What We Know About Cipher Device "Schlüsselgerät SG-41" so Far

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

Abstract

Almost everyone knows the Enigma. But the cipher device "Schlüsselgerät 41"? Never heard of it. This German cipher machine is much rarer than its famous predecessor. Only around 1500 units were manufactured towards the end of the Second World War. And information is even scarcer. Up to now, the Deutsches Museum has only been able to collect broken devices. Recent contacts to collectors reveal that functional Schlüsselgeräte 41 still exist. They could help to solve the secret of the encryption algorithm. This contribution aims to present our current state of research.

1 Menzer's Machines at OKW/ Chi

In 1941, the cryptologist Fritz Menzer (1908-2005) from the OKW/Chi (Signal Intelligence Agency of the Supreme Command of the Wehrmacht) designed a mechanical cipher device that for certain would have complicated all decipherment efforts of Bletchley Park (Mowry, 1983-1984).

Menzer was chief of the communications security for the Wehrmacht, and his staff had criticized for a long time that the German coding devices (including ENIGMA and LORENZ SZ-42) had not been mathematically checked for security. In fact, this was only carried out from 1942 onwards (Hüttenhain, 1970). Consequently, Menzer insisted - against the ignorance of the troops and their command – upon the construction of an enhanced cipher device. First, he started to develop "Schlüsselgerät 39" – an enhanced version of ENIGMA, but as we know so far, only three models existed (Mowry, 2014). In 1941, Menzer invented a second cipher machine called "Schlüsselgerät SG-41".

But despite the highly sophisticated encryption of SG 41, in fact far above the security level of ENIGMA, its development was neglected and even blocked by the army (WDGAS-14).

When it finally came to a decision to build and spread the machine, wartime shortages of aluminium and magnesium caused the machine weight up to 15 kilograms – too heavy for field use. Although already about 11.000 machines were ordered (see Sächsisches Staatsarchiv Chemnitz), only few – an unknown quantity - were really fabricated at the Wanderer Werke AG, Siegmar-Schönau (today a part of Chemnitz) and used. TICOM documents speak about 1000 pieces (Mowry, 2014).

2 About Schlüsselgerät SG-41

Menzer wanted to design a pure mechanical, lightweight, durable and practical machine. So he invented several interesting features to make the device robust and practical for military use, e.g. he developed an improved, reversible insert for the ink pad and a mechanism to quickly remove the daily key settings (Kopacz, in prep).

And Menzer was a cryptoanalyst as well who had already developed two decipherment methods to break C-36. Subsequently, his knowledge about Hagelin devices was strong. He designed SG-41 with a printer and a keyboard, and with a crank handle like Hagelin's BC-38. Cipher text and plain text would be printed on two stripes of paper.

The algorithm was based on the Hagelin C devices with a characteristic Hagelin pin-and-lug-principle, but showed an enhanced encryption because of two characteristics (WDGAS-14; Kopacz, in prep):

Proceedings of the 1st Conference on Historical Cryptology, pages 109– 111,
Uppsala, Sweden, 18-20 June, 2018

1) The wheel stepping was not only interacting but irregular – controlled by the pin positions of the wheels.

2) Five of the six wheels formed the pseudo-random key for each letter encryption. The sixth wheel, however, could accept or negate the settings of the other five wheels.

Although there are basic explanations of the working principle of the machine (e.g. WDGAS-14), it was hitherto not possible to understand the exact mode of operation of the machine and to be able to simulate it. No construction drawings were found, and interrogation papers from Menzer himself and from colleagues have not been released so far (e.g. TICOM I-71, I-72, I-73 & DF-174). In addition, only few devices are known. Mostly, they were destroyed, dumped or burnt at the end of WW2. So after all, if a device is found nowadays, it is in most cases not in working order anymore.

2.1 Standard Model

Menzer's standard Schlüsselgerät 41 had a QWERTZ keyboard and was used from 1944 until the end of the war by the Abwehr (Secret Service) (Mowry, 1983-84). The letter J replaces the space-key (Kopacz, in prep) and is marked in red on the keyboard. According to Batey (2009), Bletchley managed to decipher few messages due to handling mistakes of the user, but they could not reconstruct the principle of the machine until they captured it after the end of WW2.

The Deutsches Museum owns a SG-41 that has lately been found in the forest grounds near Munich. It seems that someone had deposited it there at the end of WW2. Of course, after approximately 70 years in the ground, it is completely corroded – so it is not possible to gain helpful information from it regarding its encryption algorithm.

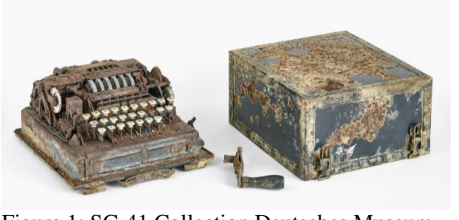

Figure 1: SG-41 Collection Deutsches Museum No. 2017-803, Photo: Konrad Rainer

Material analyses showed that the keys of the keyboard are made of nitrocellulose which is a problematic substance because it emits nitrous gases. As well, it decomposes when exposed to light and heat – facts that have to be considered when planning to store or to exhibit the object.

2.2 Special Model Z

A special model Z with ten figure traffic was constructed to be used for encrypting weather reports. Originally, 2.000 – 7.000 pieces were ordered at Wanderer Werke AG at Siegmar-Schönau/ Chemnitz (see Sächsisches Staatsarchiv Chemnitz). But TICOM documents speak of very few (TICOM I-194) or about 1.000 (TICOM I-57) pieces that were truly fabricated and used by the Luftwaffe (Air Force) from 1944 until the end of the war.

Figure 2: SG-41Z Collection Deutsches Museum No. 2013-1092, Photo: Inga Ziegler

In 2013, the Deutsches Museum was able to purchase a SG-41Z that had been dumped in a lake near Berlin at the end of WW2. As it was restored before it was put up for sale, it looks as new, at least from the outside. Internally it is - like our other model - completely corroded.

3 Sources and Outlook

The Schlüsselgerät 41 and its inventor, Fritz Menzer, are largely unknown up to date. Some interesting details have already been provided by documents from the Target Intelligence Committee, USA and UK (TICOM). Immediately after the end of the war, TICOM conducted surveys and investigations with prisoners of war and recorded these in the TICOM documents; since 2009 released by the NSA as so-called declassified documents).

But as long as the respective TICOM documents are not available it will only be possible to reconstruct the encryption algorithm by the help of a functional Schlüsselgerät. Fortunately, the engineer and specialist for cipher machines Klaus Kopacz from Stuttgart, Germany, was recently able to purchase and repair an original SG 41. A publication about the working principle and the complete technical details is planned by him in the near future.

As soon as the encryption details are published, it will be possible to simulate the algorithm and to evaluate the real impact of this device for the development of cipher machines after WW2. For example, the wheel-stepping mechanism, as well as the negation function of the sixth wheel, were implemented again in other pin-and-lug cipher devices after WW2, although mechanically solved in a different way (see H54 from Hell, and Version M of the CX52 from Crypto AG; Kopacz, in prep).

Other sources, especially German, British and U.S. American sources from archives, museums, and collectors, could provide more aspects and information. As well, we intend to perform a CT-scan to retrieve information about the internal parts of our machines. This is the focus for the next year.

Acknowledgments

First of all we would like to thank Dr. Marisa Pamplona and Christina Elsässer from the restoration research department of the Deutsches Museum for the material analysis and the helpful tips for designing the showcase, and Konrad Rainer and Inga Ziegler for the beautiful photos. We also thank Robert Jahn from Libellulafilm for his research in the Chemnitz Archive. Finally and most of all we thank Klaus Kopacz for his time and energy to explain the Schlüsselgerät 41 and to share his exciting insights with us.

References

David Mowry. 1983-1984. *Regierungs-Oberinspektor Fritz Menzer: Cryptographic Inventor Extraordinaire.* Cryptologic Quarterly Articles, 2 (3-4).

David Mowry. 2014. *German Cypher Machines of World War II*. NSA history program.

Erich Hüttenhain. 1970. *Einzeldarstellungen aus dem Gebiet der Kryptologie.* Bavarian State Library, Reading Room for Manuscripts and Rare Books. Munich.

Klaus Kopacz. In prep. *Schlüsselgerät 41*.

Mavis Batey. 2009. *Dilly, The Man Who Broke Enigmas*. ISBN 978-1-906447-01-4.

Sächsisches Staatsarchiv Chemnitz, 31030 Wanderer-Werke AG, Sigmar-Schönau, Signatures: 1975, 3156 and 1212.

TICOM I-194: *Report on German meteorological cipher systems and the German met. Intelligence service*. Released by NSA 2009. No DOCID.

TICOM I-57: *Enciphering devices worked on by Dr. Liebknecht at Wa Pruef 7*. Released by NSA 2009. DOCID: 3541302.

The cryptology of German Intelligence Services. Released by NSA 2009. DOCID: 2525898

TICOM I-194: *Report on German meteorological cipher systems and the German met. Intelligence service*. Released by NSA 2009. No DOCID.

WDGAS-14: *Volume 2 – Notes on German high level cryptography and cryptoanalysis*. Released by NSA 2009. DOCID: 3560816.