Cryptanalysis of the Enigma

Cryptanalysis of the Enigma enabled the western Allies in World War II to read substantial amounts of secret Morse-coded radio communications of the Axis powers that had been enciphered using Enigma machines. This yielded military intelligence which, along with that from other decrypted Axis radio and teleprinter transmissions, was given the codename *Ultra*. This was considered by western Supreme Allied Commander Dwight D. Eisenhower to have been "decisive" to the Allied victory.[1]

The Enigma machines were a family of portable cipher machines with rotor scramblers.[2] Good operating procedures, properly enforced, would have made the plugboard Enigma machine unbreakable.[3][4][5] However, most of the German armed and secret services and civilian agencies that used Enigma employed poor procedures, and it was these poor operating procedures that allowed the Enigma machines to be reverse-engineered and the ciphers to be read.

The German plugboard-equipped Enigma became Nazi Germany's principal crypto-system. It was broken by the Polish General Staff's Cipher Bureau in December 1932, with the aid of French-supplied intelligence material obtained from a German spy. A month before the outbreak of World War II, at a conference held in Warsaw, the Polish Cipher Bureau initiated the French and British into its Enigma-breaking techniques and technology. During the German invasion of Poland, core Polish Cipher Bureau personnel were evacuated, via Romania, to France where they established the PC Bruno signals-intelligence station with French facilities support. Successful cooperation among the Poles, the French, and the British at Bletchley Park continued until June 1940, when France surrendered.

From this beginning, the British Government Code and Cypher School (GC&CS) at Bletchley Park built up an extensive cryptanalytic facility. Initially, the decryption was mainly of *Luftwaffe* and a few Army messages, as the *Kriegsmarine* (German navy) employed much more secure procedures for using Enigma. Alan Turing, a Cambridge University mathematician and logician, provided much of the original thinking that led to the design of the cryptanalytical Bombe machines and the eventual solving of naval Enigma. However, the German Navy introduced an Enigma version with a fourth rotor for its U-boats resulting in a prolonged period when these messages could not be decrypted. With the capture of relevant cipher keys and the use of much faster US Navy Bombes, regular, rapid reading of U-boat messages resumed.

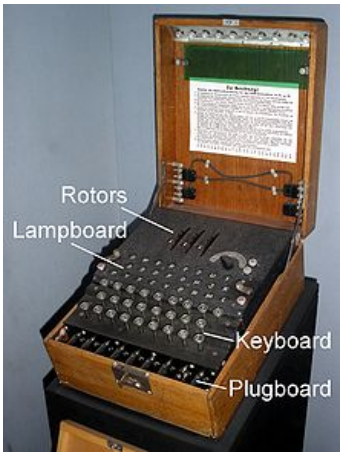
Contents

General principles

The Enigma machines produced a polyalphabetic substitution cipher During World War I, inventors in several countries realized that a purely random key sequence, containing no repetitive pattern, would, in principle, make a polyalphabetic substitution cipher unbreakable.[6] This led to the development of rotor cipher machines which alter each character in the plaintext to produce the ciphertext, by means of a scrambler comprising a set of *rotors* that alter the electrical path from character to character, between the input device and the output device. This constant altering of the electrical pathway produces a very long period before the pattern—the key sequence or substitution alphabet—repeats.

Decrypting enciphered messages involves three stages, defined somewhat differently in that era than in modern cryptography.[7] First, there is the *identification* of the system in use, in this case Enigma; second, *breaking* the system by establishing exactly how encryption takes place, and third, *solving*, which involves finding the way that the machine was set up for an individual message *i.e.* the *message key*.[8] Today, it is often assumed that an attacker knows how the encipherment process works (see Kerckhoffs's principle) and *breaking* is often used for *solving* a key. Enigma machines, however, had so many potential internal wiring states that reconstructing the machine, independent of particular settings, was a very difficult task.

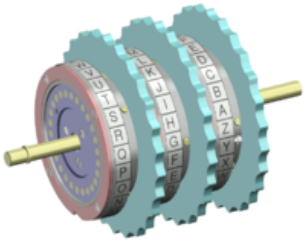
The Enigma machines



The Enigma machine was used commercially from the early 1920s and was adopted by the militaries and governments of various countries—most famously Nazi Germany.

The Enigma rotor cipher machine was potentially an excellent system. It generated a polyalphabetic substitution cipher, with a period before repetition of the substitution alphabet that was much longer than any message, or set of messages, sent with the same key

A major weakness of the system, however, was that no letter could be enciphered to itself. This meant that some possible solutions could quickly be eliminated because of the same letter appearing in the same place in both the ciphertext and the putative piece of plaintext. Comparing the possible plaintext *Keine besonderen Ereignisse* (literally, "no special occurrences"—perhaps better translated as "nothing to report"), with a section of ciphertext, might produce the following:


A series of three rotors from an Enigma machine scrambler When loaded in the machine, these rotors connect with the entry plate on the right and the reflector drum on the left.

Exclusion of some positions for the possible plaintext *Keine besonderen Ereignisse*

Ciphertext	O	H	J	Y	P	D	O	M	Q	N	J	C	O	S	G	A	W	H	L	E	I	H	Y	S	O	P	J	S	M	N	U
Position 1			K	E	I	N	E	B	E	S	O	N	D	E	R	E	N	E	R	E	I	G	N	I	S	S	E				
Position 2				K	E	I	N	E	B	E	S	O	N	D	E	R	E	N	E	R	E	I	G	N	I	S	S	E				
Position 3					K	E	I	N	E	B	E	S	O	N	D	E	R	E	N	E	R	E	I	G	N	I	S	S	E			
	Positions 1 and 3 for the possible plaintext are impossible because of matching letters. The red cells represent these *crashes*. Position 2 is a possibility																														

Structure

The mechanism of the Enigma consisted of a keyboard connected to a battery and a current entry plate or wheel (German: *Eintrittswalze*), at the right hand end of the scrambler (usually via a plugboard in the military versions).[9] This contained a set of 26 contacts that made electrical connection with the set of 26 spring-loaded pins on the right hand rotor. The internal wiring of the core of each rotor provided an electrical pathway from the pins on one side to different connection points on the other. The left hand side of each rotor made electrical connection with the rotor to its left. The leftmost rotor then made contact with the reflector (German: *Umkehrwalze*). The reflector provided a set of thirteen paired connections to return the current back through the scrambler rotors, and eventually to the lampboard where a lamp under a letter was illuminated.[10]

Whenever a key on the keyboard was pressed, the stepping motion was actuated, advancing the rightmost rotor one position. Because it moved with each key pressed it is sometimes called the *fast rotor*. When a notch on that rotor engaged with a pawl on the middle rotor, that too moved; and similarly with the leftmost ('slow') rotor

There are a huge number of ways that the connections within each scrambler rotor—and between the entry plate and the keyboard or plugboard or lampboard—could be arranged. For the reflector plate there are fewer, but still a large number of options to its possible wirings.[11]

Each scrambler rotor could be set to any one of its 26 starting positions (any letter of the alphabet). For the Enigma machines with only three rotors, their sequence in the scrambler—which was known as the *wheel order (WO)* to Allied cryptanalysts—could be selected from the six that are possible.

Possible rotor sequences—also known as *Wheel Order (WO)*

Left	Middle	Right
I	II	III
I	III	II
II	I	III
II	III	I
III	I	II
III	II	I

Later Enigma models included an *alphabet ring* like a tyre around the core of each rotor. This could be set in any one of 26 positions in relation to the rotor's core. The ring contained one or more notches that engaged with a pawl that advanced the next rotor to the left.[12]

The plugboard (*Steckerbrett*) was positioned at the front of the machine, below the keys. In the above photograph, two pairs of letters have been swapped (A↔J and S↔O). During World War II, ten leads were used, leaving only six letters 'unsteckered'.

Later still, the three rotors for the scrambler were selected from a set of five or, in the case of the German Navy, eight rotors. The alphabet rings of rotors VI, VII and VIII contained two notches which, despite shortening the period of the substitution alphabet, made decryption more difficult.

Most military Enigmas also featured a plugboard (German: *Steckerbrett*). This altered the electrical pathway between the keyboard and the entry wheel of the scrambler and, in the opposite direction, between the scrambler and the lampboard. It did this by exchanging letters reciprocally, so that if *A* was plugged to *G* then pressing key *A* would lead to current entering the scrambler at the *G* position, and if *G* was pressed the current would enter at *A*. The same connections applied for the current on the way out to the lamp panel.

For an enemy to decipher German military Enigma messages required that the following were known.

Logical structure of the machine (unchanging)

- The wiring between the keyboard (and lampboard) and the entry plate.
- The wiring of each rotor
- The number and position(s) of turnover notches on the rings of the rotors.
- The wiring of the reflectors.

Internal settings (usually changed less frequently than external settings)

- The selection of rotors in use and their ordering on the spindle (*Walzenlage* or "wheel order").
- The positions of the alphabet ring in relation to the core of each rotor in use (*Ringstellung* or "ring settings").

External settings (usually changed more frequently than internal settings)

- The plugboard connections (*Steckerverbindungen* or "stecker values").
- The rotor positions at the start of enciphering the text of the message.

Discovering the logical structure of the machine may be called "breaking" it, a one-off process except when changes or additions were made to the machines. Finding the internal and external settings for one or more messages may be called "solving"[13] - although breaking is often used for this process as well.

Security properties

The various Enigma models provided different levels of security. The presence of a plugboard (*Steckerbrett*) substantially increased the security of the encipherment. Each pair of letters that were connected together by a plugboard lead, were referred to as *stecker partners*, and the letters that remained unconnected were said to be *self-steckered*.[14] In general, the unsteckered Enigma was used for commercial and diplomatic traffic and could be broken relatively easily using hand methods, while attacking versions with a plugboard was much more difficult. The British read unsteckered Enigma messages sent during the Spanish Civil War,[15] and also some Italian naval traffic enciphered early in World War II.

The strength of the security of the ciphers that were produced by the Enigma machine was a product of the large numbers associated with the scrambling process.

1. It produced a polyalphabetic substitution cipher with a period (16,900) that was many times the length of the longest message.
2. The 3-rotor scrambler could be set in 26 × 26 × 26 = 17,576 ways, and the 4-rotor scrambler in 26 × 17,576 = 456,976 ways.
3. With six leads on the plugboard, the number of ways that pairs of letters could be interchanged was 100,391,791,500 (100 billion)[16] and with ten leads, it was 150,738,274,937,250 (151 trillion).[17]

However, the way that Enigma was used by the Germans meant that, if the settings for one day (or whatever period was represented by each row of the setting sheet) were established, the rest of the messages for that network on that day could quickly be deciphered.[18]

The security of Enigma ciphers did have fundamental weaknesses that proved helpful to cryptanalysts.

1. A letter could never be encrypted to itself, a consequence of the reflector.[19] This property was of great help in using *cribs*—short sections of plaintext thought to be somewhere in the ciphertext—and could be used to eliminate a crib in a particular position. For a possible location, if any letter in the crib matched a letter in the ciphertext at the same position, the location could be ruled out.[20] It was this feature that the British mathematician and logician Alan Turing exploited in designing the British bombe.
2. The plugboard connections were reciprocal, so that if A was plugged to N, then N likewise became A. It was this property that led mathematician Gordon Welchman at Bletchley Park to propose that a *diagonal board* be introduced into the bombe, substantially reducing the number of incorrect rotor settings that the bombes found.[21]

3. The notches in the *alphabet rings* of rotors I to V were in different positions, which helped cryptanalysts to work out the *wheel order* by observing when the middle rotor was turned over by the right-hand rotor.[22]
4. There were substantial weaknesses, in both policies and practice, in the way that Enigma was used (see 'Operating shortcomings' below).

Key setting

Enigma featured the major operational convenience of being symmetrical (or self-inverse). This meant that decipherment worked in the same way as encipherment, so that when the ciphertext was typed in, the sequence of lamps that lit yielded the plaintext.

Identical setting of the machines at the transmitting and receiving ends was achieved by key setting procedures. These varied from time to time and across different networks. They consisted of *setting sheets* in a *codebook*.[23][24] which were distributed to all users of a network, and were changed regularly. The message key was transmitted in an *indicator*.[25] as part of the message preamble. The word *key* was also used at Bletchley Park to describe the network that used the same Enigma setting sheets. Initially these were recorded using coloured pencils and were given the names *red*, *light blue* etc., and later the names of birds such as *kestrel*.[26] During World War II the settings for most networks lasted for 24 hours, although towards the end of the war, some were changed more frequently.[27] The sheets had columns specifying, for each day of the month, the rotors to be used and their positions, the ring positions and the plugboard connections. For security, the dates were in reverse chronological order down the page, so that each row could be cut off and destroyed when it was finished with.[28]

The top part of an early setting sheet looked something like this[29]

Datum **[Date]**	***Walzenlage*** **[Rotors]**	***Ringstellung*** **[Ring settings]**	***Steckerverbindungen*** **[Plugboard settings]**	***Grundstellung*** **[Initial rotor settings]**
31	I II III	W N M	HK CN IO FY JM LW	RAO
30	III I II	C K U	CK IZ QT NP JY GW	VQN
29	II III I	B H N	FR LY OX IT BM GJ	XIO

Up until 15 September 1938,[30] the transmitting operator indicated to the receiving operator(s) how to set their rotors, by choosing a three letter *message key* (the key specific to that message) and enciphering it twice using the specified initial ring positions (the *Grundstellung*). The resultant 6-letter indicator, was then transmitted before the enciphered text of the message.[31] Suppose that the specified *Grundstellung* was *RAO,* and the chosen 3-letter message key was *IHL,* the operator would set the rotors to *RAO* and encipher *IHL* twice. The resultant ciphertext, *DQYQQT,* would be transmitted, followed by the message enciphered using message key *IHL.* The receiving operator would use the specified *Grundstellung RAO* to decipher the first six letters, yielding *IHLIHL.* The receiving operator, seeing the repeated message key would know that there had been no corruption and use *IHL* to decipher the message.

The weakness in this indicator procedure came from two factors. First, use of a global *Grundstellung* —this was changed in September 1938 so that the operator selected his initial position to encrypt the message key, and sent the initial position in clear followed by the enciphered message key. The second problem was the repetition of message key within the indicator, which was a serious security flaw.[32] The message setting was encoded twice, resulting in a relation between first and fourth, second and fifth, and third and sixth character. This security problem enabled the Polish Cipher Bureau to break into the pre-war Enigma system as early as 1932. On 1 May 1940 the Germans changed the procedures to encipher the message key only once.

British efforts

In 1927, the UK openly purchased a commercial Enigma. Its operation was analysed and reported. Although a leading British cryptographer, Dilly Knox (a veteran of World War I and the cryptanalytical activities of the Royal Navy's Room 40), worked on decipherment he had only the messages he generated himself to practice with. After Germany supplied modified commercial machines to the Nationalist side in the Spanish Civil War, and with the Italian Navy (who were also aiding the Nationalists) using a version of the commercial Enigma that did not have a plugboard, Britain could intercept the radio broadcast messages. In April 1937[33] Knox made his first decryption of an Enigma encryption using a technique that he called *buttoning up* to discover the rotor wirings[34] and another that he called *rodding* to solve messages.[35] This relied heavily on cribs and on a crossword-solver's expertise in Italian, as it yielded a limited number of spaced-out letters at a time.

Britain had no access to the messages broadcast by Germany which were using the military Enigma machine.[36]

Polish breakthroughs

In the 1920s the German military began using a 3-rotor Enigma, whose security was increased in 1930 by the addition of a plugboard.[37] The Polish Cipher Bureau sought to break it due to the threat that Poland faced from Germany, but its early attempts did not succeed. Near the beginning of 1929, the Polish Cipher Bureau realized that mathematicians may make good codebreakers; the bureau invited math students at Poznań University to take a class on cryptology.[38] After the class, the Bureau recruited some students to work part-time at a Bureau branch set up in Poznań for the students. The branch operated for some time. On 1 September 1932, 27-year-old Polish mathematician Marian Rejewski and two fellow Poznań University mathematics graduates, Henryk Zygalski and Jerzy Różycki, joined the Bureau full-time and moved to Warsaw.[39] Their first task was to reconstruct a four-letter German naval cipher.[40]

Near the end of 1932 Rejewski was asked to work a couple hours a day on breaking the Enigma.[41]

Marian Rejewski c. 1932, when he first broke Enigma

Rejewski's characteristics method

Marian Rejewski quickly spotted the Germans' major procedural weakness of specifying a single indicator setting (*Grundstellung*) for all messages on a network for a day, and repeating the operator's chosen *message key* in the enciphered 6-letter indicator. That procedural mistake allowed Rejewski to decipher the message keys without knowing any of the machine's wirings. In the above example of *DQYQQT* being the enciphered indicator, it is known that the first letter *D* and the fourth letter *Q* represent the same letter, enciphered three positions

apart in the scrambler sequence. Similarly with *Q* and *Q* in the second and fifth positions, and *Y* and *T* in the third and sixth. Rejewski exploited this fact by collecting a sufficient set of messages enciphered with the same indicator setting, and assembling three tables for the 1,4, the 2,5, and the 3,6 pairings. Each of these tables might look something like the following:

First letter	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
Fourth letter	N	S	Y	Q	T	I	C	H	A	F	E	X	J	P	U	L	W	R	Z	K	G	O	V	M	D	B

A path from one first letter to the corresponding fourth letter, then from that letter as the first letter to its corresponding fourth letter, and so on until the first letter recurs, traces out a cycle group.[42] The above table contains six cycle groups.

Cycle group starting at A (9 links)	(A, N, P, L, X, M, J, F, I, A)
Cycle group starting at B (3 links)	(B, S, Z, B)
Cycle group starting at C (9 links)	(C, Y, D, Q, W, V, O, U, G, C)
Cycle group starting at E (3 links)	(E, T, K, E)
Cycle group starting at H (1 link)	(H, H)
Cycle group starting at R (1 link)	(R, R)

Rejewski recognized that a cycle group must pair with another group of the same length. Even though Rejewski did not know the rotor wirings or the plugboard permutation, the German mistake allowed him to reduce the number of possible substitution ciphers to a small number. For the 1,4 pairing above, there are only $1\times3\times9=27$ possibilities for the substitution ciphers at positions 1 and 4.

Rejewski also exploited cipher clerk laziness. Scores of messages would be enciphered by several cipher clerks, but some of those messages would have the same encrypted indicator. That meant that both clerks happened to choose the same three letter starting position. Such a collision should be rare with randomly selected starting positions, but lazy cipher clerks often chose starting positions such as "AAA", "BBB", or "CCC". Those security mistakes allowed Rejewski to solve each of the six permutations used to encipher the indicator

That solution was an extraordinary feat. Rejewski did it without knowing the plugboard permutation or the rotor wirings. Even after solving for the six permutations, Rejewski did not know how the plugboard was set or the positions of the rotors. Knowing the six permutations also did not allow Rejewski to read any messages.

The spy and the rotor wiring

Before Rejewski started work on the Enigma, the French had a spy, Hans-Thilo Schmidt, who worked at Germany's Cipher Office in Berlin and had access to some Enigma documents. Even with the help of those documents, the French did not make progress on breaking the Enigma. The French decided to share the material with their British and Polish allies. In a December 1931 meeting, the French provided Gwido Langer, head of the Polish Cipher Bureau, with copies of some Enigma material. Langer asked the French for more material, and Gustave Bertrand of French Military Intelligence quickly obliged; Bertrand provided additional material in May and September 1932.[43] The documents included two German manuals and two pages of Enigma daily keys.[44][45]

In December 1932, the Bureau provided Rejewski with some German manuals and monthly keys. The material enabled Rejewski to achieve "one of the most important breakthroughs in cryptologic history"[46] by using the theory of permutations and groups to work out the Enigma scrambler wiring.[47][48]

Rejewski could look at a day's cipher traffic and solve for the permutations at the six sequential positions used to encipher the indicator. Since Rejewski had the cipher key for the day, he knew and could factor out the plugboard permutation. He assumed the keyboard permutation was the same as the commercial Enigma, so he factored that out. He knew the rotor order, the ring settings, and the starting position. He developed a set of equations that would allow him to solve for the rightmost rotor wiring assuming the two rotors to the left did not move.[49]

He attempted to solve the equations, but failed with inconsistent results. After some thought, he realized one of his assumptions must be wrong.

Rejewski found that the connections between the military Enigma's keyboard and the entry ring were not, as in the commercial Enigma, in the order of the keys on a German typewriter. He made an inspired correct guess that it was in alphabetical order.[50] Britain's Dilly Knox was astonished when he learned, in July 1939, that the arrangement was so simple.[51][52]

With the new assumption, Rejewski succeeded in solving the wiring of the rightmost rotor. The next month's cipher traffic used a different rotor in the rightmost position, so Rejewski used the same equations to solve for its wiring. With those rotors known, the remaining third rotor and the reflector wiring were determined. Without capturing a single rotor to reverse engineer, Rejewski had determined the logical structure of the machine.

The Polish Cipher Bureau then had some Enigma machine replicas made; the replicas were called "Enigma doubles".

The grill method

The Poles now had the machine's wiring secrets, but they still needed to determine the daily keys for the cipher traffic. The Poles would examine the Enigma traffic and use the method of characteristics to determine the six permutations used for the indicator. The Poles would then use the grill method to determine the rightmost rotor and its position. That search would be complicated by the plugboard permutation, but that permutation only swapped six pairs of letters — not enough to disrupt the search. The grill method also determined the plugboard wiring. The grill method could also be used to determine the middle and left rotors and their setting (and those tasks were simpler because there was no plugboard), but the Poles eventually compiled a catalog of the $3\times2\times26\times26=4056$ possible Q permutations (reflector and 2 leftmost rotor permutations), so they could just look up the answer

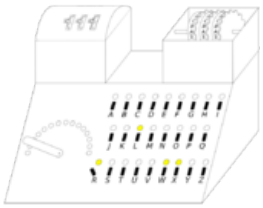
The only remaining secret of the daily key would be the ring settings, and the Poles would attack that problem with brute force. Most messages would start with the three letters "ANX" (*an* is German for "to" and the "X" character was used as a space). It may take almost $26\times26\times26=17576$ trials, but that was doable. Once the ring settings were found, the Poles could read the day's traffic.

The Germans made it easy for the Poles in the beginning. The rotor order only changed every quarter, so the Poles would not have to search for the rotor order. Later the Germans changed it every month, but that would not cause much trouble, either. Eventually, the Germans would change the rotor order every day, and late in the war (after Poland had been overrun) the rotor order might be changed during the day

The Poles kept improving their techniques as the Germans kept improving their security measures.

Invariant cycle lengths and the card catalog

Rejewski realised that, although the letters in the cycle groups were changed by the plugboard, the number and lengths of the cycles were unaffected—in the example above, six cycle groups with lengths of 9, 9, 3, 3, 1 and 1. He described this invariant structure as the *characteristic* of the indicator setting. There were only 105,456 possible rotor settings.[53][54] The Poles therefore set about creating a *card catalog* of these cycle patterns.[55]



Cyclometer, devised in the mid-1930s by Rejewski to catalog the cycle structure of Enigma permutations. 1: Rotor lid closed, 2: Rotor lid open, 3: Rheostat, 4: Glowlamps, 5: Switches, 6: Letters.

The cycle-length method would avoid using the grill. The card catalog would index the cycle-length for all starting positions (except for turnovers that occurred while enciphering an indicator). The day's traffic would be examined to discover the cycles in the permutations. The card catalog would be consulted to find the possible starting positions. There are roughly 1 million possible cycle-length combinations and only 105,456 starting positions. Having found a starting position, the Poles would use an Enigma double to determine the cycles at that starting position without a plugboard. The Poles would then compare those cycles to the cycles with the (unknown) plugboard and solve for the plugboard permutation (a simple substitution cipher). Then the Poles could find the remaining secret of the ring settings with the ANX method.

The problem was compiling the large card catalog.

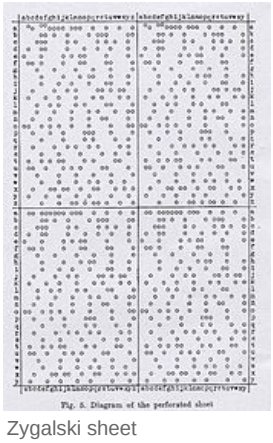
Rejewski, in 1934 or 1935, devised a machine to facilitate making the catalog and called it a *cyclometer*. This "comprised two sets of rotors... connected by wires through which electric current could run. Rotor N in the second set was three letters out of phase with respect to rotor N in the first set, whereas rotors L and M in the second set were always set the same way as rotors L and M in the first set".[56] Preparation of this catalog, using the cyclometer, was, said Rejewski, "laborious and took over a year, but when it was ready, obtaining daily keys was a question of [some fifteen] minutes".[57]

However, on 1 November 1937, the Germans changed the Enigma reflector, necessitating the production of a new catalog—"a task which [says Rejewski] consumed, on account of our greater experience, probably somewhat less than a year's time".[57]

This characteristics method stopped working for German naval Enigma messages on 1 May 1937, when the indicator procedure was changed to one involving special codebooks (see German Navy 3-rotor Enigma below).[58] Worse still, on 15 September 1938 it stopped working for German army and air force messages because operators were then required to choose their a *Grundstellung* (initial rotor setting) for each message. Although German army message keys would still be double enciphered, the days keys would not be double enciphered at the same initial setting, so the characteristic could no longer be found or exploited.

Perforated sheets

Although the characteristics method no longer worked, the inclusion of the enciphered message key twice gave rise to a phenomenon that the cryptanalyst Henryk Zygalski was able to exploit. Sometimes (about one message in eight) one of the repeated letters in the message key enciphered to the same letter on both occasions. These occurrences were called *samiczki*[59] (in English, *females*—a term later used at Bletchley Park).[60][61]



Zygalski sheet

Only a limited number of scrambler settings would give rise to females, and these would have been identifiable from the card catalog. If the first six letters of the ciphertext were ***S**ZV**S**IK*, this would be termed a 1-4 female; if *W**H**OE**H**S*, a 2-5 female; and if *AS**W**CR**W***, a 3-6 female. The method was called *Netz* (from *Netzverfahren*, "net method"), or the Zygalski sheet method as it used perforated sheets that he devised, although at Bletchley Park Zygalski's name was not used for security reasons.[62] About ten females from a day's messages were required for success.

There was a set of 26 of these sheets for each of the six possible sequences *wheel orders*. Each sheet was for the left (slowest-moving) rotor. The 51×51 matrices on the sheets represented the 676 possible starting positions of the middle and right rotors. The sheets contained about 1000 holes in the positions in which a female could occur.[63] The set of sheets for that day's messages would be appropriately positioned on top of each other in the perforated sheets apparatus. Rejewski wrote about how the device was operated:

> When the sheets were superposed and moved in the proper sequence and the proper manner with respect to each other, in accordance with a strictly defined program, the number of visible apertures gradually decreased. And, if a sufficient quantity of data was available, there finally remained a single aperture, probably corresponding to the right case, that is, to the solution. From the position of the aperture one could calculate the order of the rotors, the setting of their rings, and, by comparing the letters of the cipher keys with the letters in the machine, likewise permutation S; in other words, the entire cipher key.[64]

The holes in the sheets were painstakingly cut with razor blades and in the three months before the next major setback, the sets of sheets for only two of the possible six wheel orders had been produced.[65]

Polish *bomba*

After Rejewski's characteristics method became useless, he invented an electro-mechanical device that was dubbed the *bomba kryptologiczna* or *cryptologic bomb*. Each machine contained six sets of Enigma rotors for the six positions of the repeated three-letter key. Like the Zygalski sheet method, the *bomba* relied on the occurrence of *females*, but required only three instead of about ten for the sheet method. Six *bomby*[66] were constructed, one for each of the then possible *wheel orders*. Each *bomba* conducted an exhaustive (brute-force) analysis of the 17,576[67] possible message keys.

Rejewski has written about the device:

> The bomb method, invented in the autumn of 1938, consisted largely in the automation and acceleration of the process of reconstructing daily keys. Each cryptologic bomb (six were built in Warsaw for the Biuro Szyfrów Cipher Bureau before September 1939) essentially constituted an electrically powered aggregate of six Enigmas. It took the place of about one hundred workers and shortened the time for obtaining a key to about two hours.[68]

The cipher message transmitted the *Grundstellung* in the clear, so when a *bomba* found a match, it revealed the rotor order, the rotor positions, and the ring settings. The only remaining secret was the plugboard permutation.

Major setback

On 15 December 1938, the German Army increased the complexity of Enigma enciphering by introducing two additional rotors (IV and V). This increased the number of possible *wheel orders* from 6 to 60.[69] The Poles could then read only the small minority of messages that used neither of the two new rotors. They did not have the resources to commission 54 more bombs or produce 58 sets of Zygalski sheets. Other Enigma users received the two new rotors at the same time. However, until 1 July 1939 the *Sicherheitsdienst* (SD)—the intelligence agency of the SS and the Nazi Party—continued to use its machines in the old way with the same indicator setting for all messages. This allowed Rejewski to reuse his previous method, and by about the turn of the year he had worked out the wirings of the two new rotors.[69] On 1 January 1939, the Germans increased the number of plugboard connections from between five and eight to between seven and ten, which made other methods of decryption even more difficult.[57]

Rejewski wrote, in a 1979 critique of appendix 1, volume 1 (1979), of the official history of British Intelligence in the Second World War:

> we quickly found the [wirings] within the [new rotors], but [their] introduction ... raised the number of possible sequences of [rotors] from 6 to 60 ... and hence also raised tenfold the work of finding the keys. Thus the change was not qualitative but quantitative. We would have had to markedly increase the personnel to operate the bombs, to produce the perforated sheets ... and to manipulate the sheets.[70][71]

World War II

Italian naval Enigma

In 1940 Dilly Knox wanted to establish whether the Italian Navy were still using the same system that he had cracked during the Spanish Civil War; he instructed his assistants to use rodding to see whether the crib *PERX* (*per* being Italian for "for" and *X* being used to indicate a space between words) worked for the first part of the message. After three months there was no success, but Mavis Lever, a 19-year-old student, found that rodding produced *PERS* for the first four letters of one message. She then (against orders) tried beyond this and obtained *PERSONALE* (Italian for "personal"). This confirmed that the Italians were indeed using the same machines and procedures.[35]

The subsequent breaking of Italian naval Enigma ciphers led to substantial Allied successes. The cipher-breaking was disguised by sending a reconnaissance aircraft to the known location of a warship before attacking it, so that the Italians assumed that this was how they had been discovered. The Royal Navy's victory at the Battle of Cape Matapan in March 1941 was considerably helped by Ultra intelligence obtained from Italian naval Enigma signals.

Polish disclosures

As the likelihood of war increased in 1939, Britain and France pledged support for Poland in the event of action that threatened its independence.[72] In April, Germany withdrew from the German–Polish Non-Aggression Pact of January 1934. The Polish General Staff, realizing what was likely to happen, decided to share their work on Enigma decryption with their western allies. Marian Rejewski later wrote:

> [I]t was not [as Harry Hinsley suggested, cryptological] difficulties of ours that prompted us to work with the British and French, but only the deteriorating political situation. If we had had no difficulties at all we would still, or even the more so, have shared our achievements with our allies as our contribution to the struggle against Germany.[70][73]

At a conference near Warsaw on 26 and 27 July 1939, the Poles revealed to the French and British that they had broken Enigma and pledged to give each a Polish-reconstructed Enigma, along with details of their Enigma-solving techniques and equipment, including Zygalski's perforated sheets and Rejewski's cryptologic bomb.[74] In return, the British pledged to prepare two full sets of Zygalski sheets for all 60 possible wheel orders.[75] Dilly Knox was a member of the British delegation. He commented on the fragility of the Polish system's reliance on the repetition in the indicator, because it might "at any moment be cancelled".[76] In August two Polish Enigma doubles were sent to Paris, whence Gustave Bertrand took one to London, handing it to Stewart Menzies of Britain's Secret Intelligence Service at Victoria Station.[77]

Gordon Welchman, who became head of Hut 6 at Bletchley Park, wrote:

> Hut 6 Ultra would never have gotten off the ground if we had not learned from the Poles, in the nick of time, the details both of the German military version of the commercial Enigma machine, and of the operating procedures that were in use.[78]

Peter Calvocoressi, who became head of the Luftwaffe section in Hut 3, wrote of the Polish contribution:

> The one moot point is—how valuable? According to the best qualified judges it accelerated the breaking of Enigma by perhaps a year. The British did not adopt Polish techniques but they were enlightened by them.[79]

PC Bruno

On 17 September 1939, the day the Soviet Union began its invasion of Poland, Cipher Bureau personnel crossed their country's southeastern border into Romania. They eventually made their way to France, and on 20 October 1939, at *PC Bruno* outside Paris, the Polish cryptanalists resumed work on German Enigma ciphers in collaboration with Bletchley Park.[80]

PC Bruno and Bletchley Park worked together closely, communicating via a telegraph line secured by the use of Enigma doubles. In January 1940 Alan Turing spent several days at *PC Bruno* conferring with his Polish colleagues. He had brought the Poles a full set of Zygalski sheets that had been punched at Bletchley Park by John Jeffreys using Polish-supplied information, and on 17 January 1940, the Poles made the first break into wartime Enigma traffic—that from 28 October 1939.[81] From that time, until the Fall of France in June 1940, 17 percent of the Enigma keys that were found by the allies, were solved at *PC Bruno*.[82]

Just before opening their 10 May 1940 offensive against the Low Countries and France, the Germans made the feared change in the indicator procedure, discontinuing the duplication of the enciphered message key. This meant that the Zygalski sheet method no longer worked.[83][84] Instead, the cryptanalysts had to rely on exploiting the operator weaknesses described below, particularly the cillies and the Herivel tip.

After the June Franco-German armistice, the Polish cryptological team resumed work in France's southern *Free Zone*, although probably not on Enigma.[85] Marian Rejewski and Henryk Zygalski, after many travails, perilous journeys and Spanish imprisonment, finally made it to Britain,[86] where they were inducted into the Polish Army and put to work breaking German *SS* and *SD* hand ciphers at a Polish signals facility in Boxmoor. Due to their having been in occupied France, it was thought too risky to invite them to work at Bletchley Park.[87]

After the German occupation of Vichy France, several of those who had worked at *PC Bruno* were captured by the Germans. Despite the dire circumstances in which some of them were held, none betrayed the secret of Enigma's decryption.[88]

Operating shortcomings

Apart from some less-than-ideal inherent characteristics of the Enigma, in practice the system's greatest weakness was the way that it was used. The basic principle of this sort of enciphering machine is that it should deliver a very long stream of transformations that are difficult for a cryptanalyst to predict. Some of the instructions to operators, however, and their sloppy habits, had the opposite effect. Without these operating shortcomings, Enigma would, almost certainly not have been broken.[89]

The set of shortcomings that the Polish cryptanalysts exploited to such great effect included the following:

- The production of an early Enigma training manual containing an example of plaintext and its genuine ciphertext, together with the relevant message key. When Rejewski was given this in December 1932, it "made [his reconstruction of the Enigma machine] somewhat easier".[33]
- Repetition of the message key as described in Rejewski's characteristics method, above. (This helped in Rejewski's solving Enigma's wiring in 1932, and was continued until May 1940.)
- Repeatedly using the same stereotypical expressions in messages, an early example of what Bletchley Park would later term cribs. Rejewski wrote that "... we relied on the fact that the greater number of messages began with the letters *ANX*—German for "to", followed by *X* as a spacer".[90]
- The use of easily guessed keys such as *AAA* or *BBB*, or sequences that reflected the layout of the Enigma keyboard, such as "three [typing] keys that stand next to each other [o]r diagonally [from each other]...".[91] At Bletchley Park such occurrences were called *cillies*.[92][93] Cillies in the operation of the four-rotor *Abwehr* Enigma included four-letter names and German obscenities. Sometimes, with multi-part messages, the operator would not enter a key for a subsequent part of a message, merely leaving the rotors as they were at the end of the previous part, to become the message key for the next part.[94]
- Having only three different rotors for the three positions in the scrambler. (This continued until December 1938, when it was increased to five and then eight for naval traffic in 1940.)
- Using only six plugboard leads, leaving 14 letters *unsteckered*. (This continued until January 1939 when the number of leads was increased, leaving only a small number of letters unsteckered.)

Other useful shortcomings that were discovered by the British and later the American cryptanalysts included the following, many of which depended on frequent solving of a particular network:

- The practice of re-transmitting a message in an identical, or near-identical, form on different cipher networks. If a message was transmitted using both a low-level cipher that Bletchley Park broke by hand, and Enigma, the decrypt provided an excellent crib for Enigma decipherment.[95]
- For machines where there was a choice of more rotors than there were slots for them, a rule on some networks stipulated that no rotor should be in the same slot in the scrambler as it had been for the immediately preceding configuration. This reduced the number of wheel orders that had to be tried.[96]
- Not allowing a wheel order to be repeated on a monthly setting sheet. This meant that when the keys were being found on a regular basis, economies in excluding possible wheel orders could be made.[97]
- The stipulation, for Air Force operators, that no letter should be connected on the plugboard to its neighbour in the alphabet. This reduced the problem of identifying the plugboard connections and was automated in some Bombes with a Consecutive Stecker Knock-Out (CSKO) device.[98]
- The sloppy practice that John Herivel anticipated soon after his arrival at Bletchley Park in January 1940. He thought about the practical actions that an Enigma operator would have to make, and the short cuts he might employ. He thought that, after setting the alphabet rings to the prescribed setting, and closing the lid, the operator might not turn the rotors by more than a few places in selecting the first part of the indicator. Initially this did not seem to be the case, but after the changes of May 1940, what became known as the Herivel tip proved to be most useful.[92][99][100]
- The practice of re-using some of the columns of wheel orders, ring settings or plugboard connections from previous months. The resulting analytical short-cut was christened at Bletchley Park *Parkerismus* after Reg Parker, who had, through his meticulous record-keeping, spotted this phenomenon.[101]
- The re-use of a permutation in the German Air Force METEO code as the Enigma *stecker* permutation for the day.[102]

Mavis Lever, a member of Dilly Knox's team, recalled an occasion when there was an extraordinary message.

> The one snag with Enigma of course is the fact that if you press *A*, you can get every other letter but *A*. I picked up this message and—one was so used to looking at things and making instant decisions—I thought: 'Something's gone. What has this chap done? There is not a single *L* in this message.'
>
> My chap had been told to send out a dummy message and he had just had a fag [cigarette] and pressed the last key on the keyboard, the *L*. So that was the only letter that didn't come out. We had got the biggest crib we ever had, the encypherment was *LLLL*, right through the message and that gave us the new wiring for the wheel [rotor]. That's the sort of thing we were trained to do. Instinctively look for something that had gone wrong or someone who had done something silly and torn up the rule book![103]

Postwar debriefings of German cryptographic specialists, conducted as part of project TICOM, tend to support the view that the Germans were well aware that the un-steckered Enigma was theoretically solvable, but thought that the steckered Enigma had not been solved.[5]

Crib-based decryption

The term *crib* was used at Bletchley Park to denote any *known plaintext* or *suspected plaintext* at some point in an enciphered message.

Britain's Government Code and Cipher School (GC&CS), before its move to Bletchley Park, had realised the value of recruiting mathematicians and logicians to work in codebreaking teams. Alan Turing, a Cambridge University mathematician with an interest in cryptology and in machines for implementing logical operations—and who was regarded by many as a genius—had started work for GC&CS on a part-time basis from about the time of the Munich Crisis in 1938.[104] Gordon Welchman, another Cambridge mathematician, had also received initial training in 1938,[105] and they both reported to Bletchley Park on 4 September 1939, the day after Britain declared war on Germany.

Most of the Polish success had relied on the repetition within the indicator. But as soon as Turing moved to Bletchley Park—where he initially joined Dilly Knox in the research section—he set about seeking methods that did not rely on this weakness, as they correctly anticipated that the German Army and Air Force might follow the German Navy in improving their indicator system.

The Poles had used an early form of crib-based decryption in the days when only six leads were used on the plugboard.[58] The technique became known as the *Forty Weepy Weepy* method for the following reason. When a message was a continuation of a previous one, the plaintext would start with *FORT* (from *Fortsetzung*, meaning "continuation") followed by the time of the first message given twice bracketed by the letter *Y*. At this time numerals were represented by the letters on the top row of the Enigma keyboard. So, "continuation of message sent at 2330" was represented as *FORTYWEEPYYWEEPY*.

Top row of the Enigma keyboard and the numerals they represented

Q	W	E	R	T	Z	U	I	O
1	2	3	4	5	6	7	8	9
(Zero was represented by P)								

Cribs were fundamental to the British approach to solving Enigma keys, but guessing the plaintext for a message was a highly skilled business. So in 1940 Stuart Milner-Barry set up a special *Crib Room* in Hut 8.[106][107]

Foremost amongst the knowledge needed for identifying cribs was the text of previous decrypts. Bletchley Park maintained detailed indexes[108] of message preambles, of every person, of every ship, of every unit, of every weapon, of every technical term and of repeated phrases such as forms of address and other German military jargon.[109] For each message the traffic analysis recorded the radio frequency, the date and time of intercept, and the preamble—which contained the network-identifying discriminant, the time of origin of the message, the callsign of the originating and receiving stations, and the indicator setting. This allowed cross referencing of a new message with a previous one.[110] Thus, as Derek Taunt, another Cambridge mathematician-cryptanalyst wrote, the truism that "nothing succeeds like success" is particularly apposite here.[97]

Stereotypical messages included *Keine besonderen Ereignisse* (literally, "no special occurrences"—perhaps better translated as "nothing to report"),[111] *An die Gruppe* ("to the group")[112] and a number that came from weather stations such as *weub null seqs null null* ("weather survey 0600"). This was actually rendered as *WEUBYYNULLSEQSNULLNULL*. The word *WEUB* being short for *Wetterübersicht*, *YY* was used as a separator and *SEQS* was common abbreviation of *sechs* (German for "six").[113] Field Marshal Erwin Rommel's Quartermaster started all of his messages to his commander with the same formal introduction.[114]

With a combination of probable plaintext fragment and the fact that no letter could be enciphered as itself, a corresponding ciphertext fragment could often be tested by trying every possible alignment of the crib against the ciphertext, a procedure known as *crib-dragging*. This, however, was only one aspect of the processes of solving a key. Derek Taunt has written that the three cardinal personal qualities that were in demand for cryptanalysis were (1) a creative imagination, (2) a well-developed critical faculty, and (3) a habit of meticulousness.[115] Skill at solving crossword puzzles was famously tested in recruiting some cryptanalysts. This was useful in working out plugboard settings when a possible solution was being examined. For example, if the crib was the word *WETTER* (German for "weather") and a possible decrypt before the plugboard settings had been discovered, was *TEWWER*, it is easy to see that *T* with *W* are *stecker partners*.[116] These examples, although illustrative of the principles, greatly over-simplify the cryptanalysts' tasks.

A fruitful source of cribs was re-encipherments of messages that had previously been decrypted either from a lower-level manual cipher or from another Enigma network.[117] This was called a *kiss* and happened particularly with German naval messages being sent in the *dockyard cipher* and repeated *verbatim* in an Enigma cipher. One German agent in Britain, Nathalie Sergueiew, code named *Treasure*, who had been *turned* to work for the Allies, was very verbose in her messages back to Germany, which were then re-transmitted on the *Abwehr* Enigma network. She was kept going by MI5 because this provided long cribs, not because of her usefulness as an agent to feed incorrect information to the *Abwehr*.[118]

Occasionally, when there was a particularly urgent need to solve German naval Enigma keys, such as when an Arctic convoy was about to depart, mines would be laid by the RAF in a defined position, whose grid reference in the German naval system did not contain any of the words (such as *sechs* or *sieben*) for which abbreviations or alternatives were sometimes used.[119] The warning message about the mines and then the "all clear" message, would be transmitted both using the *dockyard cipher* and the U-boat Enigma network. This process of *planting* a crib was called *gardening*.[120]

Although *cillies* were not actually cribs, the *chit-chat* in clear that Enigma operators indulged in amongst themselves, often gave a clue as to the cillies that they might generate.[121]

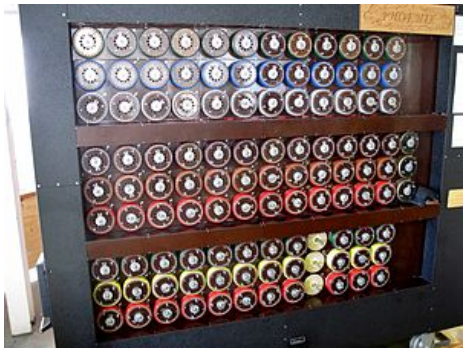
When captured German Enigma operators revealed that they had been instructed to encipher numbers by spelling them out rather than using the top row of the keyboard, Alan Turing reviewed decrypted messages and determined that the word *eins* ("one") appeared in 90% of messages. Turing automated the crib process, creating the *Eins Catalogue*, which assumed that *eins* was encoded at all positions in the plaintext. The catalogue included every possible rotor position for *EINS* with that day's *wheel order* and plugboard connections.[122]

British *bombe*

The British bombe was an electromechanical device designed by Alan Turing soon after he arrived at Bletchley Park in September 1939. Harold "Doc" Keen of the British Tabulating Machine Company (BTM) in Letchworth (35 kilometres (22 mi) from Bletchley) was the engineer who turned Turing's ideas into a working machine—under the codename CANTAB.[123] Turing's specification developed the ideas of the Poles' *bomba kryptologiczna* but was designed for the much more general crib-based decryption.

The bombe helped to identify the *wheel order*, the initial positions of the rotor cores, and the *stecker partner* of a specified letter. This was achieved by examining all 17,576 possible scrambler positions for a set of *wheel orders* on a comparison between a crib and the ciphertext, so as to eliminate possibilities that contradicted the Enigma's known characteristics. In the words of Gordon Welchman "the task of the bombe was simply to reduce the assumptions of *wheel order* and scrambler positions that required 'further analysis' to a manageable number".[107]

The demountable drums on the front of the bombe were wired identically to the connections made by Enigma's different rotors. Unlike them, however, the input and output contacts for the left-hand and the right-hand sides were separate, making 104 contacts between each drum and the rest of the machine.[124] This allowed a set of scramblers to be connected in series by means of 26-way cables. Electrical connections between the rotating drums' wiring and the rear plugboard were by means of metal brushes. When the bombe detected a scrambler position with no contradictions, it stopped and the operator would note the position before restarting it.



The working rebuilt bombe at Bletchley Park museum. Each of the rotating drums simulates the action of an Enigma rotor There are 36 Enigma-equivalents and, on the right end of the middle row, three *indicator* drums.

Although Welchman had been given the task of studying Enigma traffic callsigns and discriminants, he knew from Turing about the bombe design and early in 1940, before the first pre-production bombe was delivered, he showed him an idea to increase its effectiveness.[125] It exploited the reciprocity in plugboard connections, to reduce considerably the number of scrambler settings that needed to be considered further. This became known as the *diagonal board* and was subsequently incorporated to great effect in all the bombes.[21][126]

A cryptanalyst would prepare a crib for comparison with the ciphertext. This was a complicated and sophisticated task, which later took the Americans some time to master. As well as the crib, a decision as to which of the many possible *wheel orders* could be omitted had to be made. Turing's Banburismus was used in making this major economy. The cryptanalyst would then compile a *menu* which specified the connections of the cables of the patch panels on the back of the machine, and a particular letter whose *stecker partner* was sought. The menu reflected the relationships between the letters of the crib and those of the ciphertext. Some of these formed loops (or *closures* as Turing called them) in a similar way to the *cycles* that the Poles had exploited.

The reciprocal nature of the plugboard meant that no letter could be connected to more than one other letter. When there was a contradiction of two different letters apparently being *stecker partners* with the letter in the menu, the bombe would detect this, and move on. If, however, this happened with a letter that was not part of the menu, a false stop could occur. In refining down the set of stops for further examination, the cryptanalyst would eliminate stops that contained such a contradiction. The other plugboard connections and the settings of the alphabet rings would then be worked out before the scrambler positions at the possible true stops were tried out on Typex machines that had been adapted to mimic Enigmas. All the remaining stops would correctly decrypt the crib, but only the true stop would produce the correct plaintext of the whole message.[127]

To avoid wasting scarce bombe time on menus that were likely to yield an excessive number of false stops, Turing performed a lengthy probability analysis (without any electronic aids) of the estimated number of stops per rotor order. It was adopted as standard practice only to use menus that were estimated to produce no more than four stops per *wheel order*. This allowed an 8-letter crib for a 3-closure menu, an 11-letter crib for a 2-closure menu and a 14-letter crib for a menu with only one closure. If there was no closure, at least 16 letters were required in the crib.[127] The longer the crib, however, the more likely it was that *turn-over* of the middle rotor would have occurred.

The production model 3-rotor bombes contained 36 scramblers arranged in three banks of twelve. Each bank was used for a different *wheel order* by fitting it with the drums that corresponded to the Enigma rotors being tested. The first bombe was named *Victory* and was delivered to Bletchley Park on 18 March 1940. The next one, which included the diagonal board, was delivered on 8 August 1940. It was referred to as a *spider bombe* and was named *Agnus Dei* which soon became *Agnes* and then *Aggie*. The production of British bombes was relatively slow at first, with only five bombes being in use in June 1941, 15 by the year end,[128] 30 by September 1942, 49 by January 1943[129] but eventually 210 at the end of the war.

A refinement that was developed for use on messages from those networks that disallowed plugboard (*Stecker*) connection of adjacent letters, was the *Consecutive Stecker Knock Out*. This was fitted to 40 Bombes and produced a useful reduction in false stops.[130]

Initially the bombes were operated by ex-BTM servicemen, but in March 1941 the first detachment of members of the Women's Royal Naval Service (known as *Wrens*) arrived at Bletchley Park to become bombe operators. By 1945 there were some 2,000 Wrens operating the bombes.[131] Because of the risk of bombing, relatively few of bombes were located at Bletchley Park. The largest two outstations were at Eastcote (some 110 bombes and 800 Wrens) and Stanmore (some 50 bombes and 500 Wrens). There were also bombe outstations at Wavendon, Adstock and Gayhurst. Communication with Bletchley Park was by teleprinter links.

When the German Navy started using 4-rotor Enigmas, about sixty 4-rotor bombes were produced at Letchworth, some with the assistance of the General Post Office.[132] The NCR-manufactured US Navy 4-rotor bombes were, however, very fast and the most successful. They were extensively used by Bletchley Park over teleprinter links (using the Combined Cipher Machine) to OP-20-G[133] for both 3-rotor and 4-rotor jobs.[134]

Luftwaffe Enigma

Although the German army, SS, police, and railway all used Enigma with similar procedures, it was the *Luftwaffe* (Air Force) that was the first and most fruitful source of Ultra intelligence during the war. The messages were decrypted in Hut 6 at Bletchley Park and turned into intelligence reports in Hut 3.[135] The network code-named 'Red' at Bletchley Park was broken regularly and quickly from 22 May 1940 until the end of hostilities. Indeed, the Air Force section of Hut 3 expected the new day's Enigma settings to have been established in Hut 6 by breakfast time. The relative ease of solving this network's settings was a product of plentiful cribs and frequent German operating mistakes.[136] Luftwaffe chief Hermann Göring was known to use it for trivial communications, including informing squadron commanders to make sure the pilots he was going to decorate had been properly deloused. Such messages became known as "Göring funnies" to the staff at Bletchley Park.

Abwehr Enigma

Dilly Knox's last great cryptanalytical success before his untimely death in February 1943, was the solving, in 1941, of the *Abwehr* Enigma. Intercepts of traffic which had an 8-letter indicator sequence before the usual 5-letter groups led to the suspicion that a 4-rotor machine was being used.[137] The assumption was correctly made that the indicator consisted of a 4-letter message key enciphered twice. The machine itself was similar to a Model G Enigma, with three conventional rotors, though it did not have a plug board. The principal difference to the model G was that it was equipped with a reflector that was advanced by the stepping mechanism once it had been set by hand to its starting position (in all other variants, the reflector was fixed). Collecting a set of enciphered message keys for a particular day allowed *cycles* (or *boxes* as Knox called them) to be assembled in a similar way to the method used by the Poles in the 1930s.[138]

Enigma Model G, used by the *Abwehr*. It had three ordinary rotors and a rotating reflector, multiple notches on the rotor rings, but no plugboard.

Knox was able to derive, using his *buttoning up* procedure,[34] some of the wiring of the rotor that had been loaded in the fast position on that day. Progressively he was able to derive the wiring of all three rotors. Once that had been done, he was able to work out the wiring of the reflector.[138] Deriving the indicator setting for that day was achieved using Knox's time-consuming *rodding* procedure.[35] This involved a great deal of trial and error, imagination and crossword puzzle-solving skills, but was helped by *cillies*.

The *Abwehr* was the intelligence and counter-espionage service of the German High Command. The spies that it placed in enemy countries used a lower level cipher (which was broken by Oliver Strachey's section at Bletchley Park) for their transmissions. However, the messages were often then re-transmitted word-for-word on the *Abwehr's* internal Enigma networks, which gave the best possible crib for deciphering that day's indicator setting. Interception and analysis of *Abwehr* transmissions led to the remarkable state of affairs that allowed MI5 to give a categorical assurance that all the German spies in Britain were controlled as double agents working for the Allies under the Double Cross System.[118]

German Army Enigma

In the summer of 1940 following the Franco-German armistice, most Army Enigma traffic was travelling by land lines rather than radio and so was not available to Bletchley Park. The air Battle of Britain was crucial, so it was not surprising that the concentration of scarce resources was on *Luftwaffe* and *Abwehr* traffic. It was not until early in 1941 that the first breaks were made into German Army Enigma traffic, and it was the spring of 1942 before it was broken reliably, albeit often with some delay.[139] It is unclear whether the German Army Enigma operators made deciphering more difficult by making fewer operating mistakes.[140]

German Naval Enigma

The German Navy used Enigma in the same way as the German Army and Air Force until 1 May 1937 when they changed to a substantially different system. This used the same sort of setting sheet but, importantly, it included the ground key for a period of two, sometimes three days. The message setting was concealed in the indicator by selecting a trigram from a book (the *Kenngruppenbuch*, or K-Book) and performing a bigram substitution on it.[141] This defeated the Poles, although they suspected some sort of bigram substitution.

The procedure for the naval sending operator was as follows. First they selected a trigram from the K-Book, say YLA. They then looked in the appropriate columns of the K-Book and selected another trigram, say YVT, and wrote it in the boxes at the top of the message form:

.	Y	V	T
Y	L	A	.

They then filled in the "dots" with any letters, giving say:

Q	Y	V	T
Y	L	A	G

Finally they looked up the vertical pairs of letters in the Bigram Tables

$$QY \rightarrow UB\ YL \rightarrow LK\ VA \rightarrow RS\ TG \rightarrow PW$$

and wrote down the resultant pairs, UB, LK, RS and PW which were transmitted as two four letter groups at the start and end of the enciphered message. The receiving operator performed the converse procedure to obtain the message key for setting his Enigma rotors.

As well as these *Kriegsmarine* procedures being much more secure than those of the German Army and Air Force, the German Navy Enigma introduced three more rotors (VI, VII and VIII), early in 1940.[142] The choice of three rotors from eight meant that there were a total of 336 possible permutations of rotors and their positions.

Alan Turing decided to take responsibility for German naval Enigma because "no one else was doing anything about it and I could have it to myself".[143] He established Hut 8 with Peter Twinn and two "girls".[144] Turing used the indicators and message settings for traffic from 1–8 May 1937 that the Poles had worked out, and some very elegant deductions to diagnose the complete indicator system. After the messages were deciphered they were translated for transmission to the Admiralty in Hut 4.

German Navy 3-rotor Enigma

The first break of wartime traffic was in December 1939, into signals that had been intercepted in November 1938, when only three rotors and six plugboard leads had been in use.[145] It used "Forty Weepy Weepy" cribs.

A captured German *Funkmaat* ("radio operator") named Meyer had revealed that numerals were now spelt out as words. EINS, the German for "one", was present in about 90% of genuine German Navy messages. An EINS catalogue was compiled consisting of the encipherment of EINS at all 105,456 rotor settings.[146] These were compared with the ciphertext, and when matches were found, about a quarter of them yielded the correct plaintext. Later this process was automated in Mr Freeborn's section using Hollerith equipment. When the ground key was known, this EINS-ing procedure could yield three bigrams for the tables that were then gradually assembled.[145]

Further progress required more information from German Enigma users. This was achieved through a succession of *pinches*, the capture of Enigma parts and codebooks. The first of these was on 12 February 1940, when rotors VI and VII, whose wiring was at that time unknown, were captured from the German submarine *U-33*, by minesweeper HMS *Gleaner*.

On 26 April 1940, the Narvik-bound German patrol boat *VP2623*, disguised as a Dutch trawler named *Polares*, was captured by HMS *Griffin*. This yielded an instruction manual, codebook sheets and a record of some transmissions, which provided complete cribs. This confirmed that Turing's deductions about the trigram/bigram process was correct and allowed a total of six days' messages to be broken, the last of these using the first of the bombes.[145] However, the numerous possible rotor sequences, together with a paucity of usable cribs, made the methods used against the Army and Air Force Enigma messages of very limited value.

At the end of 1939, Turing extended the clock method invented by the Polish cryptanalyst Jerzy Różycki. Turing's method became known as "Banburismus". Turing said that at that stage "I was not sure that it would work in practice, and was not in fact sure until some days had actually broken."[147] Banburismus used large cards printed in Banbury (hence the Banburismus name) to discover correlations and a statistical scoring system to determine likely rotor orders (*Walzenlage*) to be tried on the bombes. The practice conserved scarce bombe time and allowed more messages to be attacked. In practice, the 336 possible rotor orders could be reduced to perhaps 18 to be run on the bombes.[148] Knowledge of the bigrams was essential for Banburismus, and building up the tables took a long time. This lack of visible progress led to Frank Birch, head of the Naval Section, to write on 21 August 1940 to Edward Travis, Deputy Director of Bletchley Park:

> "I'm worried about Naval Enigma. I've been worried for a long time, but haven't liked to say as much... Turing and Twinn are like people waiting for a miracle, without believing in miracles..."[149]

Schemes for capturing Enigma material were conceived including, in September 1940, Operation Ruthless by Lieutenant Commander Ian Fleming (author of the James Bond novels). When this was cancelled, Birch told Fleming that "Turing and Twinn came to me like undertakers cheated of a nice corpse..."[150]

A major advance came through Operation Claymore, a commando raid on the Lofoten Islands on 4 March 1941. The German armed trawler *Krebs* was captured, including the complete Enigma keys for February, but no bigram tables or K-book. However, the material was sufficient to reconstruct the bigram tables by "EINS-ing", and by late March they were almost complete.[151]

Banburismus then started to become extremely useful. Hut 8 was expanded and moved to 24-hour working, and a crib room was established. The story of Banburismus for the next two years was one of improving methods, of struggling to get sufficient staff, and of a steady growth in the relative and absolute importance of cribbing as the increasing numbers of bombes made the running of cribs ever faster.[152] Of value in this period were further "pinches" such as those from the German weather ships *München* and *Lauenburg* and the submarines *U-110* and *U-559*.

Despite the introduction of the 4-rotor Enigma for Atlantic U-boats, the analysis of traffic enciphered with the 3-rotor Enigma proved of immense value to the Allied navies. Banburismus was used until July 1943, when it became more efficient to use the many more bombes that had become available.

M4 (German Navy 4-rotor Enigma)

On 1 February 1942, the Enigma messages to and from Atlantic U-boats, which Bletchley Park called "'Shark," became significantly different from the rest of the traffic, which they called "Dolphin."[153]

This was because a new Enigma version had been brought into use. It was a development of the 3-rotor Enigma with the reflector replaced by a thin rotor and a thin reflector. Eventually, there were two fourth-position rotors that were called Beta and Gamma and two thin reflectors, Bruno and Caesar which could be used in any combination. These rotors were not advanced by the rotor to their right, in the way that rotors I to VIII were.

The introduction of the fourth rotor did not catch Bletchley Park by surprise, because captured material dated January 1941 had made reference to its development as an adaptation of the 3-rotor machine, with the fourth rotor wheel to be a reflector wheel.[154] Indeed, because of operator errors, the wiring of the new fourth rotor had already been worked out.

This major challenge could not be met by using existing methods and resources for a number of reasons.

1. The work on the Shark cipher would have to be independent of the continuing work on messages in the Dolphin cipher.
2. Solving Shark keys on 3-rotor bombes would have taken 50 to 100 times as long as an average Air Force or Army job.
3. U-boat cribs at this time were extremely poor.[155]

It seemed, therefore, that effective, fast, 4-rotor bombes were the only way forward. This was an immense problem and it gave a great deal of trouble. Work on a high speed machine had been started by Wynn-Williams of the TRE late in 1941 and some nine months later Harold Keen of BTM started work independently. Early in 1942, Bletchley Park were a long way from possessing a high speed machine of any sort.[156]

Eventually, after a long period of being unable to decipher U-boat messages, a source of cribs was found. This was the Kurzsignale (short signals), a code which the German navy used to minimize the duration of transmissions, thereby reducing the risk of being located by direction finding techniques. The messages were only 22 characters long and were used to report sightings of possible Allied targets.[157] A copy of the code book had been captured from *U-110* on 9 May 1941. A similar coding system was used for weather reports from U-boats, the *Wetterkurzschlüssel* (Weather Short Code Book). A copy of this had been captured from *U-559* on 29 or 30 October 1942.[158] These short signals had been used for deciphering 3-rotor Enigma messages and it was discovered that the new rotor had a neutral position at which it, and its matching reflector, behaved just like a 3-rotor Enigma reflector. This allowed messages enciphered at this neutral position to be deciphered by a 3-rotor machine, and hence deciphered by a standard bombe. Deciphered Short Signals provided good material for bombe menus for Shark.[159] Regular deciphering of U-boat traffic restarted in December 1942.[160]

The German Navy 4-rotor Enigma machine (M4) which was introduced for U-boat traffic on 1 February 1942.

American *bombes*

Unlike the situation at Bletchley Park, the United States armed services did not share a combined cryptanalytical service. Before the US joined the war, there was collaboration with Britain, albeit with a considerable amount of caution on Britain's side because of the extreme importance of Germany and her allies not learning that its codes were being broken. Despite some worthwhile collaboration amongst the cryptanalysts, their superiors took some time to achieve a trusting relationship in which both British and American bombes were used to mutual benefit.

In February 1941, Captain Abraham Sinkov and Lieutenant Leo Rosen of the US Army, and US naval Lieutenants Robert Weeks and Prescott Currier, arrived at Bletchley Park bringing, amongst other things, a replica of the 'Purple' cipher machine for the Bletchley Park's Japanese section in Hut 7.[161] The four returned to America after ten weeks, with a naval radio direction finding unit and many documents[162] including a "paper Enigma".[163]

The main American response to the 4-rotor Enigma was the US Navy bombe, which was manufactured in much less constrained facilities than were available in wartime Britain. Colonel John Tiltman, who later became Deputy Director at Bletchley Park, visited the US Navy cryptanalysis office (OP-20-G) in April 1942 and recognised America's vital interest in deciphering U-boat traffic. The urgent need, doubts about the British engineering workload and slow progress, prompted the US to start investigating designs for a Navy bombe, based on the full blueprints and wiring diagrams received by US naval Lieutenants Robert Ely and Joseph Eachus at Bletchley Park in July 1942.[164][165] Funding for a full, $2 million, Navy development effort was requested on 3 September 1942 and approved the following day

Commander Edward Travis, Deputy Director and Frank Birch, Head of the German Naval Section travelled from Bletchley Park to Washington in September 1942. With Carl Frederick Holden, US Director of Naval Communications they established, on 2 October 1942, a UK:US accord which may have "a stronger claim than BRUSA to being the forerunner of the UKUSA Agreement," being the first agreement "to establish the special Sigint relationship between the two countries," and "it set the pattern for UKUSA, in that the United States was very much the senior partner in the alliance".[166] It established a relationship of "full collaboration" between Bletchley Park and OP-20-G.[167]

US Navy bombe. It contained 16 four-rotor Enigma-equivalents and was much faster than the British bombe.

An all electronic solution to the problem of a fast bombe was considered,[168] but rejected for pragmatic reasons, and a contract was let with the National Cash Register Corporation (NCR) in Dayton, Ohio. This established the United States Naval Computing Machine Laboratory. Engineering development was led by NCR's Joseph Desch, a brilliant inventor and engineer. He had already been working on electronic counting devices.[169]

Alan Turing, who had written a memorandum to OP-20-G (probably in 1941),[170] was seconded to the British Joint Staff Mission in Washington in December 1942, because of his exceptionally wide knowledge about the bombes and the methods of their use. He was asked to look at the bombes that were being built by NCR and at the security of certain speech cipher equipment under development at Bell Labs.[171] He visited OP-20-G, and went to NCR in Dayton on 21 December. He was able to show that it was not necessary to build 336 Bombes, one for each possible rotor order, by utilising techniques such as Banburismus.[172] The initial order was scaled down to 96 machines.

The US Navy bombes used drums for the Enigma rotors in much the same way as the British bombes, but were very much faster. The first machine was completed and tested on 3 May 1943. Soon, these bombes were more available than the British bombes at Bletchley Park and its outstations, and as a consequence they were put to use for Hut 6 as well as Hut 8 work.[173] A total of 121 Navy bombes were produced.[174] In Alexander's "Cryptographic History of Work on German Naval Enigma", he wrote as follows.

> When the Americans began to turn out bombes in large numbers there was a constant interchange of signal - cribs, keys, message texts, cryptographic chat and so on. This all went by cable being first encyphered on the combined Anglo-American cypher machine, C.C.M. Most of the cribs being of operational urgency rapid and efficient communication was essential and a high standard was reached on this; an emergency priority signal consisting of a long crib with crib and message text repeated as a safeguard against corruption would take under an hour from the time we began to write the signal out in Hut 8 to the completion of its decyphering in Op. 20 G. As a result of this we were able to use the Op. 20 G bombes almost as conveniently as if they had been at one of our outstations 20 or 30 miles away.[175]

The US Army also produced a bombe. It was physically very different from the British and US Navy bombes. A contract was signed with Bell Labs on 30 September 1942.[176] The machine was designed to analyse 3-rotor, not 4-rotor traffic. It did not use drums to represent the Enigma rotors, using instead telephone-type relays. It could, however, handle one problem that the bombes with drums could not.[173][174] The set of ten bombes consisted of a total of 144 Enigma-equivalents, each mounted on a rack approximately 7 feet (2.1 m) long 8 feet (2.4 m) high and 6 inches (150 mm) wide. There were 12 control stations which could allocate any of the Enigma-equivalents into the desired configuration by means of plugboards. Rotor order changes did not require the mechanical process of changing drums, but was achieved in about half a minute by means of push buttons.[177] A 3-rotor run took about 10 minutes.[174]

German suspicions

The German navy was concerned that Enigma might be compromised. Key schedules were printed in water-soluble inks so they could not be salvaged.[178] The navy policed what its operators did and disciplined them when errors that could compromise the cipher were made.[179] The navy minimized its exposure. For example, Enigma machines were not carried by ships that might be captured or run aground. When ships were lost in circumstances where they might be salvaged, the Germans investigated.[180] After investigating some losses in 1940, Germany changed some message indicators.[181]

In April 1940, the British sank eight German destroyers in Norway. The Germans concluded that it was unlikely that the British were reading Enigma.[178]

In May 1941, the British deciphered some messages that gave the location of some supply ships for the battleship *Bismarck* and the cruiser *Prinz Eugen*. As part of the *Operation Rheinübung* commerce raid, the Germans had assigned five tankers, two supply ships, and two scouts to support the warships. After the *Bismarck* was sunk, the British directed its forces to sink the supporting ships *Belchen*, *Esso Hamburg*, *Egerland*, and some others. The Admiralty specifically did not target the tanker *Gedania* and the scout *Gonzenheim* figuring that sinking so many ships within one week would indicate to Germany that Britain was reading Enigma. However, by chance, British forces found those two ships and sank them.[182] The Germans investigated, but concluded Enigma had not been breached by either seizures or brute force cryptanalysis. Nevertheless, the Germans took some steps to make Enigma more secure. Grid locations (an encoded latitude and longitude) were further disguised using digraph tables and a numeric offset.[183] The U-boats were given their own network, *Triton*, to minimize the chance of a cryptanalytic attack.

In August 1941, the British captured *U-570*. The Germans concluded the crew would have destroyed the important documents, so the cipher was safe. Even if the British had captured the materials intact and could read Enigma, the British would lose that ability when the keys changed on 1 November.[184]

Although Germany realized that convoys were avoiding its wolfpacks, it did not attribute that ability to reading Enigma traffic. Instead, Dönitz thought that Britain was using radar and direction finding.[184] The *Kriegsmarine* continued to increase the number of networks to avoid superimposition attacks on Enigma. At the beginning of 1943, the *Kriegsmarine* had 13 networks.[185]

The *Kriegsmarine* also improved the Enigma. On 1 February 1942, it started using the four rotor Enigma.[186] The improved security meant that convoys would have less information to avoid wolfpacks, so if sinkings increased it would give the Germans a clue that Enigma had been read before the change. That recognition did not happen because other things changed at the same time, the United States had entered the war and Dönitz had sent U-boats to raid the US East Coast where there were lots of easy targets.[187]

In early 1943, Dönitz worried that the Allies were reading Enigma. Germany's own cryptanalysis of Allied communications showed surprising accuracy in its estimates of wolfpack sizes. It was concluded, however, that Allied direction finding was the source. The Germans also recovered a cavity magnetron from a downed British bomber. The conclusion was the Enigma was secure. The Germans were still suspicious, so each submarine got its own key net in June 1944.[188]

By 1945, almost all German Enigma traffic (Wehrmacht military; comprising the Heer, Kriegsmarine and Luftwaffe; and German intelligence and security services like the Abwehr, SD, etc.) could be decrypted within a day or two, yet the Germans remained confident of its security.[189] They openly discussed their plans and movements, handing the Allies huge amounts of information, not all of which was used effectively. For example, Rommel's actions at Kasserine Pass were clearly foreshadowed in decrypted Enigma traffic, but the information was not properly appreciated by the Americans.

After the war, Allied TICOM project teams found and detained a considerable number of German cryptographic personnel.[190] Among the things learned was that German cryptographers, at least, understood very well that Enigma messages might be read; they knew Enigma was not unbreakable.[5] They just found it impossible to imagine anyone going to the immense effort required.[191] When Abwehr personnel who had worked on Fish cryptography and Russian traffic were interned at Rosenheim around May 1945, they were not at all surprised that Enigma had been broken, only that someone had mustered all the resources in time to actually do it. Admiral Dönitz had been advised that a cryptanalytic attack was the least likely of all security problems.

Since World War II

Modern computers can be used to solve Enigma, using a variety of techniques.[192] There were also projects to decrypt some remaining messages using distributed computing.[193] Stefan Krah led an effort in Germany to crack three messages intercepted in 1942 by HMS *Hurricane*; the messages were published by Ralph Erskine in a 1995 letter to *Cryptologia*. Two of these messages were cracked in 2006,[194][195] and the final one was deciphered in 2013.[196] As of January 2018, the Enigma@home project is working on Enigma M4 message Nachricht P1030680, which was sent from U-534 on May 1, 1945.[197][198]

See also

- Cryptanalysis of the Lorenz cipher
- Tadeusz Pełczyński
- John Herivel
- I.J. Good
- Good–Turing frequency estimation
- Kiss (cryptanalysis)
- The Imitation Game

References and notes

1. Winterbotham 2000, pp. 16–17
2. Reuvers, Paul; Simons, Marc (2010) *Enigma Cipher Machine* (http://www.cryptomuseum.com/crypto/enigma/index.htm), retrieved 22 July 2010
3. Welchman 1997, p. 3
4. Calvocoressi 2001, p. 66
5. Huttenhain & Fricke 1945, pp. 4,5.
6. Singh 1999, p. 116
7. Churchhouse 2002, p. 4

8. Churchhouse 2002, pp. 4,5
9. Alexander c. 1945 "Background" Para. 2 Alexander (c. 1945) "Background" Para. 2
10. Ellsbury 1998a
11. Churchhouse 2002, pp. 202–204
12. Sale, Tony, *The components of the Enigma machine* (http://www.codesandciphers.org.uk/enigma/enigma2.htm), Enigma rotors (or wheels) retrieved 1 January 2010
13. Huttenhain & Fricke 1945, p. 2.
14. Copeland 2004, p. 245
15. Smith 2006, p. 23
16. Singh 1999, p. 136
17. Sale, Tony, *Military Use of the Enigma: The complexity of the Enigma machine* (http://www.codesandciphers.org.uk/enigma/enigma3.htm), retrieved 2 June 2010
18. Copeland 2004, p. 250
19. Mahon 1945, p. 3
20. Mahon 1945, p. 16
21. Welchman 1997, p. 245
22. Bauer 2002, p. 135
23. Sale, Tony, *Military Use of the Enigma: The Message Key and Setting Sheets* (http://www.codesandciphers.org.uk/enigma/enigma3.htm), Codes and Ciphers in the Second World War: The history, science and engineering of cryptanalysis in World War II, retrieved 21 October 2008
24. Rijmenants, Dirk, "Enigma Message Procedures" (http://users.telenet.be/d.rijmenants/en/enigmaproc.htm) *Cipher Machines and Cryptology*, retrieved 19 November 2009
25. Churchhouse 2002, pp. 33, 86
26. Hinsley, F.H. and Stripp, Alan (1993) p. xviii and Hinsley (1992) p. 2
27. One element of the key, the sequence of rotors in the machine, was at first changed quarterly; but from 1 January 1936 it was changed monthly; from 1 October 1936, daily; and later, during World War II, as often as every eight hours. Marian Rejewski, *Summary of Our Methods for Reconstructing ENIGMA and Reconstructing Daily Keys..*, Appendix C to Władysław Kozaczuk, *Enigma* (1984) p. 242
28. US Army 1945, p. 2
29. Sale, Tony, *Bigrams, Trigrams and Naval Enigma: The Daily Key, (Tagschluessel)* (http://www.codesandciphers.org.uk/lectures/naval1.htm), Lecture on Naval Enigma, retrieved 7 June 2010
30. The German Navy adopted a more complex and secure indicator procedure on 1 May 1937—see "German naval Enigma".
31. Gaj, Kris; Orłowski, Arkadiusz, *Facts and myths of Enigma: breaking stereotypes* (https://web.archive.org/web/20080414141147/http://teal.gmu.edu/courses/ECE543/viewgraphs_F03/EUROCRYPT_2003.pdf) (PDF), George Mason University Fairfax, VA 22030, U.S.A.; Institute of Physics, Polish Academy of Sciences Warszawa, Poland, Section 3.2, archived from the original (http://teal.gmu.edu/courses/ECE543/viewgraphs_F03/EUROCRYPT_2003.pdf) (PDF) on 14 April 2008, retrieved 1 February 2009
32. Gaj, Kris; Orłowski, Arkadiusz, *Facts and myths of Enigma: breaking stereotypes* (https://web.archive.org/web/20080414141147/http://teal.gmu.edu/courses/ECE543/viewgraphs_F03/EUROCRYPT_2003.pdf) (PDF), George Mason University Fairfax, VA 22030, U.S.A.; Institute of Physics, Polish Academy of Sciences Warszawa, Poland A, Section 7, archived from the original (http://teal.gmu.edu/courses/ECE543/viewgraphs_F03/EUROCRYPT_2003.pdf) (PDF) on 14 April 2008, retrieved 1 February 2009
33. Hodges (1983) p. 176
34. Carter, Frank (2004), *Buttoning Up: A method for recovering the wiring of the rotors used in a non-stecker Enigma* (http://www.bletchleypark.org.uk/content/buttoningup.pdf) (PDF), retrieved 20 January 2009
35. Carter, Frank (2004), *Rodding* (https://web.archive.org/web/20070411064026/http://www.bletchleypark.org.uk/content/rodding.pdf) (PDF), archived from the original (http://www.bletchleypark.org.uk/content/rodding.pdf) (PDF) on 11 April 2007, retrieved 20 January 2009
36. Gordon Corera (23 March 2012), *The Spanish link in cracking the Enigma code* (http://www.bbc.co.uk/news/magazine-17486464), BBC News
37. Wilcox 2001, p. 2
38. The course began on 15 January 1929. A letter dated "Warsaw, 29 January 1929, To Professor Z. Krygowski, in Poznań, ul. Głogowska 74/75," and signed by the "Chief of the General Staf, *Piskor* [i.e., Tadeusz Piskor], *Generał Dywizji*," reads: "I hereby thank *Pan Profesor* for his efforts and assistance given to the General Staf in organizing the cipher [i.e, cryptology] course opened in Poznań on 15 January 1929." The letter is reproduced in Stanisław Jakóbczyk and Janusz Stokłosa, *Złamanie szyfru Enigma* (The Breaking of the Enigma Cipher), 2007, p. 44.
39. Rejewski & Woytak 1984b, p. 231
40. Kozaczuk 1984, pp. 10–12
41. Rejewski's work on this may have started in late October or early November 1932. Kozaczuk 1984, p. 232.
42. Also referred to as a *box shape* or a *chain*. See Alexander c. 1945 Ch. II Para. 4
43. Sebag-Montefiore 1990, pp. 22–23
44. Rejewski & Woytak 1984b, p. 256
45. The documents were *Instructions for Using the Enigma Cipher Machine* and *Keying Instructions for the Enigma Cipher Machine*, and the pages of Enigma keys were for September and October 1932 which fortunately had different rotor orders.
46. Kahn 1991, p. 974
47. Wilcox 2001, p. 5
48. Hodges 1983, p. 170
49. Solve save for an arbitrary rotation.
50. Gaj & Orlowski 2003
51. Copeland 2004, p. 234
52. Rejewski & Woytak 1984b, p. 257 citing Fitzgerald, Penelope (1977), *The Knox Brothers*, London: Macmillan, ISBN 1-58243-095-0
53. 105,456 is the number of possible rotor settings (17,576) multiplied by the six *wheel orders* that were possible at this time. Singh 1999, p. 131

54. The characteristic does not make the rings disappear; the rings can make the card catalog fail because stepped entries won't be there (a factor of 6 if only single steps are considered). The characteristic allows the actual letters (and therefore the plugboard permutation) to be ignored. Furthermore, Rejewski's notion of characteristic may be differerent: it may be the cycles rather than the cycle lengths. See Rejewski July 1981, Annals of Hist Computing, 3, 3, pp 217–218.
55. Alexander c. 1945, Ch. II Para. 4
56. Rejewski 1984e, p. 285
57. Rejewski 1984c, p. 242
58. Mahon 1945, p. 13
59. Kozaczuk 1984, pp. 54, 63 note 2
60. In Welchman 1997, p. 72 he suggests that this arose from the nomenclature for plugs (male) and sockets (female) because the success of this method depended on a number of overlying sheets having their apertures in register
61. Sebag-Montefiore 2004, p. 362 cites Alfred Dillwyn Knox, who attended the 25 July 1939 Warsaw conference, as having given a more frankly biological etymology, discreetly veiled in French.
62. Instead they were called Jeffreys sheets after the head of the Bletchley Park section that produced them.
63. Welchman 1997, p. 215
64. Rejewski 1984e, p. 289
65. Welchman 1997, p. 216
66. *Bomby* is the plural of *bomba*.
67. 17,576 = 26^3, since Enigma used 26 letters on each of 3 rotors.
68. Rejewski 1984e, p. 290
69. Kozaczuk 1984, p. 54
70. Rejewski 1982, p. 80
71. Also quoted in Kozaczuk 1984, p. 63
72. Chamberlain, Neville (31 March 1939), "European Situation (2.52 p.m.)"(http://hansard.millbanksystems.com/commons/1939/mar/31/european-situation-1) *Hansard*, UK Parliament, **345**, retrieved 3 January 2009
73. Kozaczuk 1984, p. 64
74. Erskine 2006, p. 59
75. Herivel 2008, p. 55
76. Copeland 2004, p. 246
77. Bertrand 1973, pp. 60–61
78. Welchman 1984, p. 289
79. Calvocoressi, Peter (23 March 1984), "Credit to the Poles", *The Times*, London, p. 13
80. Kozaczuk 1984, pp. 69–94, 104–11
81. Kozaczuk 1984, pp. 84, 94 note 8
82. Rejewski 1982, pp. 81–82
83. Rejewski 1984c, p. 243
84. Rejewski 1984d, pp. 269–70
85. It is not clear whether, after the June 1940 fall of France, the Cipher Bureau broke Enigma. Rejewski, the principal Polish source, wrote in a posthumously published 1980 paper that at Cadix "We worked on other ciphers, no longer on Enigma." (Kozaczuk 1984, p. 270). Colonel Stefan Mayer of Polish Intelligence, however, mentioned the Poles breaking "interesting [machine-enciphered messages] from [Germany's 1941] Balkan campaign coming [in over] the 'Luftwaffe' network..." (Kozaczuk 1984, p. 116). And French intelligence Gen. Gustave Bertrand wrote of Enigma having been read at Cadix. (Kozaczuk 1984, p. 117). Tadeusz Lisicki, Rejewski's and Zygalski's immediate chief later in wartime England but sometimes a dubious source, wrote in 1982 that "Rejewski in [a letter] conceded that Bertrand was doubtless right that at Cadix they had read Enigma, and that the number given by Bertrand, of 673 [Wehrmacht] telegrams, was correct.... The British did not send keys to Cadix; these were found using various tricks such as the sillies [and] Herivel tip described by Welchman, Knox's method, as well as others that Rejewski no longer remembered." Kozaczuk 1984, p. 117).
86. The third mathematician, Jerzy Różycki, had perished together with three Polish and one French colleague in the 1942 sinking of the passenger ship *Lamoricière* as they were returning to France from a tour of duty in Algeria.
87. Kozaczuk 1984, pp. 148–55, 205–9
88. Kozaczuk 1984, p. 220
89. Churchhouse 2002, p. 122
90. Rejewski 1984c, pp. 243–44
91. Rejewski & Woytak 1984b, p. 235
92. Kahn 1991, p. 113
93. Sebag-Montefiore 2004, p. 92
94. Copeland 2004, p. 235
95. Alexander c. 1945 "Background" Para. 38
96. Bauer 2007, p. 441
97. Taunt 1993, p. 108
98. Budiansky 2000, p. 240
99. Welchman 1997, pp. 98–100
100. John Herivel, cited by Smith 2007, pp. 50–51
101. Welchman 1997, pp. 130, 131, 167
102. Bauer 2007, p. 442
103. Smith 2007, pp. 59, 60

104. Hodges 1995
105. Welchman 1997, p. 12
106. Mahon 1945, p. 24
107. Welchman 1997, p. 120
108. *Bletchley Park Archives: Government Code & Cypher School Card Indexes* (http://www.bletchleypark.org.uk/edu/archives/gccscoll.rhtm), retrieved 8 July 2010
109. Budiansky 2000, p. 301
110. Welchman 1984, p. 56
111. Milner-Barry 1993, p. 93
112. Smith 2007, p. 38
113. Taunt 1993, pp. 104, 105
114. Lewin 2001, p. 118
115. Taunt 1993, p. 111
116. Singh 1999, p. 174
117. Mahon 1945, p. 44
118. Smith 2007, p. 129
119. Mahon 1945, p. 41
120. Morris 1993, p. 235
121. Smith 2007, p. 102
122. *The 1944 Bletchley Park Cryptographic Dictionary* http://www.codesandciphers.org.uk/documents/cryptdict/page34.htm Dictionary entry for EINS CATALOGUE
123. Harper, John (ed.), "BTM - British Tabulatuing Machine CompanyLtd" (https://web.archive.org/web/20131204202741/http://www.jharper.demon.co.uk/bombe1.htm), *The British Bombe CANTAB* (http://www.jharper.demon.co.uk/bombe1.htm) archived from the original (http://www.jharper.demon.co.uk/btm1.htm) on 2013-12-04
124. Sale, Tony, "Alan Turing, the Enigma and the Bombe" (http://www.codesandciphers.org.uk/virtualbp/tbombe/tbombe.htm) in Sale, Tony, *The Enigma cipher machine* (http://www.codesandciphers.org.uk/enigma/)
125. Hodges 1983, p. 183
126. Ellsbury 1998b
127. Carter, Frank (2004), *From Bombe 'stops' to Enigma keys* (https://web.archive.org/web/20100108030414/http://www.bletchleypark.org.uk/content/bombestops.pdf) (PDF), archived from the original (http://www.bletchleypark.org.uk/content/bombestops.pdf) (PDF) on 8 January 2010, retrieved 1 March 2009
128. Copeland 2004, pp. 253–256
129. Budiansky 2000, p. 230
130. Bauer 2002, p. 482
131. Smith 2007, p. 75
132. Harper, John (ed.), "Bombe Types" (https://web.archive.org/web/20131204202741/http://www.jharper.demon.co.uk/bombe1.htm) *The British Bombe CANTAB* (http://www.jharper.demon.co.uk/bombe1.htm) archived from the original (http://www.jharper.demon.co.uk/types1.htm) on 2013-12-04
133. Mahon 1945, p. 89
134. Wenger, Engstrom & Meader 1998
135. Calvocoressi 2001, p. 74
136. Calvocoressi 2001, p. 87
137. Twinn 1993, p. 127
138. Carter, Frank, *The Abwehr Enigma Machine* (http://www.bletchleypark.org.uk/resources/file.rhtm/261894/web+abwehr2.pdf) (PDF)
139. Calvocoressi 2001, p. 99
140. Sullivan & Weierud 2005, p. 215
141. Supreme Command of the Navy (1940), "The Enigma General Procedure (Der Schluessel M Verfahren M Allgemein)" (http://www.codesandciphers.org.uk/documents/egenproc/egenproc.pdf) (PDF), *The Bletchley Park translated Enigma Instruction Manual, transcribed and formatted by Tony Sale*, Berlin: Supreme Command of the German Navy retrieved 26 November 2009
142. Copeland 2004, p. 225
143. Alexander c. 1945 Ch. II Para. 11
144. Copeland 2004, p. 258
145. Mahon 1945, p. 22
146. Alexander c. 1945 Ch. II Para. 21
147. Mahon 1945, p. 14
148. Alexander c. 1945 "Background" Para. 42
149. Mahon 1945, p. 2
150. Batey 2008, pp. 4–6
151. Mahon 1945, p. 26
152. Alexander c. 1945 Ch. III Para. 5
153. Alexander c. 1945 Ch. III Para. 20
154. Mahon 1945, p. 62
155. Alexander c. 1945 Ch. III Para. 21
156. Mahon 1945, p. 63
157. Sale, Tony, *The Breaking of German Naval Enigma: U Boat Contact Signals* (http://www.codesandciphers.org.uk/virtualbp/navenigma/navenig10.htm) Codes and Ciphers in the Second World War: The history, science and engineering of cryptanalysis in World War II, retrieved 1 December 2008

158. Budiansky 2000, pp. 341–343
159. Mahon 1945, p. 64
160. Mahon 1945, p. 77
161. Budiansky 2000, p. 176
162. Budiansky 2000, p. 179
163. Jacobsen 2000
164. Budiansky 2000, p. 238
165. Wilcox 2001, p. 21
166. Erskine 1999, pp. 187–197
167. Budiansky 2000, p. 239
168. Budiansky 2000, p. 241
169. Desch, Joseph R. (21 January 1942), *1942 Research Report* (http://www.daytoncodebreakers.org/wp-content/uploads/42rep.pdf) (PDF), retrieved 20 July 2013
170. Turing c. 1941, pp. 341–352
171. *Bletchley Park Text: November 1942: Departure of Alan Turing from BP* (http://cipherweb.open.ac.uk/cgi-bin/cipher-demo/mobile/sms_categories_xml.py?) retrieved 16 April 2010
172. Budiansky 2000, p. 242
173. Welchman 1997, p. 135
174. Wenger 1945, p. 52
175. Alexander c. 1945 Ch. VIII para. 11
176. Sebag-Montefiore 2004, p. 254
177. Wenger 1945, p. 51
178. Kahn 1991, p. 201
179. Kahn 1991, pp. 45–46
180. Kahn 1991, p. 199
181. Kahn 1991, p. 200
182. Kahn 1991, pp. 201–202
183. Kahn 1991, pp. 204–205
184. Kahn 1991, p. 206
185. Kahn 1991, p. 209
186. Kahn 1991, p. 210
187. Kahn 1991, pp. 210–211
188. Kahn 1991, pp. 260–262
189. Ferris 2005, p. 165
190. Rezabek 2017.
191. Bamford 2001, p. 17
192. Sullivan & Weierud 2005
193. *M4 Message Breaking Project* (http://www.bytereef.org/m4_project.html) retrieved 16 October 2008
194. Blenford, Adam (2006-03-02), *Online amateurs crack Nazi codes* (http://news.bbc.co.uk/2/hi/technology/4763854.stm) BBC
195. *Enigma project cracks second code* (http://news.bbc.co.uk/2/hi/technology/4808882.stm) BBC, 2006-03-15
196. Girard, Dan (2013-01-14), *Solution of the last of the HMS Hurricane intercepts* (http://www.enigma.hoerenberg.com/index.php?cat=M4%20Project%202006&page=Rasch%20Message) retrieved 4 January 2016
197. *Rare unbroken Enigma radio messages - P1030680 - Unbroken Enigma message (U534 - 01. May 1945)* (https://enigma.hoerenberg.com/index.php?cat=Unbroken), retrieved 2018-01-07
198. TJM (2013-02-18), *New M4 batch - U-534 P1030680* (http://www.enigmaathome.net/forum_thread.php?id=320), enigmaathome.net

Bibliography

- Alexander, C. Hugh O'D. (c. 1945), *Cryptographic History of Work on the German Naval Enigma* The National Archives, Kew, Reference HW 25/1
- Bamford, James (2001), *Body Of Secrets: How America's NSA & Britain's GCHQ Eavesdrop on the World* Century, ISBN 978-0-7126-7598-7
- Batey, Mavis (2008), *From Bletchley with Love*, Milton Keynes: Bletchley Park Trust, ISBN 978-1-906723-04-0
- Bauer, Friedrich Ludwig (2002), *Decrypted secrets: methods and maxims of cryptology* (3rd rev. and updated ed.), New York: Springer, ISBN 978-3-540-42674-5
- Bauer, F.L. (2007), "British and US cryptanalysis of the Wehrmacht Enigma", in de Leeuw, Karl; Bergstra, J. A., *The history of information security: a comprehensive handbook*, Elsevier, ISBN 978-0-444-51608-4
- Bertrand, Gustave (1973), *Enigma ou la plus grand énigme de la guerre 1939–1945 (Enigma: The Greatest Enigma of the War of 1939–1945)*, Paris: Librairie Plon
- Bloch, Gilbert (1987), "Enigma before Ultra: Polish Work and the French Contribution - Translated by C.A. Deavours", *Cryptologia* (published July 1987), **11**, pp. 142–155, doi:10.1080/0161-118791861947
- Brown, Brandi Dawn (1998), *Enigma- German Machine Cipher "Broken" by Polish Cryptologists*, retrieved 9 June 2010
- Brzezinski, Zbigniew (2005), "The Unknown Victors", in Ciechanowski, Stanisław, *Marian Rejewski, 1905-1980: living with the Enigma secret*, Bydgoszcz, Poland: Bydgoszcz City Council, pp. 15–18, ISBN 83-7208-117-4
- Budiansky, Stephen (2000), *Battle of wits: The Complete Story of Codebreaking in World War II*, Free Press, ISBN 978-0-684-85932-3
- Calvocoressi, Peter (2001) [1980], *Top Secret Ultra*, Kidderminster, England: M & M Baldwin, ISBN 0-947712-41-0

- Churchhouse, Robert (2002), *Codes and Ciphers: Julius Caesar, the Enigma and the Internet*, Cambridge: Cambridge University Press, ISBN 978-0-521-00890-7
- Copeland, Jack (2004), "Enigma", in Copeland, B. Jack, *The Essential Turing: Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life* plus *The Secrets of Enigma*, Oxford: Oxford University Press, ISBN 0-19-825080-0
- DeBrosse, Jim; Burke, Colin (2004), *The Secret in Building 26: The Untold Story of America's Ultra War Against the U-Boat Enigma Codes*, Random House, ISBN 978-0-375-50807-3
- Ellsbury, Graham (1998a), *Description of the Enigma Machine*, The Enigma Machine: Its Construction, Operation and Complexity (published 1998), retrieved 21 January 2009
- Ellsbury, Graham (1998b), "The Turing Bombe: What it was and how it worked", in Ellsbury, Graham, *The Enigma and the Bombe*
- Erskine, Ralph (1999), "The Holden Agreement on Naval Sigint: The First BRUSA?", *Intelligence and National Security*, **14** (2): 187–189, doi:10.1080/02684529908432545
- Erskine, Ralph (2006), "Alastair Denniston's", *Cryptologia* (published December 2006), **30** (4), pp. 294–305, doi:10.1080/01611190600920944
- Ferris, John Robert (2005), *Intelligence and strategy: selected essays* (illustrated ed.), Routledge, ISBN 978-0-415-36194-1
- Gaj, Kris; Orlowski, Arkadiusz (May 2003), "Facts and Myths of Enigma: Breaking Stereotypes", in Biham, Eli, *Advances in Cryptology — EUROCRYPT 2003: International Conference on the Theory and Applications of Cryptographic Techniques*, Warsaw, Poland: Springer-Verlag, pp. 106–122, ISBN 3-540-14039-5, LNCS 2656
- Gannon, James (2002), *Stealing Secrets, Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century*, Washington, D.C.: Brassey's, ISBN 978-1-57488-367-1
- Gillogly, James J. (1995), "Ciphertext-only Cryptanalysis of Enigma", *Cryptologia* (published October 1995), **19** (4), pp. 405–412, doi:10.1080/0161-119591884060, archived from the original on 7 February 2009, retrieved 1 February 2009
- Harper, John (2009), "Bombe Rebuild Project", *Resurrection: the bulletin of the Computer Conservation Society*, British Computer Society (published Spring 2009) (46), pp. 7–8, retrieved 22 May 2009
- Herivel, John (2008), *Herivelismus and the German Military Enigma*, M.& M.Baldwin, ISBN 978-0-947712-46-4
- Hinsley, F.H. (1993) [1992], "Introduction: The influence of Ultra in the Second World War", in Hinsley, F.H.; Stripp, Alan, *Codebreakers: The inside story of Bletchley Park*, Oxford: Oxford University Press, ISBN 978-0-19-280132-6
- Hodges, Andrew (1983), *Alan Turing: The Enigma* (1992 ed.), London: Vintage, ISBN 978-0-09-911641-7
- Hodges, Andrew (1995), *Alan Turing: a short biography: Part 4 The Second World War*, Alan Turing: a short biography, retrieved 23 October 2008
- Huttenhain, Orr; Fricke (1945), *OKW/Chi Cryptanalytic Research on Enigma, Hagelin and Cipher Teleprinter Messages*, TICOM This paper was written at the request of TICOM to show how the various German cipher machines could be solved. The authors assume Kerckhoffs's principle and do not address the breaking of the machines, only the solving of keys.
- Jacobsen, Philip H. (2000), *British provision of German naval Enigma information*, retrieved 26 March 2010
- Jones, R. V. (1978), *Most Secret War*, London: Book Club Associates, ISBN 978-0-241-89746-1
- Kahn, David (1991), *Seizing the Enigma: The Race to Break the German U-boat Codes, 1939-1943*, Houghton Mifflin Co., ISBN 978-0-395-42739-2
- Kahn, David (1966), *The Codebreakers: The Comprehenisve History of Secret Communication from Ancient Times to the Internet*, New York: Scribner, ISBN 0-684-83130-9
- Kozaczuk, Władysław (1984), *Enigma: How the German Machine Cipher was Broken, and how it was Read by the Allies in World War Two, edited and translated by Christopher Kasparek* (2 ed.), Frederick, Maryland: University Publications of America, ISBN 978-0-89093-547-7 A revised and augmented translation of *W kręgu enigmy*, Warsaw, Książka i Wiedza, 1979, supplemented with appendices by Marian Rejewski
- Kozaczuk, Władysław, Straszak, Jerzy (2004), *Enigma: How the Poles Broke the Nazi Code*, New York: Hippocrene Books, ISBN 978-0-7818-0941-2 Largely an abridgment of Kozaczuk 1984, minus Rejewski's appendices, which have been replaced with appendices of varying quality by other authors
- Lewin, Ronald (2001) [1978], *Ultra Goes to War: The Secret Story*, Classic Military History (Classic Penguin ed.), London, England: Hutchinson & Co, ISBN 978-1-56649-231-7
- Mahon, A.P. (1945), *The History of Hut Eight 1939 - 1945*, UK National Archives Reference HW 25/2, retrieved 10 December 2009
- Miller, A. Ray (2001), *The Cryptographic Mathematics of Enigma*, Center for Crypologic History archived from the original on 2 December 2008, retrieved 1 February 2009
- Milner-Barry, Stuart (1993), "Navy Hut 6: Early days", in Hinsley, F.H.; Stripp, Alan, *Codebreakers: The inside story of Bletchley Park*, Oxford: Oxford University Press, ISBN 978-0-19-280132-6
- Morris, Christopher (1993), "Navy Ultra's Poor Relations", in Hinsley, F.H.; Stripp, Alan, *Codebreakers: The inside story of Bletchley Park*, Oxford: Oxford University Press, ISBN 978-0-19-280132-6
- Murray, Joan (1993), "Hut 8 and naval Enigma, Part 1", in Hinsley, F.H.; Stripp, Alan, *Codebreakers: The inside story of Bletchley Park*, Oxford: Oxford University Press, ISBN 978-0-19-280132-6
- Rejewski, Marian (1942), *Sprawozdanie z prac kryptologicznych nad niemieckim szyfrem maszynowym Enigma* [*Report of Cryptologic Work on the German Enigma Machine Cipher*] (in Polish) Manuscript written at Uzès, France
- Rejewski, Marian (1967), *Wspomnienia z mej pracy w Biurze Szyfrów Oddziału II Sztabu Głównego 1932–1945* [*Memoirs of My Work in the Cipher Bureau of Section II of the [Polish] General Staff*] (in Polish) Manuscript
- Rejewski, Marian (1980), "An Application of the Theory of Permutations in Breaking the Enigma Cipher", *Applicationes mathematicae*, **16** (4), ISSN 1730-6280
- Rejewski, Marian (1982), "F.H. Hinsley", *Cryptologia* (published January 1982), **6** (1), pp. 75–83, doi:10.1080/0161-118291856867
- Rejewski, Marian; Woytak, Richard (1984b), *A Conversation with Marian Rejewski*: Appendix B of Kozaczuk 1984, pp. 229–40
- Rejewski, Marian (1984c), *Summary of Our Methods for Reconstructing ENIGMA and Reconstructing Daily Keys, and of German Efforts to Frustrate Those Methods:* Appendix C of Kozaczuk 1984, pp. 241–245
- Rejewski, Marian (1984d), *How the Polish Mathematicians Broke Enigma*: Appendix D of Kozaczuk 1984, pp. 246–271
- Rejewski, Marian (1984e), *The Mathematical Solution of the Enigma Cipher*: Appendix E of Kozaczuk 1984, pp. 272–291
- Rezabek, Randy (2017), *TICOM: the Hunt for Hitler's Codebreakers*, Independently published, ISBN 978-1521969021
- Sale, Tony, "The difficulties in breaking German Naval Enigma: Turing's Work", *Bigrams, Trigrams and Naval Enigma*, retrieved 26 November 2009
- Sebag-Montefiore, Hugh (2000), *Enigma: The Battle for the Code*, New York: John Wiley, ISBN 0-471-40738-0

- Sebag-Montefiore, Hugh (2004) [2000], *Enigma: The Battle for the Code* (Cassell Military Paperbacks ed.), London: Weidenfeld & Nicolson, ISBN 978-0-297-84251-4
- Singh, Simon (1999), *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, London: Fourth Estate, ISBN 1-85702-879-1
- Smith, Michael (2007) [1998], *Station X: The Codebreakers of Bletchley Park* (Pan Grand Strategy Series (Pan Books ed.), London: Pan McMillan Ltd, ISBN 978-0-330-41929-1
- Smith, Michael (2006), "How it began: Bletchley Park Goes to War", in Copeland, B Jack, *Colossus: The Secrets of Bletchley Park's Codebreaking Computers*, Oxford: Oxford University Press, ISBN 978-0-19-284055-4
- Sullivan, Geoff; Weierud, Frode (2005), "Breaking German Army Ciphers" (PDF), *Cryptologia*, **24** (3), pp. 193–232, doi:10.1080/01611190508951299, archived from the original (PDF) on 29 September 2017, retrieved 16 October 2008
- Taunt, Derek (1993), "Hut 6: 1941-1945", in Hinsley, F.H.; Stripp, Alan, *Codebreakers: The inside story of Bletchley Park*, Oxford: Oxford University Press, ISBN 978-0-19-280132-6
- Turing, Alan (1940), Erskine, Ralph; Marks, Philip; Weierud, Frode, eds., *Turing's Treatise on Enigma (The Prof's Book)*, retrieved 1 February 2009
- Turing, Alan (c. 1941), "Memorandum to OP-20-G on Naval Enigma", in Copeland, B. Jack, *The Essential Turing: Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life plus The Secrets of Enigma*, Oxford: Oxford University Press, pp. 341–352, ISBN 0-19-825080-0
- Twinn, Peter (1993), "The *Abwehr* Enigma", in Hinsley, F.H.; Stripp, Alan, *Codebreakers: The inside story of Bletchley Park*, Oxford: Oxford University Press, ISBN 978-0-19-280132-6
- US Army (1945), *The US 6812 Division Bombe Report Eastcote 1944*, archived from the original on 22 July 2009, retrieved 1 May 2010
- Welchman, Gordon (1984) [1982], *The Hut Six story: Breaking the Enigma codes*, Harmondsworth, England: Penguin Books, ISBN 9780140053050. An early publication containing several misapprehensions that are corrected in an *addendum* in the 1997 edition.
- Welchman, Gordon (1997) [1982], *The Hut Six story: Breaking the Enigma codes*, Cleobury Mortimer, England: M&M Baldwin, ISBN 978-0-947712-34-1. New edition updated with an *addendum* consisting of a 1986 paper written by Welchman that corrects his misapprehensions in the 1982 edition.
- Welchman, Gordon (1986), "From Polish Bomba to British Bombe: the Birth of Ultra", *Intelligence and National Security*, Ilford, England: Frank Cass & Company, **1** (1): 71–110, doi:10.1080/02684528608431842. This is reproduced as an *addendum* in the 1997 edition of Welchman's 'The Hut Six Story'.
- Wenger, J. N.; Engstrom, H. T.; Meader, R. I. (1998) [1944], *History of The Bombe Project: Memorandum for the Director of Naval Communications*, The Mariner's Museum, archived from the original on 2010-06-16
- Wenger, J. N. (1945), "Appendix II: U. S. Army Cryptanalytic Bombe", *Solving the Enigma: History of the Cryptanalytic Bombe, a NSA phamphlet*, archived from the original on 17 March 2010, retrieved 9 April 2010 (also National Archives and Records Administration Record Group 457, File 35701.)
- Wilcox, Jennifer E. (2001), "About the Enigma", *Solving the Enigma: History of the Cryptanalytic Bombe, a NSA phamphlet*, Center for Cryptologic History National Security Agency, archived from the original on 17 March 2010, retrieved 9 April 2010 ASIN: B0006RLRA4
- Winterbotham, F. W. (2000) [1974], *The Ultra secret: the inside story of Operation Ultra, Bletchley Park and Enigma*, London: Orion Books Ltd, ISBN 978-0-7528-3751-2, OCLC 222735270

External links

- Dayton Daily News, Dayton's Code Breakers
- Dayton Codebreakers Web site, DaytonCodebreakers.org
- About the Enigma (National Security Agency)
- "The Enigma Code Breach" by Jan Bury
- "Enigma" and Intelligence
- "The Enigma machine and Bletchley Park", *cybertwists.com*
- www.enigmahistory.org at the Wayback Machine (archived March 7, 2009)
- A capsule account of how the Poles and British broke the Army Enigma.
- "The German cipher machine Enigma", *Matematik Sider*, 20 September 2014
- "The Polish Enigma crackers", *Deutsche Welle*, 17 February 2015 (an audio report for general audiences)
- The Breaking of Enigma by the Polish Mathematicians