



THE CRYPTO CHALLENGE CONTEST

THE T52 STURGEON CHALLENGE – PART 6

Author: George Lasry

July 2019

Siemens and Halske T52 – Sturgeon

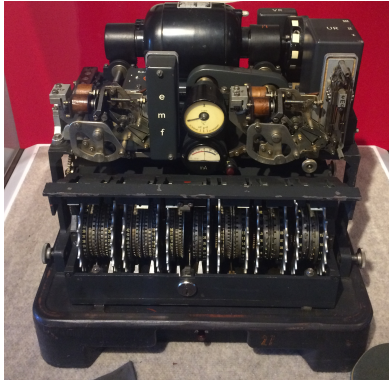


Figure: T52 Sturgeon at the National Cryptological Museum – Fort Meade, USA – Source: G. Lasry

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.

The model is known – T52c, but the key settings (wheel settings, wheel positions) are unknown.

Challenge (2/4)

The following ten, in-depth ciphertexts are provided in the British notation for the Baudot alphabet (each one has 100 symbols):

Ciphertext 1:

N4HF4PIKSOG48KOURJFOZ/WVAMIAJFYN+8TJQ4IJT3SNYM/UQVY934WIQJEPAYQKJ9UPLVV3RMMIWC+BRQ8EKT4GLNABXG3PWTJE

Ciphertext 2:

JNYXG8SYIJSR/3YYAJN/VFWVSI9DUTYAWZUTSPVHA8HMJ3EUUNLDEIRUQ3ZJMNXPJE4IJGF+RLSWTTPTFIYHWNQ3XW3BMEZ3MDSM

Ciphertext 3:

ABLTVDUWU4KFW//BGUAHGED3NBA+FYJSLUVVWMBNOMFLSSUOUK3COZ+A/GWUTWXJFARJGY+YZVCS3GQFAA08RYPFVC39MU9AD/I

Ciphertext 4:

FXCLZ3VRYTWQUQCO+980ZXRYNCMGHDFJGQDDPIKT3+CQ8QQHZF893G9/44YBKBWJX/IJSIYTNXXKVUBZHYHARLWFCG33XJGAVVM

Ciphertext 5:

SBCSVSP+XXKRT3YZHF/X+QYR+G9XJGQI+8TXYPVH/3T3PSBNDQY3AIBUTRQT8JHXNT9LESITYD3FMJY/CNS3VH/WFX8/MR/XCD8M

Ciphertext 6:

ABITGTSUCAWK/YRPPY84VUMAFDCAASXWZEWBZGXHO/3/+3TFEAENEGDSJET+RC+RC9WLDLTHGTPWN+CA/W3WQMBSK33XZWCA/Y

Ciphertext 7:

X/4IM4PPCDNSYW8LSHC/VFWKCY93L4UUCLE8JBFWRFEVFFCIPGC9RHTGSV3T/MNGSSFUDQU3GTMZSPR/ITPT83RSLGJ34QLQ3SXN

Ciphertext 8:

JNYBTF/UIUV93KE/34NJA4YYYACM+H8UWQNFKMYUWDS/LDSUNOWOTSHU8OEQXT/XWD9QZPRKWFEXNYMEFVM48RW8NZV3D3QQ3IPL

Ciphertext 9:

V/XOSPJY/USU3ZVC4CBKGZWTQHDA+FYSDL4ONPX8ZJS9YO/QW4VQD8P8MN9BTRCO/B8MUJY3DDVBXSCYFDKZ8BRBAWINVEZ3MDSM

Ciphertext 10:

SBELR8LOSOG43F/UBSX9GOW3CKUGBOYESFOQ4PTV/+YFI/SVLM3934IQTAD+AKBWJS+IMGBNDQJ9VK//LW33ZBDKPWWNLQ3GHIIN

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.