MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

The SZ42 Challenge – Part 2

Author: Nils Kopal

August 2020

Lorenz SZ42 – Tunny

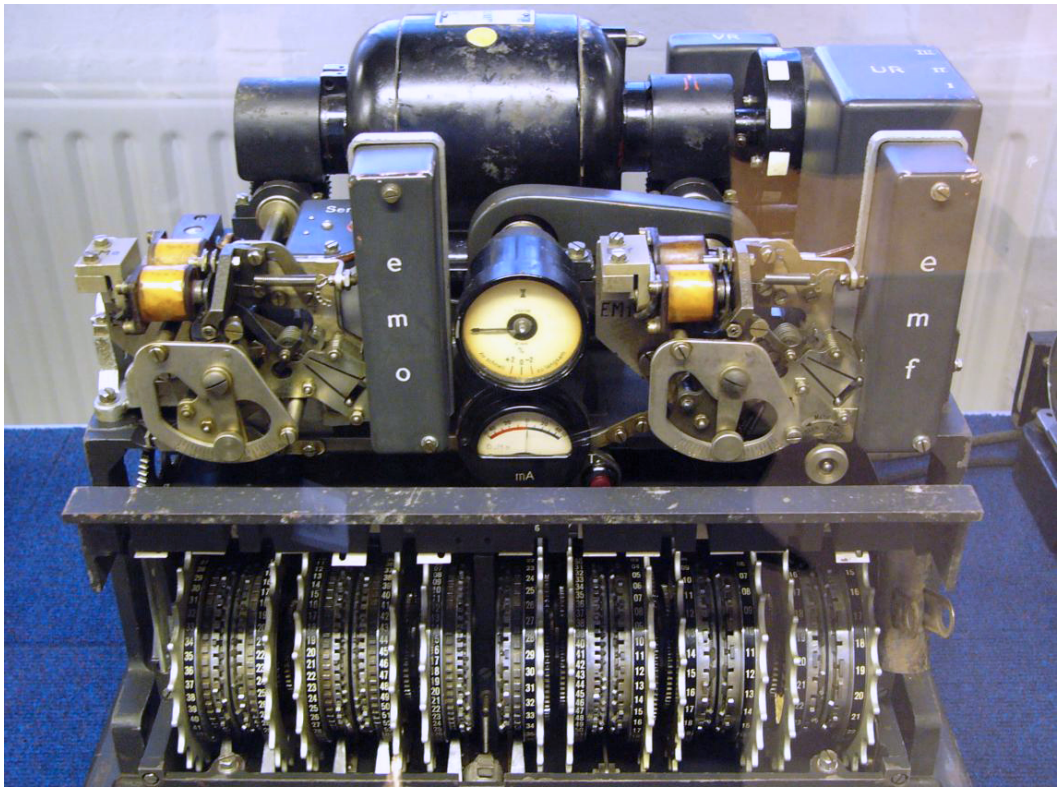

Figure: A Lorenz SZ42 machine with its covers removed on display at Bletchley Park museum.
Source: https://commons.wikimedia.org/wiki/File:Lorenz-SZ42-2.jpg

Introduction (1/2)

The Lorenz SZ42, codenamed Tunny, was a teleprinter encryption device used by Germany during WW2 for strategic communications. Its successful cryptanalysis at Bletchley Park provided the Allies with high-grade intelligence about several fronts, as well as for the preparations for the D-Day landings.

The story of Tunny's codebreaking and Colossus is well known, following the declassification of the General Report on Tunny in 2000, and the publication of several books. More details can be found in the references [CR10, Gan14, RDF15, Las20].

Introduction (2/2)

The work of the Testery, the other Tunny section at Bletchley Park, is less known. Named after its commander, Major Ralph Tester, the Testery was responsible for the development and application of hand methods, that complemented the work of machines like Colossus. For some reason, the report on the Testery was not declassified until 2018.

A detailed functional description of the SZ42 is given in the additional zip file, as well as a simulator, and hints for cryptanalysis.

Challenge (1/2)

This is the second challenge in a series of 13 level-2 challenges with the SZ42.

With this challenge, we provide 4 ciphertexts "in-depth" (thus, each ciphertext is encrypted using the same key).

Each ciphertext has 500 characters.

As described in the additional file "Lorenz_SZ42.pdf" some SZ4Z models use motor limitations which are intended to reduce the number of motor stops, making cryptanalysis more challenging . The limitation in this challenge is: CHI2_1BACK.

To solve the challenge, you have to provide the last 10 symbols of the first plaintext (in British notation for Baudot characters).

Challenge (2/2)

The attached zip file includes:

1. Additional provided material, e.g. ciphertexts (and plaintexts)
2. A simulator in Java, used to create the challenges
3. A functional description of the SZ42, including the description of the Baudot alphabet and its notations
4. Ideas for possible attacks
5. *key.txt* and *key_description.txt* containing an example key for the SZ42

References

Jack Copeland and Heath Robinson, *Colossus: Breaking the German "Tunny" code at Bletchley Park. An illustrated history*, The Rutherford Journal: The New Zealand Journal for the History and Philosophy of Science and Technology **3** (2010), http://www.rutherfordjournal.org/article030109.html.

Paul Gannon, *Colossus: Bletchley Park's Last Secret*, Atlantic Books Ltd, 2014.

George Lasry, *Solving a tunny challenge with computerized "testery" methods*, Proceedings of the 3rd International Conference on Historical Cryptology HistoCrypt 2020, no. 171, Linköping University Electronic Press, 2020, pp. 96–105.

James Reeds, Whitfield Diffie, and JV Field, *Breaking Teleprinter Ciphers at Bletchley Park: An Edition of I.J. Good, D. Michie and G. Timms: General Report on Tunny with Emphasis on Statistical methods (1945)*, John Wiley & Sons, 2015.