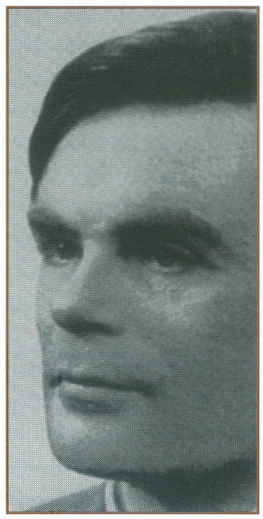
ALAN TURING, ENIGMA, and the BREAKING of GERMAN MACHINE CIPHERS in WORLD WAR II

By Lee A. Gladwin



OPPOSITE: *Compact, twenty-six-pound Enigma machines allowed mobile operation by land, sea, or air. One operator encoded as another copied the substituted letter from a lampboard. Encrypted messages were sent by radio.* RIGHT: *Alan Mathison Turing joined the Government Code and Cipher School at Bletchley Park, England, in 1939. He had written that a "universal machine" could simulate the behavior of any specific machine.*

Codes and ciphers were not new at the outbreak of the Second World War; the ancient Romans had used them. Augmenting human intelligence by technology can be traced to John Napier's invention of a calculating device in 1617 ("Napier's Bones"). Indeed, components of the computer (storage, processor, punch cards, and program) may be traced back to the "difference" and "analytical engines" of Charles Babbage in the early nineteenth century. It was only a matter of time before one machine called Enigma was applied to the creation of the "unbreakable" cipher, and another, the "bomba" or "bombe," to the formidable task of breaking that cipher.

The idea that one might construct a universal machine capable of simulating any other machine was introduced by the mathematician Alan Mathison Turing in his revolutionary essay, "On Computable Numbers" (1936). He maintained that "anything performed by a human computer [i.e., a human who worked with numbers] could be done by a machine."[1]

During World War II, the notion of a machine imitating another machine was to be implemented in the Polish "bomba" and British "bombe." These machines simulated the operation of multiple German Enigma cipher machines and allowed British intelligence to learn of German plans in time to thwart them on land, on sea, and in the air. The British later used Colossus, a prototype of the modern computer, to break messages simultaneously enciphered and transmitted over the Lorenz SZ42 teleprinters between Hitler and his generals. The intelligence reports based upon the breaking of the German ciphers by these machines were referred to as "Ultra intelligence." The fact that British intelligence was regularly breaking the German ciphers was termed the "Ultra secret." Ultra did not become publicly known until the 1970s, when some of the former codebreakers began to write about it. More recently, thousands of once-classified National Security Agency documents have been released. These documents reveal how machines were used to mechanize the basic intelligence functions of German cipher clerks and British codebreakers.

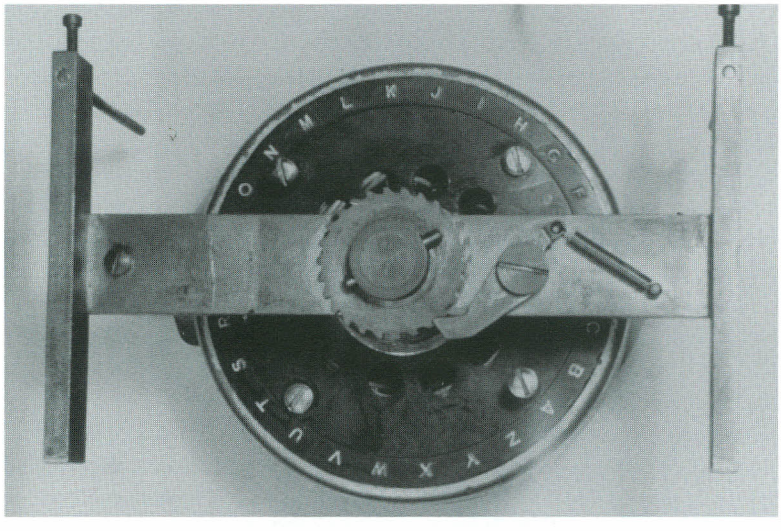
This article will describe the development of Enigma, the Polish "bomba," and its evolution into the Turing-Welchman "bombe" together with the Heath-Robinson and Colossus machines, which the British used to decipher the Lorenz SZ42 teleprinter codes. Finally, we shall consider the contribution of Ultra to the winning of the war in Europe, some hazards of substituting machine for human intelligence, and some implications of Turing's thesis for our postwar view of human and machine intelligence.

Enigma and the Polish Assault

Blitzkrieg, or lightning war, was a practice so revolutionary that the word was not even included in the 1939 edition of *Cassell's New German and English Dictionary.* After September 1, 1939, no dictionary could appear without it. The concept of *blitzkrieg* envisioned a short war won through the rapid onslaught of *Panzer* (tank) divisions supported by the *Luftwaffe* (German air force) and the speedy deployment of the *Wehrmacht* (army). An astonished world watched aghast as the German juggernaut routed the Polish cavalry and seized Poland in the space of twenty-seven days. There followed an uneasy period of quiescence, the "Phoney War." It ended with devastating suddenness on April 9, 1940, with the beginning of the spring offensive. Denmark surrendered within four hours of the German invasion. Oslo collapsed in a day; Norway, in thirty-two. Invaded on May 10, Holland surrendered after five days on May 14. Belgium held out eighteen days, finally capitulating on June 28. France, attacked on May 12, signed an ignominious surrender document on June 14 in the same train car in which Germany had sued for peace at the end of the Great War. Only Great Britain remained. But for how long?

Coordination and control of Germany's fast-advancing armies relied upon radio communications, but these Morse code messages could not be sent in clear, unenciphered text. The enemy might eavesdrop on these private exchanges between generals and armies or admirals and fleets. Code was required. Codebooks listed words to be used in place of those to be kept secret, but such books could fall into enemy hands, as indeed they had during World War I. (Unfortunately for the Germans, they did not discover that the British had been reading their messages until after the war.[2]) A way had to be found to encipher the coded messages, substituting one letter for another to produce the appearance of random gibberish. The method was a cipher machine called Enigma. The German military believed it to be impenetrable.

Enigma was patented in 1918 by German electrical engineer Arthur Scherbius, who offered it to the Imperial German Navy in the same year. Enigma was based upon the rotor principle of enciphering letters. It consisted of three rotors, each about four and a half inches in diameter with twenty-six letters arranged randomly around its circumference. There were, in turn, twenty-six corresponding electrical contacts just below the letters. Three rotors were placed inside the Enigma on a steel rod. When a typewriter key was pressed, the first rotor moved forward one notch, changing the circuit as a new contact was made and lighting up a letter on the lampboard or screen.



Enigma rotors, 4½ inches wide, had twenty-six randomly set letters and a battery connection for letter substitution in the coded message.

Assume the rotor was set at "A" before typing in text and that the text consisted solely of the letter "A" typed repeatedly. On the first occasion, the "A" key might light up the "H" on the lampboard; on a second occasion, "Y"; and on the third occasion, the "D." In fact, the rotor would have to revolve through the remaining twenty-five positions of the wheel before coming back to its starting position before an "A" would appear as itself; i.e., "A" would occur once in twenty-six rotations. Adding another rotor that rotated once whenever the first completed its cycle increased the possible circuit combinations to 26 x 26, or 676 letters. In this case, "A" would appear as itself only after depressing the "A" key 677 times! Each new rotor added a factor of twenty-six. "Four rotors produce a period of 456,976 letters; five rotors, a period of 11,881,376."[3] Small wonder that Scherbius boasted:

> The key variation is so great that, without knowledge of the key, even with an available plaintext and ciphertext and with the possession of a machine, the key cannot be found, since it is impossible to run through 6 billion (seven rotors) or 100 trillion (thirteen rotors) keys [rotor starting positions].[4]

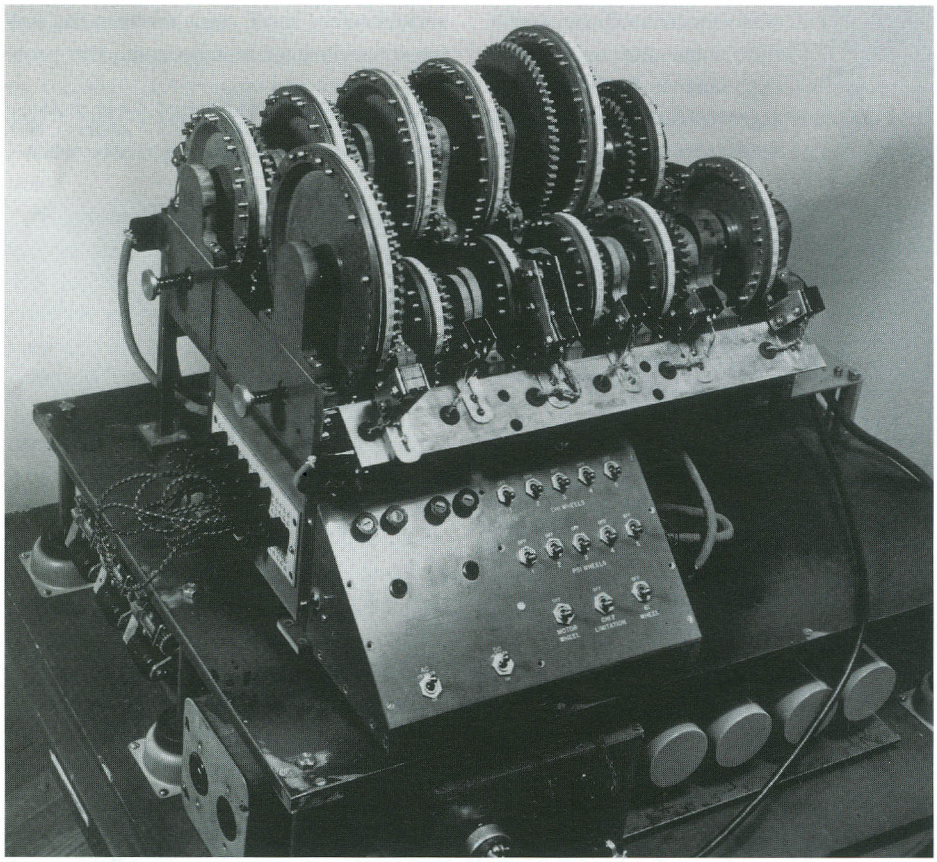
Prophetically, he added that "it would only make sense to search for a key . . . when it is known that unknown cryptograms have the same key. And when the same key is maintained for a long time."[5]

To read a message enciphered by Enigma required the recipient to calibrate his machine in exactly the same way as the sender, following the same codebook instructions. He then typed in the ciphertext. As each corresponding key was pressed, a letter lit up on the lampboard, revealing the original clear or plaintext.

Initially rejected by the German navy, Enigma was given a second chance when it was realized that codebooks were no defense against enemy cryptanalysis. A contract was signed between the navy and the *Chiffriermaschinen Aktien-Gesellschaft* to start production in 1925. A slightly altered version of Enigma was chosen for army use in 1928. About 1930, the twenty-six-socket plugboard was added to the front of the machine. Resembling a telephone switchboard, it allowed for short cables to be attached in such a way as to override the rotor substitution and make a different one; e.g., if the rotor settings produced a "K," the cable running from "K" to "X" changed the letter to an "X."[6]

This change vastly increased the invincibility of Enigma. The chance of an enemy cryptanalyst discovering the original settings (key) and deciphering German messages was one in billions!

At the same time that these changes were being made and the machine adapted for use by the German armed forces (the Luftwaffe adopted Enigma in 1935), other versions of Enigma made their way into the railroad administration, the *Polizei* (police), the *Abwehr* (military intelligence), *Sicherheitsdienst* SD (Nazi party intelligence service), the dockyards, and navy weather service.[7]



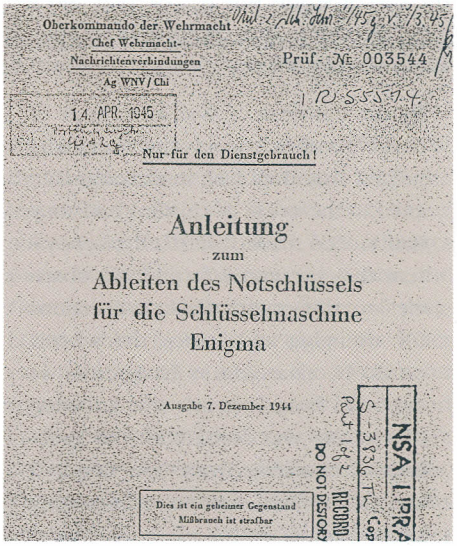
Bletchley Park-designed replicas of the German Tunny machines could be configured with newly discovered settings. Cryptanalysts could then decipher all of the relayed messages using those settings.

A Brief Introduction to the Intercepts

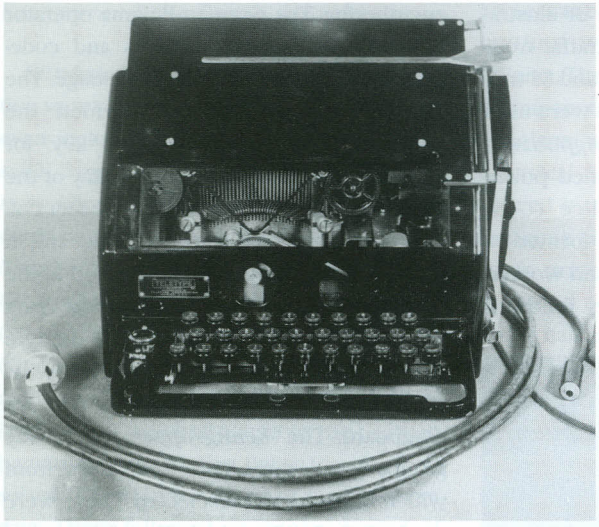
Before proceeding further with how the Enigma codes were broken after the fall of Poland, it may be well to look at the odyssey of a message from point of origin to its decipherment and translation at Bletchley Park. For the purpose of illustration, we will examine sample traffic from the German World War II police and SS traffic file.[8] These lower-level codes were used by the order police (*Ordnungpolizei*), which was made up of uniformed police (*Schutzpolizei*) and rural police (*Gendarmerie*). Police battalions formed a branch under the order police and worked in association with the SS. They followed the German army, and their chief functions were to round up, execute, or transport vanquished populations.[9] Police reports provided British intelligence with information about the effects of bombings as well as a variety of socioeconomic and industrial data.

A message might begin with an SS or police officer who handed a written plaintext message to three Enigma clerks for enciphering. The German Enigma operator worked from several manuals and codebooks in order to encode a message. The manuals and codebooks provided the Enigma operator with the day's "key" for configuring his Enigma. For each day of the month, the *Walzenlage* (wheel order) column told him which rotors to select and in what order to place them on the rod in the Enigma machine. The *Ringstellung* (ring settings) told him how to position the tyre (tire) on the side of each rotor. The *Steckerverbindungen* told him how to wire his plugboard. The *Kenngruppen* (daily key group) listed three-letter indicators from which one was to be selected. These were used to designate which "keys" or set of operator instructions the sender would use when sending the message.[10] He first typed in the coded message. As letters on the lampboard lit up, the clerk standing behind him called them out to a third clerk, who wrote them down for later transmission in Morse code by the radio operator.

The radio signals were picked up on the huge aerials at Chicksands (RAF), Chatham (army), and Beaumanor, an estate located in Leicestershire fifty miles north of Bletchley Park. Straining to hear the dots and dashes through her headset, the intercept operator recorded the wireless transmission on her Wireless/Telegraphy Red Form.[11] Basic information such as the date, radio frequency, time of transmission, and source "Police" were recorded, followed by the message in five-letter groups. Such


Oberkommando der Wehrmacht
Chef Wehrmacht-Nachrichtenverbindungen
Ag WNV / Chi
14. APR. 1945
Prüf-Nr. 003544
Nur für den Dienstgebrauch!
Anleitung
zum
Ableiten des Notschlüssels
für die Schlüsselmaschine
Enigma
Ausgabe 7. Dezember 1944
Dies ist ein geheimer Gegenstand
Mißbrauch ist strafbar
RECORD
DO NOT DESTROY
NSA

Enigma manuals contained the day's "key" for rotor rotation and circuitry settings. Safety measures included printing with water-soluble ink.



A teletype keyboard such as this one was attached to the Tunny machine to type messages to be enciphered.

Breaking Enigma—Early Polish Efforts

Poland's Cipher Bureau, so singularly successful in breaking German codes during and after the Great War, was confronted by something new and ominous in the German military messages broadcast on July 15, 1928. Frequency distributions of letters differed radically from previous naval messages. Repetition of letter groupings disappeared. Polish cryptanalysts were suddenly unable to read these early Enigma-produced messages. Within a few months of this discovery, a commercial version of the Enigma was acquired either through direct purchase or duplicating one that spent an unchaperoned weekend in the Warsaw Customs Office. Members of the Cipher Bureau carefully examined it and recruited three students from the university at Poznan to help solve the problem.

Intercept operators transferred German Morse code signals to a "Red Form" for analysis, noting date, time, and source (e.g., police or SS).

messages were the raw material to be deciphered by the cryptanalysts using both manual and machine methods. Once deciphered, they would then be translated and given to the proper service branch. An urgent message would be sent to Bletchley Park via teleprinter; otherwise, it was hand-carried by motorcycle. Wireless stations were staffed largely by members of the Women's Auxiliary Air Force (WAAF).[12]

Enigma's known vulnerabilities were acquisition of cryptographic materials or information by betrayal, accident, or seizure by the enemy. To prevent the last of these, the German navy printed its books of setting indicators and codes in water-soluble ink. These and the rotors were to be cast into the sea in the event of imminent capture by the enemy. Summarizing the challenge presented to Allied cryptanalysts on the eve of World War II, historian and former Bletchley Park cryptanalyst Francis Harry Hinsley wrote:

> By the outbreak of war, as a result of these modifications, the Germans judged that they had rendered it safe even in the event of capture; and they had indeed made it into a cypher system that presented formidable obstacles to the cryptanalyst. Instructions for arranging and setting the wheels could be changed as frequently as every 24 hours; anyone not knowing the setting was faced with the problem of choosing from one hundred and fifty million, million, million solutions.[13]

S.1319.
Brit. May. 1925. - Revd Nov., 1931

W/T RED FORM.

Ship or Station. | Set 17 | Date. 16.6.42 | Operator's Remarks.

Opr. 73 | Time Ended G.M.T. 2149 | U.S.A.

To* | Frequency & System. 37 1/2

From* POLICE

All before the Text. DDH de SOF. DDH = SOF NR 11 2225 228 ALO.

Text, Time of Origin, Signature, etc. Write across the page, code and cypher on every third line.

ARTTN	FMXBN	OIYSU	OGILL
YHUPO	HKALE	XEAHS	SFITT
EDSUG	HGEGP	VHTVL	LMUIA
LWTIF	FMAJG	HEDAT	VTDRV
SPTVR	VSYSE	FYABL	SCKOU
ECKZR	EDUOT	TGTOA	VNYAB
NDMMY	AXBTI	TUVHO	EIDKO
HVOWU	ZVXVO	XOYAE	VOETV

Do not use Left Margin

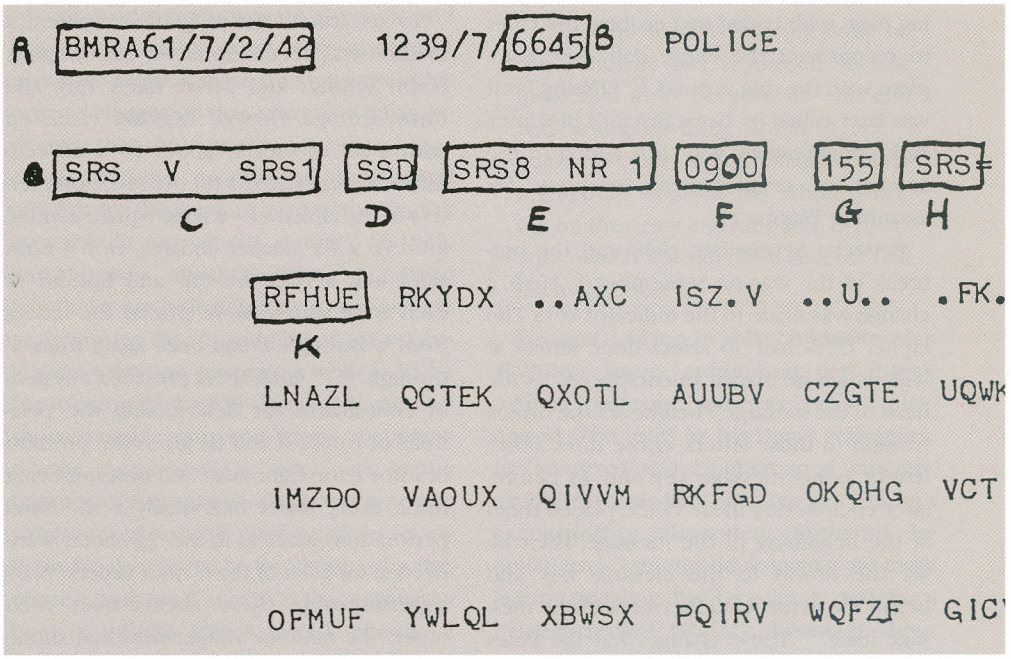
lem: Marian Rejewski, Jerzy Rozycki, and Henryk Zygalski. They began work September 1, 1932.[14]

Rejewski, a brilliant young mathematician, was removed from his friends and exiled to a separate room. He was provided with the commercial version of Enigma and "several dozen messages daily, enciphered on the military Enigma." The problem: How to discover the configuration of the Enigma that produced a given set of messages. What was the order of the three rotors? What were their internal settings (ring settings) on the shaft? How many plugs were used, and which letters were cabled together? Finally, what were the rotor starting positions?

Using mathematical set theory and calculus, Rejewski first determined the clear letters that were enciphered into three totally different letters (ciphertext) at the beginning of a message. Two sources made such solutions possible: 1) the availability of about sixty messages for a single day and 2) the shortcuts taken by German encipherers who slipped into bad habits such as typing the letter "A" three times as their indicator key. Knowledge of these individual habits identified the senders and made codebreaking easier for the Polish and subsequent codebreakers.

In the course of a day, the Germans enciphered many messages and sent them out in Morse code. The Poles then picked up and recorded these wireless messages, and the collections gradually made their way to the Cipher Bureau and Rejewski. He began by analyzing the six-letter indicators that began the radio transmissions (e.g., KYL BTG), looking for patterns that might provide clues to the Enigma settings that produced them. From an examination of sixty or more indicators and the application of basic set theory, he was able to identify certain recurring twenty-six letter patterns that suggested that pressing a certain key on the Enigma machine produced a specific letter as output on each of the three rotors. He was also able to determine how the rotors were wired using a set of six equations with four unknowns to solve.

There was some initial confusion owing to Rejewski's false assumption that the keyboard of the commercial Enigma obtained by the Poles was identical to that of the military version. This error impeded solution of the equations to the point of near abandonment. Then, "quite unexpectedly on 9 December 1932, at just the right moment, I was given a photocopy of two tables of daily keys for September and October, 1932."[15] Unknown to him, these, and later materials, were purchased by Capt. Gustave Bertrand, French Intelligence, from a financially pressed member of the *Chiffrierstelle* (Cipher Center) named Hans-Thilo Schmidt. The equations became solvable, and their solution, together with the new materials, led to methods for arriving at the daily keys or settings of the rotors, their sequence, the connections in the plugboard, and the positions of the rings—all in the space of about four months! Provided with this information, the Cipher Bureau began building its own Enigma replicas to test hypothesized keys.



Morse code transmissions translated to five-letter cryptograms that were sent to various teams at Bletchley Park. Careless habits of German operators enabled cryptanalysts to discover the initial settings and break many codes.

German Cryptological Challenges and Polish Responses, 1936–1939

Throughout the remainder of the 1930s, the Germans continued to make changes in their cipher system, and the Poles continued to discover ways to defeat these changes by manual methods. Their discoveries became the basis of Allied codebreaking during World War II. If the period 1932–1936 was characterized by the proliferation of Enigma machines throughout the German military and civilian organizations, the period following it displayed Germany's growing concern with system security. It was also the period of continued German rearmament, the reoccupation of the Rhineland (1936), the *Anschluss,* and Neville Chamberlain's sacrifice of Czechoslovakia at Munich for "peace in our time" (1938).

Changes came slowly at first. Among the first was altering the schedule for replacing the fast-moving rotor on the far right side of the Enigma machine. Through 1935, the sequence of rotors I, II, and III changed once a quarter. By October 1, 1936, changes were made daily. On that same date, the Germans increased the number of plugboard cables from six to eight. The Poles created a special machine, the Cyclometer (consisting of two sets of rotors), and a card catalog to determine rotor order. It took over a year to prepare just six card catalogs. Then, on November 2, 1937, the Germans changed one of the rotors, forcing the Poles

to re-do much of their work.[16]

Not all the news was bad. In September 1937 a new communications network made its appearance: the *Sicherheitsdienst* (SD), the Nazi party's security service. After some initial difficulties in determining ring settings, the codebreakers selected a group of letters from the middle of a message for analysis. It was typed out on an Enigma replica, using all possible rotor sequences, in order to discover a plain, unenciphered text fragment. What they found were the letters "ein." Apparently, the officer sending the message could find nothing in his codebook that would permit him to encode and transmit it as a four-letter ciphertext, so he sent it unenciphered. This "slip-up" of mixing plain with coded text enabled the Poles to reconstruct the entire daily key, complete with the ring settings.[17] "EINsing," as it was later called by Great Britain's Bletchley Park codebreakers, was thus added to the arsenal of cryptological weapons for assaulting Enigma.

Between September 1938 and the outbreak of the war on September 1, 1939, a change was made to the indicator keys. The cipher clerk had "to select three letters at will, which he placed, unenciphered, at the head of the message. Then he set the drums [rotors] to those letters, chose three other letters as his message key and, as before, after enciphering these twice, placed them at the beginning of the message. Then he set the drums to the message key and began the actual encipherment of the message itself."[18] These changes left the Poles able to read only the SD traffic.

Breaking Enigma—The Polish Bomba and the Zygalski Sheet

To discover the keys enciphered using the revised security procedures, Rejewski proposed the creation of "a device that basically comprised the sets of drums from six Enigmas and that . . . synchronously revolved the drums and (after . . . about two hours, running through all the possible 26^3 = 17,576 positions) signaled when the condition for lighting three pairs of lamps (in each pair the same) was fulfilled."[19] It was called a "bomba," possibly after a popular ice cream dessert. It sought to do mechanically what was no longer feasible to accomplish manually. Since there were six possible Enigma rotor sequences, one "bomba" was created per sequence. These were constructed and ready for use in November 1938. In this, possibly the first, example of parallel processing, the "bomba" ran through all possible Enigma settings and stopped when a likely Enigma setting was found. The operator copied the hypothesized key (settings) and tested it on an Enigma replica specially built for the purpose. If the plaintext appeared, the key was found; if not, the process began again.[20] The machine solution could, however, be frustrated by multiplying the number of plugboard cablings.

To get around the plugboard problem, a method was needed to factor out the plugboard settings and derive likely ring and rotor settings. Henryk Zygalski came up with a set of sheets, "about 60 x 60 centimeters, designated with the successive letters of the alphabet—a large square divided into 51 x 51 smaller squares. Down both sides and across the top and bottom of each large square were placed the letters from 'a' through 'z' and once again from 'a' through 'y'."[21] Each sheet provided a system of coordinates for determining the positions of rotors II and III given the position of rotor I, the right-most and fastest-moving rotor. Every sheet had nearly a thousand perforations made in it, and "26 sheets were needed for each of the 6 rotor orders."[22] By superimposing these sheets over each other, "the number of apertures that shone through gradually decreased, and if one had a sufficient number of keys with single-letter cycles, in the end there remained a single aperture that shone through all the sheets and that corresponded to the right case [probable rotor settings]."[23]

On December 15, 1938, the Germans increased the number of rotors from three to five. Instead of six possible rotor orders, there were now sixty! Each "bomba" would require thirty-six rotors, and fifty-eight additional sets of Zygalski sheets would be required. It would be a costly and time-consuming feat, and time was rapidly running out. While the SD network remained readable until July 1, 1939, only one in ten military messages could be read.[24]

Sharing the Secret

In the bleak December of 1938, Gustave Bertrand, head of cipher section of French intelligence, invited his opposite numbers from Poland and Great Britain to Paris for an Enigma conference in February 1939. The Poles were instructed to say nothing unless the French and British had something to share.[25] They didn't. Everyone left the conference frustrated. Something of this mood is reflected in a memorandum written much later:

> Early in 1939, about February, [Alastair G.] Denniston and [A. Dillwyn] Knox were asked by the French to come to Paris to discuss "E" [Enigma] with the Poles. They went, and met the Poles, but on that occasion the Poles told them little that GC&CS [Government Code & Cipher School] did not already know. Subsequent events showed that the Poles were "holding out" on the British and French.[26]

The question of sharing their discoveries with the British and French was rendered moot by subsequent events. Following Hitler's acquisition of the non-German portion of Czechoslovakia, Britain and France signed a treaty of assistance with Poland, pledging their support in event of an unprovoked attack by Germany. On April 27, 1939, Germany renounced its 1934 nonaggression agreement with Poland. May witnessed an increase in incendiary speeches by Hitler, which touched off disturbances in Poland and Germany.

On June 30, Gwido Langer, head of Poland's Cipher Bureau, called for a conference to be held in Warsaw on July 24–25. Bertrand and a French cryptologist attended for France. Denniston, Knox, and Comdr. Humphrey Sandwich represented Britain.

> It then was disclosed that the Poles had been successfully dealing with a large amount of "E." Denniston's impression is that the Poles' continuity ran well back into the early twenties. They had bombes. Knox was outraged that the Poles had been reticent in February; not realizing that the Poles

> understood English, he made very derogatory remarks while riding in a cab with Denniston and one of the Poles, to Denniston's great embarrassment. Denniston and Knox took back notes and ideas to England, set about building bombes, etc. Before GC&CS got well into "E" traffic, war broke out.[27]

Two Polish-built Enigmas were later given to Bertrand, who passed one of them on to "C," head of Secret Service, Col. Stewart Menzies, at Victoria Station on August 16.[28] World War II was less than two weeks away.

Alan M. Turing and the British Bombe

Poland fell in less than a month. Miraculously, Marian Rejewski and other members of the Cipher Bureau escaped, with French aid, to France. With Gustave Bertrand's help, they were quickly provided with quarters at the Chateau de Vignolles near Gretz-Armainvilliers, about thirty miles northeast of Paris. The relocated Polish cipher unit was designated PC (for *Poste de Commandement*) Bruno.[29]

The newly arrived Polish cipher team resumed work, and on January 17, 1940, with the aid of 1,560 Zygalski sheets provided by the GC&CS, they found the German army key (code-named Green by GC&CS) for October 28, 1939. The German *Luftwaffe* keys (Blue for "practice purposes" and Red for "operational and administrative communications") were recovered by GC&CS between mid-January and late March 1940.[30] Results of the Polish breakthroughs and the efforts of GC&CS were discussed at a meeting held in Paris early in 1940. Among those in attendance was a new member of the Allied cryptanalytic team, Alan Mathison Turing.[31] He knew something he did not share with the Poles.

Alan Turing and Bletchley Park

Bletchley Park, a complex of temporary "huts" surrounding a Victorian manor house, was located north of London. The GC&CS was moved there in 1939. Beginning with a staff of about one hundred, it rapidly expanded to about eight thousand by war's end. A sense of helpless frustration possessed its leaders in September 1940 as they viewed the daunting task of overcoming the new Enigma changes. In a letter to Comdr. Edward Travis, head of Bletchley Park, written in August 1940, Naval Section head Frank Birch wrote "that he was told when war broke out that 'all German codes were unbreakable.' I was told it wasn't worth while putting pundits onto them."[32] This was the defeatist state of affairs when Alan Mathison Turing arrived on September 4, 1939, at the Government Code and Cypher School, Bletchley Park.

A mathematical genius of independent spirit, he was recruited from Cambridge University by GC&CS through a series of special workshops given to the best and brightest at Cambridge and Oxford. Interest may have focused upon him because of his original suggestion that a machine might be devised that could imitate any other.

Alan Turing's concept of "mechanical intelligence" began with a jog in the English countryside early in the summer of 1935. Resting in a meadow, Turing pondered whether a machine might be so designed as to determine the "provability of any mathematical assertion presented to it."[33] To be "mechanical" implied predictable responses under given conditions or configurations; e.g., upper or lower case in the instance of a typewriter. Each machine had a finite set of possible configurations or settings. He proceeded to the design of a theoretical "universal" machine that scanned a tape of infinite length, noted whether a given square was blank or contained a number "1," and then, according to a "table of behavior" (program), the scanner might move forward or backward, write or erase a number. The "table" identified possible configurations and described what the scanner was to do in every situation.

This and more was eventually set down in his paper "Computable Numbers." Turing observed that the "behavior of the computer [a human doing calculations] at any moment is determined by the symbols which he is observing, and his 'state of mind' at that time."[34] Continuing his description of a human computer, he wrote: "We know the state of the system if we know the sequence of symbols on the tape, which of these are observed by the computer (possibly with a special order), and the state of mind of the computer."[35] Given a "table of behavior" describing the computer's actions and "states of mind," Turing proclaimed, "We may now construct a machine" to perform the same task.[36] If a specific "machine" could be described by a "table," then a universal machine might be designed that could simulate the behavior of any specific machine.

Through a 1945 interview with co-cryptanalyst and unit historian A. P. Mahon, Turing described Hut 8, where German naval codes were broken, at the time of his arrival:

> When Turing joined the organization in 1939, no work was being done on Naval Enigma and he himself became interested in it "because no one else was doing anything about it and I could have it to myself." Machine cryptographers were on the whole working on the Army and Air Force cyphers with which considerable success had been obtained.[37]

Shy and lacking in self-confidence, Alan Mathison Turing epitomized the absent-minded professor and was quickly nicknamed "The Prof" by his Hut 8 colleagues. He stuttered and laughed in a raucous, almost machine-like, way. Tales of Turing's eccentricities abounded. Bothered by pollen each summer, he donned a gas mask before pedaling his bicycle to and from work each day.[38] His lack of concern about personal appearance carried over to his written work as well. The paper he wrote to introduce newly hired cryptanalysts to Enigma and codebreaking (baptized "Prof's Book" by Hut 8 staff) appears to have been typed with an old ribbon on a dry platen. Mistakes or rephrasings were typed over, but the pages were never retyped. His first and final draft of "Turing's Treatise on the Enigma" are one in the same. Pages were removed and new ones added without renumbering the whole of the work. Still, this is the only work that reveals Turing's insights into Enigma and how they led him from where the Polish effort stalled to the design of the British bombe. Written in the summer of 1940, it provides a detailed, sys-

tematic account of how Enigma was broken and his design of the British bombe.[39]

The revelations came to Turing late in 1939 while looking at the intercepts provided by the Poles. He observed the relationships between the known indicators and window starting positions for four messages transmitted by the Germans on May 5, 1937:

Indicator	*Window start*
KFJX EWTW	P C V
SYLG EWUF	B Z V
JMHO UVCG	M E M
JMFE FEVC	M Y K

He observed that the "repetition of the EW combined with the repetition of V suggests that the fifth and sixth letters describe the third letter of the window position, and similarly one is led to believe that the first two letters of the indicator [JM] represent the first letter [M] of the window position, and that the third and fourth represent the second."[40] But there were still some problems; i.e., there was no similar correlation between the second and third indicator letters and the second window starting letter, suggesting that additional manual substitutions were being made. This manual substitution hypothesis was supported by further observations and by a fateful fluke of history.

A U-boat with the "call sign AFA had not been provided with the bigramme tables"[41] of letter substitutions and was forced to rely on the older system until the tables were supplied. From May 1 to May 4, 1940, U-boat AFA sent enough messages to enable the *Grundstellung* (ground setting) to be discovered. The cable pluggings had been found previously. Turing wrote:

> It was natural to assume that the Grundstellung used by AFA was the Grundstellung to be used with the correct method of indication, and as soon as we noticed the two indicators mentioned above we tried this one out and found it to be the case.[42]

Alan Turing also developed the concept of Banburismus, a method of obtaining the middle and right hand rotor wheel alphabets. (The term "Banburismus" owed its origins to the town of Banbury, where the sheets were produced.[43]) Banburismus required the construction of possible wheel alphabets in order to discover the coincidence between cipher texts, or "fits." To accomplish this, all of a given day's messages were sorted against each other, and "fits" of four or more letters were listed. "At the same time," Mahon continues, "messages were punched by hand onto Banburies, long strips of paper with alphabets printed vertically, so that any 2 messages could be compared together and the number of repeats be recorded by counting the number of holes showing through both Banburies." Turing developed a scoring system of "decibans" to record "the value of fits."[44] The value of a ban was ten, and a deciban was 1/10 of a ban. A ban of evidence made "a hypothesis ten times as likely as it had been before."

Turing confessed, however, "I was not sure that it would work in practice, and was not in fact sure until some days had actually broken."[45] The last step was to tally the score for the alphabet. The one with the highest score was tested on a "bombe." Given the scarcity of bombes and the demands made upon them by the competing service organizations, Banburismus saved vital time and resources by reducing the number of wheel alphabets to be tested. Mahon writes that "Banburismus was a delightful intellectual game" that "was eventually killed in 1943 by the rapidly increasing number of bombes which made it unnecessary to spend much time and labour in reducing the number of wheel orders to be run: it was simpler and quicker to run all wheel orders."[46]

Help from the Enemy

As the Poles had learned earlier, the German Enigma operators were frequently the source of cribs through bad habits, laziness, or the press of time on high-traffic days. If one knew the habits of an operator, the crib was easily guessed. Individual operators were identified through their radio frequencies, call signs, and the serial numbers for the day. The anonymous historian of the 6812th Signal Security Detachment U.S. Army Europe, Bletchley Park, Hut 6, described the unwitting, but indispensable, help from the enemy:

> The German operator to encode his message is given the steckers [plugboard settings], wheel order and ringstellung for the day, but not the starting position. He must pick six letters for this purpose, three for the starting position and three for a setting in which to encode the starting position. The selection of these letters is where carelessness creeps in to assist us in the "breaking". The operator is apt to pick easy stereotyped combinations, such as the first three letters on the top and middle rows of the enigma machine keyboard (QWEAST), and use them repeatedly. One operator with a girl friend back in Germany by the name of Cillie continuously used the six letters of her name. The term "Cillies" has come to be applied to all sorts of stereotyped phraseology, of which the following are examples:
>
> "Quiet night"—used by operator in North Africa
>
> "Wine barrels on hand"—used by operator in Czechoslovakia
>
> "RAF plane over airport"—used by obliging operator in France
>
> "Good morning"—used by operator in Norway.[47]

The Turing-Welchman Bombe

Based upon previous work by the Poles, the British bombe owes its existence to the work of Alan M. Turing and Gordon Welchman, head of Hut 6, who oversaw the breaking of German army and air force codes. Turing introduced the subject in chapter 6 of his "Treatise" under the heading "The Steckered Enigma, Bombe and Spider."

Invaluable as was Banburismus, manual methods, Turing admitted, "are not practicable for cases where there are many Stecker [plugboard settings], or even where there are few Stecker and many wheel orders."[48]

Turing's "bombe," an improvement over the Polish "bomba," may be thought of as a bank of thirty-six interconnected Enigmas that, when set up according to a "menu" of instructions, moved synchronously

through all 26 x 26 x 26 = 17,576 positions of each simulated Enigma.[49] At each point, a test was applied to determine whether that particular rotor setting could produce the observed crib. To clarify the approach, he provided the following example:

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
D	A	E	D	A	Q	O	Z	S	I	Q	M	M	K	B	I	L	G	M	P	W	H	A	I	V
K	E	I	N	E	Z	U	S	A	E	T	Z	E	Z	U	M	V	O	R	B	E	R	I	Q	T

The numbers 1-25 refer to the successive Enigma positions "at which the letters of the plain text were encoded." The Enigma position was dependent, in turn, upon the positions of the three wheels.[50]

Turing noted that "the method of solution will depend on taking hypotheses about parts of the keys and drawing what conclusions one can, hoping to get either a confirmation or a contradiction." The "parts" to be included in the "key" were "wheel order, the rod start of the crib, whether there are any turnovers in the crib and if so where, and the Stecker." For the purpose of his example, it was assumed that the right-hand wheel remained in the same position and that a wheel turnover would occur somewhere between positions twenty and twenty-five. He began by trying to determine "characteristics of the crib which are independent of the Stecker." These characteristics were represented pictorially in what was called a "web" or "menu."[51] Beginning with position 1, the menu and the table state that pressing Enigma key K encodes that letter as D. Turing wrote the position number below the connecting line between the letters. At position 4, N encodes as D. There are two closed loops (Z, Q, I, E, M, Z) and (I, E, A, I) where the cycles of letters repeats; i.e., after the "M" in the cycle Z, Q, I, E, M, "M" encodes as "Z," and the cycle repeats. A menu would later be further annotated along the lines to indicate hypothesized starting rotor settings; e.g., IEM, where the first of the three letters is the assumed window starting position of the left-hand wheel, the second letter, "E," of the middle wheel, and the third letter, "M," the right-hand wheel. These drawings, accompanied by directions for wheel selection, order, ring setting, and wheel starting positions were given to the Wrens (Women's Reserve Naval Service) in Hut 11 for testing on the bombes, or to follow Turing's analogy, the "spider." His actual nickname for the first bombe was Agnus Dei, which others, less gifted linguistically, shortened to "Agnes."

The defect of Turing's original design was that it depended upon the identification of closed loops and did not take advantage of nonloop associations that might be found. Gordon Welchman, working independently in a converted school on the grounds of Bletchley Park, solved these problems with his Diagonal Board. It allowed for the testing and elimination of all possible plugboard settings for the given positions in one pass. He sketched out a diagram using scrap paper and colored pencils and dashed over to Hut 8:

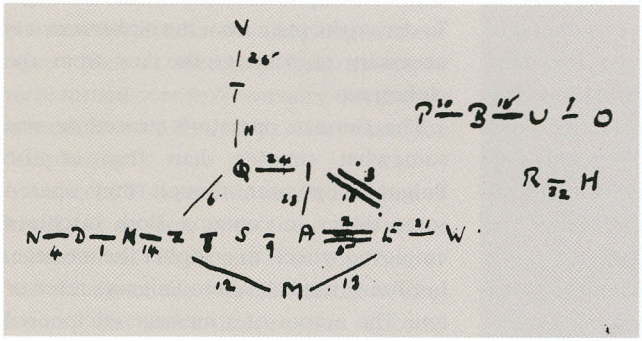
> Turing was incredulous at first, as I had been, but when he had studied my diagram he agreed that the idea would work, and became as excited about it as I was. He agreed that the improvement over the type of bombe that he had been considering was spectacular.[52]

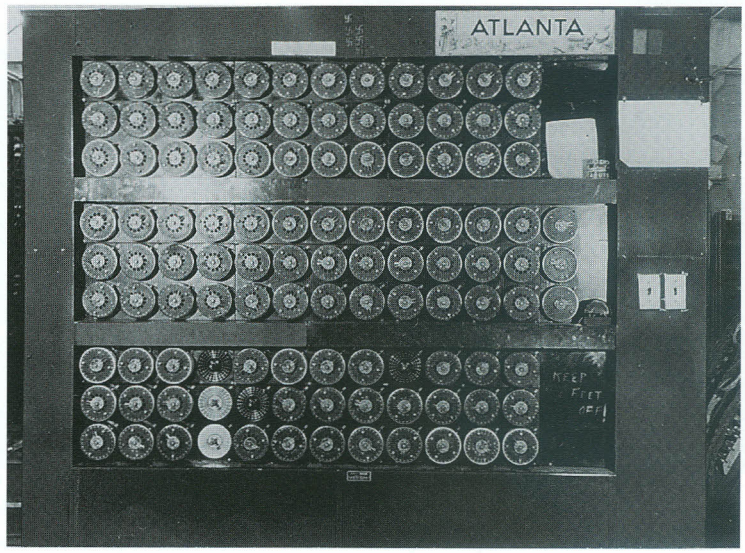
The diagram was passed along to Harold "Doc" Keen, of the British Tabulating Machine Company at Letchworth, for inclusion in the bombe. The Turing-Welchman Bombe design served as the basis for the American bombes later produced by the U.S. Army and U.S. Navy in 1943. Some of the these bombes may have been sent to Bletchley Park, where they received such nicknames as "Rochester" and "Atlanta".

Breaking Hitler's Teleprinter Network

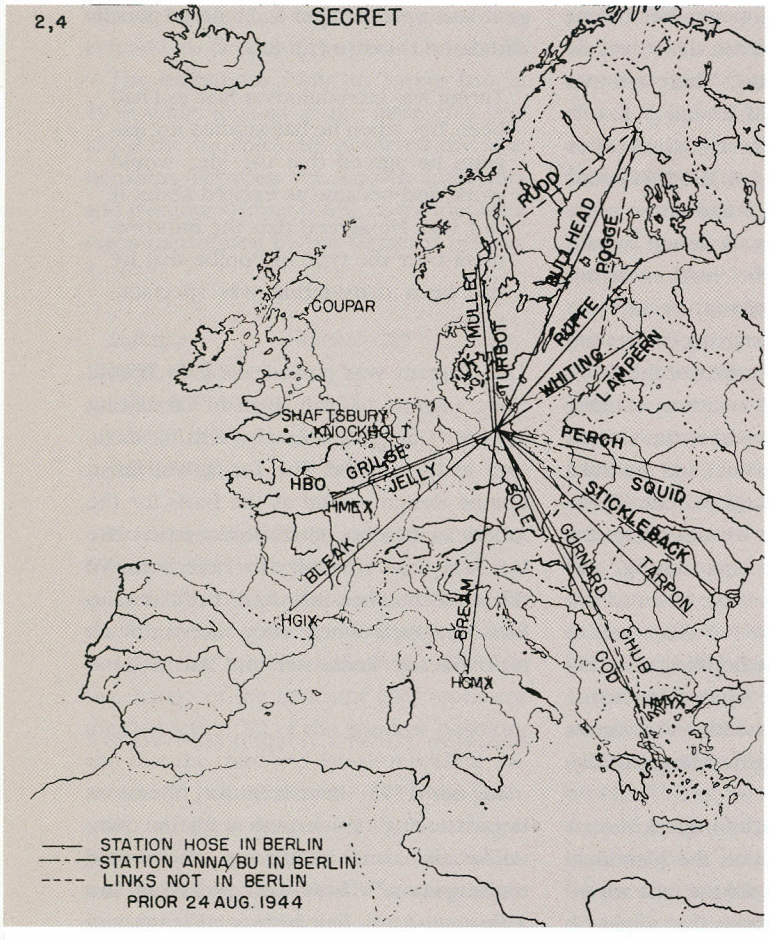
In mid-1941, British radio operators began hearing a brisk musical rhythm quite unlike the usual non-Morse enciphered transmissions.[53] These were picked up "on a German Army link between Vienna and Athens which used a machine later named 'Tunny' by GC and CS." These new messages were encrypted using the Lorenz SZ42 cipher machine.

The Germans began experimenting with unenciphered non-Morse teleprinter messages as early as 1932. By the latter half of





ABOVE: *Turing improved upon the Polish "bomba" by formulating tests to overcome several problems including the many Stecker (plugs), wheel orders, and wheel (rotor) turnovers. His sketch of a "web" or "menu" was designed to isolate the settings that might produce the "characteristics of the crib" or assumed plain text.* RIGHT: *The American military replicated and refined the British bombe designs in 1943. These machines, located in Bletchley Park, were given names such as "Rochester" and "Atlanta".*



The Germans' use of the new Lorenz SZ42 cipher machine in 1942 expanded the quantity and flow of non-Morse messages. The British charted the new German "Fish" network; the Berlin-Paris link, for example, was "Jellyfish."

1940, the first enciphered non-Morse messages were being intercepted. This traffic was termed "Fish" by GC&CS "on the strength of an Enigma reference to the fact that one non-Morse encyphered system, properly named Geheimschreiber, was being called 'Sagfisch.'" For the moment, these new messages arrived only intermittently. As the use of Tunny proliferated during 1942 and new communications links were established, additional Fish names were given to these links. "Shark" denoted the U-boat traffic link.[54] Over this network passed strategic information between Hitler's headquarters and those of his generals and between the generals themselves. "Jellyfish" was the code name given to the link with Paris. "Squid" and "Stickleback" were links to commands in the Ukraine. "Bream" connected Berlin to Rome. Other connections were "Tarpon" (Bucharest), Whiting (Königsberg-Riga), Turbot (Copenhagen), and Perch (Königsberg-Dvinak).[55] Call signs were assigned to the various cities and armies: e.g., Berlin (HBL), Königsberg (HKB), Oberfehlshaber West or Paris (HMEX), Army Group B (HBIX), and Fifth Panzer Army (HLEX). Führer HQ used ANNA when in Berlin or Rastenburg but might use WFST when elsewhere.[56]

Though a separate network, "Sturgeon," was set up using the Siemens T52 teleprinter for German air force traffic, GC&CS decided to concentrate on Tunny. By 1944 Tunny's network had two centers: "Straussberg near Berlin as the terminus for western stations and Königsberg as the terminus for eastern stations," with twenty-six links in all. To intercept the growing number of transmissions, a new British radio intercept station was established late in 1942 at Knockholt, about fifteen miles southeast of London. Staff there grew to about six hundred as links and the lengths of transmissions increased. While Enigma messages were usually kept to below 250 words, Fish messages could run into several hundred; at least one ran to sixty thousand! Hence, the need for a large number of staff.

The Lorenz SZ42 was an online "automatic ciphering machine resembling a teletype" that "enciphers at one end of a circuit and deciphers at the other automatically, using the 'Baudot alphabet.'"[57] Its output was directed to a perforated paper tape, about an inch wide, and consisted of groups of five perforation or nonperforation encodings of the Baudot alphabet. The alphabet consisted of 32 characters, including six special codes indicating carriage returns, spaces, shifts to upper or lower case, new line starts, line feeds, or simply "nothing," represented by "/". The acronym NARA would be punched as follows, with "O" representing hole punches and "." the absence of a punched hole, or a space:

N A R A (Plaintext)
. O . O
. O O O
O . . .
O . O .
. . . .

To encipher these letters, Tunny manufactured "a stream of letters which we will call key, and second, it adds them successively to the plain text" using Modulo 2 addition. Modulo 2 addition followed these basic rules:

1. . + . = . (no perforation)
2. O + O = . (no perforation)
3. . + O = O (a perforation)
4. O + . = O (a perforation)

Adding the letters D, F, X, B (our key), we obtain the ciphertext as follows:

Plaintext	+	Key	=	Ciphertext
N (..OO.)		D (O..O.)		S (O.O..)
A (OO...)		F (O.OO.)		C (.OOO.)
R (.O.O.)		X (O.OOO)		Q (OOO.O)
A (OO...)		B (O..OO)		G (.O.OO)

Tunny's eleven wheels performed this addition as the operator typed in the message. To derive the plain from the ciphertext, it is necessary to subtract the key from the ciphertext.

The German operator's procedure was somewhat simpler than that of the Enigma's operator, though they shared some things in common. Both machines employed wheels to encipher the message, but Tunny used eleven to Enigma's three or four. The output of a message enciphered on Enigma was afterward handed to a radio operator for transmission in Morse code; Tunny enciphered online as the operator typed the message. Both used codebooks. The Tunny operator first alerted the receiver that a message was about to be sent. This was followed by a second message

telling where the setting was to be found in the codebook; e.g., QEP 35 meant to use the setting at line 35. The receiver set up his machine according to the same settings and flashed back UMUM, ready to receive and transmission began. Another code indicated end of transmission. Daily machine setting changes could occur at any time during the day.[58]

> No cipher text is ever repeated. If something does not get through perfectly, the plain [text] is repeated, but the cipher continues, and, as a cipher, is uninterrupted. When a transmission is completed and has been receipted for, it is finished, and as a cipher does not exist to the Germans. There is no record of cipher text.[59]

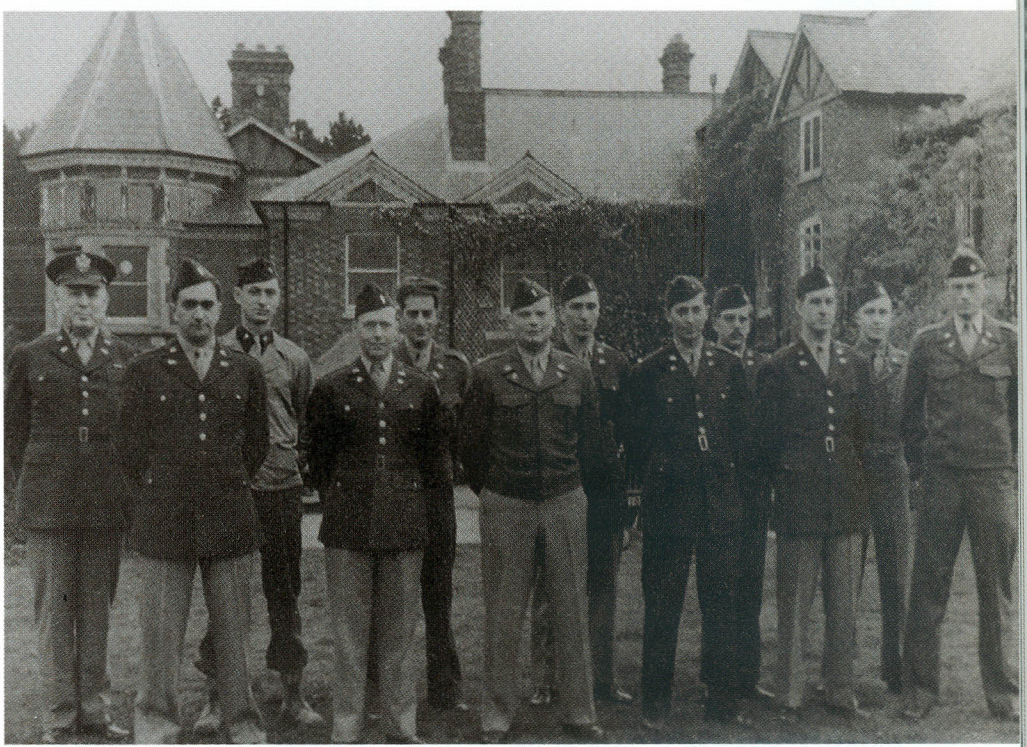
British radio operators received German signals primarily at Knockholt. There a watch of twenty-four operators monitored the network links. Their equipment consisted of "two radio receivers which operate a tape printer, a tape perforator, and an undulator tape [that recorded holes and spaces], as well as head phones." Following interception, a Red Form (Wireless/Telegraphy) with printed tape attached, perforated tape, and undulator tape were forwarded to the checkers for comparison. A manual comparison of the undulator and printed Red Form tape was made. If a discrepancy were noted, the perforated tape was corrected. When a corrected tape was made, it was transmitted to Bletchley Park over duplicate multiplex cables. About fifty people were involved in the checking of these tapes. Once at Bletchley Park, the tapes were turned over to Newmanry, the branch named after M.H.A. (Max) Newman, for deciphering.[60]

A special Fish section was established in July 1942 to deal with these non-Morse transmissions. Their task was to discover "the details of the wheels and the setting letters." But once these were known, decryption was still an exhausting process when done manually. The initial step was to mechanize the process. A research team studied the problem and concluded in December 1942 that high-speed machines were needed. The first of these, Heath-Robinson, was ready in May 1943.[61] Heath-Robinson compared two to four tapes simultaneously. To find a crib, only two tapes were required, "one with the crib, and the other with the cipher text." For a longer run, three tapes were compared: the cipher text, key, and plaintext. The machine utilized continuously looping tapes, standard telephone plugs, plugboard, and photocells. Though a vast improvement over manual methods, Heath-Robinson was slow and required great care in getting the lengths of tape in the loops precisely correct before the run.[62]

Prime Minister Winston Churchill gave the Fish program highest priority in his instructions of February 1943. While Heath-Robinson continued to be used and improved upon, attention shifted to designing and constructing "a faster and more flexible machine." This was to be Colossus, the foundation of the postwar British computer design and development program. It viewed tape four times as fast as Heath-Robinson and executed "five operations simultaneously, gaining a factor of 20" over the former machine. Both machines examined binary data (the presence or absence of perforations), "but whereas Robinson read from a loop of 5-level paper tape, Colossus generated data electronically."[63] Tony Sale, curator of the Bletchley Park Museum, explained how Colossus operated during a 1996 lecture at the National Archives:

> What Colossus does, in a nutshell, is to generate the key streams—that is, the sequence of symbols on the wheels of the Lorenz machine—internally in its electronic circuits. It reads the intercepted message tape at 5,000 characters a second, comparing the tape of the intercepted enciphered text with these internally represented key streams. Then, making some very sophisticated cross-correlations, it finds the start-wheel positions for the particular enciphered message.[64]

Colossus used twenty-five hundred valves (vacuum tubes) to generate and store the key stream, which was then compared with the five-hole punched tape input. Its output was the wheel setting used by the Lorenz operator for a given message. These settings were then used on a Tunny machine to decipher the message. The first Colossus



American liaison officers were first assigned to Bletchley Park in May 1942. The spacious grounds, located fifty miles from London, housed many cryptographic units. The officers' sensitive knowledge kept most of them there through the war.

became available in December 1943. By D day, there were ten.

When the tactical intelligence provided by Enigma was combined with the top-secret strategic knowledge gleaned from Colossus and Tunny, the intelligence thus provided a formidable weapon in Allied hands. From this Ultra intelligence, Field Marshal Bernard Montgomery and Gen. Dwight Eisenhower learned that their D day deception had convinced Hitler that Calais was the target of the coming invasion.

In Technology They Trusted

Given the complexity of Enigma and the Lorenz SZ42 machines, it is easy to understand German faith in the impregnability of their cipher machines. T4g. Walter Jacobs, Army Signal Corps, then stationed at Bletchley Park, wrote this tribute to those who broke Tunny:

> The solution of Tunny traffic is one of the great achievements of cryptanalysis. That a system of such high grade and trusted to such a degree by the Germans, could be read in any appreciable amount would be remarkable; but much more than this has been accomplished. A complete and general solution has been found, and a considerable volume of traffic is read currently [April 14, 1945]. In March, 1945, upwards of five million letters of current transmission, containing intelligence of the highest order, was deciphered.[65]

The trust of the Germans in their technology is, perhaps, best reflected in one of their own investigation reports. In 1943 the Supreme Command Armed Forces (GIS) received this startling message through its Swiss office:

> For some months, German Naval codes giving orders to operational U-Boats have been successfully broken. All orders are read currently. Note. The source is a Swiss American in an important secretarial position in the U.S. Navy Department.

Between mid-January and mid-February 1944, "the meeting or supplying of U-Boats was on 3 occasions interrupted by enemy action." Three vessels were lost! A high-level meeting was held on February 26, 1944, to consider the question, "Did the enemy read our signals as a result of cryptographic work?" The investigating committee concluded:

> As from the above arguments, reading the traffic, whether by cryptography or capture [of Enigma machines or codebooks], is shown to be out of the question, only two possibilities remain: Treachery or discovery by enemy aerial reconnaissance.[66]

Despite the use of the sophisticated Enigma machine, Germany's security was, in the end, dependent upon relatively unsophisticated cipher clerks and teleprinter operators. The detailed manual work of enciphering messages had been shifted to flawed machines operated by fallible humans—a lethal combination for the Reich.

The Triumph of Technology Over Intelligence: "The Danger of Ultra"

The British triumphed technologically over the German cipher machines, but did the work of these clandestine warriors make a difference? Did their achievements affect the outcome of the war? Of even a battle? In his appreciation of the codebreakers' accomplishments, Brig. E. T. Williams, Chief Intelligence Officer to Field Marshal Montgomery, wrote "that very few Armies ever went to battle better informed of their enemy."[67] Gen. Sir Claude Auchinleck, Commander-in-Chief Middle East, "expressed the opinion that, had we not had the 'U' [Ultra] service, Rommel would certainly have got through to Cairo."[68] An example of the importance of Ultra intelligence to Montgomery is provided by Brigadier Williams:

> What we should have done without it is idle to linger over, yet it must be made quite clear that Ultra and Ultra only put Intelligence on the map. . . . From 1939 to 1942 Intelligence was the Cinderella of the Staff and information about the enemy was frequently treated as interesting rather than valuable. Of course this attitude varied according to the commander. Yet the story of the short but drastically successful battle of Alam Halfa [August 30–September 6, 1942] may point the moral best. "The brave but battled Eighth Army" was holding an improvised line at El Alamein. A new commander arrived in the desert. It became obvious from Ultra that Rommel intended his final drive to Alexandria in the full moon of August by a sweep through the Southern flank. The Army Commander accepted the evidence and made his arrangements. Believing that the confidence of his men was the prerequisite of victory, he told them with remarkable assurance how the enemy was going to be defeated. The enemy attack was delayed and the usual jokes were made about the "crystal-gazers." A day or two later everything happened according to plan. The morale emerging from the promise so positively fulfilled formed the psychological background conditioning the victory which was to follow. Thereafter Intelligence came into its own.[69]

Ultra also provided information about the location of German Wolf Packs, allowing convoys to avoid them and Allied aircraft to hunt them down. According to Humphreys, "Air reconnaissance for a ship or convoy known to be on passage from 'U' sources was not laid on in specific terms of a search for such movement," which might have revealed the source of the intelligence. Rather, air reconnaissance "sorties were organized with cross-over points allowing for particularly full cover of crucial areas."[70]

During the D day preparations, Brig. E.T. Williams remarked that Ultra "was the only source revealing the enemy's reactions to a cover plan. Without Ultra we should never have known." He offers the example of Operation Fortitude (the Pas de Calais cover plan), noting "that without Ultra confirmation that it was selling, the plan might have been dropped."[71]

Despite these achievements, Williams cautioned that it was very easy to be seduced by the power of Ultra and lulled into either complacency or total reliance upon it. In his analysis of Ultra's contribution, he wrote:

> It should not be necessary to stress the value of the material in shaping the general Intelligence of the war. Yet it should be emphasized from the outset that the material was dangerously valuable not only because we might lose it but also because it seemed the answer to an Intelligence Officer's prayer. Yet by providing this answer it was liable to save the recipient from doing Intelligence. Instead of being the best, it tended to become the only, source. There was a tendency at all times to await the next message and, often, to be fascinated by the authenticity of the information into failing to think whether it was significant at the particular level at which it was being considered.[72]

The Battle of the Bulge [December 16, 1944–January 16, 1945] was a glaring case in point: "On the Ardennes offensive," he wrote, "we were wrong. We argued the point in early December and decided wrongly. We gave a lead but the wrong lead." The fault did not lie with Ultra "but rather in our attitude to the [Bletchley] Park. We had begun to lean: that was the danger of Ultra."[73]

He was not alone in this assessment of our intelligence failure. In response to a request from Maj. Gen. Clayton Bissell, a special report entitled "Indications of German [Ardennes] Offensive" was prepared. In a summary, the following points were made:

> Almost all evidence from ULTRA sources of military and air preparations could have been interpreted either as:
>
> (I) offensive nature, or
> (II) defensive plus building up of central reserve to restore situation.
>
> Tactical reconnaissance, active patrolling, capture for interrogation of prisoners of war and the like must, in spite of ULTRA, still remain the surest guide to enemy intent for Commanders in the field. In this case, weather and the Siegfried Line, and not lack of effort, were presumably to blame.[74]

In the war of intelligence technologies, both the Germans and the Allies fell under the spell of their machines. If the Allies were guilty of placing uncritical faith in their new oracle, the Germans no less erred in placing their trust in the invincibility of Enigma and the infallibility of its operators. As early as 1940, German cipher clerks were commanded to use a different *Grundstellung* (ground setting) "for every message." They were also warned that

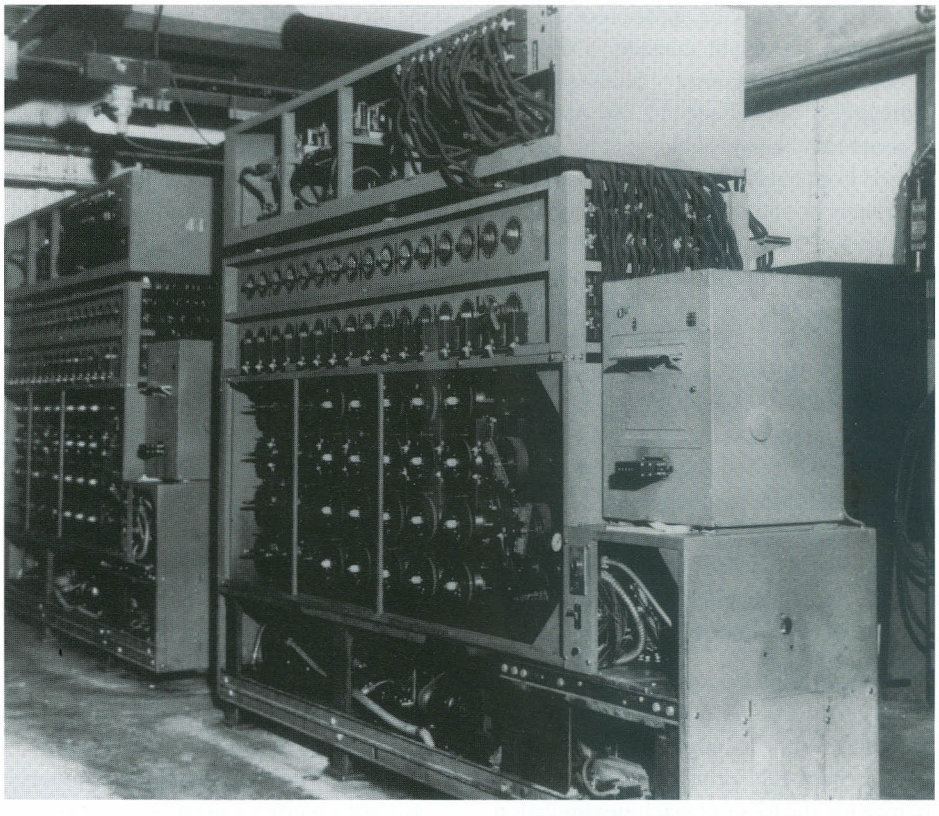
> Using any of the following for Grundstellung and Message Cipher is forbidden: any letter three times, words, abbreviations, traffic signs, call signs, letters in alphabetical order or in order of the Enigma key-board.[75]

And, yet, as we saw earlier, these orders were disobeyed, allowing Allied codebreakers to break Enigma and Allied commanders to alter the course of battle.

Both the Allies and the Germans were seduced by the power and the promise of their machines, which blinded them to the dangers of dependence upon them and to the fallibility of the mortals who operated them. They were the first to deal with the implications of mechanizing the once entirely manual tasks of enciphering and deciphering coded messages. The complexity and cognitive demands of the codebreakers' work grew so demanding that they contributed in large measure to the development of the computer, the realization of Alan Turing's "universal machine," "a single special machine" that could "be made to do the work of all."[76]

Alan Turing, Mind, and Universal Machine

Alan Turing never wrote directly about his wartime service, but he did work on Britain's Automatic Computing Engine



U.S. Army bombes, built in 1943, were modeled after the Turing-Welchman machine. Nearly six feet tall, they were motor driven and had thirty-six interconnected Enigmas with three rotors each. Advancements in machine intelligence, however, created the danger of overreliance on such sources.

(ACE) after the war. He also continued to write about the "universal machine." In his landmark essay "Computing Machinery and Intelligence" (1950), Turing raised "the question as to how far it is possible in principle for a computing machine to simulate human activities," i.e., "Can machines think?" Initially dismissing the question as "too meaningless to discuss," Turing then went on to rephrase the question in machine terms and ask: "Are there discrete state machines" that could fool a human into thinking that he or she was communicating with another human rather than a machine?[77] This is the central question of his "imitation game," which in his words asks: "Could one make a machine which would answer questions put to it, in such a way that it would not be possible to distinguish its answers from those of a man?" His answer: "I believe so."[78] He defined "discrete state machines" as those "machines which move by sudden jumps or clicks from one quite definite state to another." Turing then continued what could easily be a veiled reference to Enigma:

> As an example of a discrete state machine we might consider a wheel which clicks round through 120 [degrees] once a second, but may be stopped by a lever which can be operated from outside; in addition a lamp is to light in one of the positions of the wheel. This machine could be described as follows. The internal state of the machine (which is described by the position of the wheel) may be q1, q2 or q3. There is an input signal i0 or i1 (position of lever). The internal state at any moment is determined by the last state and input signal according to the table [not shown here] . . This example is typical of discrete state machines. They can be described by such tables provided they have only a finite number of possible states.[79]

States of mind became analogous to the states of the machines he worked with at Bletchley Park—a rather startling idea at first, perhaps, but Turing hedged his bets by narrowing the focus of machine simulation:

> The class of problems capable of solution by the machine can be defined fairly specifically. They are those problems which can be solved by human clerical labour, working to fixed rules, and without understanding.[80]

His concern was with very well structured, rule-governed domains such as chess, poker, bridge, theorem proving, and cryptography.

The essay "Intelligent Machinery" (1948) was totally devoted to "ways in which machinery might be made to show intelligent behavior" and the "analogy with the human brain." Specifically, he argued an analogy to be drawn between his "idea of an unorganized machine" and "the infant human cortex." By "unorganized machine," he meant one created "in a comparatively unsystematic way from some kind of standard components."[81]

In his famous essay "Computing Machinery and Intelligence," published in the philosophy journal *MIND*, brain (hardware) and mind (software) became indistinguishable: "In considering the functions of the mind or the brain we find certain operations which we can explain in purely mechanical terms."[82] Turing takes up the central problem of writing a program that could play the "imitation game" and clearly states the program's goal as "trying to imitate an adult human mind."[83] This goal is quickly modified to simulating a "child-brain" through programming a "child-machine." The behaviorist reward-punishment model of instruction is described, but he seems to have become more sympathetic toward the student. He goes on to describe the "child-machine" as a "system of logical inference" capable of receiving an instruction such as "Do your homework now," then establishing and ordering goals requisite to carrying it out.[84] At the heart of the system would be various propositions or rules to be followed in different situations.

Rules and propositions presumably were to come from an expert. He wrote:

> If one wants to make a machine mimic the behavior of the human computer in some complex operation one has to ask him how it is done, and then translate the answer into the form of an instruction table.[85]

Following his previous ask-the-expert suggestion, he describes a chess game based upon "an introspective analysis of my thought processes when playing" (an unfortunate choice, as he was not considered a strong player by the chess masters of Bletchley Park). In this game, the machine plays white, and some of the moves are annotated by footnotes (e.g., "Most inappropriate moves." "Head in the sand!" "Fiddling while Rome burns!"). The machine "resigns" at the thirtieth move "on the advice of his trainer."[86] Turing once followed the program's move rules in a hand-and-paper computer simulation and played and lost against a friend.

Amazingly, Turing anticipated much of the research program taken up by the new fields of artificial intelligence and cognitive science that appeared in the 1950s. His postwar writings touch upon the basic analogy of mind to machine states, computer simulations of intelligent behavior, chess-playing programs, rules derived from experts and coded into programs, and the brainware:hardware::mindware:software analogy. Underlying these provocative thoughts were his Bletchley Park experiences with the extension of human functions by machines, discrete state machines that, like their human counterparts, might be imitated by a "universal machine."

World War II witnessed the mechanization of intelligence. Machines took over the labors of weary German cipher creators and those of Allied codebreakers. The transfer of these burdensome functions occurred with no greater sense of loss than the delegation of basic arithmetic computations to the calculator, no feelings of threat or regret. Yet a line was being drawn between human and machine intelligence. Without awareness of it, how could we know where it was or when we had crossed it? Was it as near as we feared or as distant as we dreamed? If a machine could be said to be thinking, what were the implications for how we viewed human intelligence? Alan Turing raised these still disturbing and unanswered questions.✦

Notes

[1] Andrew Hodges, *Alan Turing: The Enigma* (1983), p. 109.
[2] David Kahn, *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939-1943* (1991), pp. 38-39.
[3] Ibid., pp. 32-33.
[4] Ibid., p. 33.
[5] Ibid., pp. 33-34.
[6] Ibid., pp. 41-43.
[7] Ibid., p. 51.
[8] German WWII Police and SS Traffic file, NR 4417, box 1386, Historic Cryptographic Collection, Pre-World War I Through World War II, ca. 1891-ca. 1981, Records of the National Security Agency/Central Security Service, Record Group 457, National Archives and Records Administration, Washington, DC (hereinafter cited as RG 457, NARA).
[9] Daniel Jonah Goldhagen, *Hitler's Willing Executioners: Ordinary Germans and the Holocaust* (1996), pp. 181-182.
[10] Army Machine Cipher/Areas for Use of Air Force Command Ciphers (German); NR 20, box 2, RG 457, NARA. Alan Stripp, "The Enigma Machine: Its Mechanism and Use," F. H. Hinsley and Alan Strip, eds., *Codebreakers The Inside Story of Bletchley Park* (1993), p. 87.
[11] German WWII Police and SS Traffic file, NR 4417, box 1386, Historic Cryptographic Collection, Pre-World War I Through World War II, ca. 1891-ca. 1981, RG 457, NARA.
[12] Gordon Welchman, *The Hut 6 Story: Breaking the Enigma Codes* (1982), pp. 149-151.
[13] F. H. Hinsley, et. al., *British Intelligence in the Second World War: Its Influence on Strategy and Operations,* vol. 1 (1979), p. 487.
[14] Marian Rejewski, "How the Polish Mathematicians Broke Enigma," in Wladyslaw Kozaczuk, *ENIGMA: How the German Machine Cipher Was Broken and How It Was Read by the Allies in World War Two* (1984), pp. 246-247.
[15] Ibid., pp. 255-256.
[16] Ibid., pp. 262-264.
[17] Ibid., pp. 264-265.
[18] Ibid., pp. 265-266.
[19] Ibid., pp. 266-267.
[20] Kahn, *Seizing the Enigma,* p. 73.
[21] Rejewski, "How the Polish Mathematicians Broke Enigma," p. 267.
[22] Kahn, *Seizing the Enigma*, p. 74.
[23] Rejewski, "How the Polish Mathematicians Broke Enigma," p. 268.
[24] Ibid., pp. 268-269.
[25] Hinsley, *British Intelligence,* vol. 1, p. 491.
[26] Memorandum from Lt. Col. Telford Taylor, GSC, to Colonels [Carter W.] Clarke and [W. Preston] Corderman, Jan. 22, 1944, NR 4246, box 1364, Historic Cryptographic Collection, Pre-World War I Through World War II, ca. 1891-ca. 1981, RG 457, NARA (hereinafter cited as "Early 'E' History").
[27] Ibid.
[28] Hinsley, *British Intelligence,* vol. 1, p. 492.
[29] Kahn, *Seizing the Enigma*, p. 91.
[30] Ibid., pp. 91-92; Hinsley, *British Intelligence,* vol. 1, pp. 108, 493.
[31] "Early 'E' History," RG 457, NARA; Kozaczuk, *ENIGMA*, pp. 97-98.
[32] A. P. Mahon, *History of Hut Eight, 1939-1945,* p. 14; NR 4685, box 1424, Historic Cryptographic Collection, Pre-World War I Through World War II, ca. 1891-ca. 1981, RG 457, NARA.
[33] Hodges, *Alan Turing: The Enigma,* p. 96.
[34] Ibid., p. 105.
[35] Ibid.
[36] Ibid., p. 106.
[37] Mahon, *History of Hut Eight,* p. 14.
[38] Hodges, *Alan Turing: The Enigma,* pp. 208-209.
[39] Mahon, *History of Hut Eight,* p. 14.
[40] [Alan M. Turing], "Turing's Treatise on the Enigma," pp. 135-137, NR 964, box 201, Historic Cryptographic Collection, Pre-World War I Through World War II, ca. 1891-ca. 1981, RG 457, NARA.
[41] Ibid.
[42] Ibid.
[43] Hodges, *Alan Turing: The Enigma,* pp. 196-197.
[44] Mahon, *History of Hut Eight,* pp. 17-19.
[45] Ibid., p. 14.
[46] Ibid., p. 20.
[47] European Theater of Operations 6812th Signal Security Detachment U.S. Army Europe, Bletchley Park HUT#6 Decoding of German Enigma Machine Messages, Feb.1, 1944-May 7, 1945, p. 3, NR 964, box 201, Historic Cryptographic Collection, Pre-World War I Through World War II, ca. 1891-ca. 1981, RG 457, NARA.
[48] "Turing's Treatise on the Enigma," p. 97, RG 457, NARA.
[49] Welchman, *The Hut 6 Story*, p. 297.
[50] Ibid., p. 78.
[51] "Turing's Treatise on the Enigma," pp. 97-99, RG 457, NARA.
[52] Welchman, *The Hut 6 Story,* p. 81.
[53] "Report on British Attack on Fish," p. 12, box 579, NR 1407, Historic Cryptographic Collection, Pre-World War I Through World War II, ca. 1891-ca. 1981, RG 457, NARA.
[54] [Francis Harry Hinsley?], "Draft Appendix to History of British Intelligence in World War II," pp. 1-2 (hereinafter referred to as Hinsley, Appendix Geheimschreiber [Fish]), box 1315, NR 3938, Historic Cryptographic Collection, Pre-World War I Through World War II, ca. 1891-ca. 1981, RG 457, NARA.
[55] "FISH Weekly Report Period 6th-13th August 1943," box 174, NR 803, Historic Cryptographic Collection, Pre-World War I Through World War II, ca. 1891-ca. 1981, RG 457, NARA.
[56] "Germany: Notes on the German Army Teleprinter Network," pp. 2-3, box 1338, NR 4030, Historic Cryptographic Collection, Pre-World War I Through World War II, ca. 1891-ca. 1981, RG 457, NARA.
[57] "Report on British Attack on Fish," p. 1, box 579, NR 1407, RG 457, NARA.
[58] Ibid., pp. 12-13.
[59] Ibid., p. 13.
[60] Ibid., pp. 17-18.
[61] Hinsley, Appendix Geheimschreiber (Fish), p. 3, RG 457, NARA.
[62] "Report on British Attack on Fish," p. 47, box 579, NR 1407, RG 457, NARA.
[63] Hinsley, Appendix Geheimschreiber (Fish), p. 3, RG 457, NARA.
[64] Tony Sale quoted in John Cornwell, "The Secret That Beat The Nazis," *The Sunday Times Magazine* (May 12, 1996), p. 41.
[65] "The Cryptanalysis of the Tunny Cipher Device Preface" attachment to "Report of Sgt. Walter Jacobs to Commanding Officer Signal Security Agency," May 7, 1945, p. 1, box 943, NR 2750, Historic Cryptographic Collection, Pre-World War I Through World War II, ca. 1891-ca. 1981, RG 457, NARA.
[66] Extracts from Strategic Security—Naval ENIGMA, Naval War Staff, Chief Naval Communications Division Ia 10. Supreme Command of the German Navy, Berlin, Sept. 30, 1941-Feb. 24[6], 1943[4], NR 908, box 192, NR 4246, box 1364, Historic Cryptographic Collection, Pre-World War I Through World War II, ca. 1891-ca. 1981, RG 457, NARA.
[67] E. T. Williams, "Volume, Security, Use and Dissemination of SIGINT at British Field Commands," p. 15 in Brig. Williams and Grp. Capt. Humphreys Reports Concerning Ultra, box 1424, NR 4686, Historic Cryptographic Collection, Pre-World War I Through World War II, ca. 1891-ca. 1981, RG 457, NARA.
[68] Grp. Capt. R. H. Humphreys, "The Use of 'U' in the Mediterranean and Northwest African Theaters of War—October 1945, p. 7 in Brig. Williams and Grp. Capt. Humphreys Reports Concerning Ultra, box 1424, NR 4686, Historic Cryptographic Collection, Pre-World War I Through World War II, ca. 1891-ca. 1981, RG 457, NARA.
[69] Williams, "Volume, Security, Use and Dissemination of SIGINT," p. 3.
[70] Ibid., p. 2.
[71] Ibid., p. 13.
[72] Ibid., p. 1.
[73] Ibid., p. 13.
[74] Memorandum from Col. H. M. O'Connor, G.S., to Maj.-Gen. Clayton Bissell, GSC A.C. of S., G-2 (Jan. 13, 1945), box 1119, NR 3601, Historic Cryptographic Collection, Pre-World War I Through World War II, ca. 1891-ca. 1981, RG 457, NARA.
[75] *The Enigma General Procedure,* p. 24, box 622, NR 1679, Historic Cryptographic Collection, Pre-World War I Through World War II, ca. 1891-ca. 1981, RG 457, NARA.
[76] Turing, "Lecture to the London Mathematical Society on 20 February 1947," in *Collected Works of A. M. Turing, Mechanical Intelligence,* ed. D. C. Ince (1992), p. 93.
[77] Turing, "Computing Machinery and Intelligence," in *Collected Works*, p. 142.
[78] Turing, "Digital Computers Applied to Games," in *Collected Works*, p. 164.
[79] Turing, "Computing Machinery and Intelligence," pp. 139-140.
[80] Turing, "Proposal for Development in the Mathematics Division of an Automatic Computing Engine (ACE)," in *Collected Works*, pp. 19-20.
[81] Turing, "Intelligent Machinery," in *Collected Works*, p. 113.
[82] Turing, "Computing Machinery and Intelligence," p. 154.
[83] Ibid., p. 155.
[84] Ibid., p. 157.
[85] Ibid., p. 138.
[86] Turing, "Digital Computers Applied to Games," pp. 168-169.

Related Web Sites

Bletchley Park—Britain's Best Kept Secret
http://www.cranfield.ac.uk/ccc/BPark

Alan Turing Home Page
http://www.wadham.ox.ac.uk/~ahodges/Turing.html

Enigma Simulation Programs
ftp://ftp.ox.ac.uk/pub/crypto

Index to NSA Collection (RG 457) used for this paper
http://www.nsa.gov:8080/programs/opendoor/narafindaid.html