Chronological table of the deciphering

The deciphering represents an attempt to show the difficulties of the deciphering as an understandable sequence of the individual processes this chronological table.

The events shall serve the deciphering of the "Enigma (puzzle)" as a basis for this representation. This test is based on a whole number of publications. This chronological table asks questions at the same time which have remained open also in the newer literature for the deciphering.

For this chronological table the individual process steps are looked at in a chronological order.

Because the connections can be shown clearly only by the taking apart in individual processes.

Process of the encoding Transmitter - receiver	**Process of the deciphering by the third party (activities.)**	**Remarks**
Construction of the information about the encoding		
Veiling and compression of the information by the use of the code book		
Make the key texts (secret text) and the saying key By a mechanical petition into the encryption equipment		
Handing over of the key text and the saying key to the radio operator		
Conveyance encoded radio message the about an "open radiofrequency channel"		Radio message got buggable for everyone Location of the transmitter could be found out by radio direction finding Age remark "spark is treason"; this statement is only conditionally valid.

With the following process steps the "third party" can only actively intrude on the event.

Process of the encoding	Process of the deciphering by the third party (activities.)	Remarks
Shipment encoded radio message the to the receiver Reception of the encoded radio message by the receiver	**Photo encoded radio message the through the eavesdrop stations and record keeping of the fiver groups**	**The beginning of the activities of the third party** Required time: Dependent on the saying length Faultlessness: Erroned; Radio interferences; Photo fault
The handing over of the encoded radio message to decoded	"Radio telexes encoded" construction of a machine-readable into fiver groups	Conveyance duration: Dependent on the saying length; Of the availability of a communication channel (telegraph channel/telex.
Deciphering of the encoded radio message by means of currently valid key, Attitude of the individual key wheels (order of the key wheels.) The attitude of the key wheels by means of saying key Attitude of the assignment of the signs (plug board.) The size of the individual steps was different	Conveyance and reception "encoded" radio message the in the decoding head office	Entrance in the decoding head office; Waiting on a free Decoding capacity
The beginning of the deciphering of the encoded radio message	Aid at the deciphering; **Saying key**	**Further aids:** Coordinates of the transmitter by **radio direction finding** **Ringing tone** **Radio operator**; Eavesdrop specialists could recognize the transmitters with giving the Morse signals. **Carelessnesses** in the choice of the saying keys Standard wordings in plain language. **Holes**; by two identical letters behind each other **Key documents** and got away with code books as well as encryption equipments able to work (Key means permitted one con-reading the encoded radio traffic immediately temporarily.) As well as further cryptic

		logical information
Duration of the deciphering: **Few minutes or shorter**	**The beginning of the deciphering**	**The beginning of the deciphering on the side of the third party is delayed by additional steps.** **Transformation of the encoded radio traffic in a machine-readable form (telex.)** **Conveyance in this 5 - channel format (ITA 2)** **Delay of the communication in strong message emerges.** **Cause:** **The encoded saying is taken simultaneously of several eavesdrop stations and then sent to the decoding head office.** **By the photos of the same radio messages encoded, by more independent eavesdrop stations the Fehlerrate can be reduced strongly in the process of the deciphering.**
Handing over of the decoded information to the receiver and execution of the transmitted information	**Duration of the deciphering:** **Or also lasting few minutes up to several months 1) 2)** **No information about the question has been submitted to the duration of the deciphering.** **Like sayings encoded much could you decode at the same time?**	**The duration of the deciphering decides on the value of the information**
		For the transmitter of the "information" the information has lost her value as of this time
	Deciphering successful *****Weiter... *****	

	Very sure of deciphering of the decoded saying with one method and group of people only chosen to one	**The method is solved safeguarding of the secret, this Proceed "extremist" in the case "Enigma" in this further**
	Reception of reaction corresponding to the information and introduction if necessary	For the "third party" you can assess only at this time. Whether the information has a value.

These process steps were required to solve a cipher system on the basis of an electrical mechanical operation.

1) You read to, the excellent representation of the Crypto museum Netherlands here. You find some information represented very well there. Also for the questions of the encoding means. The history of the Enigma in Germany as well as the variants of all sorts of equipment types are documented there. There the "forced idleness" of the British cryptologists is also shown after an equipment change in the U-Bootwaffe. The concept "idleness" was chosen consciously because the staff was, condemned to the idleness which operated this equipment. On the other hand, the heads smoked the cryptologist. This led to a longer "failure" of the decoding head office.

2) In some cases an immediate deciphering of the information was possible, has different causes this: Erbeutung of German submarines or other ships. Or by a long-standing supplier of the key documents, so among others KL - 7 and another systems - ,.

Author: Old Gocs, Berlin in June/July 2012

Dieses Material wird bei Kenntnis neuer Fakten aktualisiert. This material is updated at knowledge of new facts.

Publish under www.gocs.de or www.gocs.info