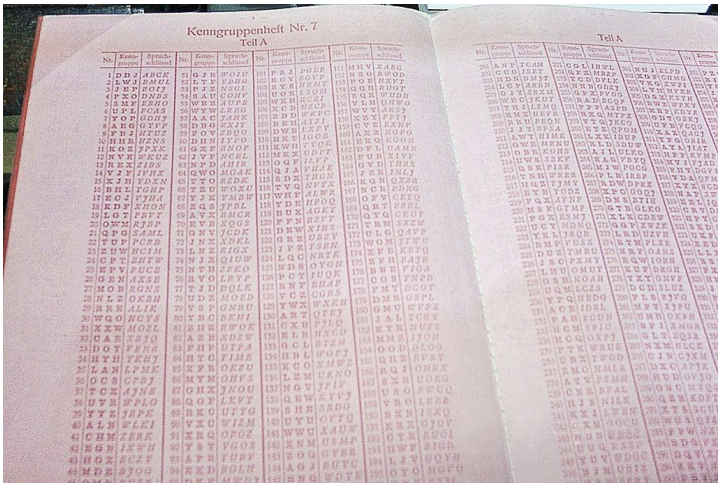
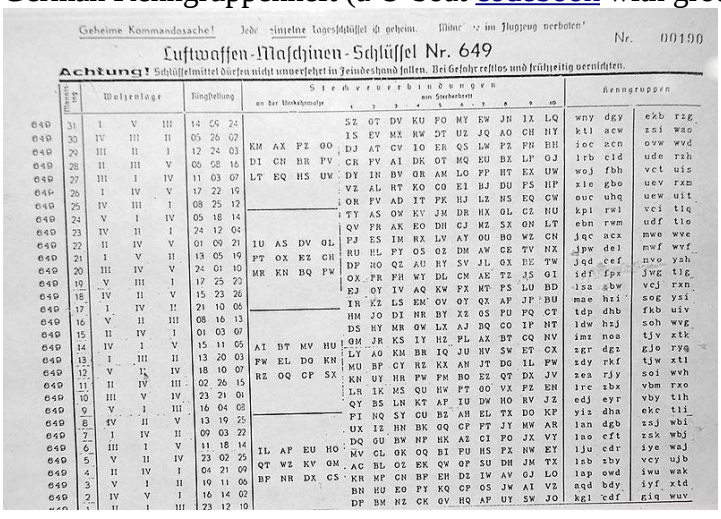
A German Enigma operator would be given a plaintext message to encrypt. For each letter typed in, a lamp indicated a different letter according to a pseudo-random substitution, based upon the wiring of the machine. The letter indicated by the lamp would be recorded as the enciphered substitution. The action of pressing a key also moved the rotor so that the next key press used a different electrical pathway, and thus a different substitution would occur. For each key press there was rotation of at least the right hand rotor, giving a different substitution alphabet. This continued for each letter in the message until the message was completed and a series of substitutions, each different from the others, had occurred to create a cyphertext from the plaintext. The cyphertext would then be transmitted as normal to an operator of another Enigma machine. This operator would key in the cyphertext and—as long as all the settings of the deciphering machine were identical to those of the enciphering machine—for every key press the reverse substitution would occur and the plaintext message would emerge.

Details



German Kenngruppenheft (a U-boat codebook with grouped key codes)



Monthly key list Number 649 for the German Air Force Enigma, including settings for the reconfigurable reflector.

In use, the Enigma required a list of daily key settings and auxiliary documents. The procedures for German Naval Enigma were more elaborate and more secure than those in other services. Navy codebooks were printed in red, water-soluble ink on pink paper so that they could easily be destroyed if they were endangered.

In German military practice, communications were divided into separate networks, each using different settings. These communication nets were termed *keys* at Bletchley Park, and were assigned code names, such as *Red*, *Chaffinch*, and *Shark*. Each unit operating in a network was assigned a settings list for its Enigma for a period of time. For a message to be correctly encrypted and decrypted, both sender and receiver had to configure their Enigma in the same way; rotor selection and order, starting position and plugboard connections must be identical. All these settings (together the key in modern terms) were established beforehand, distributed in codebooks.

An Enigma machine's initial state, the cryptographic key, has several aspects:

- Wheel order (*Walzenlage*) – the choice of rotors and the order in which they are fitted.
- Ring settings (*Ringstellung*) – the position of the alphabet ring relative to the rotor wiring.
- Plug connections (*Steckerverbindungen*) – the connections of the plugs in the plugboard.
- In very late versions, the wiring of the reconfigurable reflector.
- Initial position of the rotors – chosen by the operator, different for each message.

For example, the settings for the 18th day of the month in the German Luftwaffe Enigma key list number 649 (see image) were as follows:

- Wheel order: IV, II, V
- Ring settings: 15, 23, 26
- Plugboard connections: EJ OY IV AQ KW FX MT PS LU BD
- Reconfigurable reflector wiring: IU AS DV OL PT OX EZ CH MR KN BQ PW
- Indicator groups: lsa saw vci rxn

Enigma was designed to be secure even if the rotor wiring was known to an opponent, although in practice considerable effort protected the wiring configuration. If the wiring is secret, the total number of possible configurations has been calculated to be around 10^{114} (approximately 380 bits); with known wiring and other operational constraints, this is reduced to around 10^{23} (76 bits).[15] Users of Enigma were confident of its security because of the large number of possibilities; it was not then feasible for an adversary to even begin to try a brute force attack.

Indicator

See also: Cryptanalysis § Indicator

Most of the key was kept constant for a set time period, typically a day. However, a different initial rotor position was used for each message, a concept similar to an initialisation vector in modern cryptography. The reason is that encrypting many messages with identical or near-identical settings (termed in cryptanalysis as being *in depth*), would enable an attack using a statistical procedure such as Friedman's Index of coincidence.[16] The starting position for the rotors was transmitted just before the ciphertext, usually after having been enciphered. The exact method used was termed the *indicator procedure*. Design weakness and operator sloppiness in these indicator procedures were two of the main weaknesses that made cracking Enigma possible.

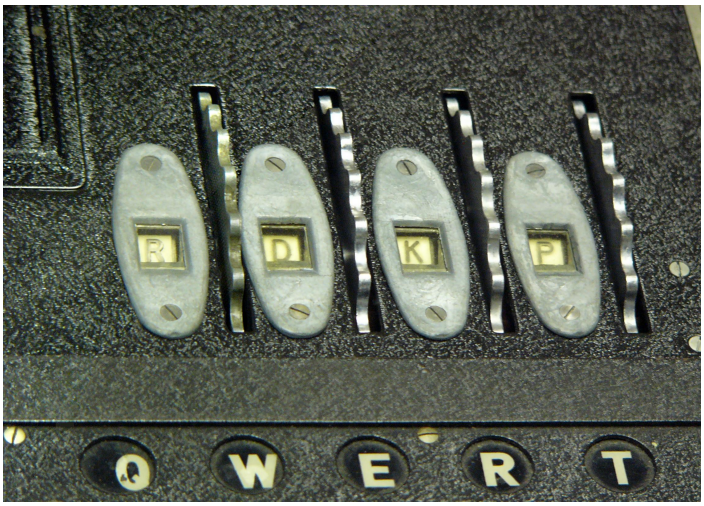


Figure 2. With the inner lid down, the Enigma was ready for use. The finger wheels of the rotors protruded through the lid, allowing the operator to set the rotors, and their current position, here *RDKP*, was visible to the operator through a set of windows.

One of the earliest *indicator procedures* was used by Polish cryptanalysts to make the initial breaks into the Enigma. The procedure was for the operator to set up his machine in accordance with his settings list, which included a global initial position for the rotors (the *Grundstellung*, meaning *ground setting*), say, *AOH*. The operator turned his rotors until *AOH* was visible through the rotor windows. At that point, the operator chose his own arbitrary starting position for that particular message. An operator might select *EIN*, and these became the *message settings* for that encryption session. The operator then typed *EIN* into the machine, twice, to allow for detection of transmission errors. The results were an encrypted indicator—the *EIN* typed twice might turn into *XHTLOA*, which would be transmitted along with the message. Finally, the operator then spun the rotors to his message settings, *EIN* in this example, and typed the plaintext of the message.

At the receiving end, the operation was reversed. The operator set the machine to the initial settings and typed in the first six letters of the message (*XHTLOA*). In this example, *EINEIN* emerged on the lamps. After moving his rotors to *EIN*, the receiving operator then typed in the rest of the ciphertext, deciphering the message.

The weakness in this indicator scheme came from two factors. First, use of a global ground setting —this was later changed so the operator selected his initial position to encrypt the indicator, and sent the initial position in the clear. The second problem was the repetition of the indicator, which was a serious security flaw. The message setting was encoded twice, resulting in a relation between first and fourth, second and fifth, and third and sixth character. This security problem enabled the Polish Cipher Bureau to break into the pre-war Enigma system as early as 1932. However, from 1940 on, the Germans changed procedure.

During World War II, codebooks were only used each day to set up the rotors, their ring settings and the plugboard. For each message, the operator selected a random start position, let's say *WZA*, and a random message key, perhaps *SXT*. He moved the rotors to the *WZA* start position and encoded the message key *SXT*. Assume the result was *UHL*. He then set up the message key, *SXT*, as the start position and encrypted the message. Next, he transmitted the start position, *WZA*, the encoded message key, *UHL*, and then the ciphertext. The receiver set up the start position according to the first trigram, *WZA*, and decoded the second trigram, *UHL*, to obtain the *SXT* message setting. Next, he used this *SXT* message setting as the start position to decrypt the message. This way, each ground setting was different and the new procedure avoided the security flaw of double encoded message settings.[17]

This procedure was used by *Wehrmacht* and *Luftwaffe* only. The *Kriegsmarine* procedures on

sending messages with the Enigma were far more complex and elaborate. Prior to encryption the message was encoded using the *Kurzsignalheft* code book. The *Kurzsignalheft* contained tables to convert sentences into four-letter groups. A great many choices were included, for example, logistic matters such as refuelling and rendezvous with supply ships, positions and grid lists, harbour names, countries, weapons, weather conditions, enemy positions and ships, date and time tables. Another codebook contained the *Kenngruppen* and *Spruchschlüssel*: the key identification and message key.[18]

Additional details

The Army Enigma machine used only the 26 alphabet characters. Punctuation was replaced with rare character combinations. A space was omitted or replaced with an X. The X was generally used as period or full-stop.

Some punctuation marks were different in other parts of the armed forces. The *Wehrmacht* replaced a comma with ZZ and the question mark with FRAGE or FRAQ.

The *Kriegsmarine* replaced the comma with Y and the question mark with UD. The combination CH, as in "*Acht*" (eight) or "*Richtung*" (direction), was replaced with Q (AQT, RIQTUNG). Two, three and four zeros were replaced with CENTA, MILLE and MYRIA.

The *Wehrmacht* and the *Luftwaffe* transmitted messages in groups of five characters.

The *Kriegsmarine*, using the four rotor Enigma, had four-character groups. Frequently used names or words were varied as much as possible. Words like *Minensuchboot* (minesweeper) could be written as MINENSUCHBOOT, MINBOOT, MMMBOOT or MMM354. To make cryptanalysis harder, messages were limited to 250 characters. Longer messages were divided into several parts, each using a different message key.

"The translated 1940 Enigma General Procedure". codesandciphers.org.uk. Retrieved 16 October 2006.

"The translated 1940 Enigma Officer and Staff Procedure". codesandciphers.org.uk. Retrieved 16 October 2006.