MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

The Heavy T52 Sturgeon Challenge – Part 4

Author: Nils Kopal

April 2020

Siemens and Halske T52D – Sturgeon

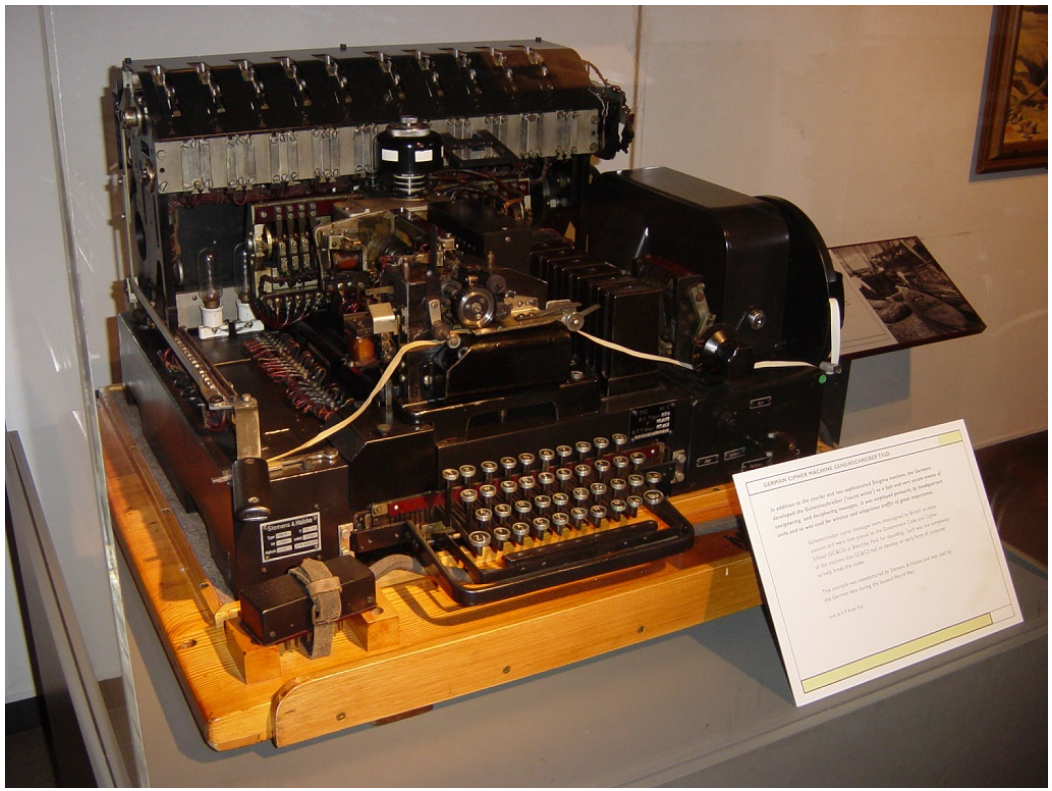

Figure: A Siemens and Halske T52D cipher machine on display at the Imperial War Museum, London.
Source: https://commons.wikimedia.org/wiki/File:T52-iwm.jpg

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 (1/5)

In this challenge, you need to recover the plaintext from ciphertexts in depth, i.e. the 6 given messages were encrypted using the same key. You are also provided with cribs for each message.

The key is partially known.

- Machine model: T52E
- Wheel settings: 9:5:V:7:II:IV:3:I:III:1
- Klartext (KTF): Off

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

Challenge (2/5)

The ciphertexts and cribs are given using 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 (3/5)

Ciphertext #1:
`ZFIMOC9CINROJAPCGNTSCLPYRUAAXQ93APUFJT/+PYKSAZDADQVUWP`
`VFH8/O3ANYUACKG8HCNQ8EQS4TGZ+NPJ/SSTDR9G4B/LPH3LJ9D9C9`
`DWO8ZJRCXRNKWG+FSAYVVYH/VJRI+4BEAOAT84VLX3CPMVYC9`
Plaintext #1 starts with: `RE9HEARS+S89AL+`

Ciphertext #2:
`JQ9VANUC9MGP4IBDFX9M+B/JPOW3BGDF3N/QLRGPCWQ3M9GOTWS/CN`
`E3X/ZKIELNTHY4SFP8VMFLXOGBRW+FDIG8POY49BPENNEWYIBRYLEQ`
`9WOGV4CR`
Plaintext #2 starts with: `PRI9ME+S89VAL+N`

Challenge (4/5)

Ciphertext #3:
`WH3CO8MJBNOPG8AV3PIPATXVK3NJFC3WPSAO4SGPCB+QPMFG8/S3NXW`
`CUJ/SFEP+UGAU+RIGFDW4RSDR9AQRBZMAHBDJUG+DYXAAG8F8YLQCWW`
`3TPNZYHR+RR8VB+CQJKKTMXNYL/NUWBOF`
Plaintext #3 starts with: `CORNELIA9SCARCE`

Ciphertext #4:
`+ZIMHDDJZAEKN+DQ8WYRG4RZF8TXEESFVWWFYOU494UEA9A3DQVUMGO`
`LB9USEG+ERKNX9HYX4TJ4MWDVDPRPKWMUILDX8/W/AKYZK9FSWJU`
Plaintext #4 starts with: `IN9HU9MAN+S89I9`

Challenge (5/5)

Ciphertext #5:
FOAVJALJZM8Y8IBD9VSOW/PZ+MMPXLKQYKVCVXHU/+4QA4KOUNK4BS
PAIJ/P3GQZNQUVHRQ8IBJVXBGBRWAFNPMAUMDCRVHGRUYAKCIFRC4+
Q9YI+RKNK4TDQIZDU3HELJXT+9YVO4BOVM
Plaintext #5 starts with: THE9OCEAN9OLD+N

Ciphertext #6:
KK3NJ9MKOABKN+PKGRZZOMNORZBS4+WB3/+AZXL/ZWHKKNXH3PHRTS
PAIEHGEIMDKV3MGBXPQAKXLRFZBJWZDZBMNJCPUUTS/NG/M/KLJXVI
/UKD+38WTKQAJLLIRFSCUWC8ZLY/WPZPWWR
Plaintext #6 starts with: HARMODIUS+N89I+

Additional Files

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.