Dešifrace ŠD-2 / CM-1

Šifrátor ŠD-2, který byl v Sovětském svazu znám pod krycím jménem CM-1, byl velmi dobrým kryptografickým zařízením. Ze zachycených šifrových textů nešlo ani při znalosti dokonalého popisu šifrátoru získat luštěním otevřený text. To potvrdily i současné kryptografické rozbory (např. Brtník, V. : Rekonstrukce šifrovacího stroje ŠD-2, Crypto-World 7-8/2009).

Prokopcem předaný popis stroje umožnil americké rozvědné službě postavit jeho funkční repliku. Také se jim podařilo získat ke spolupráci seržanta Kulikova, který byl armádním šifrérem a stroj obsluhoval. Spolupráce se jim dařila celých dlouhých 15 let tajit a on jim pravidelně dodával nastavení šifrátoru. Pak již nebylo pro centrálu obtížné dešifrovat zachycené telegramy, které byly pod tímto nastavením zašifrovány.

Seržant Kulikov nastavení šifrátoru vždy dohodnutým způsobem zformátoval a částečně zašifroval. Pak toto nastavení ponechal v mrtvé schránce, odkud jej vyzvedl jiný agent a zajistil jeho předání centrále. Zde je příklad, který dokladuje, jak takovéto zprávy vypadaly. Toto je nastavení na listopad a prosinec roku 1965:

ZBYTEK BUDE ZVEŘEJNĚN
dnes v 19.00 hod
Přeji hodně úspěchů v luštění !

K O N E C

(příběhu a soutěže ☺)