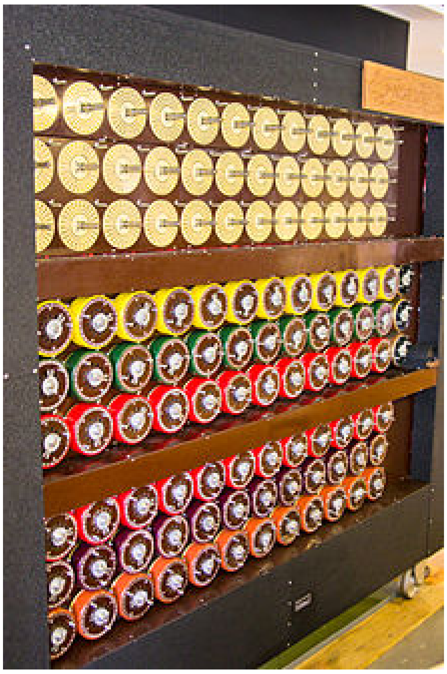
Bombe

The **bombe** (UK: /bɒmb/) was an electro-mechanical device used by British cryptologists to help decipher German Enigma-machine-encrypted secret messages during World War II.[2] The US Navy[3] and US Army[4] later produced their own machines to the same functional specification, but engineered differently from each other and from the British Bombe.



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-hand end of the middle row, three *indicator* drums. John Harper led the "Phoenix" team that rebuilt this bombe.[1] It was officially switched on by the Duke of Kent, patron of the British Computer Society on 17 July 2008.

The initial design of the bombe was produced in 1939 at the UK Government Code and Cypher School (GC&CS) at Bletchley Park by Alan Turing,[5] with an important refinement devised in 1940 by Gordon Welchman.[6] The engineering design and construction was the work of Harold Keen of the British Tabulating Machine Company. It was a substantial development from a device that had been designed in 1938 in Poland at the Biuro Szyfrów (Cipher Bureau) by cryptologist Marian Rejewski, and known as the "cryptologic bomb" (Polish: *bomba kryptologiczna*). The first bombe, code-named *Victory*, was installed in March 1940[7] while the second version, *Agnus Dei* or *Agnes*, incorporating Welchman's new design, was working by August 1940.[8]

The bombe was designed to discover some of the daily settings of the Enigma machines on the various German military networks: specifically, the set of rotors in use and their positions in the machine; the rotor core start positions for the message —the message key—and one of the wirings of the plugboard.[9][10][11]

Contents

The Enigma machine
- Four-rotor Enigma

The principle of the bombe
- Structure
- Bombe menu
- Stecker values
- Automated deduction
- In practice

The British Bombe

Response to the four-rotor Enigma
- US Navy Bombe
- US Army Bombe

Bombe rebuild

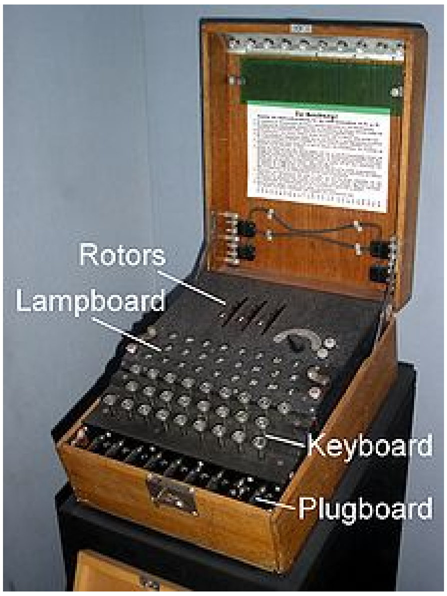
See also

Notes

References

External links

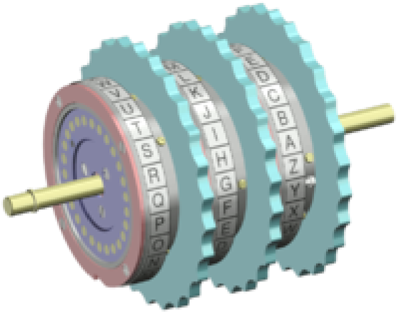
The Enigma machine



A three-rotor Enigma with plugboard (*Steckerbrett*)

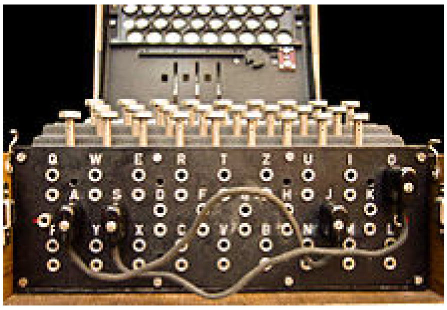
The Enigma was an electro-mechanical rotor machine used for the encryption and decryption of secret messages. It was developed in Germany in the 1920s. The repeated changes of the electrical pathway from the keyboard to the lampboard implemented a polyalphabetic substitution cipher, which turned plaintext into ciphertext and back again. The Enigma's scrambler contained rotors with 26 electrical contacts on each side, whose wiring diverted the current to a different position on the two sides. On depressing a key on the keyboard, an electric current flowed through an entry drum at the right-hand end of the scrambler, then through the set of rotors to a reflecting drum (or reflector) which turned it back through the rotors and entry drum, and out to cause one lamp on the lampboard to be illuminated.[12]

At each key depression, the right-hand or "fast" rotor advanced one position, which caused the encipherment to change. In addition, at a certain point, the right-hand rotor caused the middle rotor to advance; in a similar way, the middle rotor might cause the left-hand (or "slow") rotor to advance. Each rotor caused the "turnover" of the rotor to its left after a full rotation. The Enigma operator could rotate the wheels by hand to change the letter of the alphabet showing through a window, to set the start position of the rotors for enciphering a message. This three-letter sequence was the "message key". There were 26 × 26 × 26 = 17,576 possible positions of the set of three rotors, and hence different message keys. By opening the lid of the machine and releasing a compression bar, the set of three rotors on their spindle could be removed from the machine and their sequence (called the "wheel order" at Bletchley Park) could be altered. Multiplying 17,576 by the six possible wheel orders gives 105,456 different ways that the scrambler could be set up.



Depiction of a series of three rotors from an Enigma machine

Although 105,456 is a large number,[13] it does not guarantee security. A brute-force attack is possible: one could imagine using 100 code clerks who each tried to decode a message using 1000 distinct rotor settings. The Poles developed card catalogs so they could easily find rotor positions; Britain built "`EINS`" (a common German word) catalogs. Less intensive methods were also possible. If all message traffic for a day used the same rotor starting position, then frequency analysis for each position could recover the polyalphabetic substitutions. If different rotor starting positions were used, then overlapping portions of a message could be found using the index of coincidence.[14] Many major powers (including the Germans) could break Enigma traffic if they knew the rotor wiring. The German military knew the Enigma was weak.[15]



The plugboard of an Enigma machine, showing two pairs of letters swapped: S–O and A–J. During World War II, ten plugboard connections were made.

In 1930, the German army introduced an additional security feature, a plugboard (*Steckerbrett* in German; each plug is a *Stecker*) that further scrambled the letters. The Enigma encryption is a self inverse: it swapped letters in pairs: if **A** was transformed into **R** then **R** was transformed into **A**. The plugboard maintained the self inverse, but the plugboard transformation, unlike the rotor transformation, did not change during the encryption. This regularity was exploited by Welchman's "diagonal board" enhancement to the bombe, which vastly increased its efficiency.[16] With six plug leads in use (leaving 14 letters "unsteckered") this gives 100,391,791,500 possible ways of setting up the plugboard.[17]

An important feature of the machine from a cryptanalyst's point of view, and indeed Enigma's Achilles' heel, was that the reflector in the scrambler meant that a letter was never enciphered as itself. Any putative solution that gave, for any location, the same letter in the proposed plaintext and the ciphertext, could therefore be eliminated.[18]

In the lead up to World War II, the Germans made successive improvements to their military Enigma machines. By January 1939, additional rotors had been introduced so that there was a choice of three from five (i.e. 60 wheel orders) for the army and airforce Enigmas, and three out of eight (336 wheel orders) for the navy machines. In addition, ten leads were used on the plugboard leaving only six letters unsteckered. This meant that the airforce and army Enigmas could be set up 1.5×10^{19} ways. In 1941 the German navy introduced a version of Enigma with rotatable reflector (the M4 or Four-rotor Enigma) for communicating with its U-boats. This could be set up in 1.8×10^{20} different ways.[17]

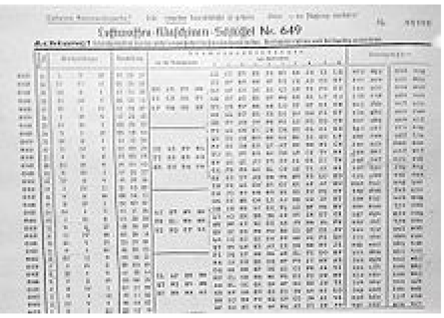
Four-rotor Enigma

By late 1941 a change in German Navy fortunes in the Battle of the Atlantic, combined with intelligence reports, convinced Admiral Karl Dönitz that the Allies could read German Navy coded communications, and a fourth rotor with unknown wiring was added to German Navy Enigmas used for U-boat communications, producing the *Triton* system, known at Bletchley Park as *Shark*. This was coupled with a thinner reflector design to make room for the extra rotor. The Triton was designed in such a way that it remained compatible with three-rotor machines when necessary. One of the extra 'fourth' rotors, the 'beta', was designed so that when it was paired with the thin 'B' reflector and rotor and ring were set to 'A', the pair acted as a standard three-rotor wide 'B' reflector. As before, the unknown wiring would prevent unauthorized reading of messages. Fortunately for the Allies, in December 1941, before the machine went into official service, a submarine accidentally sent a message with the fourth rotor in the wrong position. It then retransmitted the message with the rotor in the correct (three-rotor emulating) position. In February 1942 the change in the number of rotors used became official, and the Allies' ability to read German submarines' messages ceased until a snatch from a captured U-boat revealed not only the four-rotor machine's ability to emulate a three-rotor machine, but also that the fourth rotor did not move during a message. This along with the aforementioned mistake allowed the code breakers to eventually figure out the wiring of both the 'beta' and 'gamma' fourth rotors.

The first half of 1942 was the "Second Happy Time" for the German U-boats, with renewed success in attacking Allied shipping. This was due to the security of the new Enigma, and their ability to read Allied convoy messages sent in Naval Cipher No. 3. Between January and March 1942, German submarines sank 216 ships off the US east coast. In May 1942 the US began using the convoy system and requiring a blackout of coastal cities so that ships would not be silhouetted against their lights, but this yielded only slightly improved security for Allied shipping. The Allies' failure to change the cipher for three months plus the fact that Allied messages never contained any raw Enigma decrypts (or even mentioned that they were decrypting messages), helped convince the Germans that their messages were secure. Conversely, the Allies learned that the Germans had broken the naval cipher almost immediately from Enigma decrypts, but lost many ships due to the delay in changing the cipher

The principle of the bombe

The following settings of the Enigma machine must be discovered to decipher German military Enigma messages. Once these are known, all the messages for that network for that day (or pair of days in the case of the German navy) could be decrypted.



A German Enigma key list with machine settings for each day of one month

Internal settings (that required the lid of the Enigma machine to be opened)

- The selection of rotors in use in the Enigma's scrambler, and their positions on the spindle (*Walzenlage* or "wheel order"). Possible wheel orders numbered 60 (three rotors from a choice of five) for army and air force networks and 336 (three rotors from a choice of eight) for the naval networks.
- The positions of the alphabet ring's turnover notch in relation to the core of each rotor in use (*Ringstellung* or "ring settings"). There are 26 possible ring-settings for each rotor.

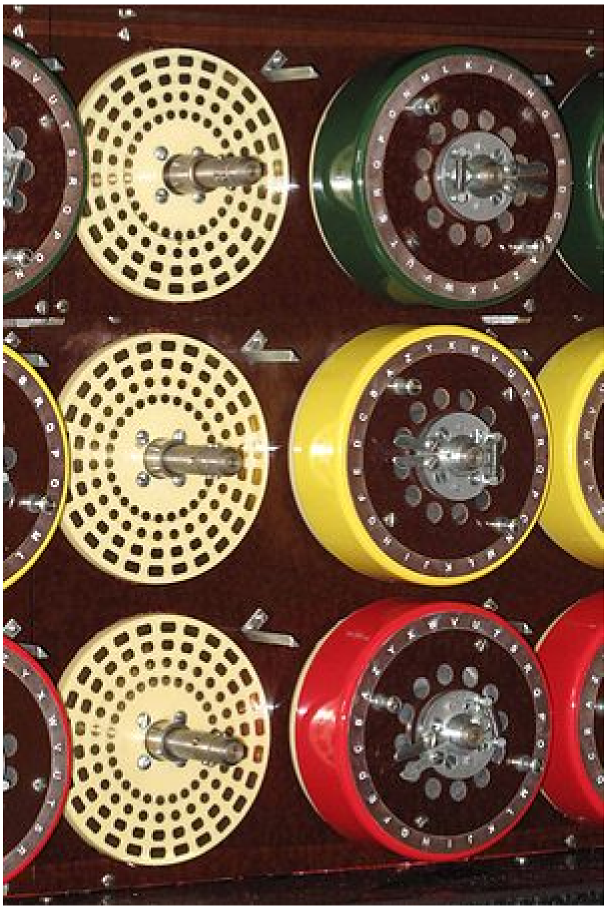
External settings (that could be changed without opening the Enigma machine)

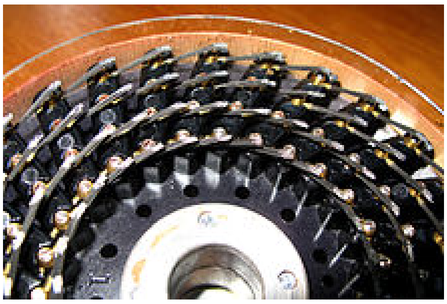
- The plugboard connections (*Steckerverbindungen* or "stecker values"). The ten leads could be arranged in $\frac{\binom{26}{2}\cdot\binom{24}{2}\cdot\binom{22}{2}\cdot\ldots\cdot\binom{8}{2}}{10!} = 150,738,274,937,250$ different combinations (approximately 151 trillion).[19]
- The scrambler rotor positions at the start of enciphering the message key (the *Grundstellung* or "indicator-setting") — up to May 1940; or thereafter the initial positions of each rotor at the start of enciphering the message (the "message key") from which the indicator-setting could be derived. There are 17,576 possible three-letter keys.

The bombe identified possible initial positions of the rotor cores and the *stecker partner* of a specified letter for a set of wheel orders. Manual techniques were then used to complete the decryption process.[20] 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".[21]

Structure

The bombe was an electro-mechanical device that replicated the action of several Enigma machines wired together. A standard German Enigma employed, at any one time, a set of three rotors, each of which could be set in any of 26 positions. The standard British bombe contained 36 Enigma equivalents, each with three drums wired to produce the same scrambling effect as the Enigma rotors. A bombe could run two or three jobs simultaneously. Each job would have a menu that had to be run against a number of different wheel orders. If the menu contained 12 or fewer letters, three different wheel orders could be run on one bombe; if more than 12 letters, only two.


The three drums of one of the 36 Enigma-equivalents, and the mounting plates for another, showing the 104 contacts for the wire brushes on the back of the drums. The top drum corresponds to the left-hand Enigma rotor, the middle drum to the middle rotor and the bottom drum to the right-hand rotor.


Wire brushes on the back of a drum from the rebuilt Bombe.

In order to simulate Enigma rotors, each rotor drum of the bombe had two complete sets of contacts, one for input towards the reflector and the other for output from the reflector, so that the reflected signal could pass back through a separate set of contacts. Each drum had 104 wire brushes, which made contact with the plate onto which they were loaded. The brushes and the corresponding set of contacts on the plate were arranged in four concentric circles of 26. The outer pair of circles (input and output) were equivalent to the current in an Enigma passing in one direction through the scrambler, and the inner pair equivalent to the current flowing in the opposite direction.

The interconnections within the drums between the two sets of input and output contacts were both identical to those of the relevant Enigma rotor. There was permanent wiring between the inner two sets of contacts of the three input/output plates. From there, the circuit continued to a plugboard located on the left-hand end panel, which was wired to imitate an Enigma reflector and then back through the outer pair of contacts. At each end of the "double-ended Enigma", there were sockets on the back of the machine, into which 26-way cables could be plugged.

Drums on the rebuilt Bombe in action. The upper drums all rotate continuously and in synchrony

The bombe drums were arranged with the top one of the three simulating the left-hand rotor of the Enigma scrambler, the middle one the middle rotor, and the bottom one the right-hand rotor. The top drums were all driven in synchrony by an electric motor. For each full rotation of the top drums, the middle drums were incremented by one position, and likewise for the middle and bottom drums, giving the total of 26 × 26 × 26 = 17,576 positions of the 3-rotor Enigma scrambler.[22][23]

The drums were colour-coded according to which Enigma rotor they emulated: I Red; II Maroon; III Green; IV Yellow; V Brown; VI Cobalt (Blue); VII Jet (Black); VIII Silver.[24]

At each position of the rotors, an electric current would or would not flow in each of the 26 wires, and this would be tested in the bombe's comparator unit. For a large number of positions, the test would lead to a logical contradiction, ruling out that setting. If the test did not lead to a contradiction, the machine would stop.

The operator would record the candidate solution by reading the positions of the indicator drums and the indicator unit on the Bombe's right-hand end panel. The operator then restarted the run. The candidate solutions, *stops* as they were called, were processed further to eliminate as many false stops as possible. Typically, there were many false bombe stops before the correct one was found.

The candidate solutions for the set of wheel orders were subject to extensive further cryptanalytical work. This progressively eliminated the false stops, built up the set of plugboard connections and established the positions of the rotor alphabet rings.[25] Eventually, the result would be tested on a Typex machine that had been modified to replicate an Enigma, to see whether that decryption produced German language.[26]

Bombe menu

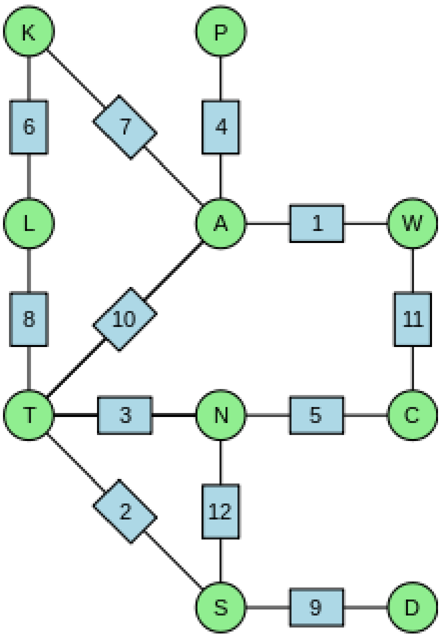
A bombe run involved a cryptanalyst first obtaining a *crib* — a section of plaintext that was thought to correspond to the ciphertext. Finding cribs was not at all straightforward; it required considerable familiarity with German military jargon and the communication habits of the operators. However, the codebreakers were aided by the fact that the Enigma would never encrypt a letter to itself. This helped in testing a possible crib against the ciphertext, as it could rule out a number of cribs and positions, where the same letter occurred in the same position in both the plaintext and the ciphertext. This was termed a *crash* at Bletchley Park.

Once a suitable crib had been decided upon, the cryptanalyst would produce a *menu* for wiring up the bombe to test the crib against the ciphertext. The following is a simplified explanation of the process of constructing a menu. Suppose that the crib is **ATTACKATDAWN** to be tested against a certain stretch of ciphertext, say, **WSNPNLKLSTCS**. The letters of the crib and the ciphertext were compared to establish pairings between the ciphertext and the crib plaintext. These were then graphed as in the diagram. It should be borne in mind that the relationships are reciprocal so that **A** in the plaintext associated with **W** in the ciphertext is the same as **W** in the plaintext associated with **A** in the ciphertext. At position 1 of the plaintext-ciphertext comparison, the letter **A** is associated with **W**, but **A** is also associated with **P** at position 4, **K** at position 7 and **T** at position 10. Building up these relationships into such a diagram provided the menu from which the bombe connections and drum start positions would be set up.

Ciphertext	W	S	N	P	N	L	K	L	S	T	C	S
Plaintext "crib"	A	T	T	A	C	K	A	T	D	A	W	N
Message position	1	2	3	4	5	6	7	8	9	10	11	12
Upper drum setting	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Middle drum setting	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z

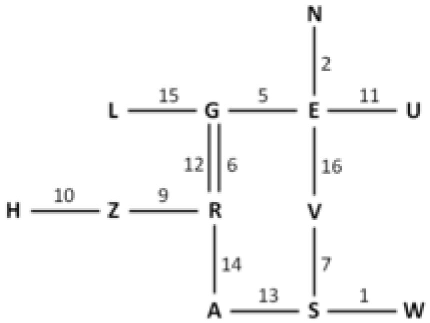
Lower drum setting	A	B	C	D	E	F	G	H	I	J	K	L

In the illustration, there are three sequences of letters which form loops (or *cycles* or *closures*), **ATLK**, **TNS** and **TAWCN**. The more loops in the menu, the more candidate rotor settings the bombe could reject, and hence the fewer false stops.



A graph of the letters of a crib and ciphertext expressed as a graph to provide a *menu* which specifies how to set up a bombe run. This example is somewhat unusual in that it contains as many as three loops.

Alan Turing conducted a very substantial analysis (without any electronic aids) to estimate how many bombe stops would be expected according to the number of letters in the menu and the number of loops. Some of his results are given in the following table.[27] Recent bombe simulations have shown similar results.



Bombe menu based on Bletchley Park display board which gives credit to Peggy Erskine-Tulloch as the originator.

Estimated number of bombe stops per rotor order

	Number of letters on the menu								
Loops	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
3	2.2	1.1	0.42	0.14	0.04	<0.01	<0.01	<0.01	<0.01
2	58	28	11	3.8	1.2	0.30	0.06	<0.01	<0.01
1	1500	720	280	100	31	7.7	1.6	0.28	0.04
0	40,000	19,000	7300	2700	820	200	43	7.3	1.0

Stecker values

The German military Enigma included a plugboard (*Steckerbrett* in German) which swapped letters (indicated here by P) before and after the main scrambler's change (indicated by S). The plugboard connections were known to the cryptanalysts as Stecker values. If there had been no plugboard, it would have been relatively straightforward to test a rotor setting; a Typex machine modified to replicate Enigma could be set up and the crib letter **A** encrypted on it, and compared with the ciphertext, **W**. If they matched, the next letter would be tried, checking that **T** encrypted to **S** and so on for the entire length of the crib. If at any point the letters failed to match, the initial rotor setting would be rejected; most incorrect settings would be ruled out after testing just two letters. This test could be readily mechanised and applied to all 17,576 settings of the rotors.

However, with the plugboard, it was much harder to perform trial encryptions because it was unknown what the crib and ciphertext letters were transformed to by the plugboard. For example, in the first position, $P(\mathtt{A})$ and $P(\mathtt{W})$ were unknown because the plugboard settings were unknown.

Turing's solution to working out the stecker values (plugboard connections) was to note that, even though the values for, say, $P(\mathtt{A})$ or $P(\mathtt{W})$, were unknown, the crib still provided known relationships amongst these values; that is, the values after the plugboard transformation. Using these relationships, a cryptanalyst could reason from one to another and, potentially, derive a logical contradiction, in which case the rotor setting under consideration could be ruled out.

A worked example of such reasoning might go as follows: a cryptanalyst might suppose that $P(\mathtt{A}) = \mathtt{Y}$. Looking at position 10 of the crib:ciphertext comparison, we observe that **A** encrypts to **T**, or, expressed as a formula:

$$\mathtt{T} = P(S_{10}(P(\mathtt{A})))$$

Due to the function P being its own inverse, we can apply it to both sides of the equation and obtain the following:

$$P(\mathtt{T}) = S_{10}(P(\mathtt{A}))$$

This gives us a relationship between $P(\mathtt{A})$ and $P(\mathtt{T})$. If $P(\mathtt{A}) = \mathtt{Y}$, and for the rotor setting under consideration $S_{10}(\mathtt{Y}) = \mathtt{Q}$ (say), we can deduce that

$$P(\mathtt{T}) = S_{10}(P(\mathtt{A})) = S_{10}(\mathtt{Y}) = \mathtt{Q}$$

While the crib does not allow us to determine what the values after the plugboard are, it does provide a constraint between them. In this case, it shows how $P(\mathtt{T})$ is completely determined if $P(\mathtt{A})$ is known.

Likewise, we can also observe that **T** encrypts to **L** at position 8. Using S_8, we can deduce the steckered value for **L** as well using a similar argument, to get, say,

$$P(\mathtt{L}) = S_8(P(\mathtt{T})) = S_8(\mathtt{Q}) = \mathtt{G}$$

Similarly, in position 6, **K** encrypts to **L**. As the Enigma machine is self-reciprocal, this means that at the same position **L** would also encrypt to **K**. Knowing this, we can apply the argument once more to deduce a value for $P(\mathtt{K})$, which might be:

$$P(\mathtt{K}) = S_6(P(\mathtt{L})) = S_6(\mathtt{G}) = \mathtt{F}$$

And again, the same sort of reasoning applies at position 7 to get:

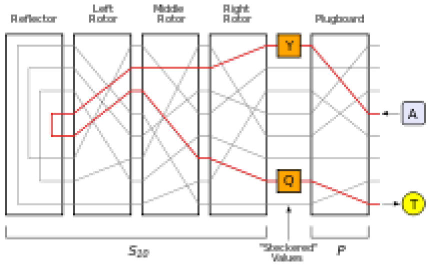
$$P(\mathtt{A}) = S_7(P(\mathtt{K})) = S_7(\mathtt{F}) = \mathtt{N}$$

However, in this case, we have derived a contradiction, since, by hypothesis, we assumed that $P(\mathtt{A}) = \mathtt{Y}$ at the outset. This means that the initial assumption must have been incorrect, and so that (for this rotor setting) $P(\mathtt{A}) \neq \mathtt{Y}$ (this type of argument is termed *reductio ad absurdum* or "proof by contradiction").

The cryptanalyst hypothesised one plugboard interconnection for the bombe to test. The other stecker values and the ring settings were worked out by hand methods.

Automated deduction

To automate these logical deductions, the bombe took the form of an electrical circuit. Current flowed around the circuit near-instantaneously, and represented all the possible logical deductions which could be made at that position. To form this circuit, the bombe used several sets of Enigma rotor stacks wired up together according to the instructions given on a menu, derived from a crib. Because each Enigma machine had 26 inputs and outputs, the replica Enigma stacks are connected to each other using 26-way cables. In addition, each Enigma stack rotor setting is offset a number of places as determined by its position in the crib; for example, an Enigma stack corresponding to the fifth letter in the crib would be four places further on than that corresponding to the first letter



A deduction step used by the bombe; while the actual intermediate values after the plugboard P — the "steckered" values — are unknown, if one is guessed then it is possible to use the crib to deduce other steckered values. Here, a guess that $P($**A**$)$ = **Y** can be used to deduce that $P($**T**$)$ = **Q** because **A** and **T** are linked at the 10th position in the crib.

In practice

Practical bombes used several stacks of rotors spinning together to test multiple hypotheses about possible setups of the Enigma machine, such as the order of the rotors in the stack.

While Turing's bombe worked in theory, it required impractically long cribs to rule out sufficiently large numbers of settings. Gordon Welchman came up with a way of using the symmetry of the Enigma stecker to increase the power of the bombe. His suggestion was an attachment called the *diagonal board* that further improved the bombe's effectiveness.[6]

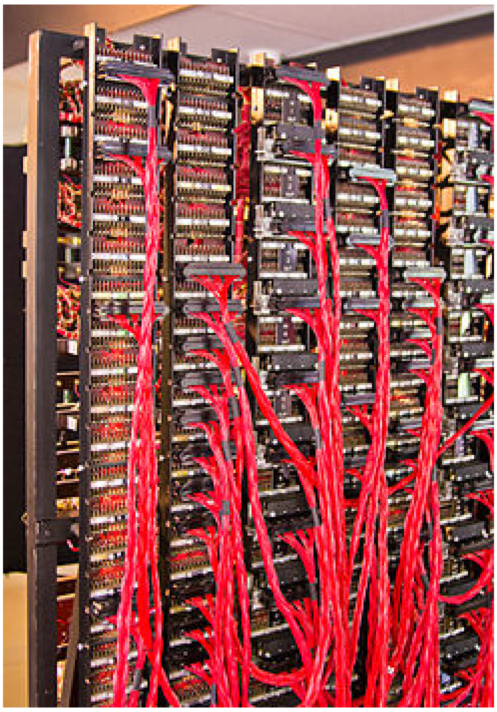
The British Bombe

The Polish cryptologic *bomba* (Polish: *bomba kryptologiczna*; plural *bomby*) had been useful only as long as three conditions were met. First, the form of the indicator had to include the repetition of the message key; second, the number of rotors available had to be limited to three, giving six different "wheel orders" (the three rotors and their order within the machine); and third, the number of plug-board leads had to remain relatively small so that the majority of letters were *unsteckered*. Six machines were built, one for each possible rotor order. The *bomby* were delivered in November 1938, but barely a month later the Germans introduced two additional rotors for loading into the Enigma scrambler, increasing the number of wheel orders by a factor of ten. Building another 54 *bomby* was beyond the Poles' resources. Also, on 1 January 1939, the number of plug-board leads was increased to ten. The Poles therefore had to return to manual methods, the Zygalski sheets.

Alan Turing designed the British bombe on a more general principle, the assumption of the presence of text, called a *crib*, that cryptanalysts could predict was likely to be present at a defined point in the message. This technique is termed a *known plaintext attack* and had been used to a limited extent by the Poles, e.g., the Germans' use of "ANX" — "AN", German for "To," followed by "X" as a spacer.

Bletchley Park's commanding officer Edward Travis acquired a £100,000 budget for the construction of Turing's machine, and the contract to build the bombes was awarded to the British Tabulating Machine Company (BTM) at Letchworth.[28] BTM placed the project under the direction of Harold 'Doc' Keen. Each machine was about 7 feet (2.1 m) wide, 6 feet 6 inches (1.98 m) tall, 2 feet (0.61 m) deep and weighed about a ton.[29] On the front of each bombe were 108 places where drums could be mounted. The drums were in three groups of 12 triplets. Each triplet, arranged vertically, corresponded to the three rotors of an Enigma scrambler. The bombe drums' input and output contacts went to cable connectors, allowing the bombe to be wired up according to the menu. The 'fast' drum rotated at a speed of 50.4 rpm in the first models[30] and 120 rpm in later ones,[31] when the time to set up and run through all 17,576 possible positions for one rotor order was about 20 minutes.[32]

The first bombe was named "Victory". It was installed in "Hut 1" at Bletchley Park on 18 March 1940. It was based on Turing's original design and so lacked a diagonal board.[33] On 26 April 1940, HMS *Griffin* captured a German trawler (*Schiff 26*, the *Polares*) flying a Dutch flag; included in the capture were some Enigma keys for 23 to 26 April.[34] Bletchley retrospectively attacked some messages sent during this period using the captured material and an ingenious Bombe menu where the Enigma fast rotors were all in the same position.[35] In May and June 1940, Bletchley succeeded in breaking six days of naval traffic, 22–27 April 1940.[36] Those messages were the first breaks of *Kriegsmarine* messages of the war, "[b]ut though this success expanded Naval Section's knowledge of the Kriegsmarines's signals organization, it neither affected naval operations nor made further naval Enigma solutions possible."[37] The second bombe, named "*Agnus dei*", later shortened to "Agnes", or "Aggie", was equipped with Welchman's diagonal board, and was installed on 8 August 1940; "Victory" was later returned to Letchworth to have a diagonal board fitted.[38] The bombes were later moved from "Hut 1" to "Hut 11". The bombe was referred to by Group Captain Winterbotham as a "Bronze Goddess" because of its colour.[39] The devices were more prosaically described by operators as being "like great big metal bookcases".[40]



Rear view of the rebuilt Bombe at Bletchley Park. This shows the patch panels and 26-way cables used to wire up the 'menus'. It includes the 'diagonal boards' which, despite their name, are physically rectangular

During 1940, 178 messages were broken on the two machines, nearly all successfully. Because of the danger of bombes at Bletchley Park being lost if there were to be a bombing raid, bombe outstations[41] were established, at Adstock, Gayhurst and Wavendon, all in Buckinghamshire.[42] In June–August 1941 there were 4 to 6 bombes at Bletchley Park, and when Wavendon was completed, Bletchley, Adstock and Wavenden had a total of 24 to 30 bombes. When Gayhurst became operational there were a total of 40 to 46 bombes, and it was expected that the total would increase to about 70 bombes run by some 700 Wrens (Women's Royal Naval Service). But in 1942 with the introduction of the naval four-rotor Enigma, "far more than seventy bombes" would be needed. New outstations were established at Stanmore and Eastcote, and the Wavendon and Adstock bombes were moved to them, though the Gayhurst site was retained. The few bombes left at Bletchley Park were used for demonstration and training purposes only.[43]

Main British (BTM) bombe types[44][45]

Type	Number of Enigma-equivalents	Mechanism	Number built
Original standard	36 (30 in pre-production)	3-rotor Enigma-equivalents	73
Jumbo	36	3-rotor Enigma-equivalents plus an additional mechanism to check each stop and print the results (dubbed the "machine gun" because of the noise its uniselectors made)	14
Mammoth	36	4-rotor Enigma-equivalents with high-speed relays to sense stops	57
Cobra	36	4-rotor Enigma-equivalents with an electronic sensing unit designed by C. E. Wynn-Williams and Tommy Flowers' team at the GPO Research Station[46] (this machine was unreliable)	12
'New'[47] standard	36	3-rotor Enigma-equivalents (with high-speed Siemens-type sense relays)	68

Production of bombes by BTM at Letchworth in wartime conditions, was nowhere near as rapid as the Americans later achieved at NCR in Dayton, Ohio.

Number of 3-rotor bombes available[48]

Year	Month	Number
1941	December	12
1942	December	40
1943	June	72
1943	December	87
1944	December	152
1945	May	155

Sergeant Jones was given the overall responsibility for Bombe maintenance by Edward Travis. Later Squadron Leader and not to be confused with Eric Jones, he was one of the original bombe maintenance engineers, and experienced in BTM techniques. Welchman said that later in the war when other people tried to maintain them, they realised how lucky they were to have him. About 15 million delicate wire brushes on the drums had to make reliable contact with the terminals on the template. There were 104 brushes per drum, 720 drums per bombe, and ultimately around 200 bombes.[49]

After World War II, some fifty bombes were retained at RAF Eastcote, while the rest were destroyed. The surviving bombes were put to work, possibly on Eastern bloc ciphers.[50] The official history of the bombe states that "some of these machines were to be stored away but others were required to run new jobs and sixteen machines were kept comparatively busy on menus. It is interesting to note that most of the jobs came up and the operating, checking and other times maintained were faster than the best times during the war periods."

Response to the four-rotor Enigma

A program was initiated by Bletchley Park to design much faster bombes that could decrypt the four-rotor system in a reasonable time. There were two streams of development. One, code-named Cobra, with an electronic sensing unit, was produced by Charles Wynn-Williams of the Telecommunications Research Establishment (TRE) at Malvern and Tommy Flowers of the General Post Office (GPO).[51] The other, code-named Mammoth, was designed by Harold Keen at BTM, Letchworth. Initial delivery was scheduled for August or September 1942.[44] The dual development projects created considerable tension between the two teams, both of which cast doubts on the viability of the opposing team's machine. After considerable internal rivalry and dispute, Gordon Welchman (by then, Bletchley Park's Assistant Director for mechanization) was forced to step in to resolve the situation. Ultimately, Cobra proved unreliable and Mammoth went into full-scale production.[52]

Unlike the situation at Bletchley Park, the United States armed services did not share a combined cryptanalytical service. Indeed, there was considerable rivalry between the US Army's facility, the Signals Intelligence Service (SIS), and that of the US Navy known as OP-20-G.[53] 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 Abe 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.[54] The four returned to America after ten weeks, with a naval radio direction finding unit and many documents[55] including a 'paper Enigma'.[56]

Currier later wrote:

> There was complete cooperation. We went everywhere, including Hut 6. We watched the entire operation and had all the techniques explained in great detail. We were thoroughly briefed on the latest techniques in the solution of Enigma and the operations of the bombes. We had ample opportunity to take as many notes as we wanted and to

> watch first hand all operations involved.[57]

The main response to the Four-rotor Enigma was the US Navy bombe, which was manufactured in much less constrained facilities than were available in wartime Britain.

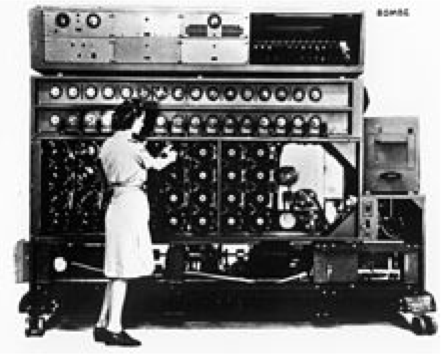
Number of 4-rotor bombes available (UK and US)[48]

Year	Month	Number
1943	June	4
1943	December	95
1944	December	160
1945	May	180

US Navy Bombe

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.[16][58] 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."[59] It established a relationship of "full collaboration" between Bletchley Park and OP-20-G.[16]


The US Navy Bombe contained 16 four-rotor Enigma-analogues and was much faster than the British three-rotor Bombes, even for a three-rotor task.

An all electronic solution to the problem of a fast bombe was considered,[16] 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.

Alan Turing, who had written a memorandum to OP-20-G (probably in 1941),[60] 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.[61] He visited OP-20-G, and went to NCR in Dayton on the 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.[16] 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. They had eight Enigma-equivalents on the front and eight on the back. The fast drum rotated at 1,725 rpm, 34 times the speed of the early British bombes. 'Stops' were detected electronically using thermionic valves (vacuum tubes)—mostly thyratrons—for the high speed circuits. When a 'stop' was found[62] the machine over-ran as it slowed, reversed to the position found and printed it out before restarting. The running time for a 4-rotor run was about 20 minutes, and for a 3-rotor run, about 50 seconds.[63] Each machine was 10 feet (3.0 m) wide, 7 feet (2.1 m) high, 2 feet (0.61 m) deep and weighed 2.5 tons.

The first machine was completed and tested on 3 May 1943. By 22 June, the first two machines, called 'Adam' and 'Eve' broke a particularly difficult German naval cipher, the *Offizier* settings for 9 and 10 June.[64] A P Mahon, who had joined the Naval Section in Hut 8 in 1941, reported in his oficial 1945 "History of Hut Eight 1939-1945":

> The American bombe was in its essentials the same as the English bombe though it functioned rather better as they were not handicapped by having to make it, as Keen was forced to do owing to production difficulties, on the framework of a 3 wheel machine. By late autumn [1943] new American machines were coming into action at the rate of about 2 a week, the ultimate total being in the region of 125.[65]

These bombes were faster, and soon more available, than the British bombes at Bletchley Park and its outstations. Consequently, they were put to use for Hut 6 as well as Hut 8 work.[66] 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.[67]

Production was stopped in September 1944 after 121 bombes had been made.[63] The last-manufactured US Navy bombe is on display at the US National Cryptologic Museum. Jack Ingram, former Curator of the museum, describes being told of the existence of a second bombe and searching for it but not finding it whole. Whether it remains in storage in pieces, waiting to be discovered, or no longer exists, is unknown.

US Army Bombe

The US Army Bombe was physically very different from the British and US Navy bombes. A contract was signed with Bell Labs on 30 September 1942.[68] The machine was designed to analyse 3-rotor, not 4-rotor traffic. It was known as "003" or "Madame X".[69][70] 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.[63][66] 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.[62] A 3-rotor run took about 10 minutes.[63]

Bombe rebuild

In 1994 a group led by John Harper of the BCS Computer Conservation Society started a project to build a working replica of a bombe.[71] The project required detailed research, and took 13 years of effort before the replica was completed, which was then put on display at the Bletchley Park museum.[72] In March 2009 it won an Engineering Heritage Award.[73]

See also

- Cryptanalysis of the Enigma
- Colossus computer
- Heath Robinson
- Jean Valentine (bombe operator)

Notes

1. Harper, John (2008), *The British Bombe: The Rebuild Project* (https://web.archive.org/web/20131204202741/http://www.jharper.demon.co.uk/bombe1.htm), Archived from the original on 4 December 2013, retrieved 23 October 2016
2. Welchman 2005, pp. 138–145
3. Wilcox 2001, p. 33
4. Wenger 1945
5. Smith 2007, p. 60
6. Welchman 2005, p. 77
7. John Fitzgerald, Peter Gorm Larsen, Paul Mukherjee, Nico Plat, Marcel Verhoef (December 6, 2005). *Validated Designs for Object-oriented Systems* (https://books.google.com/books?id=EP5zNxk8DpcC&pg=PA192&dq=Bletchley+Bombe+electro-magnetic+electronic+valve&hl=en&sa=X&ved=0ahUKEwikvpCFm_DVAhWL6oMKHWqTBggQ6AEINTAC#v=onepage&q=Bletchley%20Bombe%20electro-magnetic%20electronic%20valve&f=false). ISBN 9781846281075.
8. Simon Singh (January 26, 2011). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (https://books.google.com/books?id=o3YbiViTg70C&pg=PT258&dq=Bletchley+Bombe+Victory+Agnus+Dei+Agnes&hl=en&sa=X&ved=0ahUKEwijgoGanPDXAhVm6YMKHfwyDE0Q6AEIKjAA#v=onepage&q=Bletchley%20Bombe%20Victory%20Agnus%20Dei%20Agnes&f=false). ISBN 9780307787842.
9. Budiansky 2000, p. 195
10. Sebag-Montefiore 2004, p. 375
11. Carter, p. 1
12. Carter, Frank, "The Turing Bombe" (http://www.rutherfordjournal.org/article030108.html), *The Rutherford Journal*, ISSN 1177-1380 (https://www.worldcat.org/issn/1177-1380)
13. Kahn 1991, p. 40 states early Enigma used 3 rotors in the machine, but 5 rotors were available. That would produce about 1 million possible starting positions. Instead of 26 positions, the early naval Enigma had 29 because it include 3 umlauted characters.
14. Kahn 1991, p. 40 describing German concerns about superimposition attack.
15. Kahn 1991, p. 43 stating, "In particular, it accepted the uncomfortable conclusions of a study by Lieutenant Henno Lucan, second radio oficer of the battleship *Elsass*, that in neither physical nor cryptologic security did the Enigma meet modern requirements."
16. Budiansky 2000, pp. 238–242
17. Sale, Tony, *A quick revision of the Enigma machine, its physical and operational characteristics* (http://www.codesandciphers.org.uk/anoraks/enigma.htm), retrieved 9 June 2011
18. Sale, Tony, "The Principle of the Enigma", *The Enigma cipher machine* (http://www.codesandciphers.org.uk/enigma/enigma1.htm), retrieved 4 February 2010
19. Sale, Tony, *Military Use of the Enigma: The complexity of the Enigma machine* (http://www.codesandciphers.org.uk/enigma/enigma3.htm), retrieved 4 January 2014
20. Mahon 1945, p. 24
21. Welchman 2005, p. 120
22. Sale, Tony, *Virtual Wartime Bletchley Park: Alan Turing, the Enigma and the Bombe* (http://www.codesandciphers.org.uk/virtualbp/tbombe/tbombe.htm), retrieved 28 February 2010
23. Sale, Tony, *The Turing/Welchman Bombe* (http://www.codesandciphers.org.uk/virtualbp/tbombe/thebmb.htm), "Remember that the top, fast, drum on the Bombe corresponds to the slow left hand drum on the Enigma machine".
24. US Army 6812th Signal Security Detachment (1945), *US 6812 Bombe Report* (http://www.codesandciphers.org.uk/documents/bmbrpt/usbmbrpt.pdf) (PDF), retrieved 4 February 2010
25. Carter, p. 4

26. Sale, Tony, *Virtual Wartime Bletchley Park: The Bombe and the Ringstellung problem* (http://www.codesandciphers.org.uk/virtualbp/hsbombe/hsbombe3.htm), retrieved 30 June 2011
27. Carter, p. 3
28. Smith 2007
29. Ellsbury, Graham (1988), "2. Description of the Bombe", *The Turing Bombe: What it was and how it worked* (http://www.ellsbury.com/bombe2.htm), retrieved 1 May 2010
30. Wilcox 2001, p. 12
31. Ellsbury, Graham (1998), "4. How the Bombe Worked", *The Turing Bombe: What it was and how it worked* (http://www.ellsbury.com/bombe4.htm), retrieved 1 May 2010
32. Alexander c. 1945 Ch. I para. 44
33. Hinsley, Ransom & Knight 1988, p. 954
34. Kahn 1991, p. 116–117
35. Wright 2016
36. Erskine, Ralph. "Allied Breaking of Naval Enigma" (http://uboat.net/technical/enigma_breaking.htm). *uboat.net*. Retrieved 6 February 2017.
37. Kahn 1991, pp. 117–118
38. "Outstations - A Brief History", *Bletchley Park Jewels* (http://www.mkheritage.co.uk/bpt/Outstations/Wavendon.htm), retrieved 1 May 2010
39. Winterbotham 2001, p. 15
40. Mary Stewart, 'Bombe' Operator, interviewed in "The Men Who Cracked Enigma (http://www.imdb.com/title/tt1155383/episodes)", UKTV History Channel documentary series "Heroes of World War II (http://www.imdb.com/title/tt1157073/)", 2003
41. "Outstations from the Park", *Bletchley Park Jewels* (http://www.mkheritage.co.uk/bpt/outstations/outstations.htm), retrieved 16 April 2010
42. Toms, Susan (2005), *Enigma and the Eastcote connection* (http://www.ruislip.co.uk/eastcotemod/enigma.htm), retrieved 16 April 2010
43. Welchman, Gordon (1982), *The Hut Six Story: Breaking the Enigma Codes*, London: Allen Lane, ISBN 0-7139-1294-4, pp. 139, 141
44. Budiansky 2000, pp. 359–360
45. Harper, John (ed.), "Bombe Types" (http://arquivo.pt/wayback/20160516163621/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 16 May 2016, retrieved 4 March 2010
46. Copeland, B. Jack, ed. (2006), *Colossus: The Secrets of Bletchley Park's Codebreaking Computers*, Oxford: Oxford University Press, p. 285, ISBN 978-0-19-284055-4
47. Harper, John (ed.), "Definitiions" (http://www.jharper.demon.co.uk/defintn1.htm), *The British Bombe CANTAB* (http://www.jharper.demon.co.uk/defintn1.htm), retrieved 11 July 2011
48. Alexander c. 1945, Ch. V para. 3
49. Welchman 1982, p. 147
50. Smith 2007, p. 206
51. Smith 2014, p. 213
52. Smith 2014, pp. 213–214
53. Budiansky 2000, p. 87
54. Budiansky 2000, p. 176
55. Budiansky 2000, p. 179
56. Jacobsen, Philip H. (2000), *British provision of German naval Enigma information* (http://lists101.his.com/pipermail/intelforum/2000-August/002580.html), retrieved 26 March 2010
57. Smith 2007, p. 134
58. Wilcox 2001, p. 21

59. Erskine, Ralph (Summer 1999), "The Holden Agreement on Naval Sigint: The First BRUSA?" (http://intellit.muskingum.edu/alpha_folder/E_folder/erskine_a-o.html), *Intelligence and National Security*, **14** (2): 187–197, doi:10.1080/02684529908432545 (https://doi.org/10.1080%2F02684529908432545)
60. 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
61. *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
62. Wenger 1945, p. 51
63. Wenger 1945, p. 52
64. Budiansky 2000, pp. 294–295
65. Mahon 1945, p. 89
66. Welchman 2005, p. 135
67. Alexander c. 1945 Ch. VIII para. 11
68. Sebag-Montefiore 2004, p. 254
69. Farley 1990, p. 12
70. Burke 2002, p. 136
71. "The Bombe tops engineers' poll" (http://www.computerconservationsociety.org/news/bombe/bombe.htm). *Computer Conservation Society*. Retrieved 6 February 2017.
72. http://www.bomberebuild.webspace.virginmedia.com/
73. British Computer Society (2009), *BCS bombe team receives award* (http://www.bcs.org/server.php?show=ConWebDoc.25242) (published 31 March 2009), retrieved 2009-05-22

References

- Alexander, C. Hugh O'D. (c. 1945), *Cryptographic History of Work on the German Naval Enigma*, The National Archives, Kew, Reference HW 25/1
- Budiansky, Stephen (2000), *Battle of wits: The Complete Story of Codebreaking in World War II*, Free Press, ISBN 978-0-684-85932-3
- Burke, Colin B. (2002) [1994], *It Wasn't All Magic: The Early Struggle to Automate Cryptanalysis, 1930s-1960s* (PDF), Fort Meade: Center for Cryptologic History, National Security Agency, archived from the original (PDF) on 2016-03-05
- Carter, Frank, *From Bombe 'stops' to Enigma keys* (PDF), Technical Papers, Milton Keynes: Bletchley Park Trust, archived from the original (PDF) on 2010-01-08
- Davies, Donald (April 1999), "The Bombe — a Remarkable Logic Machine", *Cryptologia*, **23** (2): 108–138, doi:10.1080/0161-119991887793, ISSN 0161-1194
- Davies, Donald (July 1999), "Effectiveness of the Diagonal Board", *Cryptologia*, **23** (3): 229–239, doi:10.1080/0161-119991887865, ISSN 0161-1194
- Ellsbury, Graham (1988), *The Turing Bombe: what it was and how it worked*, retrieved 1 May 2010
- Farley, Robert D. (1990), *Oral History Interview NSA-OH-14-83 Campaigne, Howard, Dr. 29 June 1983* (PDF), US National Security Agency, archived from the original (PDF) on 18 September 2013, retrieved 3 January 2014
- Harper, John (2008), *The British Bombe: CANTAB The Rebuild Project*, archived from the original on 16 May 2016, retrieved 1 May 2010
- Hinsley, F.H.; Ransom, C.F.G.; Knight, R.C.C. (1988), *British Intelligence in the Second World War: Volume 3, Part 2: v. 3*, Cambridge: Cambridge University Press, ISBN 978-0-521-35196-6
- Kahn, David (1991), *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939–1943*, Houghton-Mifflin, ISBN 0-395-42739-8
- Keen, John (2003), *Harold 'Doc' Keen and the Bletchley Park bombe*, Cleobury Mortimer, England: M & M Baldwin, ISBN 978-0-947712-42-6
- Mahon, A.P. (1945), *The History of Hut Eight 1939 - 1945*, UK National Archives Reference HW 25/2, retrieved 10 December 2009

- Sale, Tony, "Alan Turing, the Enigma and the Bombe", *Virtual Wartime Bletchley Park*, retrieved 1 May 2010
- Sebag-Montefiore, Hugh (2004) [2000], *Enigma: The Battle for the Code* (Cassell Military Paperbacks ed.), London: Weidenfeld & Nicolson, ISBN 978-0-297-84251-4
- Smith, Christopher (2014), "How I learned to stop worrying and love the Bombe: Machine Research and Development and Bletchley Park", *History of Science*, **52** (2): 200–222, doi:10.1177/0073275314529861
- Smith, Michael (2007) [1998], *Station X: The Codebreakers of Bletchley Park*, Pan Grand Strategy Series (Pan Books, Revised and Extended ed.), London: Pan McMillan Ltd, ISBN 978-0-330-41929-1
- Welchman, Gordon (2005) [1997], *The Hut Six story: Breaking the Enigma codes*, Cleobury Mortimer, England: M&M Baldwin, ISBN 9780947712341 New edition updated with an *addendum* consisting of a 1986 paper written by Welchman that corrects his misapprehensions in the 1982 edition.
- US Army (1945), "The US 6812 Division Bombe Report Eastcote 1944", *Tony Sale's Codes and Ciphers*, archived from the original on 22 July 2009, retrieved 1 May 2010
- Wenger, J. N.; Engstrom, H. T.; Meader, R. I. (30 May 1944), *History of The Bombe Project: Memorandum for the Director of Naval Communications*, The Mariner's Museum (published 1998), archived from the original on 16 June 2010
- Wenger, J. N. (12 February 1945), "Appendix II: U. S. Army Cryptanalytic Bombe", *Solving the Enigma: History of the Cryptanalytic Bombe, a NSA phamphlet*, archived from the original on 2 October 2014, retrieved 24 Jan 2017 (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, ASIN B0006RLRA4, archived from the original on 17 March 2010, retrieved 9 April 2010
- Winterbotham, F.W. (2001) [1974], *The ULTRA Secret*, Orion Books Ltd, ISBN 0-7528-3751-6
- Wright, John (2016), *The Turing Bombe Victory and the first naval Enigma decrypts*, Cryptologia, doi:10.1080/01611194.2016.1219786

External links

- A bombe simulator (in Javascript)
- Museum of Learning - Bombe: The Challenge Of The Four Rotor Enigma Machine
- Enigma and the Turing Bombe by N. Shaylor, April 17, 1997. Includes a simulator (a Java applet and C)
- Dayton Codebreakers — documentary on the US Navy's Bombe; information on Desch, personnel of the US Naval Computing Machine Laboratory
- A bombe simulator using Flash that aims to be close to the real thing.
- Breaking German Navy Ciphers - The U534 Enigma M4 messages: Cracked with a Turing Bombe software

Retrieved from "https://en.wikipedia.org/w/index.php?title=Bombe&oldid=820546882"

This page was last edited on 15 January 2018, at 06:55.