MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

The Heavy T52 Sturgeon Challenge – Part 1

Author: Nils Kopal

September 2019

Siemens and Halske T52D – Sturgeon

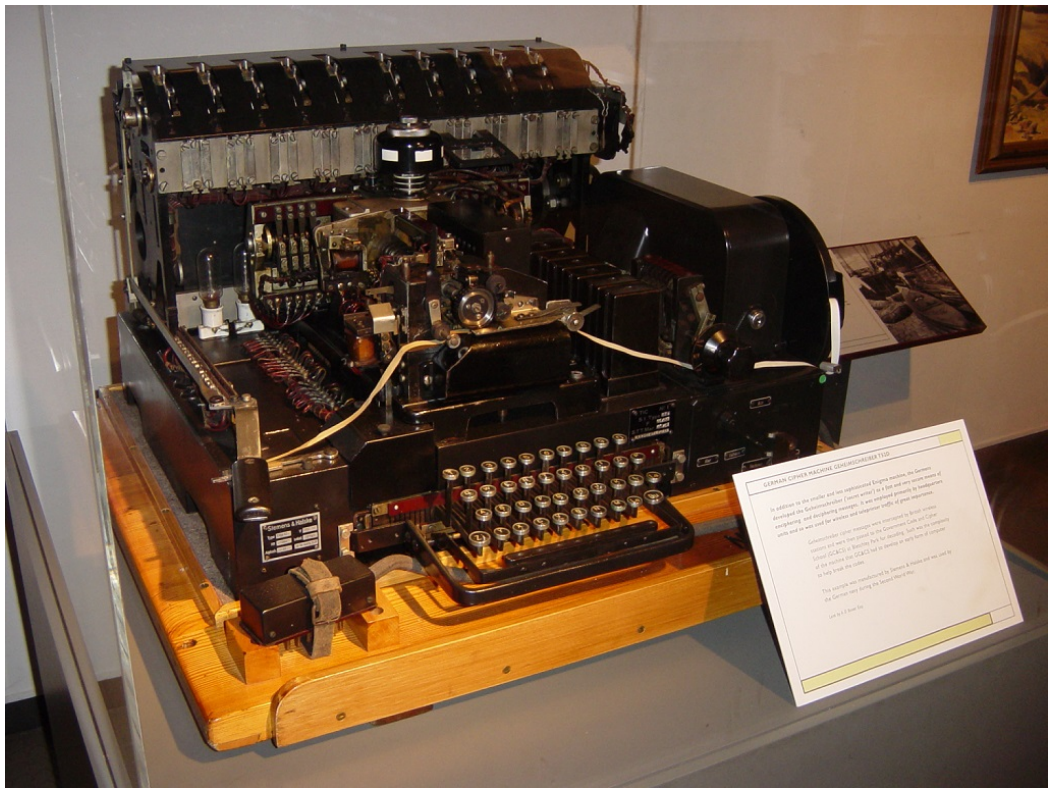

Figure: A Siemens and Halske T52D cipher machine on display at the Imperial War Museum, London.
Source: https://commons.wikimedia.org/wiki/File:T52-iwm.jpg

Introduction (1/2)

The T52, also known as the Geheimschreiber (secret writer), Schlüsselfernschreibmaschine (key teleprinter), or Sturgeon (by British cryptanalysts), was a World War II German cipher machine and teleprinter produced by the electrical engineering firm Siemens & Halske.

While Enigma was used in the field, the T52 was an online machine, heavier, and difficult to transport. But it was also considered to be more secure than Enigma. Therefore, it was mainly used by Luftwaffe (air force) and the German navy for strategic communications.

Introduction (2/2)

More details about the history of the T52 can be found in http://www.rutherfordjournal.org/article010106.html.

An overview of the machine can be found at https://en.wikipedia.org/wiki/Siemens_and_Halske_T52.

A detailed functional description of the T52 models is given in the additional zip file, as well as a simulator, and tips for cryptanalysis.

This challenge is part of a series of heavy T52 challenges that are based on George Lasry's previous twelve T52 challenges in MTC3.

Challenge (1/7)

In this challenge, you need to recover the plaintext from 10 ciphertexts in depth. The 10 messages were encrypted using the same key.

The key is unknown.

Machine model: T52D

All English plaintexts are extracted from random books from the Gutenberg library, formatted using Baudot teleprinter format.

Challenge (2/7)

The ciphertexts given use British (Bletchley Park) Baudot notation. See the file README.txt in the additional material for more details about the Baudot alphabet and the British notation.

The answer to the challenge is a 6-digit code which appears near the end of the plaintext, encoded using the Baudot alphabet in Figure Mode. For example, if the answer to the challenge is the code 207553, it will appear as +++WPUTTE888 in British notation. The symbol + (repeated 3 times) is used to move to Figure Mode, and 8 (also repeated 3 times) is used to return to Letter Mode. You should enter only the 6 digits.

Challenge (3/7)

Ciphertext #1:

```
FMFPGBYGQVTFR4BORV9BTK8BO4X+HKWVRVFOBJLQ4XSKDKAKVDEZHMWU
XEYTONOSZ+/9ZNTZPDVJINW+K/89UU3HMPUKVK4JTCX4XRV3OKVECZPT
9QAUA9MUHEN3WKLBTOH
```

Ciphertext #2:

```
ABWHFVJL3A/FR4BTCEOKVR3VSX8CN4LDSLO3EXWFXUVD+PDM8EZGNMWX
JQYHOXW4AAW84PH3D3A+9HGYCVNRCHTYFXJXUYNBY/ZJLXEFGC4UX/EC
E+CPI4X9JMR38VLIJACFIQAH
```

Ciphertext #3:

```
MFUHFVJ4GUT9GSGCOJ/KAN8F44DTREN3UKTFDYGP4ESNKDTYIBZTNVRT
3PUDBYQSZ+/8I+34HI9/LQYDS4YPMU48PE8+F8FI+PE4XRVZ43AWE/9G
F4TGKD+SLFRL/EWYFQRYSY//B/W3DFBFWVWM8DBU/4IHHH/MYB
```

Challenge (4/7)

Ciphertext #4:

3C8YCDU+EFCL4SG4P9JOUFP93UTK4X8VX4OCV93HYRAZVXEI9LF/ZR+F
GCUHACEHBJZRRAARQC4GJQQXXWGQ8JCB3TIY489CFCIXV4RTGNSUVQAI
NFABRQ+/O9OPOPYCDFYGD+GVSF+H3PPHTQ9YBVS4PJZJ3LVZMH

Ciphertext #5:

8TSJ3OCM8T/TEBI9RINW+KG+L++UIENQV43G93PEKYQ3JIFYSV3VZR+W
4S9+CANKUFFCBSFMVD+LJL4MMQY9ZAAJJZJWMIT9NVHQLOTKV3ZHVQAI
NFMORFF38EMSUX/Z+ORQYB4ETU+/MHM9YVW

Ciphertext #6:

ABTROZ3OXXVTEBSUC9EOUCYHF+9HPPNWM+DVV33HTM884BGNMN+399SZ
GJUXWVCUUSFFMWQUECN+9+RALG9VDV9AJ+JFM9+XZKZHQXYS+C8AB4EY
AFMOU/W/OOO4OIY38K4PMMKBINSOYEPQWVLBPHPZ+HDRMXYDXCALS

Challenge (5/7)

Ciphertext #7:

```
IKKFK4H+AKDJQIZHU8V9ZRBKG+9HPPNOE/BID9WJ8SSKHB/K9VDV+D4T
OC+ZZV/FV3SPJ8NRZD9TMGIVXDGHDN4+P3QVH8RJBE9/89Q/USSL/UCG
D4BMR8TIHMSVHKJ/4TGTIHKGZD+FK8PXHBAWRPEHAKEQ
```

Ciphertext #8:

```
IE9GAC+EV4+EIPITB+99TUNQW++U3GVE9QVH/3P+3IPTDL9XEFPT98SZ
RJ39ZVBUUFFCBPTJ+IMJXN3GSIE8RHKYEBJZUWLB4/ZUV8LBUCAMIVVC
FWMLJRC/9KLVAR3OSCYVDRBMV/D3W9K4JLZZOK8REDMP
```

Ciphertext #9:

```
NFUJXDIIVXL3M+BGAK+JSGNM4Q/QWC3IQXNYUMD/APLKOC4CIBUSBEAR
E8RE8URS8XPVOGTUHJ9LMYWCEHQ/CI98J+HJZVVIYCJXOZVWHO4A4URZ
VSGYRJYXJ+XJAOKGH+HUVR+LEH9ELT4JL
```

Challenge (6/7)

Ciphertext #10:

```
+A+/CXYGYKVGEBIFBT99TCGACGBAWSIVM8LAEDPJ8J+TPLFWI8D/9ISH
BCYN/CJRAXWCRLARD3JS+GFNHVMRF8XHXMIPWSKULEW/84YH/WIX4/EZ
A8WTYNH/OFDSUGJZRORZYSDEVUO
```

Challenge (7/7)

The attached zip file includes:

1. A simulator in Java, used to create the challenges. For usage, see README.txt.
2. A functional description of the T52 models, including the description of the Baudot alphabet and its notations.
3. Ideas for possible attacks.