0	0	0	4
5	17	21	0	0	0	5
6	19	5	0	0	0	6
7	7	0	0	0	0	7
8	23	14	0	0	0	8
9	0	2	0	0	0	9
10	19	13	0	0	0	10
11	19	4	0	0	0	11
12	0	2	0	0	0	12
13	2	13	0	0	0	13
14	10	0	0	0	0	14
15	4	6	0	0	0	15
16	23	22	0	0	0	17

Since the cryptanalysts had no way of knowing which rotors the Germans had selected for use that day, each combination of rotors had to be checked. The order the rotors should be placed on the machine was known as a wheel order. Supervisors received blocks, or groups, of wheel orders and

assigned one to each Bombe operator. The wheel order told the Bombe operators which rotors, I-VIII, to put on the machine and in which order they should be placed top to bottom. After a completed Bombe run, the wheel orders changed. But to keep things efficient, efforts were made to keep the number of rotor changes on a Bombe to a minimum.

It took a Bombe operator only ten minutes to set the Bombe according to the menu. Once complete, a supervisor checked it, and then the operator turned the machine on. It ran for twenty minutes, looking for the electrical pathways that allowed each of the conditions listed on the menu to be true. Any pathways that fit the menu caused the Bombe to stop and print out the rotor settings, wheel order, and stecker connections at that point. When the Bombe completed its run, the Bombe operator handed the results to the supervisor and began setting the machine with the next wheel order. Twenty-four hours a day, every day, operators used the Bombes to search for Enigma settings, playing a major role in winning the Battle of the Atlantic and World War II.

Notes

1. Much of the information used in this appendix came from CDR Gilman McDonald, USNR (R), who was a senior watch officer of Bombe operations at Nebraska Avenue.

2. Conversation between former Wave Judy Parsons and the author, 1999.

3. Ibid.

Appendix II
U.S. Army Cryptanalytic Bombe

The following description is from a "Tentative TOP SECRET Memorandum for OP-20" dated 12 February 1945.[1]

Subj: Op-20-G and S.S.A.[2] Bombes, Comparison of.

1. In accordance with your request, the following comparison of the Op-20-G and the S.S.A. Bombes is submitted.

2. The Op-20-G Bombes were constructed at the U.S. Naval Computing Machine Laboratory. A total of 121 Bombes were assembled at a cost of about six million dollars. The mechanical portion of the unit consists of 16 Enigma equivalents consisting of a set of 4 spindles and brush holders on which cross-wired wheels are loaded by hand. Automatic electronic detection is supplied on each Bombe of such a nature that only correct "stories" that satisfy all the restrictions of the "menu" are printed. A three wheel run takes 50 seconds and a 4-wheel run takes 20 minutes. Each Bombe is 8 feet long, 7 feet high and 2 feet wide.

3. The S.S.A. Bombe was constructed by the Bell Laboratories at a cost of from one to one and one-half million dollars. It consists of a telephone exchange type of installation with a total of 144 relay equivalents of the Enigma and 12 control stations. Each Enigma equivalent is mounted on a rack approximately 7 feet long, 8 feet high and one-half foot wide. The 144 Enigma equivalents can be allocated in any desired manner to the control stations by plugboards. Wheel order changes are done by push buttons at the remote stations and can be changed in about 30 seconds. The other setup data must be placed individually on the Enigma banks on the floor. Normally, about 10 stations are running simultaneously and about 10 minutes is required for each station to run through a short 3-wheel run. Although the installation is slow and space consuming, it has definite advantages in rapid wheel changes, remote control, and flexibility for handling special problems.

4. The following table shows a comparison of various aspects of the two installations. Most of the figures given below are only approximations.

Feature	Op-20-G Bombes	S.S.A. Bombes
Total Machine Cost	6 million	1 to 1 ½ million
Number of Effective Machines	121 (4 wheel)	10 (3 wheel)
Typical Day's Output	40,000 short 3-wheel runs 1,000 long 4-wheel runs	1,200 short 3-wheel runs Long 4-wheel runs not possible.
Rate At Which Machine Tries Assumptions	20,280 [tries] per second	910 [tries] per second
Running Time	50 seconds per short 3-wheel run 20 minutes per long 4-wheel run	10 minutes per short 3-wheel run Long runs not possible
Operations Personnel	700	20
Maintenance Personnel	135	40
Total Number of Enigma Equivalents	1,936 wheel banks	144 Relay Banks
Type of Detection	Prints only correct "stories"	Prints all "stops" which are then hand tested to find correct "stories"

Respectfully,
J. N. WENGER

Notes

1. J.N. Wenger, "OP-20-G Memorandum" dated 12 February 1945, (NARA Record Group 457, File 35701.)

2. S.S.A. expands to Signal Security Agency, which was the name of the cryptologic section of the Army at the time.