



THE CRYPTO CHALLENGE CONTEST

THE T52 STURGEON CHALLENGE – PART 1

Author: George Lasry

July 2019

Siemens and Halske T52 – Sturgeon

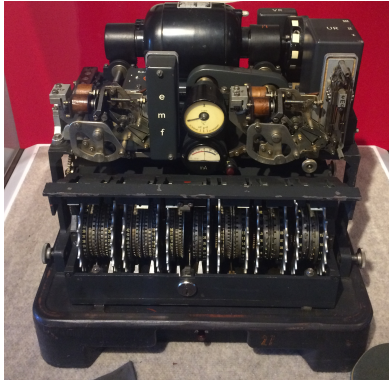


Figure: T52 Sturgeon at the National Cryptological Museum – Fort Meade, USA – Source: G. Lasry

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 plaintext. You know the ciphertext and parts of the key.

Known are:

- ▶ Model: T52a/b
- ▶ Wheel settings: IV:5-8:I:II:2-9:V:3-10:4-7:1-6:III
- ▶ Wheel positions: 53:14:68:36:64:?:?:?:?:?:?

Challenge (2/4)

The ciphertext:

V/9TJBW00ZIV3Q9PGCZEPG/CJHIC//+DDJO/ZHCPCL/DBTUCG+Y4LGNZ
+9/HZSJYYUNWLC89/E8/UMSP+XQKHO8S33/VASNK3DXT/4RUU4ZBXPZH

The ciphertext is given in the British notation for the Baudot alphabet, used at Bletchley Park.

Challenge (3/4)

The plaintext was 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 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.