Homepage
Crypto
Index
Glossary
Enigma
Hagelin
Fialka
Rotor
Pin-wheel
Voice
Data
Hand
OTP
EMU
Mixers
Phones
Bulk
FILL
Codebooks
Algorithms
Countries
Manufacturers
Spy radio
Burst encoders
Intercept
Covert
Radio
PC
Telex
Telephones
People
Agencies
Manufacturers
DONATE

← Siemens Crypto Germany Rotor

T-52 Geheimschreiber

Teleprinter cipher machine (STURGEON)

The T-52 was an electro-mechanical cipher machine for teleprinter signals (telex) developed by Siemens & Halske around 1930. It was one of the main cipher machines of the German Army during WWII, being used alongside the Enigma, the Lorenz SZ-40 and later the T-43. After the war, the machine was used in a number of countries, including France and The Netherlands.

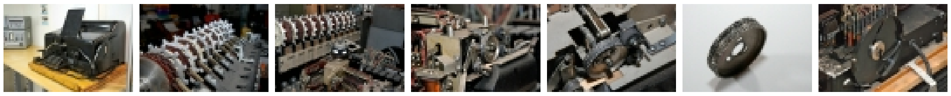
The machine is commonly called *G-Schreiber*, or *Geheimschreiber* (secret writer), but its official name was **SFM** or *Schlüsselfernschreibmaschine* (cipher teleprinter). T-52 traffic was known as *Sägefisch* (sawfish) by the Germans and was called **STURGEON** by the allied codebreakers at Bletchley Park (BP). It was occasionally broken.

The image on the right shows a *Geheimschreiber* as it was used by the Dutch Navy after WWII. The machine is extremely heavy and bulky (100 kg). The basic design consists of a large base plate with a Siemens T-36 teleprinter at the center.

Behind the teleprinter is the main cipher unit that consists of 10 notched cipher wheels. Breaking the T-52 was very difficult as the machine was mainly used via land lines and only occasionally over radio. Nevertheless, Swedish codebreakers, and later British codebreakers as well, managed to read part of the T-52 traffic, but only if the messages had been received in depth. [1]

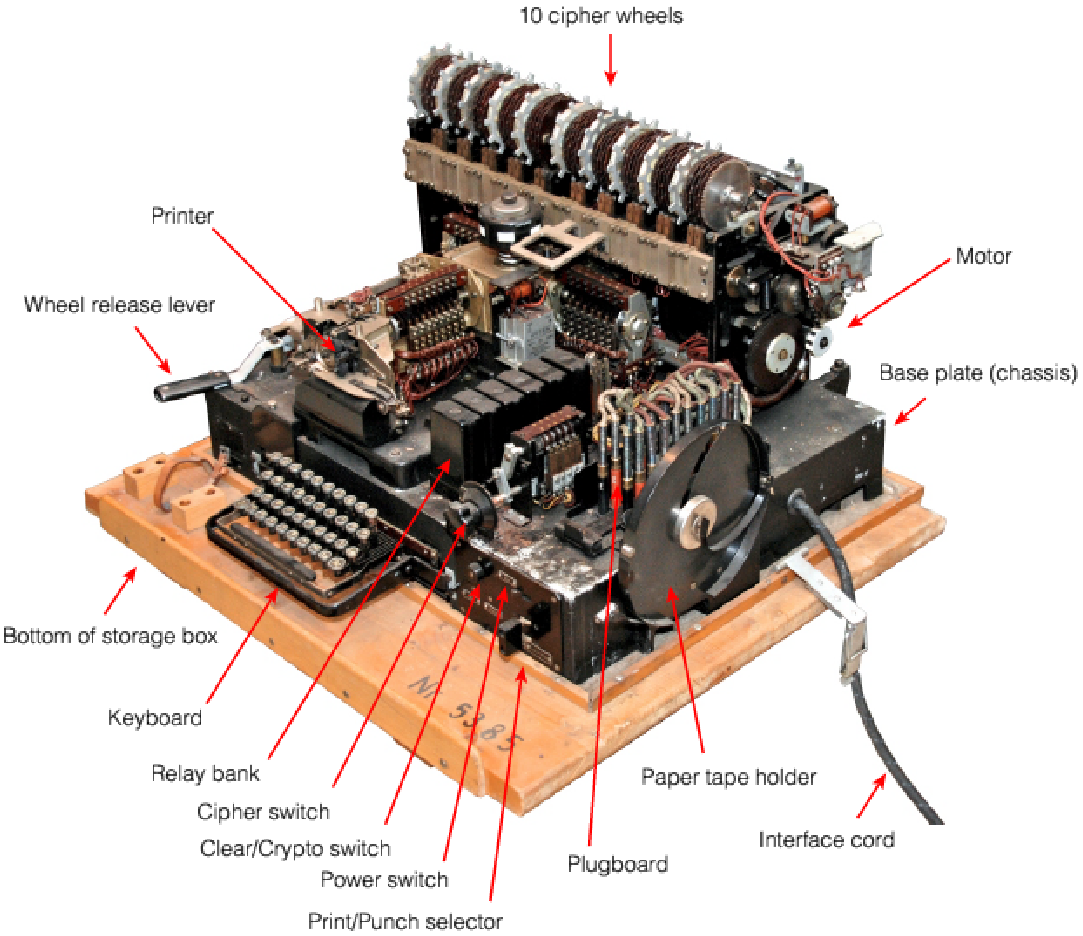
The T-52 was a so-called **online** machine, which means that it operated directly on the digital teleprinter signals. Messages, entered *in clear*, were immediately printed *in clear* at the other end. The operators never saw any enciphered text (unless they used the wrong key). As the initial version of the machine was not very secure, several attempts were made to improve its cipher security. Finally, the T-52d was so good that it was used by a number of countries after WWII.

[1] Two or more messages that have been encrypted with the same key.



Controls

Although there are many different versions of the Geheimschreiber, we'll use the T-52d to show the position of the various parts and controls, as it is the most sophisticated and secure version of the machine. In the image below, the T-52d is shown from the front right. At the heart of the machine is a Siemens T-36 teleprinter (Fernschreiber) with its keyboard sticking out at the front.



The 10 cipher wheels are clearly visible in the image above. The cipher mechanism is a complete unit that is mounted on the chassis to the rear of the teleprinter. Rather than printing onto sheets of paper, the T-52 produces its output on a paper-strip, which is fed from a holder at the right into the printer that is located just above the keyboard, leaving the machine on the left.

Introduction

During WWII, the German war machine heavily relied on cipher machines for secure communication, both over land lines and radio. Apart from a number of hand cipher methods, they mainly used three (later four) cipher machines for the bulk of their secure messages:

- Enigma
  The enigma machine was used at the lowest level of the command chain. Between 20,000 and 30,000 machines were built and used by several parts of the German Army and related organisations. Due to the sheer size of the German war theatre, the majority of enigma messages was sent over radio.

- T-52 Geheimschreiber
  The Geheimschreiber made it possible to encrypt a teleprinter line (telex). Although it was possible to use such links over radio, the majority of T-52 messages was sent over land lines. As a result, such messages were difficult to intercept. It was cryptographically more secure than the Lorenz SZ-40.

- Lorenz SZ-40/42
  Like the Geheimschreiber, the Lorenz Schlüssel Zusatz (SZ) was used for the protection of telex signals. It was a stand-alone wheel-based unit that was connected between the teleprinter and the line. The Germans used it at the highest level. The Lorenz machine was used over land lines as well as over radio. It was broken by Bletchley Park by means of the Colossus computer.

- Siemens T-43
  This was a one-time pad machine (OTP) that was introduced relatively late in the war. It was used only on a few networks. Bletchley Park probably called this machine **Trasher**. Machines like the T-43 are often called 'Mixers'.

Models

- T-52a
  This was the first version of the T-52. It was based on the T-36 teletype and was only built in small quantities from 1932-1934. It appeared to cause radio interference. It was later modified with a filter and was then called T-52a/b.

- T-52b
  The T-52b was a slighly improved version of the T-52a in wich a filter against radio interference was added. As the machine is otherwise identical to the T-52a, the two versions are generally identified as T-52a/b. The T-52b was built from 1934-1942.

- T-52c (Cäsar)
  The T-52c was developed in 1941. It had a simpler setting of the message key, but had the nasty side-effect that the number of possible alphabets was reduced dramatically. The T-52c had a switch to make it backwards compatible with the T-52a/b. The T-52c had the same cipher period as the T-52a/b and is sometimes called: the *Cäsarmaschine*.

- T-52ca
  This was an improved version of the T-52c in which the number of alphabets was increased again by fixing a flaw.

- T-52d (Dora)
  This is a serious improvement of the earlier T-52a/b. It features irregular wheel stepping of the cipher wheels and a so-called *Klartextfunction* (KTF). The T-52d was developed in 1942/43.

- T-52e (Emil)
  The same improvements that converted the T-52a/b into the T-52d, were also applied to the T-52c. This resulted in the T-52e.

- T-52f
  This version of the T-52 was developed but never taken into production. In May 1945 the design was ready but by then the war had ended [4].

Due to the nature of the various models and the later modifications, the T-52 can be divided into four distinct functional groups:

1. T-52a, T52b (T-52a/b)
2. T-52c, T52ca
3. T-52d
4. T-52e

How it works

The operation of the T-52 is not easily explained. It is a very complex machine and there are significant differences between the various models. The basic principles are best explained by first looking at the initial design and then introducing the improvements.

T-52a/b

The T-52a was the first of the Siemens T-52 machines to see the light of day. It had limited cipher security, mainly because it exhibited regular stepping of the cipher wheels.

T-52c

The T-52c was an attempt to improve security of the rather insecure T-52a/b. A large box with 5 levers, used for setting the message key, was added to the left of the keyboard. However, the wheel combining logic, that was meant to improve security, did exactly the opposite: it weakened the cryptographic strength of the machine, as it reduced the total number of alphabets.

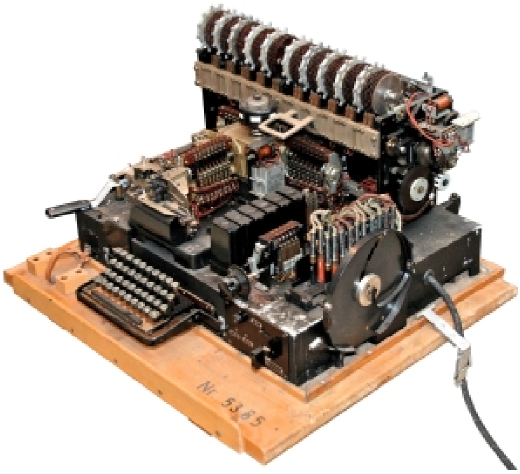
The image on the right shows the extremely rare T-52c variant. The 5-lever unit for setting the message key is clearly visible at the front left. Also note the compatibility switch at the front right. It allows the machine to be used in combination with the older T-52a/b models.

According to the serial number plate, it is a 50 baud version that was built in 1944. This is rather strange as at this time most machines had been replaced by the improved **d** and **e** models.

T-52d

The T-52d was a well-designed machine. It was in fact a T-52a/b with much improved cipher security. Its cryptographic strength was considerably better than the Lorenz SZ-40. Consequently, it was never broken by Swedish cryptanalists. It was however broken by Bletchley Park, but only if they had messages *in depth*. If the T-52d had been used from the beginning, **and** its operators had been better instructed, it seems unlikely that the machine would ever have been broken.

The image on the right shows the interior of a T-52d machine, after the black protective cover has been removed. At the right hand side of the machine, just behind the paper tape holder, the plugboard is clearly visible. This plugboard was normally protected by a lockable hood.



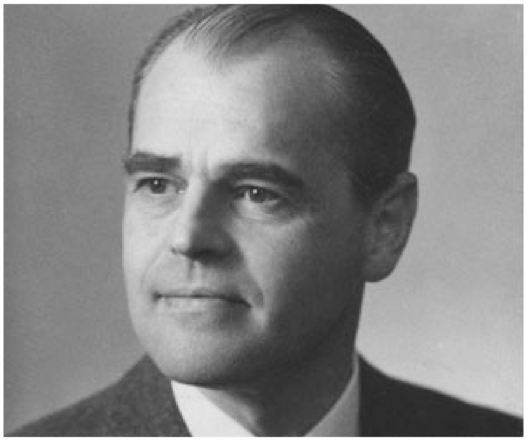
Breaking the T-52

Although the T-52 provided extremely good security for its days, it was nevertheless broken during WWII. The first to break Siemens T-52a/b traffic, was a group of Swedish cryptanalists led by Professor Arne Beurling in June 1940. The Swedish were lucky in that, after the occupation of Norway and Denmark, the Germans started using land lines for their communication.

The lines ran through Sweden and as early as May 1940, the Swedes tapped these lines and intercepted all T-52 traffic to and from Oslo. The machine was broken with hand methods, based on a set of messages *in depth*, that were intercepted on 25 and 27 May 1940 [2].

Once the messages were broken and the key was known, the bulk of information was deciphered on a T-52 emulator built by Vigo Waldemar Lindstein of the Ericsson company. After the war, Lindstein worked for Hagelin for several years as head of the Engineering division, until he started Transvertex. He developed the HC-9 cipher machine and was CEO of

Transvertex until the company was taken over by Ericsson in 1969.



In 1943, the Germans discovered the weaknesses of the T-52a/b and c, and were informed that their ciphers were being read by the Swedes. They then introduced the T-52d, which featured irregular stepping of the cipher wheels. It appeared to be too much for Beurling and his team.

Bletchley Park

The British cryptanalists at Bletchley Park (BP) were less fortunate than their Swedish collegues, mainly because the T-52 was primarily used over land lines, to which the British, unlike the Swedes, had no access. Over time however, the T-52 also occasionally appeared on radio links.

The first break by BP came in mid-1942. In the summer of 1942, the Germans started using the T-52 on the radio link between Sicily (Italy) and Libya, and later between Aegean and Sicily. As the operators were sending multiple messages *in depth* (i.e. with the same initial settings) BP cryptanalyst Michael Crum [1] managed to achieve a break and reconstruct the machine [4].

BP called all German teleprinter traffic **'FISH'**. Whilst the Lorenz SZ-40 traffic was codenamed **'TUNNY'**, the intercepted messages from the T-52 Geheimschreiber were called **'STURGEON'**.

Over time, all T-52 models encountered by BP, were eventually broken, including the much improved T-52d, but only if they had received messages *in depth*. In practice, BP found that most messages that were sent over T-52 links, were also sent via Enigma or Lorenz SZ-40. As they were better equipped to break these two, the value of broken T-52 messages was limited.

[1] After the war, Michael Crum worked for GCHQ and was involved in the development of the SAVILLE cryptographic algorithm. SAVILLE became known as an NSA Type 1 algorithm.

Post-war use

The story of the T-52 does not finish at the end of WWII. Instead a large number of machines found their way into the armies and security services of a number of countries. The machine is known to have been used by the French Foreign Office and by the Dutch Navy. The East-Germans intended to use the machine, but it is uncertain whether they actually did. Even the British Navy considered using the machine, but turned it down for unknown reasons after a series of tests [4].

REICHERT

France

The French were by far the largest post-war user of the T-52. Approximately 380 machines survived the war, of which 280 were left behind in Germany. Although these machines had to be destroyed, they were 'just' dismantled and the various parts ended up on the surplus market around 1948. Electro-mechanical firm Willy Reichert in Trier (Germany) bought large amounts of the surplus stock and re-assembled a substantial quantity of T-52d and T-52e machines. More than 235 re-assembled machines were subsequently sold to the French Foreign Office between 1949 and 1953. Some of these machines appeared on the surplus market years later.

Netherlands

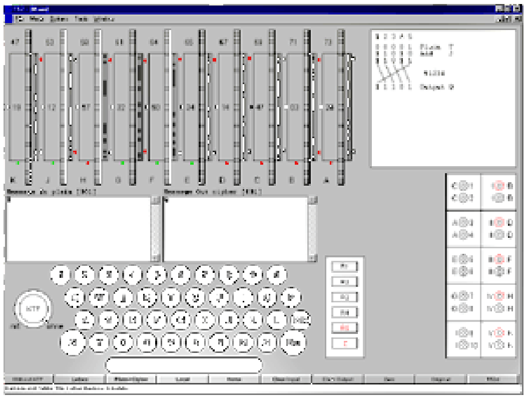
The Dutch Navy started using the T-52d during the 1950s. It is currently unknown how long and for what purpose they were used, but it is most likely that they were used on teleprinter lines between The Netherlands and the Dutch East-Indies (Indonesia). It is also unclear at present who supplied the machines to the Dutch. It is entirely possible that they too were supplied by Reichert, but they may also belong to the 100 machines that were not left behind in Germany after WWII.

T-52 Simulator

A good simulation of a T-52d has been produced by the Crypto Simulation Group (CSG). The simulator runs under Windows and is available from Frode Weierud's website.

On 23 March 2000, the CSG even managed to interface the simulator to a real T-52d machine, after which the compatibility of the simulator was confirmed. For this they used the RS-232 port of the PC and a simple relay-based telex interface. The simulator is suitable for Windows.

➤ Download T-52d Simulator (off-site)



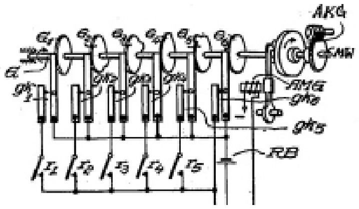
Names

The following names were used to identify the T-52 and/or its traffic:

- T-52
- G-Schreiber
- Geheimschreiber
- SFM
- Schlüsselfernschreibmaschine
- Sägefisch
- Sturgeon

Patents

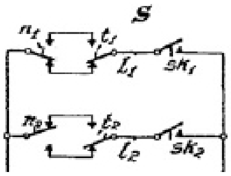
- **DE615016** - 18 July 1930
  First patent related to the T-52, filed by Siemens und Halske in Berlin-Siemensstadt. It lists August Jipp and Ehrhard Roßberg as the inventors. It was filed on 18 July 1930 and published on 29 May 1935.



- **US1912983** - 16 June 1931
  The same patent was also filed in the US, where the device was called 'Scret Telegraph System'. The patent was filed on 16 June 1931 and was published on 6 June 1933. It lists August Jipp, Ehrhard Roßberg and Eberhard Hettler as the inventors.

- **DE591974** - 11 October 1930
  This patent is similar to DE615015. It was filed later but has a lower file number. The patent was approved 2 years before DE615015.

- **DE666436** - 13 September 1930
  The is the patent for the additional security added to the T-52d, the so-called KTF (*Klartextfunction,* Clear Text Function). It was filed on 13 September 1930 and was published on 29 September 1938. Eberhard Roßberg is listed as the inventor.



References

1. Foundation for German Communication and Related Technologies
   T-52d featured on this page courtesy Arthur Bauer.

2. Bengt Beckman, *Codebreakers,*
   Arne Beurling and the Swedish Crypto Program During WWII.
   2002, ISBN 0-8218-2889-4.
   Original Swedish Title: Svenska Kryptobedrifter. 1996, ISBN 91-0-056229-7.

3. CG McKay and Bengt Beckman, *Swedish signal intelligence 1900-1945*
   2003. ISBN 0-7146-5211-5 (hard cover).

4. Frode Weierud, *BP's Sturegeon, The FISH That Laid No Eggs*
   The Rutherford Journal, Volume 1, 2005-2006. PDF version, p. 29.

5. Wolfgang Mache, *Der Siemens-Geheimschreiber,*
   Ein Beitrag zur Geschichte der Telekommunikation,
   1992: 60 Jahre Schlüsselfernschreibmaschine (German).
   Archiv für deutsche Postgeschichte Heft 2, 1992, pp. 85-94.

6. Günter Hütter, *T-52d interior*
   Interior of T-52d shown on this page, courtesy Günter Hütter, Austria.

Further information

- T-52 on Jerry Proc's crypto pages
- T-52 on Wikipedia
- T-52 technical backgrounds, by John Savard
- Other Siemens cipher machines
- Other German cipher machines
- Other cipher machines

Any links shown in red are currently unavailable. If you like the information on this website, why not make a donation?
© Crypto Museum. Created: Wednesday 05 August 2009. Last changed: Thursday, 19 April 2018 - 12:28 CET.