Dešifrace textu zašifrovaného Enigmou

Pavel Vondruška
(pavel.vondruska@crypto-world.info)

Během prvého květnového víkendu (7.5.-8.5.) si mohli radioamatéři otestovat, jak před 60-ti lety vypadala práce jejich kolegů – profesionálů v armádních službách. V éteru se opakovaně ozval signál radiové **stanice GB2HQ**, která v morseovce odvysílala text zašifrovaný Enigmou. Pro zájemce jsme nahrávku tohoto vysílání uvedli jako přílohu k e-zinu 5/2005 nebo si ji můžete stáhnout z adresy http://crypto-world.info/casop7/nedele_30m.wav .

Text odvysílaného radiogramu:
QRX QTC QTC = SPECIAL ENIGMA STN = NW QTC =
CQ CQ CQ DE GB2HQ GB2HQ GB2HQ = ENIGMA MESSAGE =
1200 20 NUP AYT =
ZCSIU ECZCD YOEFX NGRDP = RPT = ZCSIU ECZCD YOEFX NGRDP +

Význam jednotlivých Q-kódů a zkratek:
CQ = všeobecná výzva
DE = zde, tady
STN = stanice
QRX = zavolám Vás později (nebo možno doplnit časovým údajem = QRX 10.00, zavolám Vás v 10.00)
QTC = mám pro Vás telegram (QTC 3 = tři tlg)
NW = nyní
RPT = opakuji
+ = konec zprávy
GB2HQ = volací znak anglické radioamatérské organizace (HQ = HeadQuarter)

Na stránce http://www.princ7.demon.co.uk/enigma.htm pak byla zveřejněna výzva k vyluštění odvysílaného zašifrovaného textu a některé další detaily a pravidla soutěže. Organizátoři soutěže ovšem na jedné ze stránek, na které se odvolávají, zveřejnili i kompletní použité nastavení šifrovacího stroje Enigma http://www.princ7.demon.co.uk/method.htm .
Zveřejnili tedy všechny dlouhodobé směnné prvky včetně klíče použitého k zašifrování zprávy. Díky tomu se úkol rozluštit text změnil na výrazně jednodušší úkol – **text na základě známého nastavení dešifrovat.**

Pokud si chcete zahrát na německého pracovníka dešifrovací služby za druhé světové války, stačí najít vhodný simulátor, který umožňuje nastavit tyto konkrétní směnné prvky (reflektor, kola a jejich pozici, propojení předního panelu a nastavit denní klíč..).

Osobně jsem použil k dešifrování odvysílané zprávy simulátor ADVANCED ENIGMA SIMULATOR SOFTWARE PROGRAM od Dirka Rijmenantse, který naleznete zde http://w1tp.com/enigma/#Enigma .

Po nastavení všech směnných prvků získáte dešifrovaný odvysílaný text v otevřené podobě, který zní:

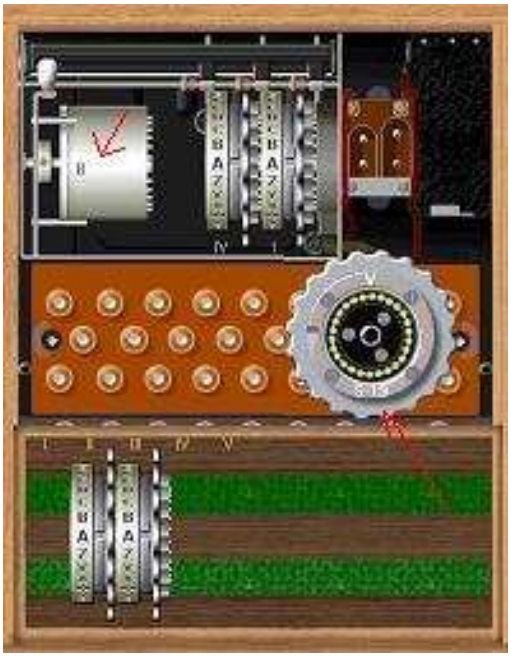
SIXTY YEARS HAVE PASSED

Následuje detailní popis nastavení směnných prvků v programu ADVANCED ENIGMA SIMULATOR SOFTWARE PROGRAM, zejména pro ty, kteří byli při dešifrování neúspěšní …

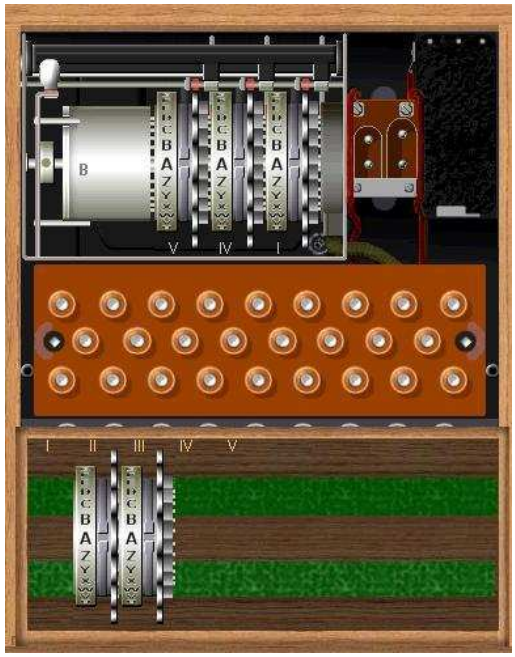
Publikované použité směnné prvky

http://www.princ7.demon.co.uk/method.htm

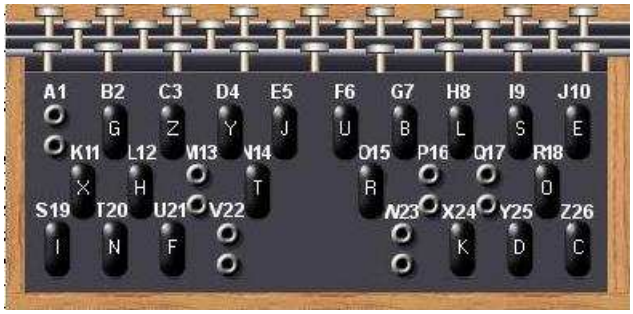
Action	The settings we used	Picture
Bring the lever forward so that the reflector disengages from the wheels	B	1
Select the three wheels for use	V IV I	2
Select each wheel in turn and set the ring setting" or to use the German term "Select each wheel in turn and set the Ringstellung".	S (19) C (3) A (1)	1
Re-plug the board with the new cable patches.	NT DY HL UF IS BG ZC EJ XK OR	3
Set the wheels to the first daily setting	NUP	4
Enter the first tri-graph	Type AYT, lamps QGQ light	5
Set the wheels to the Message Key QGQ		
Type the message	ZCSIU ECZCD YOEFX NGRDP	6
Open message	***SIXTY YEARS HAVE PASSED***	***6***



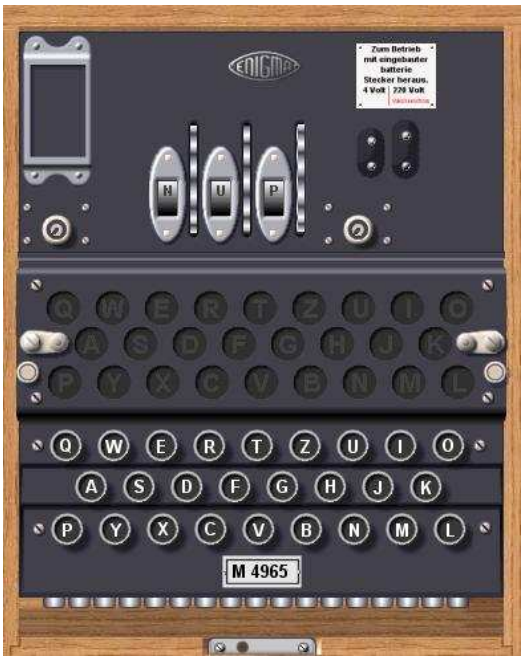
Picture 1



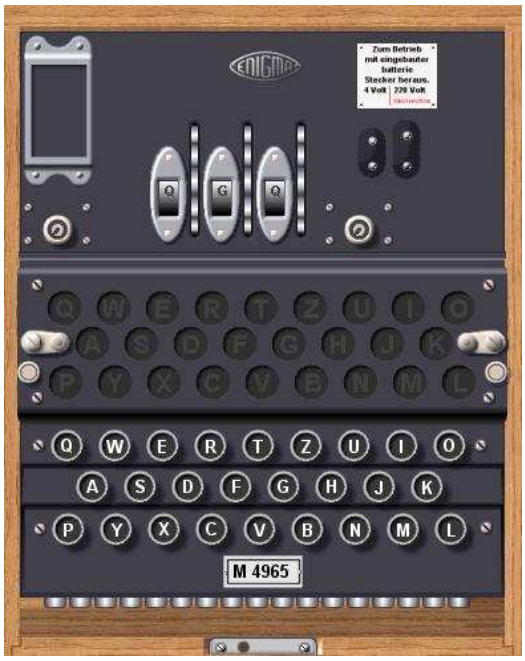
Picture 2



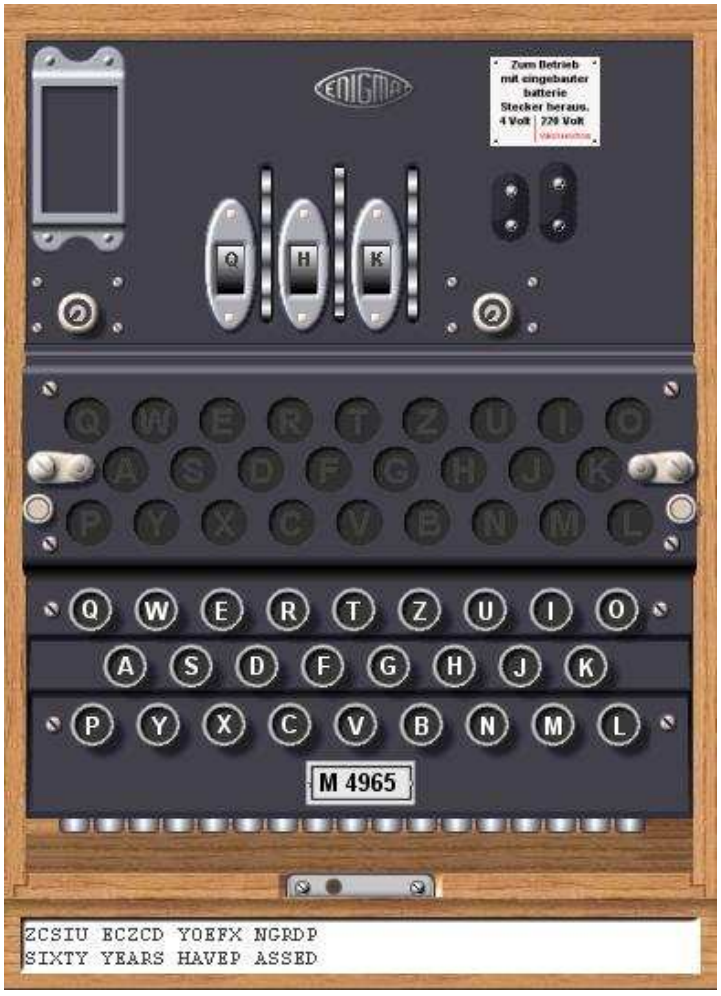
Picture 3



Picture 4



Picture 5



Picture 6