Enigma: Design and History

Ethan Urie

History of the Enigma

The Enigma Machine was Germany's main cryptographic device during the Second World War. It was invented in 1919 by Dutchman, Hugo Koch. It was first produced commercially by Arthur Scherbius in 1923. The German government took an interest in the security it provided and acquired all rights to the machine and set about to adapt and change it to its specific, military needs. As the military adopted it, its use penetrated all levels of command from the front-line to ships, tanks, and planes (Bury).
The machine, unaltered, with the three rotor, reflector and 6 plug connector set-up was capable of 3,283,883,513,796,974,198,700,882,069,882,752,878,379,955,261,095,623,685,444,055,315,226, 006,433,616,627,409,666,933,182,371,154,802,769,920,000,000,000 coding positions. Knowing that the deciphering of the Enigma without knowledge of the rotor configuration, and other factors, would require machine assistance that was had not been invented yet, the German's felt secure with the use of the Enigma, even if one was captured. Unfortunately for them, they did not always use proper communication security and this, along with the advent of the high-speed machinery needed to crack the codes helped to bring an end to the Third Reich.

The British worked to break the Enigma at Bletchley Park in England. The code breakers were organized into Huts. These Huts worked in pairs and were known only by their numbers for security reasons. Huts 3 and 6 worked together on deciphering messages from the German Army and Luftwaffe. Huts 4 and 8 worked on messages for the Navy. This history will focus mainly on the Navy's Enigma since that was the most difficult for the people at Bletchley to break.

The Navy's Enigma used many different ciphers. Each cipher had its own daily key that consisted of the rotor order, ring settings, plugboard connections and the ground setting (Erksine). Up until October, 5 1941, the primary U-Boat cipher was Heimisch or Dolphin. After that, Shark was the main cipher. The differences in the ciphers were aided by the differences in the hardware that they ran on. Dolphin ran on M3 and Shark initially ran on M3 and then switched to the new M4.

The Navy's original Enigma, M3, was of the same, three rotor design that was used by the army and luftwaffe but with the slight change of 3 additional rotors, VI, VII, and VIII. These 3 additional rotors were reserved for the Navy. The Navy also employed codebooks to shorten signals in order to protect against high frequency, land-based direction finding. The first of the two most important books were the Kurzsignalheft, the short signal book that was used for reports of sighting convoys, etc. The second book was the Wetterkurzschlüssel that was used for weather reports (Erksine). This gave Hut 8 a challenge.

The two main problems facing Hut 8 of Bletchley Park were:

1) The 8 rotors could be arranged in 336 different ways as opposed to the 60 for the army and luftwaffe. A bombe run using all the Navy's rotor combinations took five times longer than a run against the army or luftwaffe Enigma (Erksine).
2) 'Cribs', probable plaintexts that were used to program the Bombes, were non-existent until mid-1941 (Erksine).

The British were lucky enough to receive an Enigma and the first 5 rotors (I – V) from the Polish Cipher Bureau in 1939 before Germany invaded. A lot of credit goes to the Polish cryptanalyst Marian Rejewski who had reconstructed the wirings for the first 3 rotors in 1932 just by using mathematical techniques, and the wirings for the other 2 (IV and V) before the war began (Erksine). Rotors VI and VII were captured from the crew of U-33 on February 12, 1940 and the last rotor was acquired in August of 1940. These acquisitions allowed the British to actually see the construction of the Enigma and to formulate a machine to combat it.

The famous mathematician Alan Turing invented the first Bombe, a machine designed to find the keys to ciphers in 1940. This allowed the British at Bletchley to break some messages starting in April 1940 and continuing through May and June. An improved, faster Bombe was invented and began service in August of the same year.
To aid the Bombes Hut 8 needed good cribs. Many cribs were provided by Hut 10, which broke manual weather ciphers. Even more cribs were created when Hut 8 received an 1940 copy of the Wetterkurzschlüssel. This allowed Hut 8 to break U-boat weather signals that provided the cribs.

But even with the new, faster Bombes and the cribs from Hut 10, Bletchley had to live with reading delayed Dolphin messages until June and July 1941 when keys captured from weather ships became available. From August of 1941 through until the end of the war, Hut 8 was able to read Dolphin signals with little delay.

The Germans however were not sitting idly by. On February 1st, 1942 the new M4 came online on Triton (named Shark by Bletchley), a special cipher used by Atlantic and Mediterranean U-boats (Erksine). The M4 used 4 rotors instead of 3 making Bletchley unable to read and Shark messages for over 10 months. However, the M4's 4th rotor was not interchangeable with any of the 8 original rotors. So the 4th rotor, Beta, increased the M4's power by 26 but did not change the number of different rotor configurations from the M3's 336. This was not M4's only problem. At one configuration of the 4th rotor, M4 emulated M3 and all U-boats used this configuration when encrypting the short weather reports. Thi, coupled with the seizure of the second edition of the Wetterkurzschlüssel from U-559 on October 30, 1942 which gave Hut 8 cribs, lead to consistent, yet delayed decryption of weather broadcasts. These broadcasts allowed the British to locate and avoid the U-boats saving many ships and men between December 1942 and January 1943.

However, this success was short-lived. On March 10, 1943 a new version of the Wetterkurzschlüssel took effect which deprived Hut 8 of any cribs. But using short signal sighting reports as cribs, Hut 8 broke Shark again on March 19, 1943. . The Kurzsignalheft short sighting reports used the M4 in M3 emulation mode as well and the Kurzsignalheft had also been seized from U-559 (Erksine). They were able to read Shark signals for 90 out of 112 days until June 20, 1943

To combat the new M4 the British and US Navy introduced their 4-rotor Bombes into service in June and August 1943. This initially allowed them to break Shark keys in 26 days. From September 1943 on however, they were able to break the Shark keys in less than 24 hours on average.

Some notes

Dolphin and most of the 14 other ciphers that were used throughout the war by the Navy consisted of a Allgemein (general) and Offizier keys. Offizier messages were first encrypted with plugboard settings from a monthly keylist and then were encrypted with the Allgemein key. Some of the ciphers also had a Stab (staff) keys which were, like the Offizier keys, encrypted twice. But the Stab keys had their own settings. Offizier messages usually took a week to decrypt at Bletchley (Erksine).

To read more on how the Enigma was solved, read Keith Jones' paper located at:
http://www.cs.rit.edu/~kmj9907/enigma.html

Enigma Design

Over the course of the years before and during World War II, the design of the Enigma underwent changes. These changes were meant to keep the allies from cracking it. The initial design consisted of 3 rotors, rotors I, II, and III. Each rotor was constructed of 8 basic parts. This diagram is from the website run by Tony Sale, the former curator of the Bletchley Park museum, http://www.codesandciphers.org.uk/enigma/enigma2.htm.

1. The finger notches used to turn the rotors to a start position.
2. The alphabet RING or tyre round the circumference of the rotor (see below for an explanation of its significance).
3. The shaft upon which the rotors turn.
4. The catch, which locks the alphabet ring to the core (5).
5. The CORE containing the cross wiring between contacts (6) and discs (7). It is the core that effects the essential alphabetic substitution.
6. The spring-loaded contacts to make contact with the next rotor.
7. The discs embedded into the core to make contact with the spring-loaded contacts in the next rotor.
8. The CARRY notch attached to the alphabet ring (see below for explanation).

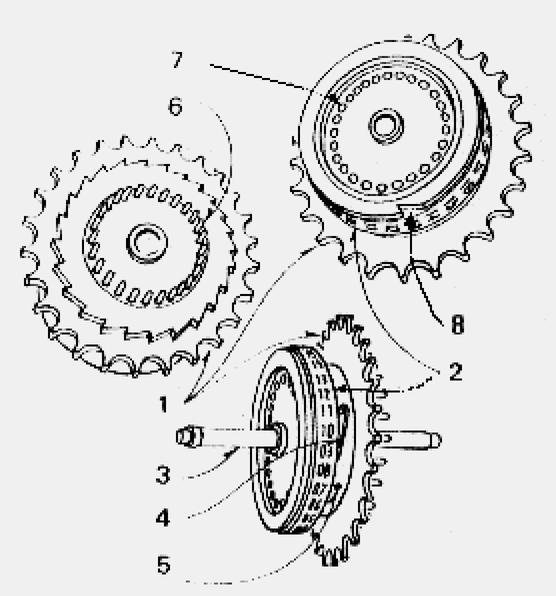


Figure 1. Diagram of the Enigma's rotors.

The Enigma was set up so that the current would pass from right to left through the rotors, hit the reflector disc and then travels back, left to right through the rotors. The signal passes through the entry disc first before passing through the rotors. The entry disc is a fixed disk with 26 contacts. It is connected to the keyboard on the right side in alphabetical order, i.e. no translation was made between the keyboard and entry disc. The rotors were interchangeable, allowing up to 6 configurations. After the current had made a complete pass through the rotors, reflector and passed back through the rotors, it would light up the cipher character on the light board. This allowed the operator to see what the character was and write it down.

One of the more important modifications made to the basic Enigma when brought in for military use was the plugboard or Stecker board. The board was situated on the front of the machine as seen in the figure below. The board acted similar to another rotor. It added a translation between the keyboard and the entry disc, and the entry disc and the light board. The board however, could be rewired by the operator, unlike the rotors. It did not rotate like the rotors did though and did not have the scrambling capacity of the rotors. The board allowed pairs of letters to be swapped and wiring it had the effect of hardwiring the swap. During the war 10 pairs of letters were generally swapped on the board. The design of the board left the machine's reciprocal properties unchanged so nothing different had to be done to decipher a message. However, it also left the property that never allowed a letter to be enciphered to itself. This was a mistake.

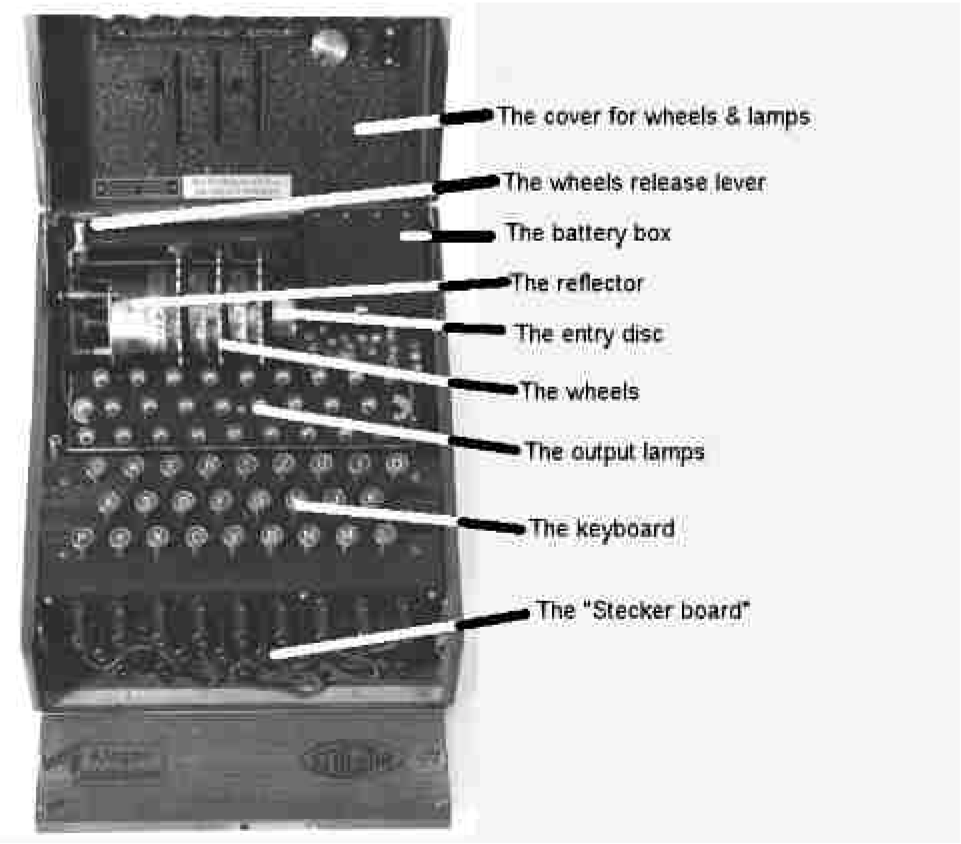


Figure 2. Picture of the Enigma with a Stecker board.

To illustrate how the machine would work with three rotors and the Stecker board, it is easier to use a diagram. The diagram in Figure 3 shows the path a signal would take from the time a key is pressed to when the light corresponding to the cipher character lights up on the light board.

The following diagram and explanation comes from the website run by Tony Sale, the former curator of the Bletchley Park museum, http://www.codesandciphers.org.uk/enigma/enigma2.htm.

In this illustration, when key W is pressed on the keyboard (5) current from the battery (4) flows to the plugboard panel socket W, but socket W has been plugged to socket X so current flows up to the entry disc (E) at point X. The current then flows through the internal wiring in the rotors (2) to the reflector (1). Here it is turned around and flows back through the rotors in the reverse direction emerging from the entry disc at terminal H. Terminal H on the Entry disc is connected to socket H on the plugboard (6) but this socket is plugged to socket I so finally the current flows to lamp I which lights up. Thus in this instance, the letter W is enciphered to I.

You can now also see that if the key I had been pressed, the lamp W would have lit up. This is because the path from W to I through the Steckers and rotors remains the same, though with the current flowing in the opposite direction.

When the W key is pressed the connection to the W lamp is broken and the I lamp lights. If the I key is now pressed down the connection to the I lamp is broken and the W lamp lights.

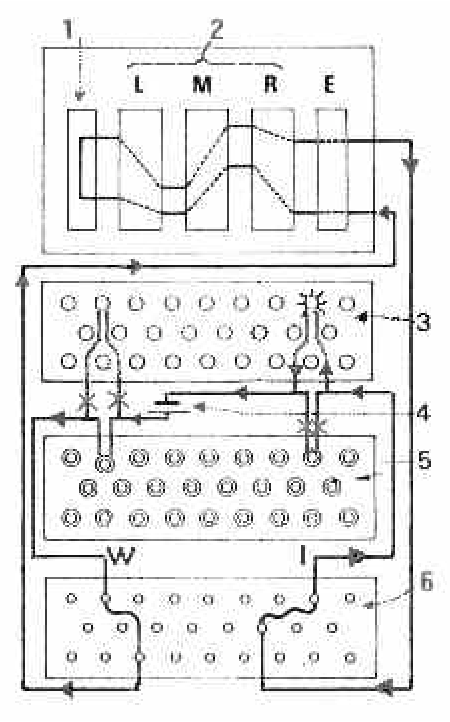
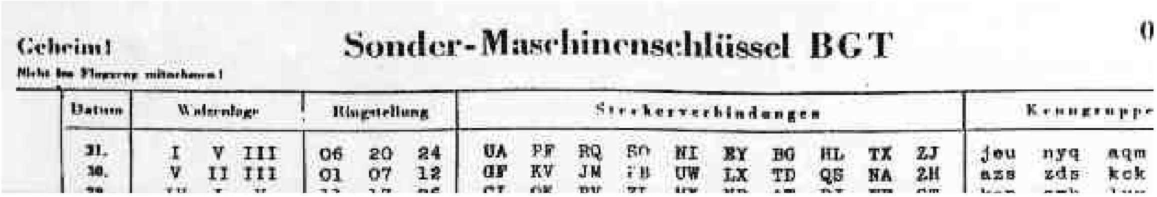


Figure 3. Circuit diagram of the Enigma with the Stecker board.

Therefore deciphering a message is the simple task of setting up the machine with the exact configuration of the machine that enciphered the message and typing in the ciphertext. The plaintext of the message will light up on the light board for the typist to copy down.

The rotors, true their name, rotated with every key press. Before the machine sent the current through the plugboard and into the entry disc, the machine would rotate the rightmost rotor one letter or 1/26th of a full rotation. Then, depending on the catch notch on the alphabet ring shown as (4) in Figure 1, the first rotor would carry the middle rotor with it. The same thing occurred when the middle rotor's catch notch met the third rotor. The carry point of each rotor was the catch notch which was attacked to the alphabet ring and not the core. So it would turn with the ring. The notch was put in different places on every rotor. The notch was set by turning the alphabet ring, which changed the letter that showed through the window of the machine. This did not change the overall essential scrambling of the letters but it did affect the indicator systems that relied on the window position of the rotor.

The settings that were used by all German operators were printed on sheets of paper, one month at a time. The sheets contained settings for each day of the month therefore changing the cipher used by any Enigma operator every 24 hours. A partial picture of one of these sheets is shown in Figure 4. The first column contains the date. The second column shows the rotor configuration. The Third column shows the ring settings, and the fourth column is the wiring settings for the Stecker board. So, for the 31st of the month, the rotors would be in the configuration: I V III, in that order, left to right. The ring setting for the leftmost rotor would be 6, or F. In other words the alphabet ring would be turned so that the letter F was next to the catch. The middle rotor would



Geheim!

Nicht im Flugzeug mitnehmen!

Sonder-Maschinenschlüssel BGT

Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppe		
31.	I	V	III	06	20	24	UA	PF	RQ	SO	NI	EY	BG	HL	TX	ZJ	jeu	nyq	aqm
30.	V	II	III	01	07	12	GF	KV	JM	IB	UW	LX	TD	QS	NA	ZH	azs	zds	kck

Figure 4. Part of a settings sheet for the Enigma.

be set to 20 (T), and the rightmost rotor would be set to 24 (X). The Stecker board would be wired so that the letters U and A are wired together, P and F, R and Q, etc. The one thing that the paper did not tell the operator was the start position for the rotors. This the operator had to decide and encode in the message somehow. There were many systems used to do this and they changed over time and depending on the branch of the military. The simplest method was that the operator would choose a start (indicator) position and choose three letters for the key. They would be sent in clear text and repeated once. Then those three characters were typed into the machine and the enciphered characters were sent. Then the rotors were turned to the positions of the three enciphered key characters. Then the message would be typed in and sent. The basic steps are outlined below.

Sending and receiving a message using the simple Enigma indicator system

To send a message:

1. Set the Enigma machine into the base configuration for the day as given in the setting sheet for the month.
2. Select a three letter start position, (the indicator), from which to encipher the selected three letter message key.
3. Turn the rotors to the indicator position, key in the message key, twice, and note down the lamps that light.
4. Turn the rotors to the message key letters and key in the message to be sent, noting down the lamps as they light.
5. Give the enciphered message plus its preamble to the radio operator for it to be transmitted by Morse code.

On receiving a message:

1. Set the Enigma machine into the same base configuration for the day from the setting sheet.
2. Turn the rotors to the indicator letters received in the preamble to the message.
3. Key in the next six letters to reveal the repeated message key as the lamps light.
4. Turn the rotors to the message key letters. Key in and decrypt the cipher text.

Other modifications

The Enigma was modified in other ways throughout the years of its use. To increase the complexity of the cipher, some Enigmas were equipped with UHR’s or clocks. The clock plugs were substituted for the original plugs in the Enigma’s plugboard. This way the current was passed through the clock which could select between 40 different plug arrangements by simply turning the large knob on the front of the clock (Bury).

Other modifications included an additional rotor, which was introduced with the M4 Enigma. The Navy also added 3 more rotors, VI, VII, VIII to add to the number of possible configurations.

But even with the ingenious design of the original Enigma and all the enhancements and modifications to further increase the security that it afforded, the Enigma was broken. Many of the small things that lead to the cracking of the Enigma were things like making the catch notch different on each rotor, allowing the British to figure out which rotor was in the rightmost position. Other mistakes included the property that did not allow a letter to be enciphered to itself, decreasing the number of possible cipher texts. So the machine was obviously not immune to attacks, and the advent of fast computational machinery allowed for the kinds of attacks that were unforeseen when the Enigma was first invented and enlisted into use for the military. The German Navy took the most precautions, creating a very tough time for the people at Bletchley but again, oversights made cracking possible. The small detail of the use of the M4 in M3 mode when sending weather reports was, in retrospect, quite a big mistake. But despite these mistakes and miscalculations on the German’s part, the machine is formidable and an incredible piece of workmanship. It is quite clear why it has gone down in history as one of the most famous cipher machines ever.

Works Cited

Bury, Jan. The Enigma – A Polish View. 25 October 2001.
http://webhome.idirect.com/~jproc/crypto/enigs1.html,
http://webhome.idirect.com/~jproc/crypto/enigma.html

Erksine, Ralph. Allied Breaking of Naval Enigma. 25 October 2001.
http://www.uboat.net/technical/enigma_breaking.htm

Sale, Tony. The Enigma Cipher Machine. 5 November 2001.
http://www.codesandciphers.org.uk/enigma/