MysteryTwister

THE CRYPTO CHALLENGE CONTEST

The Fialka Challenge – Part 1

Author: madness

August 2024

The Fialka machine

FIGURE 1: The Fialka cipher machine, photo with courtesy of enigmamuseum.com

Fialka was a electro-mechanical rotor cipher machine used by the USSR during the Cold War. Like Enigma, it had rotors and a reflector. There were ten rotors, and the plugboard was replaced with a punchcard reader that could affect a full permutation of the alphabet. The alphabet that it used was a subset of the Russian one and had thirty letters.

An excellent and thorough description of the machine can be found in the linked document by Paul Reuvers and Marc Simons [1].

There is also a simulator for Windows available: [2]

The challenge

A piece of English text was taken, and all punctuation was removed so that only letters and spaces remained. The letters were converted to Cyrillic according to the Polish version of the Fialka keyboard, and spaces to `Й`.

The result was encrypted with rotors from Series 3K and the following key:

- daily key: `КЗДЕИ БВГЖА`
- message key: `ЗУДЮЯ ?????`
- punchcard: see Fig. 2

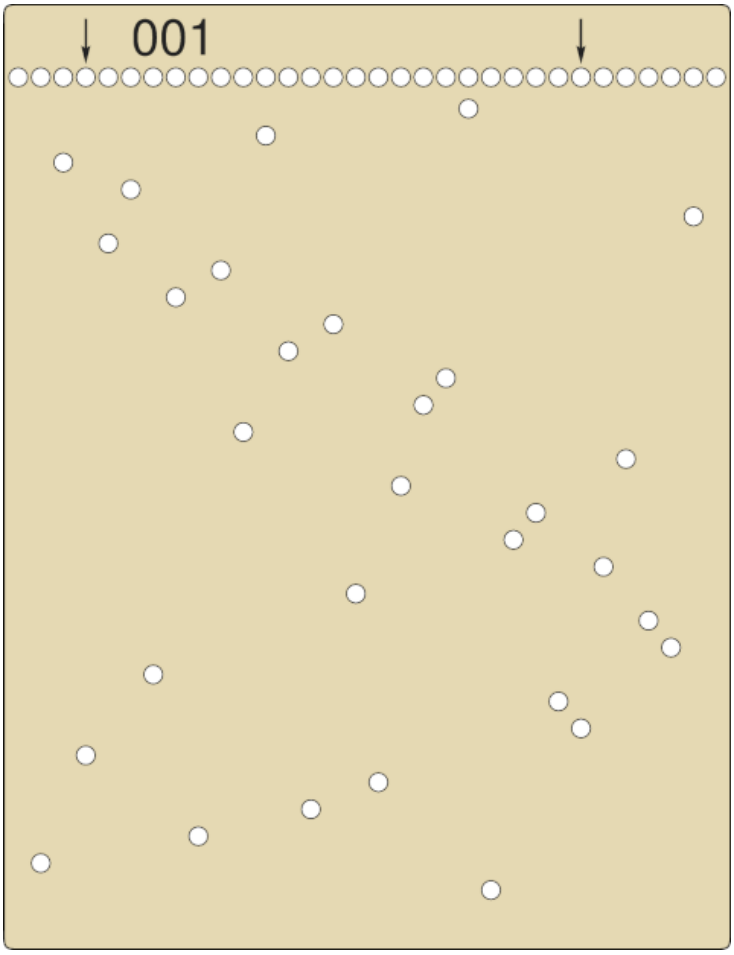

FIGURE 2: Fialka key punchcard

Attached to this challenge are the Cyrillic and English ciphertexts.
The former contains the encrypted text in Cyrillic, and the latter contains the same text in English letters and digits (according to the same Polish keyboard).

Your task

Your task is to find the five missing letters in the message key. Please submit them in their English / digit equivalents, according to the Polish keyboard.

For example, if you find that the message key is `ЗУДЮЯ ХЛЕЩИ`, then you would enter `QKTOB` as your answer.

In the next part of this series of 3 challenges about the Fialka, the Fialka machine will have configurable rotors.

Additional files

- `ciphertext-cyrillic.txt` – Original ciphertext in Cyrillic
- `ciphertext-engl.txt` – Ciphertext in English, according to the Polish keyboard
- `fialka1-punchcard.png` – The punchcard used for encryption

References

[1] Reuvers, P. & Simons, M.: Documentation on the fialka *cryptomuseum.com*

[2] cryptomuseum.com: Fialka simulator