The Auxiliary Devices of OKW/Chi

Carola Dahlke
Deutsches Museum, Germany
c.dahlke@deutsches-museum.de

Abstract

Between 1942 and 1945, section IVb of OWK/Chi designed mechanical and electro-mechanical devices to statistically evaluate intercepted encrypted messages. By the help of TICOM protocols and a never published dissertation draft written by Willi Jensen in 1955, an overview of the cryptanalytic devices is given. Most probably all the equipment was destroyed at the end of the war. Only dredged-up remnants of one type of equipment could be recovered by German divers.

1 Hindered Research on German Signal Intelligence

Thanks to the recent declassification and publication of many TICOM files (Target Intelligence Committee interrogation protocols and summaries), it has become possible to take a closer look at the German side of cryptanalysis during the Second World War. As Weierud & Zabell (2019) already listed in detail, there are three main difficulties that complicate research on German signal intelligence: First of all, Germany lost the war, and destroyed almost all relevant documents and equipment. Even after the 1970s, when the allied nations finally began to talk about their signal intelligence achievements, German cryptanalysts kept their experiences in the Second World War secret until their death. Only a handful of papers exist which, although not published, have nevertheless been written by German cryptanalysts, and were given to archives, libraries or universities for safekeeping (e.g. Hüttenhain 1970, Jensen 1955).

Apart from the lack of sources and remaining artefacts, historic research is hampered by the fact that Germany had not only one but eight different intelligence sections[1] during the Second World War, some of which worked completely independently of each other:

- **OKW/Chi**: Cipher department of the High Command of the Armed Forces ("Chiffrierstelle des Oberkommandos der Wehrmacht").
- **In 7/IV, In 7/VI:** Inspectorate 7 group 4 and 6 ("Inspektion 7 Gruppe 4 und 6"), the cipher department of the army; in 1944 reorganized and combined as **OKH/GdNA:** Signal intelligence agency of the High Command of the army ("General der Nachrichtenaufklärung des Oberkommandos des Heeres").
- **OKM/B-Dienst:** Intelligence service of the Naval High Command (Beobachtungs-dienst der deutschen Kriegsmarine).
- **O.b.L/Chi:** Signal intelligence agency of the German Air Force ("Chiffrierstelle, Chi-Stelle" des Oberbefehlshabers der Luftwaffe"); in 1944, reorganized and renamed in **OKL/LN Abt 350:** Aerial news division 350 of the Airforce High Command ("Luftnachrichten Abteilung 350 des Oberkommandos der Luftwaffe").
- **RLM/FA:** Research office of the State Ministry of Aviation ("Forschungsamt des Reichsluftfahrtministeriums"), i.e. the cryptological service of the Nazi party.
- **AA/Pers Z S & Pers Z Chi:** Cipher department of the Foreign Office (Chiffrierstelle des Auswärtigen Amts).

1 For comprehensive descriptions, see e.g. Mowry (1989); Weierud & Zabell (2019); EASI Vol 2-7.

- **Abwehr**: Secret service of the military; part of the High Command of the Armed Forces OKW until 1944, then reorganized and integrated into the espionage section of the SS.
- **RSHA/Amt IV E:** Secret service of the Reich Security Administration, i.e. of the SS ("Abwehr des Reichssicherheits-hauptamts") until 1944; then reorganized and combinded with the Abwehr of OKW into **RSHA/Amt VI.**

This polycratic appearing coexistence of competing institutions with similar competences was typical for the regime of National Socialism. Attempts had been made to create a central intelligence office, but were not realized (see e.g. TICOM DF-187, p. 14[2]; Bauer 1997, p. 31). Instead, the consisting signal intelligence offices were partly reorganized, e.g. as a result of the coup attempt on the 20th of July 1944. This means that the few historical sources that are available can often only be assigned to one of the different departments, or to a person who may have changed affiliation or departments several times during the war.

This study will focus on the cipher department of the Oberkommando der Wehrmacht (OKW/Chi), and on the deciphering devices that have been designed and used there.

2 OKW/Chi

The OKW/Chi had originally been the cipher office of the Reich War Ministry. It was renamed the cipher office of the OKW in 1938 with about 30 staff members initially, but grew up to 250 in 1942, and sank to only 120 persons by the end of war (TICOM I-206, p. 9). A description of the organization of OKW/Chi can be found e.g. in EASI Vol 3, in TICOM I-39, in Rezabek (2013), and very detailed information on the mathematical staff is summarized by Weierud & Zabell (2019).

OKW/Chi was two-fold: One part of the organization was mainly concerned with monitoring the broadcast or news of enemy and neutral states. The other part dealt with signal intelligence. The cipher telegrams of about 30 countries were watched by OKW/Chi, and the task was to decipher only important diplomatic letters, i.e. telegraphic communications of diplomats, military attachés, government and economic authorities etc. (EASI, Vol 3, p. 15). According to the interrogation papers of Wilhelm Fenner, who was in charge of the OKW/Chi's cryptanalysis sections IV and V, the successful years of OWK/Chi were between autumn 1939 and autumn 1943. His team deciphered about 100 messages per day, sometimes several pages long (TICOM DF-187A, p. 16), although never attaining its full potential due to bombing attacks, broken furniture, dirt, cold and chronic undernourishment of the staff (TICOM I-206, p. 9).

In general, it can be said that OKW/Chi did not achieve great successes, but at least constantly managed many minor decipherments (EASI Vol 3, p. 55). The OKW/Chi's cryptanalytic successes are e.g. mentioned in TICOM I-31, pp. 5ff, and are summarized in EASI Vol 3, chapter IV.

In 1944, the OKW/Chi (apart from its archive[3]) was transferred from Berlin to Halle/ Saale, where it continued its work until April 1945. Dr. Buggisch stated (TICOM I-176, p. 12) that all OKW/Chi machinery was taken to Halle, too.

On the 13th of April 1945, the remaining staff[4] of OKW/Chi took a train from Halle to Werfen/

2 According to TICOM interrogation protocols, attempts were made by Willhelm Fenner, Franz Thiele (who was hanged after the coup attempt on Adolf Hilter on the 20th of July 1944) and brigade commander Schlieberg, to set up a joint cryptanalysis agency. The plan was to take the best analysts from all the agencies that had existed so far and put them under Fenner's care.

3 The archive of the OKW/Chi went to the intercept station at Lauf, and remained there until spring 1945. On the 10th of April 1945, the Lauf station moved south to the lake Schliersee, where the staff dumped about nine-tenth of its equipment and the complete OKW/Chi archive into the lake (EASI Vol 3, p. 34). The boxes with the archives were recovered shortly after by the TICOM Team 5 (TICOM Team 5, Rezabek 2013), kept classified until 2013 and is now available at the Politisches Archiv in Berlin.

4 In the end of the war, parts of the OKW/Chi leadership, namely Mettig, Kettler, Dr. Hüttenhain and Fricke, travelled to the north of Germany (EASI Vol 3, p. 34+35). Please note: neither the dates of the disintegration of OKW/Chi nor the accounts about the changes in the organization of OKW/Chi were consistent in the

Salzach in Austria, to join with the "General der Nachrichtenaufklärung Süd", i.e. the Southern cipher department of the Oberkommando of the Heer (OKH/GdNA) – one of the other pendants of competing intelligence offices mentioned before. OKW/Chi was disbanded that day. Fenner stated that since the American invasion was expected, all material was set on fire or thrown into the river Salzach (TICOM DF-187, p. 14).

2.1 Sub-section IVb

Under the head of Dr. Hüttenhain a special OKW/Chi subsection IVb was installed in 1942 to develop cryptanalytic machinery. IVb consisted of 28 staff members, i.e. two graduate engineers, three working engineers and 25 mechanics. The main idea of the mechanical devices was "*to replace the speed of fingers in statistical operations*" (Fenner, TICOM DF-187A, p. 20).

In general, Hollerith machines were used whenever possible, but so-called "Hilfsgeräte" (auxiliary devices; in the TICOM protocols they are entitled as rapid analytical machinery) were developed for special cryptanalytic purposes.

Fenner stated that these devices were mainly experimental models, and the technical possibilities could not be exhausted (TICOM DF-187, p. 15). Nevertheless, the machines that were developed in this section were mentioned as an outstanding achievement of OKW/Chi in the TICOM reports (EASI Vol 3, p. 72). As well, TICOM documents refer to the visit of an Italian cryptanalyst Augusto Bigi, who saw the OKW/Chi machines in 1942 and was impressed (see EASI Vol 3, p. 73 & TICOM IF-1517, pp. 14-15).

2.2 A Dissertation Never Published

Willi Jensen, a freshly graduated engineer, born in Kiel, was among the twenty-eight members of subsection IVb, under the command of the telecommunication engineer Mr. Rotscheidt (formerly with Siemens).

Ten years after the end of the war, Willi Jensen submitted a dissertation at the Technical University of Munich with the title "Hilfsgeräte der Kryptografie" (auxiliary devices of cryptography, Jensen 1955). According to Bauer (2009, p. 388), the professor in question did not feel responsible, and the work remained unevaluated. We cannot be sure, but presumably, the professor in question was the mathematician Professor Robert Sauer, in whose estate at the Technical University of Munich a copy of the work was found (see the TUM university library, section mathematics and computer science, in Garching, signature 0109/I 305+306).

Apparently, Jensen did not submit this work anywhere else either [5]. He apparently never received the doctorate. So far, the author of this article knows nothing about Jensen's life after 1955. Since he submitted the draft of his dissertation with the German title "Postrat" (i.e. a councillor of a post office), he was most probably spending some time of his life in the postal service as a telecommunication engineer.

In his dissertation manuscript Jensen describes fourteen auxiliary devices that OKW/Chi apparently developed and constructed under his supervision. It is of course not surprising and due to the post-war period that he does not mention any other people who worked with him on the equipment. In TICOM interrogation protocol I-37, p. 8, Dr. Hüttenhain states that both graduate engineers Rotscheidt and Jensen were responsible for developing the rapid machinery according to the specifications of the cryptanalysts of OKW/Chi.

Jensen's manuscript is divided into seven sections. First, the basics of cryptography and second, the basic problems of deciphering are explained. This is followed by a third chapter on the cryptographic elements of the auxiliary devices. A fourth short chapter notes some technical matters on the subject of reading punched tapes. The fifth chapter explains the modular components from which the auxiliary devices were built. Chapter six explains the design and function of the devices. In addition, chapter seven is an elaborate second volume with

interrogation protocols of TICOM; more details can be found in EASI Vol 3, pp. 33-35.

5 Today a second copy is in the possession of the Bayerische Staatsbibliothek Munich which was probably in the ownership of Dr. Hüttenhain before. (Manuscript section, BSB signature Cgm 9303)

technical drawings of all equipment that complements the manuscript.

While Jensen speaks of fourteen devices, the TICOM protocols list only eight, and TICOM also describes that some devices were only in the planning stage and had not yet been fully constructed at the end of the war. The attempt to match the devices from Jensen's manuscript with those from the TICOM protocols was complicated by the fact that the German terms and names of the devices were not always compatible to the TICOM interrogation. This is probably primarily due to the fact that neither Jensen nor Rotscheidt, who were mainly responsible for the development of the auxiliary devices, were ever interviewed by TICOM. As well it should be mentioned that Jensen's approach to describe the machinery was primarily technically, and less cryptanalyticly, driven.

3 The Auxiliary Devices of OKW/Chi

As mentioned before, OKW/Chi used Hollerith machines [6] whenever possible. Dr. Hüttenhain stated that IBM machines could be used for sorting processes in the first place (I-37, p. 2). But for all other applications, section IVb developed special apparatus from 1942 on.

In general, a kind of modular system was created, so that the OKW/Chi's cryptanalysts could reassemble the devices according to their needs (see e.g. I-37, p. 9). This modular system consisted of three major components:

With the so-called reading apparatus "**Abtast-werke**" (see Jensen 1955, pp. 48-55) punched tape was scanned for the criterion: hole or no hole. The result was converted into electrical impulses. Initially OKW/Chi used already available mechanical sensing levers of the punched tape transmitters from Siemens and Lorenz. But soon it became clear that this was too slow. As a result, photoelectric scanning units were developed (see fig. 1).

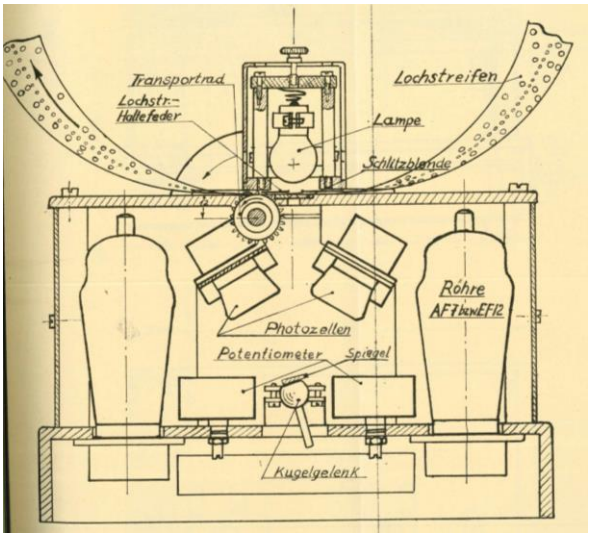

Fig. 1: Photoelectric reading apparatus (drawn by Jensen 1955, Annex 7)

After reading the punched tapes, "**Auswertewerke"** evaluated the information, i.e. the information from the punched tape went in and came out again as groups of letters or numbers. Telegraph relays and telephone relays were mainly used here as so-called cascade converters.

Logical operations, like e.g. XOR, were carried out for statistical calculation of the punched tape information. Jensen called these labyrinths (e.g. character comparison labyrinth, or superimposition labyrinth). These labyrinths were not permanently soldered but pluggable, to remain programmable. Extra calculation cascades performed addition, or subtraction modulo 10 automatically. Jensen described simple cascades versus cascades with a storage function.

Last, so-called "**Registrierwerke**" recorders were used to either display the output of the evaluation on counters or to transfer it to paper or punched tape, by the help of available tape punchers or via automatic typewriter, i.e. a modified Mercedes-Elektra typewriter equipped with electromagnets.

As counters, post office counters were used, but these proved to be impractical, as only five counts per second were possible. Furthermore, they could not be reset to 00000. For this reason, an overrun counter was developed on the basis of a voice coil, or plunger coil.

6 TICOM protocols report that in general, cryptanalytic machinery was first introduced in Germany with the adoption of Hollerith machines (I.B.M. machinery) by the army in 1941 (see EASI Vol 3 p. 72, & TICOM I-93, p. 5). According to these reports, OKW/Chi did not own any Hollerith machines, but – most probably - used the IBM equipment of the army's cryptanalytic agency (OKH/ln 7/VI), since they were housed in adjacent buildings in Berlin.

Jensen divided the auxiliary devices of OKW/Chi into five major categories according to their application:

- Recognition of secret messages
- Deciphering of recognized ciphers
- Decryption of solved ciphers
- Security scrutiny of own ciphers
- Production of secret keys

Analogue to this classification, the equipment will now be described, taking all information into account that could be found in Jensen (1955) and in the relevant TICOM literature.

Almost each of these following devices would be worth going into more detail with an own study. For reasons of space only a superficial description can be given here as a basis for further follow-up studies.

3.1 Recognition of secret messages

The simple counting apparatus (**"einfaches Zählgerät"**) determined the frequency distribution of up to 100 different elements. By means of a lever it was possible to switch between the five-digit telegraph alphabet and the 100-digit numbers from 0-99. It was composed of a mechanical scanning unit, a cascade converter with digit-bigram cascade and 100 post office counters to display the results. Due to the relatively low operating speed of the post counters, the device worked about five times faster than one would have needed by hand. (Jensen 1955, p. 35 & 77-81; TICOM I-37, p. 7)

The statistics' recording apparatus **("Auswahlzählgerät")**, improved the simple counting apparatus: It determined the frequency distribution of up to 1024 different elements position, as well as feature-related frequencies, vowel spacing, and word lengths. For this purpose, photoelectric scanning units, a bigram cascade of 68 relays and a recorder system consisting of 1036 tracking counters ("Nachlaufzähler"), which were particularly developed from plunger coils, were used.

In TICOM I-37 (p. 8) Dr. Hüttenhain mentioned it as a device that was planned or under construction, to be ready in four months. This statement does not correspond to Jensen's description. According to him, the device performed the work of 14 working hours in two minutes (Jensen, 1955, p.35 & 82-86).

The **"Sawyer's Jack"** phase-search apparatus & **"Tower clock"** statistical depth increaser **("Perioden- und Phasensuchgerät, Sägebock & Turmuhr")** automatically calculated coincidences of single letters, bigrams, trigrams etc. (i.e. index of coincidence[7]) within one or two cipher texts. As well, the apparatus was able to statistically find out if cipher text passages had been encrypted with the same key, i.e. were in depth. This device was composed of two photoelectric scanning units, a character comparison labyrinth with a large storage bank of telegraph relays, and a special recorder system.

TICOM assumed that OKW/Chi wrote the statistics by hand, because the idea of using such a large and unnecessary bank of relays for this purpose seemed absurd to the interrogators (EASI Vol 2 p. 57). But in fact following Jensen's description, a huge storage bank of relays had been used here.

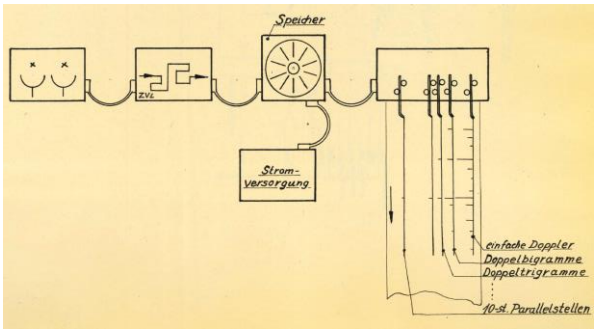

Fig 2. Sägebock & Turmuhr, drawn by Jensen 1955, Annex 43

Interestingly, TICOM documents treat this machine as two machines (see e.g. EASI Vol 2, chart no. 2-3), but Jensen describes it as one apparatus. Bauer (1997, p.303) cites this device from OKW/Chi as well, and repeats Jensen's statement that it was hundred times faster than manual statistic would have been. In addition, it delivered the results in a very concise way (Jensen, 1955, p. 36-37 & 87-92; TICOM I-31, p. 4; TICOM DF-187A, p. 23).

The repeat finder **("Parallelstellen-suchgerät")** was designed to scan text passages for repeats at ultra-high-speed, i.e. approximately

7 Kappa test, Friedman-test, introduced in 1920

10 000 comparisons per second. This should have limited large amounts of text to a few with a higher than average frequency of repeats, allowing them to be examined more intensively with the Sawyer's jack and Tower clock device. It was also intended to test whether scanning at such high speed would still produce accurate results. To be fast, the cipher text passages being compared were not punched on punched tape, but on normal film. For this purpose, a special 2-out-of-10 alphabet was used. Along with photoelectric scanners, the apparatus consisted of a device which, when a repeat passage occurred, produced a spark that burned a hole in an aluminum foil covered with thin paper.

However, Jensen reports that the apparatus had to be destroyed shortly before completion. It seems to have been of particular interest to Jensen, as he uses many pages to describe this device. This device is regretfully mentioned in the TICOM documents that it was unfortunate that there were hardly any technical details about it available (Jensen, 1955, p. 37 & 93-101; EASI Vol 2, p. 64-65; Bauer, 1997, p. 311).

3.2 Deciphering of recognized ciphers

The periodic substitution cipher tester ("**Spaltencäsaren-Textgerät**") decided whether a cipher text piece had been encrypted with a known periodic substitution or not. For this purpose, the frequency analyses per cipher text alphabet of the known periodic substitution cipher had to be calculated and stored in the device beforehand. It consisted of a two-headed scanning unit, a cascade converter with the stored frequencies per alphabet and an electromagnetically controlled recorder with rack and writing pen.

This device does not appear at all in the TICOM documents. It is not known to the author if and how successful is has been. Jensen states a working speed of 40 times faster that manual evaluation (Jensen, 1955, p. 38 & p. 102-103).

The bigram weight recorder ("**Bigramm-bewertungsgerät")** was a device for making frequency evaluations of digraphs. It consisted of two tape readers, a bank with five relays[8], a plugboard to weight the bigrams according to their usual frequencies in plain language, and a recording pen and drum. It most probably represents the only device of which contemporary photos exist (see fig. 3).

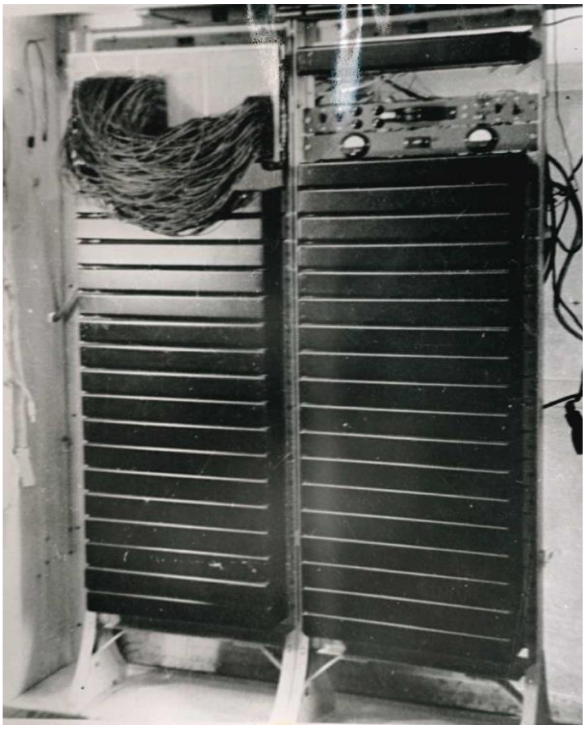

Fig.3: The cascade converter of the bigram weight recorder (Jensen, 1955, p. 106)

According to Dr. Hüttenhain (TICOM I-31, p. 4), it was used to solve the Japanese two-letter transposed code J-19, or Fuji. Solutions could be found in less than 2 hours, doing the work of 20 people (Jensen, 1955, p. 39 & 104-107; Bauer, 1997, p. 399).

The differencing device with storage ("**Differenzenrechengerät mit Speicher")** is used to automatically form all differences with modulo 10 from a group of cipher text passages that are (most probably) in depth. If two cipher text messages encrypted with the same key are subtracted from each other, the key is removed from both cipher text passages – according to Kahn (1996, p. 440) this was one of the most typical procedures of cryptanalysis during the Second World War. It delivered the base to solve super-enciphered code problems, i.e. after stripping off the key, known codes of suspected words could be added to decrypt the cipher text passages.

The device consisted of a two-headed scanning mechanism, a calculation cascade with storage and an automatic typewriter with digits. This meant that it was possible to work four

8 Dr. Hüttenhain speaks of 700 telegraph relays (see TICOM I-37, p. 6), and Fenner as well mentiones 26^2 relays according to the numbers of bigrams normally possible (TICOM DF-187A, p. 23).

times as fast as by hand, with the result being immediately available in an orderly and clear form, and could be run through without interruption even at night (Jensen, 1955, p. 39-40 & 108-110; Bauer, 1997, p. 339; EASI Vol 2, p. 60-61; TICOM DF-187A, p. 22).

If the text material to be examined was not extensive enough, the difference forming device ("**Differenzenbildungsgerät für Handbetrieb")** could be used for manual operation. It was also known as the roller apparatus. A maximum of 30 text passages in depth could be subtracted from each other, and codes of suspected words could be added experimentally. The device functioned purely mechanically with the help of five thin metal rods on which 30 small metal rollers were arranged. Each roller contained the numbers from 0 - 9, and according to Jensen, the device was made in two different versions, one for reading with a hanger to place the device comfortably in front of oneself on the table (see fig. 4), and one as a printing device with numbers in mirror writing. The rows of numbers could thus be painted with paint in every intermediate position. A rubber roller was used to make an imprint of the entire constellation of numbers on a sheet of paper laid over it, and a statistician was given the opportunity to examine it. In this way, 10 statisticians could work continuously with only one device.

The printing variant was already the subject of a study by Gallehawk et al (2017). In EASI Vol 2, p. 57ff, this device is described being equivalent to the National Cash Register differencing calculator from the American rapid analytic machinery.

Although the above mentioned eight different cipher departments worked more or less independently, there were nevertheless exchanges from time to time. All of the machines developed by OKW/Chi were shown to the three military Services and the Foreign Office; some were constructed for the other Services, particularly the Roller apparatus (see TICOM I-31, p.5). This could mean that considerably more pieces were made of this device than of others. (Jensen 1955, p. 40 & 111-112; TICOM I-37, p. 2-3; EASI Vol 2, p. 57-60; TICOM DF-187A, p. 21-22).

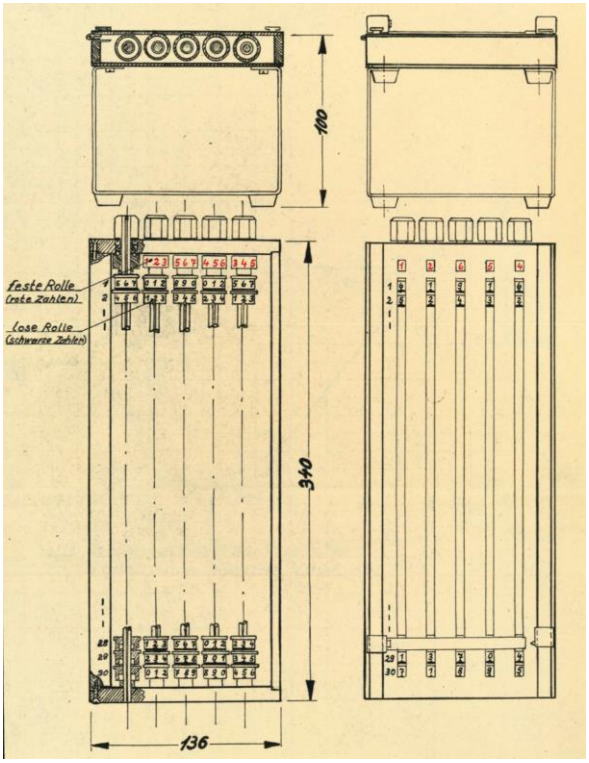

Fig. 4: Roller apparatus (drawn by Jensen, 1955, Annex 62)

If code groups in depth had already been cleared from the key by difference calculation, this manual device called likely-additive selector **("Reduktionsgerät, Witzkiste")** could help to check the code groups for the most frequently used codes. It was designed especially for the decipherment of four-digit-codes, and it worked with the superposition of probabilities in a photographically way on 4x4 lattices: Most frequent codes as well as the code groups to be examined were engraved as bright coordinates in two blackened glass plates. When the overlapping plates were illuminated, patterns were created on film material that represented the most probable reduction number. A sketch drawn by Jensen can be seen in fig. 5.

The name "Witzkiste" (i.e. brainbox; "Witz" can mean joke or brain in German) referred to its inventor Prof. Dr. Witt, who worked at OKW/Chi (Jensen, 1955, p. 40-41, 113-120, EASI Vol 2, p. 61-63; TICOM I-31, p. 21; TICOM I-37, p. 8; Weierud & Zabell, 2019, p. 4-5).

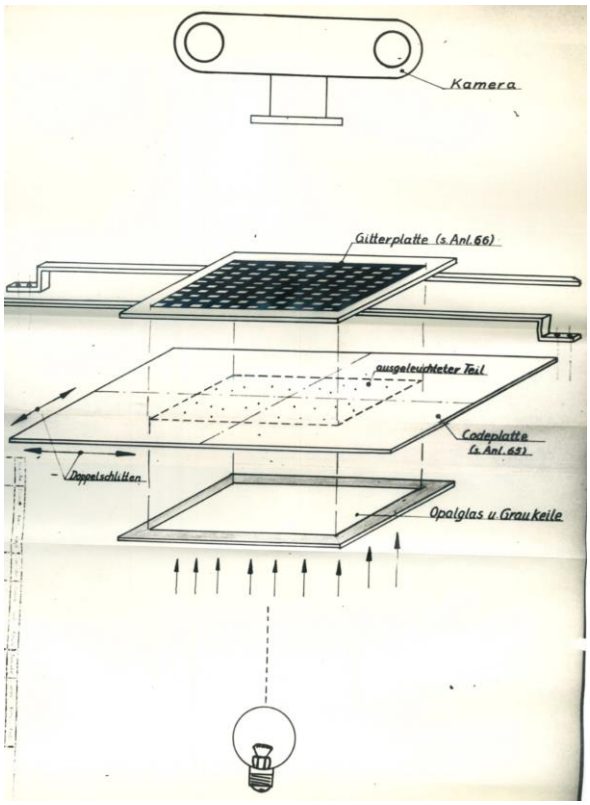

Fig. 5: “Witzkiste” (drawn by Jensen, 1955, Annex 67)

3.3 Decryption of solved ciphers

The differencing calculator (“**Differenzen-rechengerät ohne Speicher“**) was used to subtract an already recognized encryption number with modulo 10 from a secret code. It could also perform the steps of differentiating between ciphertext passages in depth, but was not as convenient. It was composed of a two-headed photoelectric scanning, a simple computing cascade and an automatic typewriter for digits. It could also be used for encryption (Jensen, 1955, p. 42 & 121-122, TICOM I-37, p. 4).

The converter (“**Tauschumsetzer”)** was used to quickly convert text passages encrypted with an already deciphered cipher text alphabet into plain text. For this purpose, an automatic typewriter was extended with an extra panel to plug in the exchange letters. It could also be operated fully automatically with punched tape (Jensen 1955, p. 42 & p. 123; TICOM DF-187A, p. 22).

3.4 Security Scrutiny of own ciphers

The mechanical grille columnar transposition device (“**Rasterwürfelgerät”)** was a tool to assess the security of the cipher "columnar transposition encoded with grille". Neither the columnar transposition nor the grille were considered secure. In combination a satisfactory level of security was assumed. The grille created gaps which could be fixed with this device. It was also ideally suited for solving simple columnar transpositions. The structure reminded of a system of co-ordinates made of metal, on which grid fields could be moved and labelled. It was not mentioned in any TICOM document (Jensen, 1955, p. 43 & p. 124).

The superimposing device **(“Überlagerungs-gerät”)** was used for the security check of cipher machines with regular rotation of the drums. Jensen did not say this explicitly, but he must have meant the Enigma variants. In order to check sub-periods in different phase positions, the impulse superposition was tested on two punched strips: two scanning units, or two Lorenz transmitters, an overlay labyrinth with 10 telegraph relays and a receiver tape-puncher. The speed of the device was slow because of the puncher. It is not mentioned in TICOM documents as a device (Jensen, 1955, p. 43 & p. 125-126).

3.5 Production of Secret Keys

In the lack of a true random generator, one-time-tapes were created using a Siemens T-52c secret writer: the key of the secret writer was over-encrypted with itself and printed on punched tape (Jensen, 1955, p. 44 & p. 127-130).

4 Lost & Found

The interesting question to be posed now is: What happened to the rapid analytical machinery? In Jensen's manuscript it can already be read in the introduction that all the devices were destroyed at the end of the war (Jensen, 1955, p. 2). Fenner (TICOM DF_187, p. 14) reports a mass destruction of just this machinery at the Salzach River near Werfen/ Austria.

It is possible that TICOM employees took devices with them to the USA or to UK. The author has therefore made a request to the depots of the NSA museum and the depot of the GHCQ. Unfortunately, the employees of these institutions have not yet been able to find any relics of these devices.

However, between 2005 and 2007 divers succeeded in recovering one type of device several times from a depth of 40m of fresh water: the Roller Apparatus. Unfortunately, the

community of divers and treasure hunters does not allow finding out more about the location of these artefacts. In the beginning there was talk about a lake in Austria and later on about Schliersee. The finding place Schliersee would at least fit to the fact that the whole OKW/Chi-archive including equipment was dumped into the lake[9]. But unfortunately there is no direct contact to the divers to ask for more details.

The devices found so far were resold by a collector in East Germany. According to the author's knowledge, a handful of these devices should exist. Three artifacts are directly known. One of them is located in England and led to the already mentioned paper of Gallehawk et al. (2017).

On a second unit, owned by a private collector in Germany, at least the nameplate with the serial number "SW19" is clearly visible (fig. 6). So now we know that these machines were manufactured by the manufacturer F. Zimmermann & Co. in Berlin. Unfortunately, this company was dissolved in 2004 for financial reasons after 86 years of existence. Whether a company archive still exists, could not yet be found out.

Fig 6: Roller Apparatus, freshly recovered from a lake; by courtesy of Klaus Kopacz, 2019

The third device is owned by the Museumsstiftung Post und Telekommunikation MSTP depot of the Communication Museum in Frankfurt Heusenstamm (fig. 7).

Unfortunately, so far nothing more is known about remaining OKW/Chi auxiliary devices. The author would be very grateful for hints and further knowledge.

9 The TICOM Team 5 mentioned, that in August 1945 the northern shore of the Schliersee was still littered with radios and teleprinters (see TICOM Team 5, p. 5)

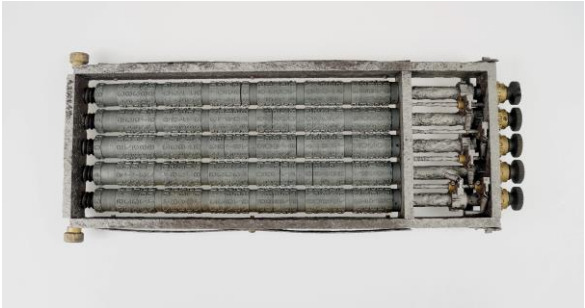
Fig 7: Roller Apparatus, recovered from a lake and cleaned, by courtesy of the MSPT Heusenstamm, Inv. No. 4.2008.450

Acknowledgments

The author would like to thank Frank Gnegel and the Depot Heusenstamm, Frankfurt as well as Klaus Kopacz for their friendly support and the provision of photos. Furthermore, many thanks go to Katja Rasch, Tina Kubot and Dermot Turing as well as to three anonymous reviewers for their valuable comments.

References

John Alexander, John Gallehawk, John Jackson, Allen Pearce & Edward Simpson. 2017. *A German machine for differencing and testing additives*. Cryptologia, 41:3, 269-280, DOI: 10.1080/01611194.2017.1289718

Friedrich L. Bauer. 1997. *Decrypted Secrets. Methods and Maxims of Cryptology*. Springer-Verlag Berlin Heidelberg

Friedrich L. Bauer. 2009. *Historische Notizen zur Informatik*. Springer-Verlag Berlin Heidelberg

EASI European Axis Signal Intelligence Volume 2: *Notes on German High Level Cryptography and Cryptanalysis*. 1945. TICOM DOCID: 3560816. source: https://archive.org/stream/ticom/

EASI European Axis Signal Intelligence Volume 3: *The Signal Intelligence Agency of the Supreme Command, Armed Forces*. TICOM DOCID: 3560827. Source: https://archive.org/stream/ticom/

Erich Hüttenhain. 1970. *Einzeldarstellungen aus dem Gebiet der Kryptologie.* Manuscripts collection, Bayerische Staatsbibliothek, Signature Cgm 9304a, München

Willi Jensen. 1955. *Hilfsgeräte der Kryptographie, Hauptband + Anlagenband*. Universitäts-bibliothek TUM, Signatures 0109/I 305+306, Garching

David Kahn. 1996. *The Codebreakers*. Scribner, New York

David Mowry. 1989. *German Clandestine Activities in South America in World War II*. TICOM DOCID: 3525901. Source: https://archive.org/stream/ticom/

Randy Rezabek. 2013. *TICOM and the Search for OKW/Chi*. Cryptologia, 37:2, 139-153, DOI: 10.1080/01611194.2012.687430

Frode Weierud & Sandy Zabell. 2019. *German mathematicians and cryptology in WWII*. Cryptologia, DOI: 10.1080/01611194.2019.1600076

TICOM DF-187, 1949. *The Career of Wilhelm Fenner with special regard to his activity in the field of cryptography and cryptanalysis*. Source: https://archive.org/stream/ticom/

TICOM DF-187A, 1949. *Organization of the cryptologic agency of the armed forces high command, with names, activities, and number of emplyes together with a descriptoipn of the devices used*. Source: https://archive.org/stream/ticom/

TICOM I-31. 1945. *Detailed Interrogations of Dr. Huettenhain, Formerly Head of Research Section of OKW/Chi*. DOCID: 6587332. Source: http://chris-intel-corner.blogspot.com/2017/

TICOM I-37. 1945. *Translation of Paper Written by Reg. Rat. Dr. Huettenhain of OKW/Chi on Special Apparatus Used as Aids to Cryptanalysis*. Source: https://archive.org/stream/ticom/

TICOM I-176. 1945. *Homework by 'Wachtmeister Dr. Otto Buggisch of OKH/Chi and OKW/Chi.* Source: https://archive.org/stream/ticom/

TICOM IF-1517. 1944. *First Detailed Interrogation of Bigi, Augusto*. TICOM REF ID: A65381. Source: https://archive.org/stream/ticom/

TICOM IF-167. 1945. *Final Report of the Visit of TICOM Team 5 to the Schliersee Area 3rd August 1945 to 7th October 1945*. DOCID: 3745507. Source: https://archive.org/stream/ticom/

TICOM I-206. 1947. *Extracts from Homework written by Min. Rat Wilhelm Fenner of OKW/Chi*. Source: https://archive.org/stream/ticom/