MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

The T52 Sturgeon Challenge – Part 10

Author: George Lasry

July 2019

Siemens and Halske T52 – Sturgeon

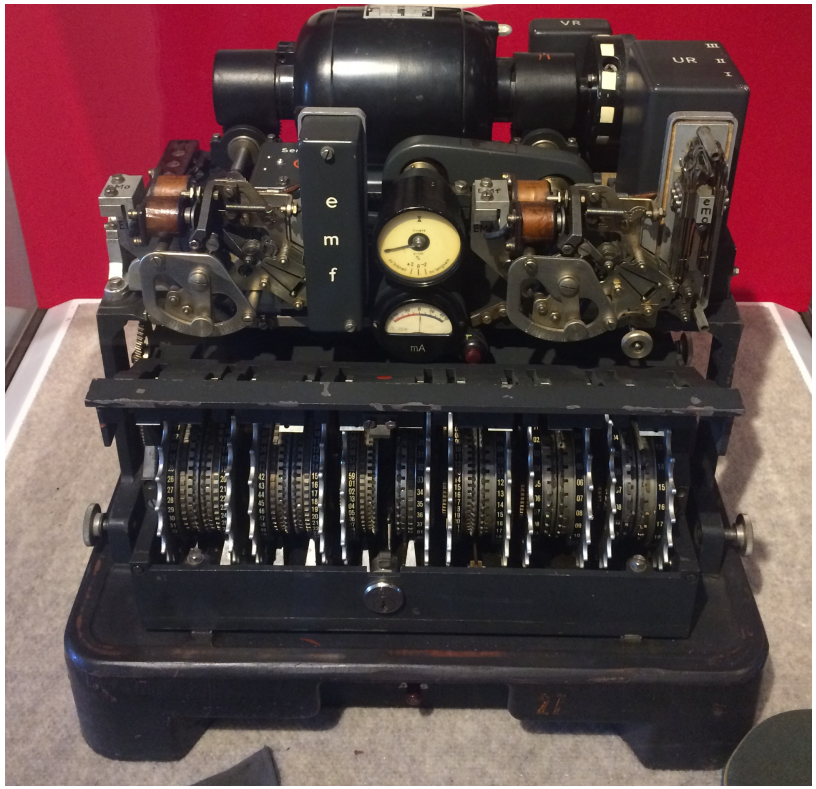

Figure: T52 Sturgeon at the National Cryptological Museum – Fort Meade, USA – Source: G. Lasry

Introduction

The Siemens and Halske T52 was a family of teleprinter encryption devices used during WW2 by the German Army, Navy, Air Force, and diplomatic services. It was considered more secure than the Enigma machine, and it was mainly used for strategic communications.

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

An overview 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.

Challenge (1/4)

This challenge is part of a series of challenges with T52. In this challenge, you need to recover the plaintexts from a series of ciphertexts *in depth*, that is, a series of plaintexts which were all encrypted using the same key settings. You are also provided with cribs (known-plaintext fragments) for each message.

The model is known - T52ca, but the key settings are unknown.

Challenge (2/4)

Six in-depth ciphertexts are provided, the beginning of each plaintext is given as a crib (all using the British notation for the Baudot alphabet):

```
Ciphertext 1:  (plaintext starts with:  CHIEF9JUSTICE+M89WHA):
+XVVGOMC3K9AGVZILLG43NTGWLVHJZGCLXBXVBFPQM9UL/A9WXVP9VZUNOYPQQC/SMRNY9MIHRS+RYUEKW+DTFFBHWIN+VWXOX9T
SSZDZHD4/4VD
Ciphertext 2:  (plaintext starts with:  HAM+M89I9SHALL9IN9AL):
PI43BIEVNPUGXI+T4XYTNWS8ZKWM4O3O/VPP9+LRFTZIQW/QG/JUDQQUOOYPQOBFVREXLBKXTIYAG+QHC3NMYI/3KYGBZXK+MBUY
Ciphertext 3:  (plaintext starts with:  DUKE9OF9BURGUNDY+M84):
FCNVJJTGLLMKPDUQFNK/BW3M8V8U8OIBCFE/Y4LCFG/EQ+WE4UPW4R3B8P+8/DQCFQOWF4NZWCS3SPT3/O+DUOFAEYUJVE+FOYDR
Ciphertext 4:  (plaintext starts with:  KING+M89A9HUNDRED9TH):
JKR/HRPGEQULAXPXEXLBDTTHBC8EUAZJEXRAVDDRPBB/SEL8UKC8BOYKUQRRVABALPPDKYBKXPLH/CRXJHFFWTD3M/MMGTCFSP9I
Ciphertext 5:  (plaintext starts with:  ROM+M89AND9BAD+S8ST9):
BZ43BIEIMMSNVX9YK8LDEYZWQ9GN/ECNMNFENDCAHV9VMDHO+QCZF9ZKODRVXDQC3NPW/OHFPCYIOZ+PNYUQVV9IBNMRTGPELLP8
Ciphertext 6:  (plaintext starts with:  SMITH+M89+K8ASIDE+L8):
UBVHDUWFN3TIVZGFZ4WVTNTGPLCOKZLY/QRIUCGGCD9EPLDPSJMW3SP44XI/UR9MP8MXMY3OJYJ9VCNYNYV+HCYABPRTEXSE4GHH
```

Challenge (3/4)

The plaintexts were extracted from Shakespeare writings, adapted to Baudot teleprinter format, and encrypted. 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 *first 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 (4/4)

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.