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:

```
BEGIN1
PHIMB ADHJX UAZAJ YMTNM JTMKX NAJAS
BMTHB VNMDA JTHPM IMPBH JANXC ZMJAD
MUOXK IHUDV KXNXU SHBUM TVTXN THYBM
TXJXC HUUVT MTAHN SADDA NEJXT BHKNM
CHUUV TMTAH NSADD ANEMN EDXJF HINHT
MCAJX DHIOX INXIH OXIXN MCTAO XVBCX
NMPBX ICFHZ AUAPB KNAUA OXIXN MCTAP
BXIMN GUAFX JDGPH YVIOX NXUMT XJCFH
KMNGJ TMCAJ PBMKN XBHZD VJTAT UXPBX
ICFHZ AZPBM KGOXI NMMZO XIXNM CTPBX
KHIHK MTMWV DYMTX THJAS BGOXO MYHHW
KGYDX NMJTM KXNAC HUUVT MTHBV IKHOA
CXUAU HTMWV DYVOJ HVVKX IXNGK CMJTA
IKXAE HBYVD AYHK
END1
BEGIN2
Q=Q W=L X=R Z=Z
1 00000000000000000000000000
5 11000001000001100001001000
3 00010000000001000011010000
4 00010001010010000000000100
2 01010001000000000001000010
R 00000000000000000000000000
SADDA NE 123456
IAJCM NEDXJ 7891011
END2
```

Díky replice šifrátoru a získaným klíčům dešifrovala rozvědka celou řadu důležitých telegramů. Jako ukázka je uveden přísně tajný telegram, který byl poslán z pražské ambasády do Moskvy a informuje se v něm o velmi závažném rozhodnutí.

SUPPM IPFKI RBKRU PXKOJ BYAOV MUEOB XYHGD UQFQW PFBQU JTDRU IMTNA BWRQO
DUBJR XQIOQ ISBWC YCENW MDBXW BOBFY DIWCR MPPYM LIZMA YDPYV DYUYI EBCOW
KTJUF JMQDE WHUVF RANFX WBVIS FZDTQ MORHD QEROE NRIKV NEPOC MKRVB ZQAKQ
EKWID BYMIU XMWKC VYZHQ XHXNE ZBPKS TTVVK XNCEF ALXUF HDMAG XRECX UXRHJ
NCHQD GAENS CBXVP TADPY OCEOV XTXRP UEGTK TTKXL TYFCV WQBIP IGXEY SQKOD
GQZSP NZBVS OGYBK YJWAC VWNVN ALMYX ZXETI DUFJA THERE TZJTH IVGRN DAXZP
NBLKK WUSDE LOCZA RRWOH WJQLA KQXMZ YBRVP XPIVA XINXO VWPGO KRBEQ AQSAZ
FEGEH ZMJLF CDFLL MUIRP HEMRZ LZVRT RQKSA EHPLF HJYST HUZBE KXPIU PAYYU
PURKX OVOAN MMUOI VJCKW LHIRM QDHQS EROQC NRAER PNQRX GKGKG MWBTH GYUPL
BMRKF NNLVG PITVC OGCZE KUEAY HOEXV XSTPE RXZES PUJLS LJHUH WKWYJ GKVYF
TRNVC OAWXV WQBIE AXVHN KVQHE ZQYEM BXBCI RNOGB IRYDC TQPZZ QQYND MFLVF
QOZYU IVKYC RNIDZ WIDDA TLSSK ONBPK EHIBW YOMZS QSSAZ EKDVE EFMFS SUMXS
LXKRD MIAKD LJSLU YORYK DFNCG ABAOW FLKDT QEYMZ GZMJQ RBHHR HYIOQ GXKTD
JWLNM JIOZG ECTTK AHQXC DLMNB XPFEL TOKZD XQBXH GWXLQ FGHEK XMHGP SIWDD
LYGZJ SURDL PCSYT SSOGO QTNPO WGOQD AFGBD AKEPZ FHWFK QDOXQ VLRTR HFEBA
JAESJ WELPX DDHIZ HNTKH MWSBY IKFDY JKDES KGZKL NMBJH ALJSV TMBDU KDBSI
VDZEF UXFBL KVVRC GZOWC LTUHA YJVHK ZLXLA AZHMR DESAA QRUWW HQCAW ONBLT
CXXLR CBLIL TLSTM GDIIU YPQLN EMEWX PKEQQ ORSKB QDIAZ DASJJ WQ

K O N E C

(příběhu a soutěže ☺)