The Soviets' Unbreakable Code

by Anna Borshchevskaya **(/experts/anna-borshchevskaya)**

Apr 27, 2019

ABOUT THE AUTHORS

Anna Borshchevskaya (/experts/anna-borshchevskaya)

Anna Borshchevskaya is a senior fellow at The Washington Institute, focusing on Russia's policy toward the Middle East.

Articles & Testimony

Rather than acknowledge history and face the future, the Russian government keeps celebrating a past in which the people were suppressed, secrecy was championed, and fear nurtured.

In the early days of the Cold War, the Soviet Union needed a foolproof way to encrypt the messages it sent to its allies. This was a daunting task: The previous pinnacle in cryptography, the German Enigma machine, had been cracked. And not only would any new communications system have to be unbreakable, but it would also have to work across languages as diverse as Polish, Hungarian, German, Romanian, Spanish, and, of course, Russian. The Soviet Union needed a technological wonder.

Enter the Fialka—Russian for "violet." Created at the end of World War II and introduced in 1956, the Fialka replaced the Albatross, a Soviet cipher machine that was itself more complex than the Enigma. By the 1970s, Fialka encryption machines had been widely adopted by Warsaw Pact and other communist nations, and they remained in use until the early 1990s.

Yet the Fialka's existence remained a well-kept secret. Russia did not declassify information about the machine until 2005. To this day, gathering details on the device remains a challenge. But the average American can finally see one in person: A specimen went on display this year at the new KGB Espionage Museum in New York City. The model is among the first of the machines ever to be shown anywhere.

The Fialka's encryption methods were advanced, but the basic technology was old. Like the Enigma, it was an electromechanical wheel-based cipher machine. Its keyboard resembled a typewriter, but its body looked more like a very advanced adding machine, equipped with a series of rotors that swapped in letters for other letters as the typist hit keys. The machine encoded a message, and then a commutator, or electrical switch, further randomized the letters. That message was punched as holes into a ticker tape, and the tape could then be fed into a sister machine and quickly decoded. Primarily used by the military, the Fialka was so secret that soldiers trained in using it reportedly had to sign special contracts specifying that they wouldn't travel abroad for two years.

The Fialka overcame the Enigma's shortcomings: The encryption on the Russian machine was more secure because it used 10 rotating wheels of letters, compared with the Enigma's three or four. Each rotation enabled the Fialka to encrypt each letter individually. All in all, the machine could produce more than 500 trillion codes.

The Soviets' encryption was so advanced, according to Stephen Budiansky, who examined the U.S. National Security Agency's efforts to crack Soviet ciphers in his book *Code Warriors*, that it could be broken only by human error, theft, or defiance. "It has always been easier to make a good code than to break a good code," he said. "The significant breaks that both [the United States] and the Soviets made throughout the Cold War in each other's systems came either through 'direct' means," such as stealing key lists of codes, "or blunders in procedures that gave away crucial details about the internal scrambling patterns of the coding systems."

Although tools such as the Fialka have become kitsch, the stuff of spycraft collector websites, secrecy isn't going anywhere. Paranoid thinking increasingly permeates the Kremlin, and rather than acknowledge history and face the future, the current Russian government encourages celebration of a past in which its people were suppressed, secrecy was championed, and fear nurtured.

These days, the craft of keeping secrets has changed. The ciphers of the past have been trumped by an encrypted device far more powerful than anything the Cold Warriors could have dreamed of: the smartphone.

Anna Borshchevskaya is a senior fellow at The Washington Institute. ❖

Foreign Policy

RECOMMENDED

ARTICLES & TESTIMONY

How to Make Russia Pay in Ukraine: Study Syria

Feb 15, 2022

◆

Anna Borshchevskaya

(/policy-analysis/how-make-russia-pay-ukraine-study-syria)

BRIEF ANALYSIS

Bennett’s Bahrain Visit Further Invigorates Israel-Gulf Diplomacy

Feb 14, 2022

◆

Simon Henderson

(/policy-analysis/bennetts-bahrain-visit-further-invigorates-israel-gulf-diplomacy)

BRIEF ANALYSIS

Libya’s Renewed Legitimacy Crisis

Feb 14, 2022

◆

Ben Fishman

(/policy-analysis/libyas-renewed-legitimacy-crisis)