**Enigma Bombe**

From Wikipedia, the free encyclopedia

*This article is about the decryption device used at Bletchley Park. For the earlier Polish decryption device, see* [*Bomba (cryptography)*](https://en.wikipedia.org/wiki/Bomba_%28cryptography%29)*. For the European dessert of the same name, see* [*Bombe glacée*](https://en.wikipedia.org/wiki/Bombe_glac%C3%A9e)*.*

The working rebuilt bombe at [Bletchley Park](https://en.wikipedia.org/wiki/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](https://en.wikipedia.org/wiki/John_Harper_%28computer_engineer%29) led the "Phoenix" team that built this. It was officially switched on by [the Duke of Kent](https://en.wikipedia.org/wiki/Prince_Edward%2C_Duke_of_Kent), patron of the [British Computer Society](https://en.wikipedia.org/wiki/British_Computer_Society) on 17 July 2008.

The **bombe** was an electromechanical device used by British [cryptologists](https://en.wikipedia.org/wiki/Cryptologist) to help decipher [German](https://en.wikipedia.org/wiki/Germany) [Enigma-machine](https://en.wikipedia.org/wiki/Enigma_machine)-encrypted secret messages during [World War II](https://en.wikipedia.org/wiki/World_War_II) The [US Navy](https://en.wikipedia.org/wiki/United_States_Navy) and [US Army](https://en.wikipedia.org/wiki/United_States_Army) later produced their own machines to the same functional specification, but engineered differently from each other and from the British Bombe.

The initial design of the bombe was produced in 1939 at the UK [Government Code and Cypher School (GC&CS)](https://en.wikipedia.org/wiki/Government_Communications_Headquarters#Government_Code_and_Cypher_School_.28GC.26CS.29) at [Bletchley Park](https://en.wikipedia.org/wiki/Bletchley_Park) by [Alan Turing](https://en.wikipedia.org/wiki/Alan_Turing), with an important refinement devised in 1940 by [Gordon Welchman](https://en.wikipedia.org/wiki/Gordon_Welchman). The engineering design and construction was the work of [Harold Keen](https://en.wikipedia.org/wiki/Harold_Keen) of the [British Tabulating Machine Company](https://en.wikipedia.org/wiki/British_Tabulating_Machine_Company). It was a substantial development from a device that had been designed in 1938 in Poland at the [Biuro Szyfrów](https://en.wikipedia.org/wiki/Biuro_Szyfr%C3%B3w) (Cipher Bureau) by cryptologist [Marian Rejewski](https://en.wikipedia.org/wiki/Marian_Rejewski), and known as the "[cryptologic bomb](https://en.wikipedia.org/wiki/Bomba_%28cryptography%29)" ([Polish](https://en.wikipedia.org/wiki/Polish_language): *bomba kryptologiczna*).

The bombe was designed to discover some of the daily settings of the Enigma machines on the various German military [networks](https://en.wikipedia.org/wiki/Telecommunications_network): specifically, the set of [rotors](https://en.wikipedia.org/wiki/Enigma_machine#Rotors) in use and their positions in the machine; the rotor core start positions for the message—the message [key](https://en.wikipedia.org/wiki/Key_%28cryptography%29)—and one of the wirings of the [plugboard](https://en.wikipedia.org/wiki/Steckerbrett).

**The Enigma machine**

Main article: [Enigma machine](https://en.wikipedia.org/wiki/Enigma_machine)

|  |
| --- |
| **The Enigmacipher machine** |
|  |
| * [Enigma machine](https://en.wikipedia.org/wiki/Enigma_machine)
	+ [Enigma rotors](https://en.wikipedia.org/wiki/Enigma_rotor_details)
* [Breaking Enigma](https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma)
	+ [Polish Cipher Bureau](https://en.wikipedia.org/wiki/Polish_Cipher_Bureau)
		- [Doubles](https://en.wikipedia.org/wiki/Polish_Enigma_doubles)
		- [Grill](https://en.wikipedia.org/wiki/Grill_%28cryptology%29)
		- [Clock](https://en.wikipedia.org/wiki/Clock_%28cryptography%29)
		- [Cyclometer](https://en.wikipedia.org/wiki/Cyclometer)
		- [Bomba](https://en.wikipedia.org/wiki/Bomba_%28cryptography%29)
		- [Zygalski sheets](https://en.wikipedia.org/wiki/Zygalski_sheets)
	+ [Bletchley Park](https://en.wikipedia.org/wiki/Bletchley_Park)
		- [Banburismus](https://en.wikipedia.org/wiki/Banburismus)
		- [Herivel tip](https://en.wikipedia.org/wiki/John_Herivel)
		- [Crib](https://en.wikipedia.org/wiki/Known-plaintext_attack)
		- **Bombe**
		- [Hut 6](https://en.wikipedia.org/wiki/Hut_6)
		- [Hut 8](https://en.wikipedia.org/wiki/Hut_8)
	+ [PC Bruno](https://en.wikipedia.org/wiki/PC_Bruno)
* [Ultra](https://en.wikipedia.org/wiki/Ultra)
 |
|  |

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

A series of three rotors from an Enigma machine

The Enigma was an [electro-mechanical](https://en.wikipedia.org/wiki/Electromechanics) [rotor machine](https://en.wikipedia.org/wiki/Rotor_machine) used for the [encryption](https://en.wikipedia.org/wiki/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 lamp board implemented a [polyalphabetic substitution](https://en.wikipedia.org/wiki/Polyalphabetic_cipher) cipher, which turned [plaintext](https://en.wikipedia.org/wiki/Plaintext) into [ciphertext](https://en.wikipedia.org/wiki/Ciphertext) and back again. Used properly, this provided a very high degree of security. 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](https://en.wikipedia.org/wiki/Enigma_machine#Reflector) (or reflector) which turned it back through the rotors and entry drum, and out to cause one lamp on the lamp board to be illuminated.

At each key depression, at least one of the rotors (the right-hand or "fast" rotor) advanced one position, which caused the encipherment to alter. At a certain point, the right-hand rotor caused the middle rotor to advance and in a similar way, the middle rotor caused 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.

The plugboard of an Enigma machine, showing two pairs of letters swapped: S–O and A–J. During [World War II](https://en.wikipedia.org/wiki/World_War_II), ten plugboard connections were made.

In 1930 an additional security feature was introduced for the military Enigmas. This was a plugboard (*Steckerbrett* in German, shortened to "Stecker") that further scrambled the letters. Letters were swapped in pairs: if **A** was transformed into **R** then **R** was transformed into **A**. This regularity was exploited by Welchman's "diagonal board" enhancement to the bombe, which vastly increased its efficiency. With six plug leads in use (leaving 14 letters "unsteckered") this gives 100,391,791,500 possible ways of setting up the plugboard.

An important feature of the machine from a cryptanalyst's point of view, and indeed Enigma's [Achilles' heel](https://en.wikipedia.org/wiki/Achilles%27_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.

In the lead up to [World War II](https://en.wikipedia.org/wiki/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 air force 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 air force and army Enigmas could be set up 1.5×1019 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](https://en.wikipedia.org/wiki/U-boat). This could be set up in 1.8×1020 different ways.

**Four-rotor Enigma**

By late 1941 a change in German Navy fortunes in the [Battle of the Atlantic](https://en.wikipedia.org/wiki/Battle_of_the_Atlantic_%281939%E2%80%931945%29), combined with intelligence reports, convinced Admiral [Karl Dönitz](https://en.wikipedia.org/wiki/Karl_D%C3%B6nitz) 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](https://en.wikipedia.org/wiki/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.

**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 different combinations (approximately 151 trillion).

* 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. In the words of [Gordon Welchman](https://en.wikipedia.org/wiki/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".

**Structure**

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.

The bombe was an electro-mechanical device that replicated the action of several [Enigma machines](https://en.wikipedia.org/wiki/Enigma_machine) wired together. A standard German Enigma employed, at any one time, a set of three [rotors](https://en.wikipedia.org/wiki/Rotor_machine), each of which could be set in any of 26 positions. The standard British bombe contained thirty six 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](https://en.wikipedia.org/wiki/Bombe#Bombe_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.

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.

The drums were color-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.

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](https://en.wikipedia.org/wiki/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. Eventually, the result would be tested on a [Typex](https://en.wikipedia.org/wiki/Typex) machine that had been modified to replicate an Enigma, to see whether that [decryption](https://en.wikipedia.org/wiki/Decryption) produced [German language](https://en.wikipedia.org/wiki/German_language).

**Bombe menu**

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.

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

A bombe run involved a cryptanalyst first obtaining a [*crib*](https://en.wikipedia.org/wiki/Crib_%28cryptanalysis%29) — a section of [plaintext](https://en.wikipedia.org/wiki/Plaintext) that was thought to correspond to the [ciphertext](https://en.wikipedia.org/wiki/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.

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. Recent bombe simulations have shown similar results.

|  |
| --- |
| 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](https://en.wikipedia.org/wiki/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 mechanized 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(***A***)* and *P(***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(***A***)* or *P(***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(***A***)* = **Y**. Looking at position 10 of the crib:ciphertext comparison, we observe that **A** encrypts to **T**, or, expressed as a formula:

**T** = *P(S10(P(***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(***T***) = S10(P(***A***))*

This gives us a relationship between *P(***A***)* and *P(***T***)*. If *P(***A***)* = **Y**, and for the rotor setting under consideration *S10(***Y***)* = **Q** (say), we can deduce that

*P(***T***)* = *S10(P(***A***)) = S10(***Y***)* = **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(***T***)* is completely determined if *P(***A***)* is known.

Likewise, we can also observe that **T** encrypts to **L** at position 8. Using *S8*, we can deduce the steckered value for **L** as well using a similar argument, to get, say,

*P(***L***)* = *S8(P(***T***)) = S8(***Q***)* = **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(***K***)*, which might be:

*P(***K***)* = *S6(P(***L***)) = S6(***G***)* = **F**

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

*P(***A***)* = *S7(P(***K***)) = S7(***F***)* = **N**

However, in this case, we have derived a [contradiction](https://en.wikipedia.org/wiki/Contradiction), since, by hypothesis, we assumed that *P(***A***)* = **Y** at the outset. This means that the initial assumption must have been incorrect, and so that (for this rotor setting) *P(***A***)* ≠ **Y** (this type of argument is termed [*reductio ad absurdum*](https://en.wikipedia.org/wiki/Reductio_ad_absurdum) or "proof by contradiction").

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.

The cryptanalyst hypothesized 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.

**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](https://en.wikipedia.org/wiki/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]](https://en.wikipedia.org/wiki/Bombe#cite_note-H6StoryP77-6#cite_note-H6StoryP77-6)

**The British Bombe**

The Polish cryptologic [*bomba*](https://en.wikipedia.org/wiki/Bomba_%28cryptography%29) (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](https://en.wikipedia.org/wiki/Zygalski_sheets).

[Alan Turing](https://en.wikipedia.org/wiki/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*](https://en.wikipedia.org/wiki/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.

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.

Bletchley Park's commanding officer [Edward Travis](https://en.wikipedia.org/wiki/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](https://en.wikipedia.org/wiki/British_Tabulating_Machine_Company) (BTM) at [Letchworth](https://en.wikipedia.org/wiki/Letchworth) BTM placed the project under the direction of [Harold 'Doc' Keen](https://en.wikipedia.org/wiki/Harold_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. 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](https://en.wikipedia.org/wiki/Rpm) in the first models and 120 rpm in later ones, when the time to set up and run through all 17,576 possible positions for one rotor order was about 20 minutes.

The first bombe, which was based on Turing's original design and so lacked a diagonal board, was installed in "Hut 1" at Bletchley Park on 18 March 1940 and was named "Victory". 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. The bombes were later moved from "Hut 1" to "Hut 11". The bombe was referred to by Group Captain [Winterbotham](https://en.wikipedia.org/wiki/Frederick_Winterbotham) as a "Bronze Goddess" because of its color. The devices were more prosaically described by operators as being "like great big metal bookcases".

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[[32]](https://en.wikipedia.org/wiki/Bombe#cite_note-32#cite_note-32) were established, at [Adstock](https://en.wikipedia.org/wiki/Adstock), [Gayhurst](https://en.wikipedia.org/wiki/Gayhurst) and [Wavendon](https://en.wikipedia.org/wiki/Wavendon). 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. 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](https://en.wikipedia.org/wiki/Stanmore) and [Eastcote](https://en.wikipedia.org/wiki/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.

|  |
| --- |
| Main British ([BTM](https://en.wikipedia.org/wiki/British_Tabulating_Machine_Company)) bombe types  |
| **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](https://en.wikipedia.org/wiki/Stepping_switch) 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](https://en.wikipedia.org/wiki/C._E._Wynn-Williams) and [Tommy Flowers](https://en.wikipedia.org/wiki/Tommy_Flowers)' team at the [GPO Research Station](https://en.wikipedia.org/wiki/Post_Office_Research_Station) (this machine was unreliable) | 12 |
| 'New' 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](https://en.wikipedia.org/wiki/NCR_Corporation) in Dayton, Ohio.

|  |
| --- |
| Number of 3-rotor bombes available |
| **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](https://en.wikipedia.org/wiki/Edward_Travis). Later Squadron Leader and not to be confused with [Eric Jones](https://en.wikipedia.org/wiki/Eric_Malcolm_Jones), he was one of the original bombe maintenance engineers, and experienced in [BTM](https://en.wikipedia.org/wiki/British_Tabulating_Machine_Company) techniques. Welchman said that later in the war when other people tried to maintain them, they realized 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.

After World War II, some fifty bombes were retained at [Eastcote](https://en.wikipedia.org/wiki/Eastcote), while the rest were destroyed. The surviving bombes were put to work, possibly on [Eastern bloc](https://en.wikipedia.org/wiki/Eastern_bloc) ciphers. 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."

A team led by [John Harper](https://en.wikipedia.org/wiki/John_Harper_%28computer_engineer%29) conducted a 13-year project to reconstruct a working bombe. This was successful, and the reconstructed bombe can be seen at [Bletchley Park](https://en.wikipedia.org/wiki/Bletchley_Park) Museum. In March 2009 it won an Engineering Heritage Award.

**Response to the Four-rotor Enigma**

A program was initiated by [Bletchley Park](https://en.wikipedia.org/wiki/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](https://en.wikipedia.org/wiki/Charles_Wynn-Williams) of the [Telecommunications Research Establishment](https://en.wikipedia.org/wiki/Telecommunications_Research_Establishment) (TRE) at Malvern and [Tommy Flowers](https://en.wikipedia.org/wiki/Tommy_Flowers) of the [General Post Office](https://en.wikipedia.org/wiki/General_Post_Office) (GPO). The other, code-named Mammoth, was designed by [Harold Keen](https://en.wikipedia.org/wiki/Harold_Keen) at [BTM](https://en.wikipedia.org/wiki/British_Tabulating_Machine_Company), Letchworth. Initial delivery was scheduled for August or September 1942. 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](https://en.wikipedia.org/wiki/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.

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](https://en.wikipedia.org/wiki/United_States_Army) facility, the [Signals Intelligence Service (SIS)](https://en.wikipedia.org/wiki/Signals_Intelligence_Service), and that of the [US Navy](https://en.wikipedia.org/wiki/United_States_Navy) known as [OP-20-G](https://en.wikipedia.org/wiki/OP-20-G).[[45]](https://en.wikipedia.org/wiki/Bombe#cite_note-45#cite_note-45) 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](https://en.wikipedia.org/wiki/Purple_%28cipher_machine%29) for the Bletchley Park's Japanese section in [Hut 7](https://en.wikipedia.org/wiki/Hut_7). The four returned to America after ten weeks, with a naval radio [direction finding](https://en.wikipedia.org/wiki/Direction_finding) unit and many documents including a 'paper Enigma'.

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.[[49]](https://en.wikipedia.org/wiki/Bombe#cite_note-49#cite_note-49)

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)[[39]](https://en.wikipedia.org/wiki/Bombe#cite_note-AlexanderP56-39#cite_note-AlexanderP56-39) |
| **Year** | **Month** | **Number** |
| 1943 | June | 4 |
| 1943 | December | 95 |
| 1944 | December | 160 |
| 1945 | May | 180 |

**US Navy Bombe**

Colonel [John Tiltman](https://en.wikipedia.org/wiki/John_Tiltman), who later became Deputy Director at Bletchley Park, visited the US Navy cryptanalysis office ([OP-20-G](https://en.wikipedia.org/wiki/OP-20-G)) in April 1942 and recognized 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](https://en.wikipedia.org/wiki/Blueprint) and wiring diagrams received by US Naval Lieutenants Robert Ely and Joseph Eachus at Bletchley Park in July 1942. Funding for a full, $2 million, navy development effort was requested on 3 September 1942 and approved the following day.

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.

Commander [Edward Travis](https://en.wikipedia.org/wiki/Edward_Travis), Deputy Director and [Frank Birch](https://en.wikipedia.org/wiki/Francis_Birch_%28cryptographer%29), Head of the German Naval Section travelled from Bletchley Park to Washington in September 1942. With [Carl Frederick Holden](https://en.wikipedia.org/wiki/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](https://en.wikipedia.org/wiki/1943_BRUSA_Agreement) to being the forerunner of the [UKUSA Agreement](https://en.wikipedia.org/wiki/UK%E2%80%93USA_Security_Agreement)," being the first agreement "to establish the special [Sigint](https://en.wikipedia.org/wiki/Signals_intelligence) 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." It established a relationship of "full collaboration" between Bletchley Park and OP-20-G.

An all-electronic solution to the problem of a fast bombe was considered,[[11]](https://en.wikipedia.org/wiki/Bombe#cite_note-Budiansky238-242-11#cite_note-Budiansky238-242-11) but rejected for pragmatic reasons, and a contract was let with the [National Cash Register Corporation](https://en.wikipedia.org/wiki/NCR_Corporation) (NCR) in [Dayton, Ohio](https://en.wikipedia.org/wiki/Dayton%2C_Ohio). This established the [United States Naval Computing Machine Laboratory](https://en.wikipedia.org/wiki/United_States_Naval_Computing_Machine_Laboratory). Engineering development was led by NCR's [Joseph Desch](https://en.wikipedia.org/wiki/Joseph_Desch).

[Alan Turing](https://en.wikipedia.org/wiki/Alan_Turing), who had written a memorandum to OP-20-G (probably in 1941),[[52]](https://en.wikipedia.org/wiki/Bombe#cite_note-52#cite_note-52) 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. 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 utilizing techniques such as [Banburismus](https://en.wikipedia.org/wiki/Banburismus). 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](https://en.wikipedia.org/wiki/Revolutions_per_minute), 34 times the speed of the early British bombes. 'Stops' were detected electronically using [thermionic valves](https://en.wikipedia.org/wiki/Vacuum_tube) (vacuum tubes)—mostly [thyratrons](https://en.wikipedia.org/wiki/Thyratron)—for the high speed circuits. When a 'stop' was found 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. 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. A P Mahon, who had joined the Naval Section in Hut 8 in 1941, reported in his official 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.

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. 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 enciphered on the combined Anglo-American cypher machine, [C.C.M.](https://en.wikipedia.org/wiki/Combined_Cipher_Machine) 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 deciphering 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.

Production was stopped in September 1944 after 121 bombes had been made. The last-manufactured US Navy bombe is on display at the US [National Cryptologic Museum](https://en.wikipedia.org/wiki/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](https://en.wikipedia.org/wiki/Bell_Labs) on 30 September 1942. The machine was designed to analyses 3-rotor, not 4-rotor traffic. It was known as "003" or "Madame X". 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. 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.[[54]](https://en.wikipedia.org/wiki/Bombe#cite_note-WengerWilcoxP51-54#cite_note-WengerWilcoxP51-54) A 3-rotor run took about 10 minutes.

**Bombe rebuild**

In 1994 a group led by [John Harper](https://en.wikipedia.org/wiki/John_Harper_%28computer_engineer%29) of the BCS Computer Conservation Society started a project to build a working replica of a bombe. 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](https://en.wikipedia.org/wiki/Bletchley_Park) museum.

**See also**

* [Cryptanalysis of the Enigma](https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma)
* [Colossus computer](https://en.wikipedia.org/wiki/Colossus_computer)
* [Heath Robinson](https://en.wikipedia.org/wiki/Heath_Robinson_%28codebreaking_machine%29)
* [Jean Valentine (bombe operator)](https://en.wikipedia.org/wiki/Jean_Valentine_%28bombe_operator%29)
* This page was last modified on 13 January 2016, at 12:29.