Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 9, číslo 10/2007 **15. říjen 2007**

10/2007

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1215 registrovaných odběratelů)

Obsah : str.

Příloha: ---

A. Štěpán Schmidt v Černé komoře (doprovodný text k III.kolu soutěže)

Pavel a Vlastimil Vondruškovi

(Zveřejněné části příběhu:
Prolog – Štěpán Schmidt http://soutez2007.crypto-world.info/pribeh/prolog.pdf
Část I. – Mládí Štěpána Schmidta http://soutez2007.crypto-world.info/pribeh/cast_I.pdf
Část II. – Štěpán Schmidt odchází do Vídně…http://soutez2007.crypto-world.info/pribeh/cast_II.pdf)

Hned druhý den ráno poté, co jsem rozluštil šifrovaný dopis barona Ignáce von Kocha, jsem navštívil katedrálu svatého Štěpána, která stála nedaleko císařského Hofburgu, abych se pomodlil ke svému patronovi. Potom jsem se procházel městem a ze zvědavosti se zašel podívat, stejně jako mnoho jiných Vídeňáků, do kapucínského kláštera na náhrobek císaře Karla VI., který před měsícem zemřel. Zde jsem se vroucně modlil a prosil Boha, aby vedl mé další kroky po této zemi.
Stál jsem před důležitým rozhodnutím. Ale už když jsem se vracel vídeňskými ulicemi zpět, věděl jsem, jak se rozhodnu. To jsem ovšem ještě netušil, co to vlastně Černá komora je. A nevěděl to vlastně nikdo kromě několika zasvěcených.
Odpoledne jsem vstoupil do dveří velikého paláce s ponurým tmavým průčelím, kde sídlila císařská komora, úřad nejmilostivějšího panovníka. Zatímco dvorská komora představovala vládu monarchie a veliký vliv na ni měla šlechta, císařská komora byla úřadem, o němž si rozhodoval panovník zcela sám. A kde soustředil skutečnou, i když ne vždy viditelnou moc. Když jsem tehdy poprvé procházel vjezdem mezi masivními mramorovými sloupy, ještě jsem ani stínem netušil, kolik moci se v těchto zdech ukrývá. A kolik zla.
Komorník barona von Kocha na mne čekal na schodišti. Uvedl mne do obyčejné místnosti, kde stál jen stůl, dvě pohodlná křesla, police s papíry a u okna prastarý globus. Na stěně visela tabule a na ní byl křídou napsaný jakýsi text. Komorník na něj ukázal a neosobním, skoro lhostejným hlasem řekl, abych se ujal práce. To už jsem se podobným věcem nedivil. Věděl jsem, že svět tajného písma má své rituály.

Úloha III/1 (přijímací test)

```
XIEBV KBAJV CPIGN MKHOS EEXCJ YOFBM PFLGW KBZSJ
GXVPQ WMNTX MBCGE NDSBZ XCHOE EJSER JTOEB VJUMY
BCSGM FVKCV CNVSY FSIYX ICZIC HMGKN GEGYN OGQGK
ANSJG IKGFO KEERF FTSFM YLSCR RNNOX QBMTG GYGON
JAIEY DVQIE FGQQY HGVFV CUMOV TNQWK RCRPK ZQCGP
RQOUC ZOCYO EQQAD BKATI UEIRM UHQFP IXLIB BONUX
VADCJ IENSX DFUVR ZPEJS YOAEU XRGAX WBCYR DIEAI
URKBV ZCRZX NOJES FBGGE RMEPX OYURV FCUTQ QBCEV
EBEIC HMBRS GLFCA XOFWJ IEWVF TCSFC JMFIJ NTOVA
DRTGL FCRFS TCIIL RRAEL SEYVV NEJGI FFMQV NTSBH
TSGUQ JEFQJ RTMHK FZCCX VUONJ MQRTG LFEIT BMBVM
QLCMA XSOVR TBRRZ EXWFS ASKTR ZADYG BVZNM FORKN
OBFSV MDBUN FAGKI CDSBZ XCEHZ MCVZV TOFQN ZIEMJ
NRYJZ IJPTE MRDVB AGKIC ZCNDU MZWUO DVFGY YYDOJ
UXDFE ABOPN ZLREU RSKHB SKLGX URVKH QBRCV HEVAY
GYVFD KRKRX DNQGR RMSWN GEYMF CAUIJ GERCZ OAEJS
GNMKH WIRPT SLPEV NWCLS MCQNS STDCM ANFRE OXJAB
                    BOEL
```

Sedl jsem ke stolu a dal se do luštění. Asi po hodině práce jsem vztekle praštil papírem se spoustou písmen o zem. Protože nic z toho, co jsem napsal, nedávalo smysl. Vstal jsem a začal se pomalu procházet po místnosti. Zastavil jsem se u okna a lhostejně sledoval kočáry, které s hrkotáním kol projížděly širokou ulicí. „Copak jsem takový hlupák?“ vztekal jsem se. Vrátil jsem se ke stolu a znovu se zabral do podivného textu na tabuli. Už jsem to chtěl vzdát, když se mi hlavou mihla vzpomínka na dopolední vycházku. Jako by se smiloval sám Bůh, ke kterému jsem se tak vroucně modlil. Před očima se mi objevil text nápisu, který jsem četl v kapucínském klášteře. Tehdy ho znal snad každý obyvatel Vídně. A přesně tenhle text byl zašifrován jako úloha pro mne.

Bylo to vlastně úplně prosté. Šifrový systém jsem znal, již dříve jsem se s ním setkal, ale zmátla mne velká délka použitého klíče. Rozesmál jsem se jako blázen, pak jsem uchopil brk a začal psát. Když jsem skončil, vstal jsem a chtěl vyjít ven. Ale dveře byly zamčené. Byl jsem jako ve vězení. Pokrčil jsem rameny, protože jsem se nebál. Vrátil jsem se ke stolu a sedl si. Poslouchal jsem, zda neuslyším zvuk klíče v zámku. Z chodby ke mně doléhaly tlumené kroky lidí, kteří kamsi spěchali. Ale dveře neotevřel nikdo. Teprve pozdě odpoledne se ozval klíč.

Dveře se otevřely a v nich stála služebná. V ruce nesla podnos s jídlem. Usmála se a řekla, abych jí předal papír s tím, co jsem napsal, že dostanu najíst. Neznal jsem tu ženu a okamžitě mne napadlo, že bych jí nic dávat neměl. To, co jsem vyluštil, nebylo určeno pro ni a navíc jsem nevěděl, zda zkoušku neskládá ještě někdo jiný. Kdyby mu ukázala můj list papíru, přišel by k řešení bez práce. Zavrtěl jsem hlavou a odpověděl, že nic nemám.

„Pokud mi nedáš ten list, nedostaneš najíst,“ řekla zlostně, otočila se a zmizela. Dveře za sebou pečlivě zamkla. To se večer opakovalo znovu. Přespal jsem v sedě v křesle u stolu. Nebylo to zrovna pohodlné, ale dalo se to vydržet. Domyslel jsem si, že to je součást zkoušky a netrápil jsem se tím.
Ráno se služebná s jídlem objevila znovu. Cítil jsem, jak mi v žaludku kručí hladem. Zrovna když jsem ji chtěl vyhnat, objevil se za ní baron von Koch. Byl hubený, vysoký, měl na sobě přiléhavý tmavý kabát s krátkými šosy a vysokým tuhým límcem. Tvářil se přísně, ale jeho oči si mě přátelsky prohlížely. Pak ukázal služce, aby podnos postavila na stůl a odešla. Pokynul mi rukou, abych se dal do jídla.
„Splnil jsi úkol. V naší práci nejde jen o to, abys dokázal přečíst to, co jiní nedokáží. Ale ještě těžší je o tom mlčet a tajemství chránit. To si pamatuj!“ řekl baron Ignác von Koch a pak mi začal vysvětlovat, co mne čeká.
„Už od časů prvních císařů se vládci domlouvají tak, aby o tom nikdo nepovolaný nevěděl,“ začal přátelsky. Posadil se ke stolu, nalil si číši vína, chvíli si s ní hrál v prstech a proti oknu pozoroval rudé odlesky. Pak pokračoval: „Naše století je věkem vědy. A potřeba tajit myšlenky se stala uměním. V tomhle paláci je spousta kanceláří, kde se sepisují listiny, o nichž nikdo netuší, k čemu to vlastně je. Každý písař se stará jen sám o sebe. A o to, aby se zalíbil nadřízeným. Nic víc. V několika takových kancelářích sídlíme i my.“
„Odpusťte, vznešený pane barone,“ řekl jsem s plnými ústy. „My znamená kdo? Jsme přece všichni služebníci našeho císaře.“
Zasmál se a pak se zeptal, zda ho zkouším. Potom mi vysvětlil, co je Černá komora. Tajná kancelář, kde se šifrují dopisy a kde se nejlepší muži císařství pokoušejí rozluštit dopisy jiných panovníků, které se podařilo tajné službě získat.
Brzy jsem pochopil, proč si mě vybrali. Nás mladých bylo více. Doba byla velmi napjatá. Císař Karel VI. po dlouhé nemoci zemřel. Bez synů. Jeho jediným potomkem byla dcera. Marie Terezie byla rázná žena a její otec si za cenu obrovských ústupků pojistil od všech okol-

ních vládců slib, že ji po jeho smrti uznají za vládce habsburských zemí. Jenže v Černé komoře zachytili dopis pruského kurfiřta bavorskému vévodovi, kde se oba domlouvají na tom, že bez ohledu na slib, který dali Karlu VI., vtrhnou do habsburských zemí. Země se chystala na válku. Nikdy se nešifrovalo tolik spisů, jako právě v onom roce 1740, kdy jsem se stal řádným členem Černé komory.

Úloha III/2 (dopis pruského kurfiřta)
Nomenklátor

Do Černé komory byly jednou dodány tři velmi podobné šifrové texty. Každý byl poslán po jiném poslu. Tušili jsme, že obsahuje velmi důležité sdělení, které zašifrovali pomocí stejného nomenklátoru různí úředníci.

```
q A n C H M R r F c A Q H N F U m z g p l O y S f m p m n y q g r c C w k z
C * k s C G x p c r e * w F z l w g C s r b q h w p l r j b c r a R 31 32 y
S k p a x m H g k a d x d B w x o F f A q M d B f g O x q w z l e l y a w g
U l U a C N G d t n J c z r b M o t p m o a Y a r a T z s J R q H r c q N a
H * f t d s n g q B x l q h n m z y O p g e M c c K n g f r b H h Y a r M y
q l A H a C w m z x M U l z g p h q n h f r s Y b r r G y q m w d * H A e c
I l f w B k g k t x O n N e g M d s z z c o J F q o Q o g q d G C F I c C l
p a x C g k t y O n N e * B z t o B k a d x d A w x o * k s C t n y o a o z
g w * M K P f r s O f e N J a z H C p c I * O o A f d G A z s e m p t n N U
s z m n g f r t q A H r b x f C S U t z t r c R 31 32 H b f a U l x p l d H
h M f s n f h H A x q m w N m q * H l z g d S c k c d x d B w o G a K H d G
T s q z s k s M d G p m A e b I K m q G y S k p b y m q * H h x m O f w H l
x e * y o S o P p J x o S o t w B r A H a U g f O o p a f B H * q F H m y o
b q * e h p * x p h H x o s s f O C h f O y p m O w G z m w m C t r b q * w
p m r j J l x r b C w k * q x q p S C G n l H r a R 31 32 O f q l r B n * H
b k a n N l 2 d A k O q a k h n r a y l q H d P K q 11 12 f w A k G
```

```
q B n C H M R r G b A Q H N G U m z h p m O x S f l p m n y q * r a C w k z
C g k t C G y p b r e g w F z m w h C t r b q h w p m r j a a r b R 31 32 x
S k p b x m H * k c d y d A w y o F f B q M d A f * O x q w z l e m x b w g
U l U c C N G d s n J b z r c M o s p m o a Y c r a T z t J R q H r a q N a
H * f s d s n h q A x m q h n m z y O p g e M b c K n * f r a H g Y b r M y
q l B H a C w m z y M U l z h p h q n * f r t Y b r r F y q l w d h H A e b
I m f w B k h k s x O n N e g M d s z z c o J G q o Q o g q d G C G I a C l
p c x C * k t x O n N e * B z s o B k a d y d A w y o g k s C s n x o b o z
* w g M K P f r t O f e N J c z H C p c I * O o A f d G A z t e m p s n N U
t z l n g f r t q A H r a x f C S U s z s r a R 31 32 H a f a U l y p m d H
g M f t n f g H A x q l w N l q g H m z g d S c k c d y d B w o F b K H d G
T t q z t k t M d G p l A e c I K m q F y S k p a y l q * H g y m O f w H m
x e * x o S o P p J y o S o s w B r A H c U g f O o p a f A H h q G H l x o
b q h e h p h y p g H y o t s f O C h f O x p m O w F z l w l C s r b q h w
p m r j J m y r b C w k g q y q p S C F n l H r a R 31 32 O f q m r A n g H
c k a n N l 2 d A k O q a k * n r c y m q H d P K q 11 12 f w B k F
```

```
q A n C H M R r F b B Q H N F U l z h p l O y S f m p m n x q * r c C w k z
C * k s C G y p b r e g w G z l w h C t r b q * w p m r j c a r a R 31 32 y
S k p c x l H h k a d y d B w y o F f A q M d A f * O y q w z m e l x b w *
U l U c C N F d s n J c z r b M o t p m o c Y c r b T z s J R q H r c q N b
H h f t d t n * q A y l q h n m z x O p g e M a b K n g f r a H h Y c r M x
q m A H a C w m z y M U m z h p g q n h f r s Y a r r G x q m w d h H B e c
I l f w B k g k s y O n N e g M d t z z a o J F q o Q o g q d F C G I c C l
p b x C h k t y O n N e h A z s o A k a d x d B w y o g k t C s n x o b o z
```

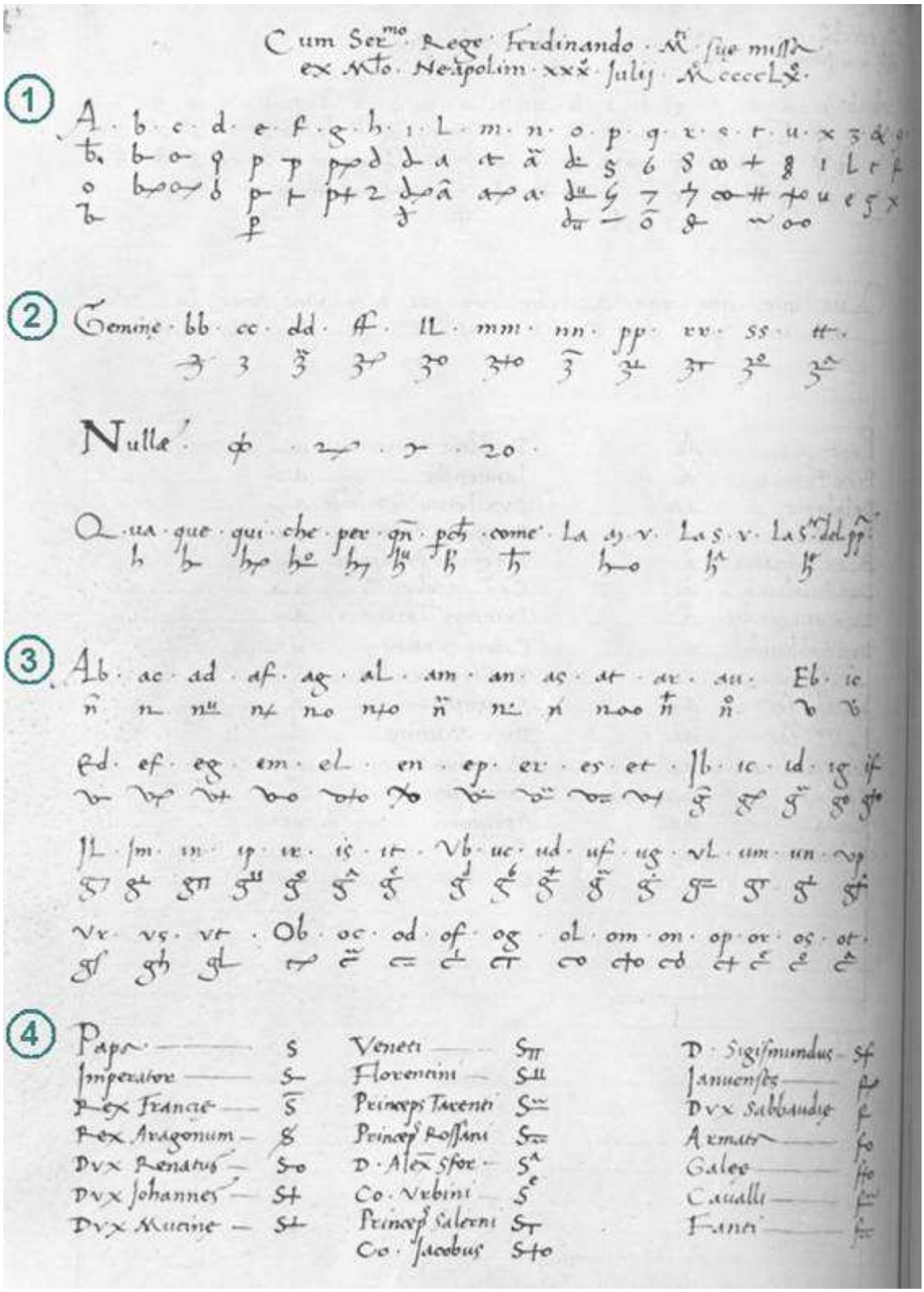
```
h w h M K P f r s O f e N J c z H C p a I * O o B f d G B z s e m p t n N U
t z m n h f r t q A H r b y f C S U s z s r c R 31 32 H b f a U m y p l d H
* M f s n f g H A y q l w N m q g H l z g d S b k c d x d A w o F b K H d F
T s q z t k t M d F p l B e c I K m q F x S k p b x l q g H g x m O f w H l
x e h x o S o P p J x o S o t w A r B H a U g f O o p c f B H * q G H m y o
a q * e * p h x p g H x o s s f O C h f O x p m O w G z l w m C t r c q g w
p l r j J m x r c C w k * q y q p S C G n l H r a R 31 32 O f q m r B n g H
b k a n N m 2 d A k O q c k * n r b y l q H d P K q 11 12 f w A k G
```

Ani jsem se pořádně nerozkoukal a opravdu se stalo, co zřejmě muselo. Ještě neuběhlo ani pár týdnů od pohřbu císaře Karla VI., a do českých zemí vtrhli nepřátelé. Tehdy jsem dostal své první skutečné dopisy, které jsem sám musel rozluštit. Většina zachycených šifrových textů byla psána pomocí nomneklátorů a část pomocí jiných systémů, které byly však méně důmyslné a jejich řešení nám nedělalo tak velké problémy. Luštění textů psaných pomocí nomenklátorů, zvláště těch velkých a dobře sestavených, nám často činilo potíže, ale jakmile jsem měl dostatečný počet zašifrovaných textů, vyřešil jsme je! To však už nebyla hra, jako dříve. Tady šlo o válku, o lidské životy a o osud celého habsburského rodu. Byly dny, kdy jsme ani Černou komoru neopouštěli, zvláště pokud jsme zachytili nějaký nový dopis od nepřátel, s nímž jsme si nevěděli rady. Celkem se nám dařilo, na rozdíl od rakouské armády. Ta zpočátku prohrávala na všech frontách. Teprve časem se podařilo postup nepřátel zastavit, ale osud země byl stále na vážkách.

Z té doby si pamatuji vlastně jen horu papírů, řetězce čísel, kódy a prach kanceláře, který mne neustále dráždil ke kašli. Nakonec jsem z toho znovu onemocněl. Mé zdraví nebylo nikdy pevné. Léčil jsem se několik měsíců v Bad Ischl. Bydlel jsem v luxusním hostinci a vše platila císařská pokladna. Chodil jsem na procházky, hodně jedl a užíval si teplé koupele. Abych nevypadl ze cviku, začal jsem jen tak sám sobě pro radost pracovat na tabulkách, které by sjednotily složitý systém rakouských měr a vah. Práci jsme dokončil až po mnoha letech.

Do Černé komory jsem se vrátil právě v době, kdy válka vrcholila. Trvala už sedmý rok a všichni z ní byli unavení. A stále více mocných volalo po míru. Začala se připravovat jednání, která měla stanovit podmínky, za nichž by evropští vládci uznali právo Marie Terezie vládnout. Dosud tohle právo měli jen mužští potomci a šlo by o nebývalý průlom v tradičních zvycích. A za něj si chtěli nechat ostatní vládci dobře zaplatit. Otázka ovšem byla, kolik.

Císařské diplomaty samozřejmě zajímalo, jaké představy má nepřítel a s čím by se spokojil. Podařilo se sice získat jakýsi návrh, který vypracovali generálové pruského kurfiřta. Jenže nikdo ho nedokázal přečíst.
„Je to zatracená smůla," rozčiloval se baron von Koch. Pak mi onen důležitý dokument podal a řekl, že jsem si v lázních odpočinul a tak ať se do toho pustím sám. A jestli uspěji, slibuje mi měsíc pobytu v lázních každý rok. Seděl jsem nad tím dokumentem dva dny a uspěl jsem. Stál jsem na vrcholu slávy. Všichni mne začali považovat za pravou ruku barona von Kocha. Nejsložitější šifry svěřovali mně. A já chtěl všem dokázat, že jsem nejlepší.



Ukázka typické struktury nomenklátoru.
1 – homofony pro abecedu otevřeného textu, 2 – znaky šifrové abecedy pro speciální části textu (zdvojení písmen, „klamače“ – vkládané znaky, které v otevřeném textu nic neznamenají, 3 – náhrada slabik (pravých bigramů), 4 – kódy pro vybraná, v textu předpokládaná slova

---

Úloha III/3 (dopis carevny Kateřiny)
Nomenklátor

```
n V n F l y w r e O1 z m v n F S1 i b x r k i F H p V n F p f i u r i G F u
i R v w i r C1 O1 R R r L w k i R m x V a m b h l u r v u i v w v i r p b Z
f t F S1 b Z m s Z o g h p v g L s L x Z h F n Z m a v o p Z i F h p v s L
x z R1 3 Z R r R a e Z m z e i f H p f 4 m v n L s F q R a w V o V H m z S2
G s o O2 P1 S1 Z R2 a n Z i b y L q Z i f p G V i R e o Z w m O2 n v n f n
Z m a V o O1 r n R S1 L Z y b x Z i e o z w o i F H p F R2 e m v a m V n L
s f H O2 s o Z H r g h g R n Z y b i F H p z e l q H p z y l q O1 Z o Z k
R2 g R a V n R n b C1 w R1 s b C1 k i r y f a m b C1 k i R h Z s z q S2 n e
V i m L S1 i f H p v x z i h p v p l i f m v z q S2 n l C1 L G m z q r w l
w i a v G O1 S2 n q H O2 C1 e r o v p w b q V R x z i v e m z y V a n L x m
Z P1 p F w y b w L h o l p h R g f Z x r a v y b n z t Z i w z P1 e S1 Z o
Z z k i r g l n y b a z s b m f o n f q n z m a v o x Z i 3 R r r C1 x R e
v w V g a w z e G z p O1 V n k i R k Z w V F a m z n f q e a m V S2 m b S1
i b x n l q V m v a Z w Z G V o m v k R1 e L e o z w m O2 G e i F h p F q Z
p l x Z i V e m z P1 p f w y b g v m g l m z R2 p F a m z o i F h p z e l q
h p Z y b k i v S1 Z o z P1 w P1 R2 e z g s Z y h y f i h p b w f n m v y l
G m R p w l n r m V m R G Z p k R2 g r e m b q Z p L G Z G o F S1 z Z l i w
r m v i m r 1 2
```

Můj život se skládal jen z práce a krátkých pobytů v lázních. Bylo to s podivem, ale čím více jsem pracoval, tím zdravější jsem byl. Do lázní jsem jezdil spíše pro radost duše, než z naléhavé potřeby těla. Zamiloval jsem si zasmušilé horské svahy porostlé řídkou trávou, na nichž jsem potkával pastýře se stády krav a dlouhé hodiny s nimi hovořil o životě. Obdivoval jsem jejich radost, jakou měli z drobností, které život v horách přinášel. To, co ve Vídni každý považoval za samozřejmé, bylo pro ně zázrakem božím. Vysoko v horách, na pastvinách zalitých sluncem, jsem se mnohokrát sám sebe ptal, jaký smysl má to, co dělám. A jaký smysl má vůbec veškerý zápas panovníků o další země, o další poddané, o další zlato. Vždyť k životu stačilo tak málo. Ale kdykoli jsem se ocitl zpátky v kanceláři, zapomínal jsem na pocit čisté radosti, který jsem tam vysoko v Alpách cítil.

Zde se mi také podařilo vyluštit krátký text, na který jsem nemohl dlouhou dobu přijít. Vlastně proto jsem si dokument odvezl s sebou do lázní, ač bylo přísně zakázáno vynášet jakékoli listiny z Černé komory.

Úloha III/4 (atypická šifra vyluštěná v Bad Ischlu)

```
NZAEE SRNOA LKAEP UCKNN EEIED TIEBS
UIPAD YCBPR NDIKH RIARH BKMAI UIBSN
SVJKP EUUAD RTSAI URZNB TOESE HUOIA
EUNCN JRVMS OOYDZ MJTEA IKTTC SERNS
ODLAY HMYIR PAEIA ASVLU EEPIT HJRPO
IASUS ERAER JYAOA SLVIV PEONP ULJTO
DETBO YRZAO TOEIB OLIVN LABMS OATBR
                    AD
```

V Bad Ischlu mne místní znali a myslím, že mě měli rádi. Možná proto, že jsem s nimi mluvil jako s rovnými. Což se o většině urozených hostů říci nedalo. Cítil jsem se tam jako doma a snad proto jsem zapomněl, že Černá komora není jen ve Vídni.
Jednou, právě když jsem se vracel z dlouhé procházky, jsem na kraji obce potkal mladou dívku se slunečníkem. Sledoval jsem střechy domů, na nichž tančilo slunce, a ani se na ni nepodíval. Proto mne překvapilo, když mne oslovila. Trhl jsem sebou, jako by mne uštkl had. Rychle se jí podíval do tváře. Byla to má dávná láska – Klementina. Zakoktal jsem něco nejapného, co tady dělá.
Usmála se a řekla, že se tu léčí. Soucitně jsem se optal, co jí schází. Řekl jsem to spíše proto, aby řeč nestála. Měl jsem raději přikývnout a jít dál. Ale léta setřela pocit zrady a zklamání. Velice jí to slušelo a v očích měla zvláštní smutek. A kolem rtů něhu. Najednou jsem si uvědomil, že ji vlastně stále miluji. A vždycky jsem ji miloval. Proto jsem se nikdy nedvořil žádné jiné dívce. Nevím, co mě to napadlo. Uchopil jsem ji za ruku a řekl, že jí to moc sluší.
„Léčím si tu nervy," řekla a na tváři se jí mihl ruměnec. „Manžel mi zemřel a já… Nemohu se s tím vyrovnat. V noci nemohu usnout. Nemohu jíst. Víš… Bůh mne potrestal!" vyhrkla najednou a rozplakala se. Nevím přesně, jak to bylo dál. Jen si pamatuji, že jsem ji najednou objímal a hladil po tváři. Pak jsme se dlouho líbali.

Kéž by mne raději uštkl had!

Ukázky některých důležitých šifer, které Štěpán Schmidt během svého působení v Černé komoře vyluštil.

Úloha III/5 (šifra z roku 1757, obležení Prahy)
Homofonní šifra

```
10 G z 14 l N g M r 25 6 m R M c I f g 3 m 2 19 d 24 L 10 21 i M 18 P 3 ch
R 1 J e z 2 r H 15 a e y 22 f r 19 G g N T 21 17 f C ch R l f b N s 13 f 21
s N 10 e ch O S a f M 18 f 23 l e l d 2 22 11 d h M ch P 3 6 b 3 A h 19 t L
11 H 18 L B d r l d 3 6 N c Q e 23 26 A 23 H C f m f L 5 5 G K 27 1 12 d 19
13 T r m N R 17 P 1 23 4 M T y f G 4 M 13 2 A H N b 27 22 2 s e K d a N 12
S 11 CH 16 Q M s H m 2 13 10 2 k L a 26 B h L 15 a 27 K H m f 18 P 3 r f K
e 14 27 1 m CH i N J CH 6 T 15 h 3 c 19 c R O 19 j 27 k r d P 27 S x 23 G A
e m e x 19 r L I f t 6 P x CH A d 19 i M R k P 1 I M 22 19 j M R j L Q S m
R m d 17 O 1 24 e 14 11 3 j 19 e m 1 13 4 L m f 19 I M L 6 y 24 d 5 S L 6
24 27 C g N 5 T 19 e b K CH z CH 19 H J l f Q 1 k N R 20 k d L 6 4 CH K 25
24 d 6 d m d 7 d m e Q 1 K e 14 6 1 S m e 15 O L y ch L 6 K CH 12 20 14 e
20 e 22 26 11 G s 11 H 15 24 20 r P G C 2 S r j 3 t 21 e 21 m H 13 G S i M
I H m 1 3 a 27 A ch M 13 l 2 4 2 K d R 4 P z f J H 16 O 2 ch S 23 L a I d x
d l H 16 O M r L x e 10 f m 2 19 e 23 L 11 20 i L 16 L B f r m d 21 G J m e
11 20 CH K x f 4 L R D 2 t 19 a L z H 18 L 15 N B H 23 d 22 G r d z 21 t 23
CH 17 Q L r N m 3 20 d 22 N 11 d m 19 j 1 O 3 5 1 23 27 16 Q 1 C N 23 1 I 3
l L 24 25 17 K 2 m a H t 24 25 1 a 27 A h N 13 l f 17 P H s f J d y C d I 2
y m H C G I CH b H t 23 S y 3 g 2 10 CH 14 f T s N i d 13 11 G y 4 26 m 3
17 Q 3 23 f i P CH 5 K L 1 r 1 k L a i I CH C CH 15 f 20 s Q d 5 P 3 k N T
19 j e 1 Q 15 1 6 27 16 O N t M m 3 O H x S 10 H 24 e K G r e I S 13 11 H y
5 27 19 M S 20 r Q e 5 G r 6 N s 25 4 l d L 6 4 G J 25 R 23 e 20 l CH B f k
S r K H P e 12 2 y a L z CH 14 CH I N 20 t CH 18 P S 21 k 25 k R O D H Q t
D O H f 5 O H C g s M h L 10 13 d l 3 6 O S g 27 22 i 22 d s l T J e r 2 16
1 m e r G 19 CH A 21 d 5 13 20 d r 18 2 5 d 21 2 r 20 f 4 15
```

Úloha III/6 (Švédové se chystají uplatnit své nároky v Baltském moři)

```
OKCEC IJICS RZONZ NOYSO IODYT IRPHM PDTAE ADSEP
MRIEV UAPYE MCOEE UEKEE NLVST EZPTE OVVCE IZYDI
DNAEU IDEFE IPIAB ENTEV AZEXP EVETS RPNSY HESPN
OAVKS OPRAT JVSMH MVIRE IAOTU UERJJ RERPN STROA
JADIA UYIAS SEITB ICTUY OUOAO AZSOT LRORA ODAOL
MPVET PAIOU LOLEZ BSEHC ABVUA ENAET VSPED CEVOR
AUUAJ IEIKF FCHKE NZSCC KSEAN PAYAO YRELC ZUARE
TSUOL ATAHI EAAPB SUAAO OEYSR IKCLT YYTSE DEJUL
IDBOM EAAKV ALMII KETOS CEUOS NJHEO NSYIR HOALE
KLHIE KNRCO SNHHT USNOE SSYDD ISDIN UJOHT NDROK
RZSCR NVKIS THCRV XRRAL ATIOA VCUSO OOPNY RKSOU
RROIM SLULM HZTNJ VSRMI ESPTA OIIAU GLAAN LSMBV
JIILP NOLEI ZLBJD HCJST ZEIUK TNMPS KTORY UIENK
ZENSA KIZHK EJOAE AVZIV LDACR FOOEU EUNVM JNPCR
KTDMO TCOVD EHDHR MVUSZ OBLKE JNRIS SAAMV PRAZP
          NEKPJ SPHIZ PONRA MAARA RVLX
```

Poznámka pro soutěžící :
Začátkem listopadu bude zveřejněna závěrečná část příběhu, která bude obsahovat jednu úlohu. Termín publikování bude předem uveden v NEWS na domovské stránce e-zinu Crypto-World a dále v aktualitách soutěže. Zde také budou průběžně zveřejňovány nápovědy k úlohám třetího kola.

B. Z dějin československé kryptografie, část III. , Paměti armádního šifranta,

Jeroným Knížek, knizek@centrum.cz

Motto:

Na vojně jsem získal zkušenost, jak je pro stát nezbytná ochrana utajovaných skutečností a její součást - šifrová služba, a kam až vede zrada. Za tehdejší studené války organizovala Bezpečnost veřejné výstavy, kde bylo možno si ohmatat vybavení zadržených špiónů, kteří byli do ČSR infiltrováni ze západu. Byly tam vysílačky, maskované např. jako plechovky autooleje, tužka či rukavice schopné vystřelit, izolované nůžky na ostnatý drát, potápěčská výstroj, heslové minibloky k šifrování, optické čtečky mikroteček, tajné inkousty, mikroaparáty, telekamery, ruční zbraně a výbušniny, balóny, návody k sabotáži, ke špionáži a podávání zpráv přes mrtvé schránky, apod. - vše s orig. značkou výrobce. I v ČSLA byly takové putovní výstavy s obrázky, např. o špionážním tunelu US Army v Berlíně, o britském umělém špionážním pařezu v Moskvě, aj. Pro každý stát je životně nezbytné mít bezpečnostní aparát a utajovat, co uzná za potřebné; utajované skutečnosti musí ostražitě chránit před novodobými špióny a záškodníky, a to i šifrovou službou, přičemž šifry i ostatní utajovací prostředky musí zůstat pro nepovolané osoby neluštitelné. Domnívám se, že to musí platit za každého režimu.

1) Bylo mi 22 let, když jsem ostříhaný dohola 1. října 1950 narukoval k ženistům do starých Fučíkových kasáren u pražské zastávky v Písku. Měl jsem jen měšťanku ve Škvorci a pokračovací školu v Pečkách, vyučen jako stavitel pian u firmy Brož ve Velimi. Sotva jsem absolvoval tzv. přijímač, složil vojenskou přísahu a začal poddůstojnickou školu (PŠ), byla ministrem Čepičkou zahájena velká reorganizace a redislokace armády. Museli jsme do noci stěhovat voj. materiál a vagonovat. Do budovy bývalé filiální nemocnice u pražské zastávky se nastěhovalo Velitelství 2. armádního sboru v čele s generálem Bernasem. Můj mateřský 2. ženijní pluk zanikl, jeho části přešly k divizím v Č. Budějovicích, Sušici a Kolíně. V kasárnách zůstaly jen nově organizované sborové útvary včetně 22. ženijního praporu s PŠ, kde naší četě velel npor. Hronek. Odtud jsem byl již v únoru 1951 vyslán do ŠDZ [1] v Seredi nad Váhom. Cvičili jsme plavbu, minování a stavbu cest u Váhu, stavbu mostu v Bratislavě přes Dunaj, další činnosti pak na soustředění ve VVP[2] Lešť. Navštívili jsme i tehdejší trosky Bratislavského hradu. Jako četař absolvent jsem se v září vrátil do Písku, složil zkoušky na vzorného ženistu a v říjnu 1951 jsem již velel četě nováčků.

2) V březnu 1952 jsem byl vyslán do Administrativního kurzu C v Tloskově u Neveklova, což byl krycí název dvouměsíčního kurzu šifr. důstojníků v záloze. Tehdejším náčelníkem šifrové služby GŠ byl plk. Sedlák a jeho oddělení čítalo asi 20 osob. Náčelníkem kurzu byl ustanoven škpt. Strzala z ŠO[3] velitelství 1. voj. okruhu v Praze. Učiteli tříd byli důstojníci z ŠO GŠ. Naší první četě velel npor. Prachatický, dalšími učiteli byli mjr. Marzín, kpt. Háza, npor. Vydra, por. Štefek, por. Zbořil a další. V kurzu nás bylo na 300 absolventů ŠDZ ode

[1] **ŠDZ** – škola na důstojníky v záloze
[2] **VVP** – vojenský výcvikový prostor
[3] **ŠO** – šifrový orgán (pracoviště)

všech druhů vojsk. Seznámili nás s historií a rozvojem kryptologie (kryptografie), naučili nás šifrovat ručními prostředky za použití převodových tabulek a písmenkových heslových materiálů, ale také klíčů pro paměť, tvořit signální či hovorové tabulky a kódování map, naučili nás používat německý diskový šifrovací stroj Enigma a nastavovat k použití diskový šifrovací stroj ANNA, etablovaný na dálnopisných stanicích svazků Stroje ANNA udržoval (snad jediný) technik od spoj. vojska - kpt. Hník. Dále nás naučili užívat polní spojovací prostředky včetně sovětské přenosné radiostanice A7b a kořistního dálnopisu Hell. Ten byl zajímavý tím, že se dal připojit k radiostanici a pracoval pouze v pevném rytmu (pokud se nestačila stisknout klávesa, byla vyslána mezera). Vyučující základního kurzu mjr. Marzín vzpomínal důstojníka (myslím že Knotka), který byl šifrantem v čs. londýnské misi za druhé sv. války a přinesl do poválečné armádní šifrové služby některé tehdejší nevědecké praktiky. Šifry používané v londýnské misi byly málo bezpečné.

Kromě odborného školení jsme zkráceně absolvovali taktiku do stupně pluku a informativně svazku. V Dejvicích u hřiště ATK nám předvedli laboratorní sálový počítač, na němž se programovalo propojováním zdířek v desce cca 60x60 cm a předvedli nám tisk obrázku složeného z písmen. V našem kurzu se školil i četař abs. Kortus od píseckého dělostřeleckého útvaru. Na závěr kurzu jsme absolvovali dvoudenní komplexní závěrečné cvičení ve funkci šifranta svazku. V průběhu kurzu jsem byl přijat za vojáka z povolání v hodnosti poručíka.

Za zastavení stojí zvláštnosti ručního šifrování. Např. při nadepisování otevřeného textu zprávy k heslu se užívaly klamače, které měly ztížit luštění. Jako klamače se vkládaly např. číslovky – PRVADRUHATRETI (v různé délce řetězce), aby zakryly frekventovaná slova (např. PRAPOR). Užívala se zkrácená mezinárodní abeceda o 25 znacích.

Nejvíce se užívala ultrareciproká tabulka, mající na okraji shora tučně abecedu a u každého písmena první řádek černý a pod ním řádek červený. Černý řádek obsahoval srovnanou abecedu a červený řádek abecedu ultrarecipročně přiřazenou. Šifrant si zapamatoval ultrareciproké trigramy z tabulky pomocí mnemotechnicky přiřazených slov (např. slovo CiBuLe se pamatovalo pro trigram CBL, CLB atd. v řádcích tabulky). Písmeno otevřeného textu (nebo šifrtextu) spojené s písmenem hesla se doplnilo třetím písmenem z trigramu a při dvou stejných písmenech bylo výsledným znakem písmeno X. Tato metoda byla nejrychlejší.

Hesla se vytvářela různě, nejčastěji asi pomocí šifrovacích strojů a tiskla na listy, z nichž byla sešita kniha A4 (typ BETON). Jindy byly vytvořeny planšety se žlábky, v nichž se svisle posouvaly tuhé pásky s různě rozházenými dvěma abecedami a po určeném nastavení se proti nežádoucímu posunu proužky zajišťovaly dřevěnými lištami pomocí křídlových šroubů. Tím vznikaly řádky hesla k použití. Hodně se užívalo hesel v pětimístných skupinách na kotoučku pásky (typ Hájek). Numerické šifrování se z počátku téměř neužívalo, rozšířilo se později.

3) Po návratu k ženijnímu praporu do Písku jsme byli s čet. abs. Kortusem odveleváni na výpomoc a zastupování ke sborovému ŠO, které řídil pplk. Vaněk. Působil jsem na tomto ŠO i v době letního soustředění vojsk ve VVP Boletice. Sbor, jemuž nově velel genmjr. Sedláček, sídlil přímo v Boleticích (v pozdějších létech v Polné), vojska 1. pěší divize měla stanový tábor v Oticích, 8. mech. divize ve Chvalšinách a sborové útvary v Třebovicích. Vojska 2. pěší divize měla tábor ve VVP Voda u Hartmanic na Slučím tahu. Všechny šifrové materiály včetně jimi šifrovaných zpráv – šifrovek (v otevřené řeči) byly označovány jako Přísně tajné a představovaly tedy státní tajemství. Podotýkám, že prostor, kde se šifrovalo (ŠO), byl nepřístupný ostatním osobám (kromě přímých nadřízených a pracovníků šifrové služby). Uklízečka mohla dovnitř jen pokud byly materiály sklizeny, přesto musela být pro tuto činnost schvále-

na. Měli jsme schválený seznam funkcionářů, kteří směli užívat šifrspojení. Podobné výsady měla například mobilizační pracoviště. Funkce šifrantů budily všude respekt, např. když šifrant přijížděl do tábora vojsk na kontrolu, prchali funkcionáři okny stanů pryč. Svého času měli šifranti právo podle schváleného plánu odposlouchávat vojenské hovory, cenzurovat voj. tiskoviny a dozírat na dodržování předpisů k ochraně utajovaných skutečností (kontrolovat všechna pracoviště a stav zabezpečení voj. objektů, zejména činnost spisoven). Za porušování předpisů o ochraně utajovaných skutečností zákon ukládal vysoké tresty, proto osoby určené k seznamování se státním tajemstvím byly předem prověřovány kontrarozvědkou, nesměly se bez předchozího povolení stýkat s podezřelými osobami, libovolně cestovat, apod., dokonce jim bylo bráněno se oženit s nespolehlivou nevěstou. Trpěl tím rodinný život. Manželky důstojníků se v posádkách sdružovaly v tzv. babinci, totiž ve Sdružení žen vojáků z povolání, pro něž političtí pracovníci organizovali v kasárnách různé akce.

4) Koncem r. 1952 jsem byl s několika dalšími absolventy jarního šifrantského kurzu pozván na šifrovací oddělení GŠ, kde jsme byli připravováni na funkce učitelů vznikající Školy na výchovu šifrových důstojníků v záloze na zámku Tloskov a byl jsem jmenován mladším učitelem. Již v průběhu roku došlo k vystřídání náčelníka ŠO GŠ plk. Sedláka plk. Rubešem (z hlavní kádrové správy MNO) a za něho pak došlo k přejmenování ŠO na 6. oddělení (sovětské ŠO měly krycí označení 8. oddělení). Náčelníkem školy byl záhy jmenován pplk. Vaněk z ŠO píseckého sboru. Frekventanty tříměsíčních kurzů této školy byli záložní důstojníci, povolaní z civilu. Když byl pplk. Vaněk z Písku odvelen k řízení školy a jeho zástupce npor. Škrdla byl vážně nemocen, povolal k svému zastupování náčelníka ŠO sušické 2. divize npor. Gondu a ten byl záhy ustanoven náčelníkem 6. oddělení 2. as. Ve škole se mi práce učitele dařila, leč nebylo mi souzeno tam zůstat. Osamocený náčelník 6. odd. 2. armádního sboru npor. Gonda o mne požádal náčelníka ŠO GŠ a tak jsem se po ukončení prvního běhu frekventantů školy vrátil do Písku a od dubna 1953 stal jeho zástupcem.

5) Práce u sboru bylo mnoho. Kdykoli došla šifrovaná zpráva nebo bylo třeba něco zašifrovat, musel šifrant neodkladně práci splnit. Po pracovní době bylo nutné držet pohotovost a dostavit se ihned na pracoviště kdykoli bylo třeba odeslat nebo dešifrovat zprávu, což bylo na denním pořádku. Vždy při opuštění pracoviště musel šifrant operačnímu dozorčímu sdělit místa a čas, kde se bude zdržovat, aby pro něho mohla být vyslána spojka. Pohotovostní práce nebyla důvodem k poskytnutí náhradního volna. Pokud šifrant ochořel či odjížděl na dovolenou apod., musel si zajistit zastupování nejbližším ŠO a oznámit to svým nadřízeným. Šifrovalo se ručně (tužkou), výjimečně Enigmou, k přepravě zpráv se užívalo dálnopisné pracoviště anebo se zpráva diktovala po skupinách telefonem. Sbor byl podřízen Velitelství 1. voj. okruhu, které sídlilo v budově bývalého sněmu ve Sněmovní ulici v Praze. Tam byl náčelníkem ŠO škpt. Nálepka a jeho zástupcem škpt. Strzala. V době fungování sboru v Písku mělo ŠO za úkol vydávat také průkazky ke vstupu do VVP Boletice a DobráVoda a kontrolovat dodržování ochrany utajovaných skutečností na sboru i u podřízených svazků a vojsk. Přitom vojska 2. as byla rozmístěna od Čáslavi po Třeboň a Domažlice a nebylo ani za rok možné všechny posádky zkontrolovat. Měsíčně jsme museli odesílat okruhu souhrnné hlášení o celkové činnosti vlastního i podřízených ŠO, zúčastňovat se cvičení v terénu, nebo posilovat ŠO okruhu nebo i GŠ při provádění vojskových prověrek či cvičných mobilizací v celé ČSR, tj. cestovat i s kontrolovanými vojsky, sledovat a vyhodnocovat jejich činnost a denně dodávat závěry o stavu zkontrolovaných útvarů po své odbornosti. Denně bylo třeba navštívit až 5 útvarů a nebylo snadné se k nim vůbec dostat. Šifranti tehdy neměli žádný dopravní prostředek a přepravovali se s ostatními. Přitom stále museli mít zajištěnou pohotovost ŠO doma i v terénu.

6) V roce 1954 se konalo ve VVP Doupov sborové taktické cvičení, řízené ministrem Čepičkou. Řídící skupina GŠ sídlila v Doupově, štáb sboru byl u Pustého zámku, já byl nasazen západně jako rozhodčí strany modré u ŠO 2. střelecké divize, kde byl šifrantem npor. Šulha. Mým úkolem bylo sledovat/hodnotit utajení a podávat šifrovaná hlášení řídící skupině GŠ. K tomu mi plk. Rubeš přidělil nový ruční šifrovací stroj (nebo spíše strojek), vyvinutý v součinnosti se vznikající Zvláštní správou MV. Jedním z konstruktérů tohoto stroje byl npor. Málek. Stroj se podobal šifrovacímu stroji MAGDA, ale byl lehčí a patrně neměl průhledné okénko. Šifrování v něm zprostředkovával otočný bubínek s lištami, nesoucími suvně nastavitelné jezdce a klikový mechanismus. Zleva vyčnívalo točítko k vyhledání písmene a zprava klička, jejímž otočením se přiřadila odpovídající šifra/znak; znaky se tiskly ve skupinách na papírovou pásku. Stroj byl uzamčen v pancéřové skříně velikosti cca 15x15x12 cm se sklopným držadlem, vážil necelý kilogram a měl se nosit na opasku. Nějakou dobu se stroj ještě užíval na ŠO svazků, ale zanedlouho byl jako nepraktický (pomalý) stažen.

7) V 60-tých létech bývaly štáby v poli jen ve stanech; šifrant tam měl skládací stůl a židli, telefon, polní lůžko se slamníkem, bednu s materiálem, lampu a v zimě kamínka. Ubytování zajišťovala velitelská rota, která měla nákladní auta. Velitel sboru či svazku míval k dispozici polní automobil Jeep s radisospojením, ostatní příslušníci se přepravovali na korbě nákladního auta, později též ve štábním autobusu operačního oddělení. Týlové složky štábu měly vlastní stanoviště, vzdálené až 20 km za velitelstvím. Spojaři v poli umísťovali přenosné šňůrové ústředny a dálnopisy na holé zemi, před nimi měli vyhloubenou jámu pro nohy obsluhy (vystlanou chvojím) a nad tím jednoduchý přístřešek ze stanového dílce; poruchy pak vznikaly i následkem povětrnostních vlivů. Při poruchách spojení se uplatnila morseovka.

8) Pro každé připravované cvičení od pluku výše musel šifrant dodat svou přílohu k plánu cvičení (Nařízení k ochraně utajovaných skutečností), kde mimo jiné byly uvedeny typy a druhy kódovacích pomůcek podle druhů vojsk a stupňů řízení. ŠO GŠ vydávalo pravidla tvorby takových pomůcek podřízeným ŠO a pro některé účely také konkrétní tištěné tabulky s rozpisem platnosti heslových materiálů. Tím se podřízené stupně musely řídit a vydávat zbývající materiály podle místních potřeb. Vzpomínám, jak jsme vyráběli listy signálních tabulek na lihovém rotaprintu nebo fotocestou a ručně i jejich obaly. K tomu jsme si opatřovali staré rentgenové snímky a po očištění z nich dělali kapsové průhledné obaly. Jako podklady k centrální výrobě museli šifranti všech stupňů měsíčně dodávat stanovený počet ručně sestavených řádků hesel, k čemu dostali sady číslovaných koleček k náhodnému výběru z urny. Samozřejmě museli zajistit, aby se kódovací pomůcky dostaly jen k určeným funkcionářům a ti se je naučili používat. Šifrant s nimi prováděl školení a průběžně sledoval, které výrazy je třeba změnit či doplnit.

9) V terénu bylo třeba mít šifrantské potřeby pod stálým dohledem v brašně a být někým chráněn. Tehdy stačilo mít v zapečetěné krabičce od pásky do psacího stroje kotouček dálnopisné pásky s natištěnými pětimístnými písmenovými skupinami hesla (typ Hájek), baterku a tužku s čistým blokem a v hlavě pak mít převodovou ultrareciprokou tabulku (viz výše). Stále se vymýšlely nejen na GŠ nové pomůcky. Šifrant z budějovického KVS měl osobní styk s továrnou na slídová pravítka a navrhnul z nich kódovací pomůcku k určování bodů z mapy. Podobné to bylo s hovorovými tabulkami, ke kterým bylo podáno mnoho návrhů. Hesla se v nich měnila vpisováním přerušované řady čísel či posouváním proužků (slidex). Neosvědčily se. Kódování map vycházelo ze čtvercové sítě, kde se svisle a vodorovně vepisovaly do map stanovené řady číselných kódů. K pojmenování vybraných funkcionářů se používaly Pseu-

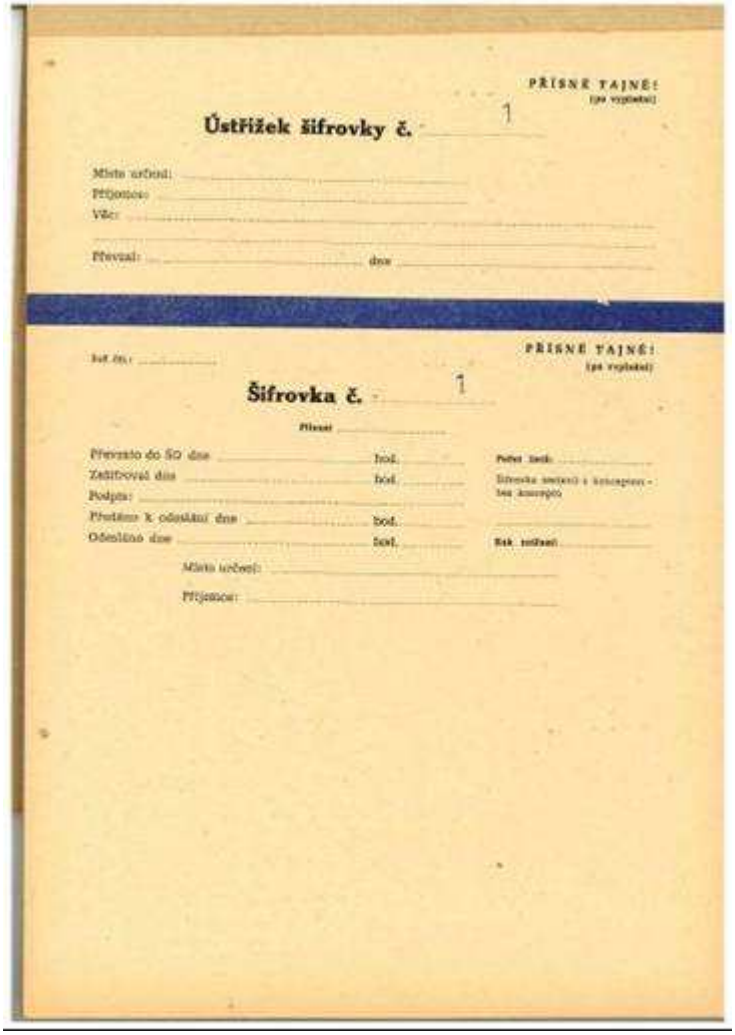
donymy a k pojmenování terénních celků Krycí jména terénních předmětů. K tomu byly vydány obsáhlé brožury neopakujících se jmen. Ani to se neosvědčilo. Pamatuji, jak z ŠO tehdejšího 1. voj. okruhu nám došla šifrovka, že s námi v následujících 3 dnech provedou zatěžovací test. V zápětí nám začali kluci z dálnopisu nosit došlé zašifrované zprávy a v nich pokyny, co máme zjistit a ihned příslušnou šifrou odpovědět. Měli jsme k dispozici Enigmu, heslovou písmenkovou knihu Beton, klíč Vak a planšetovou tabulku s posuvnými proužky hesla. Tehdy ještě nebyly ruské bloknoty (číselné heslové sešity). Začal jsem pracovat sám (náčelník Gonda pokračoval v dřívější práci) a za chvíli byl na stole štos nezpracovaných zpráv. Pracoval jsem i v noci a ráno mi teprve začal náčelník pomáhat; museli jsme povolat i kolegu z kurzu Kortusa. Nakonec vše dobře dopadlo, vše bylo dešifrováno a odeslány všechny šifrované odpovědi.

Stroj Enigma, jejž jsme užívali, byl určen do pole; proto měl bednu barvy khaki a nosil se na zádech. K němu příslušelo ploché dřevěné pouzdro s dalšími dvěma disky. Uvnitř bedny byly ve víku uloženy propojovací dvoupramenné šňůry, na obou koncích opatřené vidlicí; ty se podle denního nastavení zasouvaly do párových zdířek (označených písmeny) komutačního panelu na čelní straně stroje. Na vrchní straně byla klávesnice a za ní tři řady znaků; ty se při důkladném stisku klávesy podle vytvořené kombinace rozsvěcovaly a šifrant je tužkou zapisoval do pětimístných skupin šifrogramu (nebo jako otevřený text na tiskopis šifrovky). Před nimi vpravo byl vložen velký el. článek se vzdušnou depolarizací (nebo transformátorek se šňůrou a vidlicí) a vlevo pole se třemi disky na ose, pořadí se podle určení měnilo. Na každém disku se nastavovalo překlápěním vlastní krokování (nepravidelné pootáčení při stisku klávesy); disky měly po obou stranách kontakty, jimiž procházel výsledný impuls k žárovičkám písmen. Před použitím bylo třeba kontakty ošetřit. Práce se strojem byla úmorná, pomalejší než s tištěným heslem a ultrareciproční převodovou tabulkou. Stroj byl jen jako záložní prostředek.

Enigma byla někdy kolem r. 1955 stažena a postupně se přecházelo na sovětské numerické heslové sešity (bloknoty), k nimž se užívala číselná převodová tabulka. Většina písmen/znaků a vybrané bigramy či trigramy se zaměňovaly dvojcifernými čísly, číslice se zaměňovaly trigramem této číslice.

10) Tiskopisy šifrovek jsme používali asi od r. 1955; ty k odeslání měly červený rámeček, došlé černý; nahoře Přísně tajné! Opis zakázán! Výpis povolen, od koho - komu; dole vlevo číslo šifrovky, datum/hod. a podpis šifranta, vpravo totéž a podpis adresáta + dalších osob. Podobně jsme měli velké a malé bloky rastrovaných šifrogramů, pak deníky - přijatých x odeslaných šifrovek, kde bylo: číslo šifrovky, odesilatel a adresát, časové údaje a údaje o použitém prostředku s detaily - délka, čísla a množství použitý materiál, podpis šifranta a poznámka. Měli jsme doručovací sešity k předání zpráv k odeslání spojařům a k převzetí došlých šifrovek, často jsme adresáty upomínali k vrácení šifrovky. Adresát ji musel s podpisy všech, kdo se s obsahem seznámil (spolu s příp. výpisy ke kontrole obsahu) do týdne na ŠO vrátit k dlouhodobému uložení.

Šifrovky jsme ukládali do složek v trezoru; stávalo se, že si adresát znovu šifrovku vypůjčil (pokud jejím textem potřeboval argumentovat, směl si pořídit výpis, nikoli doslovný opis). Při doručování měl šifrant všude přednostní právo přístupu k adresátovi (i na uzavřená jednání), vzdáleného adresáta musel o došlé šifrovce předem informovat (ne o obsahu), často ale adresát byl odesilatelem uvědomen dříve, než šifrovka došla.


PŘÍSNĚ TAJNÉ!

Ústřižek šifrovky č. 1

Místo určení:
Přijmout:
Věc:
Převzal: dne

PŘÍSNĚ TAJNÉ!

Šifrovka č. 1

Přenos

Převzato do ŠO dne hod.
Zašifrovat dne hod.
Podpis:
Předáno k odeslání dne hod.
Odesláno dne hod.

Místo určení:
Přijmout:

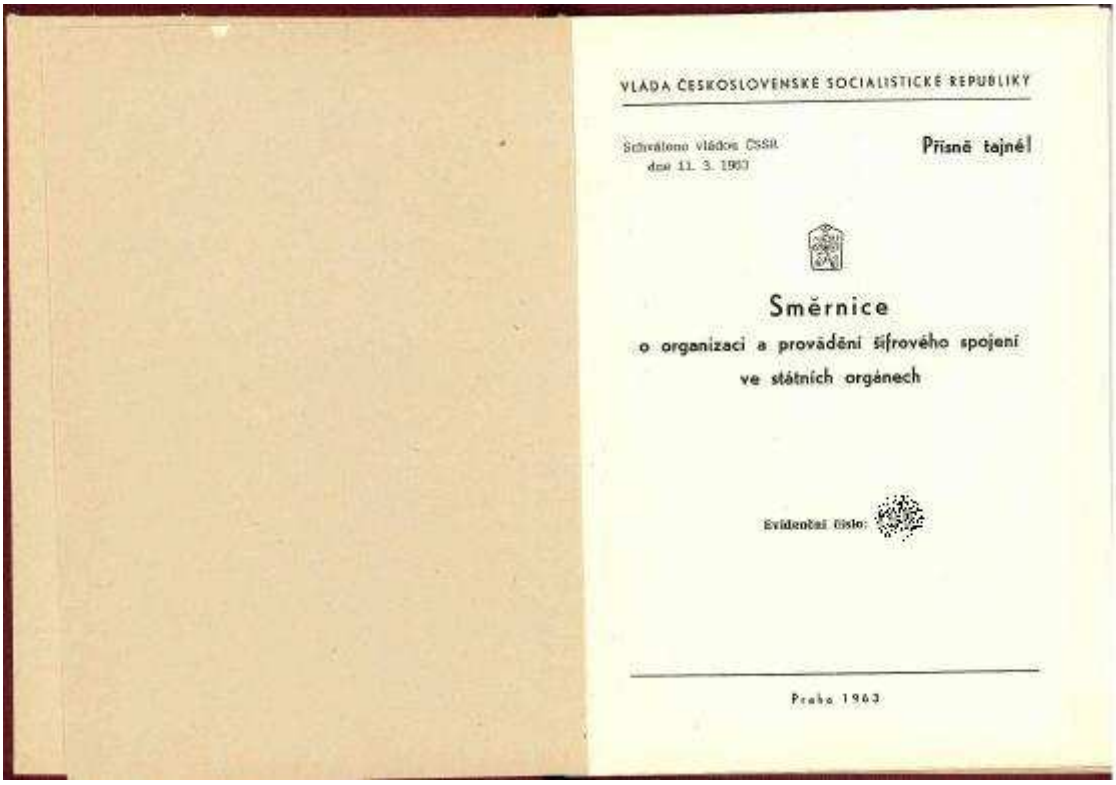
Dešifrovaný text jsme psali strojem, nebo lepili pásku pomocí nůžek a lepičky s válečkem. Šifrovky často zhatili funkcionářům i celým štábům a vojskům jejich plány, zvláště při vojskových a štábních cvičeních, ale i při zhoršení mezinárodně-politické situace. Většinou byly odesilatem označovány nejvyšší prioritou - MP (mimo pořadí). Pro některé nouzové situace však platily dohodnuté signály; ty byly zapečetěné u velitelů či operačních dozorčích, aby akce mohly být rychle zahájeny. Postup měl dozorčí orgán v pokynech (denně upřesňovaných při hlášení o převzetí x předání služby). Tam měl stanovené i povinnosti vůči šifrantům.

11) Každý člen štábu (tedy i šifrant) se také musel vzdělávat. K tomu byly stanoveny pondělní tzv. velitelské dny s programem: pořadový výcvik, tělocvik, seznámení se zbraněmi a předpisy, taktika, výuka s testy ze všech voj. odborností včetně práva, střeleb, politické přípravy, aj. Všechna činnost musela být plánována, každý musel mít schválený osobní plán a vyhodnocovat jej. Ke zvýšení znalostí rozhodl ministr svým rozkazem, že důstojníci, kteří neabsolvovali alespoň vojskové učiliště, musí si jej ve večerních kurzech doplnit. Tak jsem i já po dvouletém studiu při zaměstnání musel vykonat v litoměřickém ženijním učilišti příslušné zkoušky. Byl mi vydán absolventský odznak, který jsem musel na blůze viditelně nosit. Podobných zkoušek z různých kurzů jsem za dobu voj. služby musel složit desítky, např. i z řidičského kurzu voj. autoškoly.

12) V roce 1956 došlo k další větší reorganizaci a bylo zrušeno velitelství píseckého 2. armádního sboru. Příslušníci jeho štábu byli převeleni k jiným útvarům. Kpt. Gonda se stal náčelníkem ŠO dělostřelecké brigády v Jincích a já se stal náčelníkem ŠO 2. střelecké divize v Sušici. Tehdy tam velel plk. Kvapil, jeho zástupcem byl pplk. Rusov (pozdější NGŠ) a po

něm plk. Procházka (pozdější velitel Západního okruhu). Byla napjatá mezinárodní situace, útvary upravovaly skrytá pohraniční opevnění. Navázal jsem styky s ŠO tamní brigády PS.

Po dvou letech služby v Sušici jsem byl převelen na místo PNSS[4] u KVS v Liberci, jelikož tam delší dobu nebyla funkce šifranta obsazena. Spadal jsem pod ŠO SÚMNO[5] na Malostranském náměstí v Praze. Podařilo se mi zlepšit vztah pracovníků k ochraně utajovaných skutečností u KVS i podřízených OVS a z vyššího pověření vyškolit desítky pracovníků spisoven útvarů MNO, dislokovaných na území kraje. Musel jsem také dozírat na fungování spojení a zajišťovat šifrové spojení pro místní raketometnou brigádu. Jako svého zástupce jsem si musel vyškolit náčelníka 1. oddělení KVS.



VLÁDA ČESKOSLOVENSKÉ SOCIALISTICKÉ REPUBLIKY

Schváleno vládou ČSSR dne 11. 3. 1963

Přísně tajné!

Směrnice

o organizaci a provádění šifrového spojení ve státních orgánech

Evidenční číslo:

Praha 1963

13) V roce 1960 došlo k reorganizaci státní správy a Liberecký kraj byl zrušen. Proto jsem byl převelen k 1. tankové divizi ve Slaném jako pomocník náčelníka 8. oddělení (ŠO). Náčelníkem 8. oddělení zde byl mjr. Mareš, který byl kdysi náčelníkem 6. oddělení 8. mechanizované divize v Kolíně, spadající pod tehdejší písecký armádní sbor. Kolem r. 1960 došlo k vymístění 1.armády (bývalého 1. Vojenského okruhu) z Prahy do Příbrami - Zdaboře a r. 1965 tam z ní vzniklo velitelství Západního vojenského okruhu (ZVO), jemuž velel generál Procházka, kterého jsem znal ze Sušice. Naše 1. td byla nadále podřízena 1. armádě v Příbrami, kde byl z prvu náčelníkem ŠO pplk. Vydra. V té době pplk. Nálepka nahradil plk. Rubeše v čele 8. oddělení GŠ a plk. Rubeš byl převelen za PNSS KVS Plzeň (prý za porušení ochrany mobilizačního pracoviště GŠ). Všechna 8. oddělení nedlouho poté přešla na všech stupních velení ke spojovacímu vojsku. V oné době byla pracoviště 8. oddělení vybavována ruským dálnopisným strojem a šifrovacím strojem ŠDl (což byl doplněk k dálnopisnému stroji, kde docházelo k šifrování či dešifrování v průběhu psaní či příjmu textu za pomoci heslové pě-

[4] **PNSS** - pomocník náčelníka (KVS) pro specielní spojení
[5] **SÚMNO** – Správa útvarů MNO

tistopé děrné pásky s číslovanými úseky). Později byly tyto šifrovací stroje nahrazeny typy ŠD3.

14) Když jsem v květnu 1960 nastoupil k ŠO 1. td ve Slaném, naše ŠO bylo v přízemí, velká místnost byla rozdělena plentou; v druhé půlce sídlil topograf se skladem map a ještě tělocvikář. Stroje ani vozidlo jsme ještě neměli, pracovali jsme jen s ručními prostředky, ukládanými v trezoru. Asi po dvou letech zrušili v naší štábní budově posádkovou věznici s celami, zřídili tam místnost pro OD (oper. dozorčího) a ze tří cel zřídili naše ŠO, kde první dvě cely spojili vybouráním příčky a třetí sloužila jako šifrovna a sklad. U stropu byla malá zamřížovaná okna (já si tam zkazil zrak), v mezistěně kamna Club a uhlí v šopě na dvoře (kdo přišel v zimě první, musel vynést popel, donést topivo a zatopit). Až časem nám udělali větší okno (jen v kanceláři), záclony jsem přinesl z domova.

Asi po šesti letech jsem byl na shromáždění štábu divize zvolen za soudce vyššího voj. soudu v Příbrami a zúčastňoval jsem se zasedání senátu. Průpravou a praxí u soudu jsem si rozšířil právní vědomosti, které jsem mohl uplatňovat např. při zpracování znaleckých posudků z oboru ochrany utajovaných skutečností.

15) Asi r. 1963 jsme ke svazku dostali nový stroj ŠD1 s ruským páskovým dálnopisem a zavedli k nám pobočku dálnopisné linky ze spoj. uzlu, odkud nám ji na požadavek přednostně přepínali. Mašina to byla velká, tvaru kvádru, v kovovém zaobleném krytu natřeném zeleným čeřínkovým lakem, rozměrů cca 40x60x35 cm. Vlevo nahoře měla odklopnou část krytu s držákem k vkládání kotouče pětistopého děrnopáskového hesla s trojcifernými čísly úseků (tuším po dvaceti kombinacích), kolíčkový snímač s řezačkou užité pásky (řezal při každém kroku snímače) a pod ním šuplíček na odstřihnuté proužky. Hlavní částí stroje byly dva mechanické kombinátory/dekombinátory, podobné typovým košům v dálnopisu, minimum elektrotechnických dílů a motor. Jako u jiných dálnopisů i u ŠD1 se musely upravovat a kontrolovat dlouhou ladičkou s průzorem otáčky dle stroboskopických značek na motoru. Uprostřed na spodku čelní strany byl pákový přepínač a nad ním prosklené okénko; v poloze vlevo se rozsvítil zelený rámeček a tak se zapnulo šifrování. Před zapnutím se muselo vzájemně nastavit a odsouhlasit číslo úseku hesla. Stroj byl opatřen kabelem s kolíkovou dálnopisnou zástrčkou, vestavěnou dálnopisnou zásuvkou (k připojení ovládacího dálnopisu) a síťovým přívodem s vidlicí. Ke stroji se dodávala asi 8cm dlouhá trubičková maznička s olejem (její víčko mělo na vnitřní straně malý šroubováček), náhradní uhlíkové kartáčky motoru, ladička otáček, náhradní klíčovací relé a štětec k čištění. Stroj měl svou přikrývku s miskou k zapečetění. Často byl volán velitel divize k šifrovému hovoru s nadřízeným a šifrant psal z jeho diktátu. Oba texty (přijímaný i odesíla-

ný) se tiskly na dálnopisnou pásku, která se lepila na šifrovku. V knize i na šifrovku se uváděl Rozhovor - koho a s kým. Stroj se mohl použít jen pro přímé oboustranné spojení a nevím, že by se užíval v poli. Pokud nebyl šifrant na pracovišti, musel ho OD smluveným způsobem povolat. Na zavádění strojů ŠD1 se podílel z ŠO GŠ kpt. Racek (spolužák ze zákl. kurzu), který později přešel na řízení a mat. zajišťování spojení ZAS k velitelství spoj. vojska (v té době byla ŠO součástí spoj. vojska).

16) Někdy kolem r. 1965 byly stroje ŠD1 nahrazeny stroji ŠD3 opět české výroby. Byly odvozeny od již zavedeného reléového dálnopisu s číselnicí k přímé volbě účastníka. Reléový dálnopis s válcovými mechanickými díly, ozubenými převody a číselnicí prý vynalezl nějaký německý inženýr[6] (to mám od mechanika Rosy z ŠO v Příbrami). Stroje ŠD3 užívaly k šifrování opět kotouč pětistopé heslové děrné pásky. Byly vyrobeny z lehkých kovů, rozměru cca 40x45x35 cm, s mnoha mech. a el. díly; zaoblený povrch byl natřen šedým nebo zeleným čeřínkovým lakem. Stroj byl připevněn k základně laminátového krytu téže barvy a přikrýván víkem s klapacími uzávěry, sklopnými držadly a miskou k zapečetění. Ve vozidle se upevňoval ke stolu řemeny. Oproti dálnopisu měl rozšířenou levou a zadní část (měl více relé). V levé horní odklopné části byly držák kotouče heslové pásky, snímač s řezačkou užité heslové pásky (u novějších strojů byla řezačka vypuštěna) a zleva na boku měl vestavěnou víceřadou zásuvku k připojení vysílače děrné pásky. Na čelní straně byla vystouplá zešikmená klávesnice, vpravo pákový přepínač s miliampérmetrem a pod klávesnicí vysouvací zásobník dálnopisné pásky. Nad klávesnicí uprostřed čela byla číselnice a pod ní vedení dálnopisné pásky se zakrytým tiskacím mechanismem (typovým kolečkem a kladívkem) a také páčka k přepínání plynulého tisku či tisku do skupin. Na horní ploše byl sklopný pultík. Vzadu byla dálnopisná zásuvka kam se zasouval vlastní linkový kolík při předběžném šifrování (místo do linkové zásuvky) a pak kabely - linkový s kolíkem a síťový s vidlicí.

Stroj se užíval k přímému šifrovému spojení a k předběžnému za- i od- šifrování klávesnicí (včetně tištěných skupin na pásce). Otevřený text určený k aut. odeslání přídavným vysílačem se musel předem naděrovat na jiném zařízení, jelikož stroj ŠD3 neměl děrovač (nepamatuji, jak se tehdy páska předděrovávala, později se děrovala dálnopisem Siemens). Ve výbavě bylo pouzdro se dvěma klíčovacími relé, náhradní uhlíkové kartáče motorku, ladička otáček, dvě tuby s olejem, šroubovák a štětec s hadříkem - vše v podélném pouzdru z umělé hmoty. Stroj byl dost citlivý na hrubé zacházení a hodně se využíval v polních podmínkách (převážně ve skříňovém vozidle, s připojením k radiostanici R-118). Nejvíce zlobily jeho válečkové spínací

[6] ***Poznámka Mgr. Karla Šklíby*** : Podle dostupných informací to byl Ing. Weber, který byl údajně před válkou šéfkonstruktérem šifrátoru ANNA. Tento šifrátor měl 12 disků a byl používán Rommelovou armádou v severní Africe. Řada trofejních kusů se dostala po válce i do Československa a byla používána v čs. armádě (o šifrátoru ANNA se připravuje samostatný článek). Ing. Weber se později stal šéfkonstruktérem československého (armádního) dálnopisu Dalibor, o kterém je zřejmě řeč v tomto odstavci. Mechanické konstrukční části dálnopisu Dalibor byly extrémně náročné, některé rozměry ve výkresech byly uváděny v mikrometrech. Mezi konstruktéry se spekulovalo, proč zůstal Ing. Weber v Československu. Říkalo se, že mechanická náročnost konstrukce dálnopisu Dalibor znemožní sériovou výrobu tohoto dálnopisu v České zbrojovce Brno. Tento dálnopis však byl vyráběn ve velkých sériích a v armádě byl používán až do 80. let. (Postupně byl nahrazován licenčním dálnopisem Siemens T 100). Druhý Ing. Weber, který byl bratrem šéfkonstruktéra dálnopisu Dalibor, pracoval jako šéfkonstruktér u firmy Standard Elektrik Lorenz (SEL), což byl jeden ze dvou největších výrobců šifrovacích zařízení v tehdejším západním Německu. Je tedy možné, že konstruktérem ANNY byl tento druhý Ing. Weber.

magnety. Stroje ŠD3 se užívaly snad do r. 1980, kdy začalo jejich nahrazování stroji s optickými snímači děrné pásky.

17) Když ještě neměli šifranti vlastní pojízdné ŠO, byla jim vyhrazována kabinka štábního autobusu operačního oddělení. Tam měl i ŠD3, napojený na radiostanici R118. Jinak měl k dispozici stan a bednu s materiály. Často před přemístěním velitelského stanoviště se nashromáždilo u šifranta několik zpráv k odeslání a štáb pak musel na něho čekat, až je odešle. Rádiospojení však často nebylo spolehlivé, zpráva se musela z důvodu rušení odesílat opakovaně. Stávalo se, že během přesunu zachytila radiostanice šifrogram a motospojka ho za přesunu doručila šifrantovi. Během nejbližší zastávky šifrant musel zprávu ručně dešifrovat, případně po ukončení přesunu si ji nechat zopakovat v přímém strojovém šifrspojení.

Průzkumný prapor naší slánské divize měl předsunuté stanoviště na hraniční čáře u vrchu Tišina v okrese Tachov (naproti výcvikovému prostoru americké armády Grafewöhr a Hohenfels), které jsem na místě vybavil šifrovacím strojem ŠD3 a zajišťoval materiálem. Mým nejbližším ŠO byl rádiový (zpravodajský) prapor v Kladně, s nímž jsme si navzájem pomáhali (např. při výpadku spojení či poruše stroje ŠD3).

18) Kromě strojového šifrování se nadále užívaly heslové sešity s pětimístnými numerickými skupinami (buď bloknoty sovětské výroby, nebo vyráběné ZS MV), listy sešitu byly prokládány černým papírem, čím mělo být bráněno jejich zneužití. Na heslové listy se psal text zprávy převedený na čísla nebo došlý šifrový text a jednotkovým sčítáním se vytvářel šifrovaný či dešifrovaný text. Šifrovaný text (číselné skupiny) se mohl odesílat libovolnými dostupnými pojítky (i oklikami). Sešity i jednotlivé listy podléhaly přísné evidenci (v deníku se uváděly s údaji o zprávách (šifrovkách) zároveň údaje o použitých sešitech a listech). V této době již mělo každé ŠO k dispozici skříňové vozidlo Praga V3S nebo Tatra 805 jako pojízdné pracoviště, vybavené spojovacími rozvody, elektrocentrálou, stabilizátorem napětí, psacím strojem a dalšími prvky k ruční i strojové práci a také k přípravě stravy a k odpočinku.

Některá ŠO měla zdvojené vybavení pro případ mobilizace, kdy mírový zástupce (pomocník) se stával náčelníkem ŠO mobilizovaného útvaru. Zažil jsem vyhlášení cvičné mobilizace, kdy základní vojska svazku vyjela na cvičení, do posádek byli povolání záložníci včetně šifrantů a během tří dnů byl záložní vojskový svazek schopen bojového nasazení, včetně zorganizovaného velení a spojení. K tomu byla organizována pravidelná dvou až třítýdenní cvičení záložních kádrů u svazků i vojsk. Na všech ŠO kde jsem sloužil, jsem takto ročně doškoloval asi 5 – 8 šifrantů v záloze v současných podmínkách, včetně ostrého šifrování, účasti na cvičeních a provádění kontrol.

19) Ze Slaného jsem byl nejprve odvelen do krátkodobého kurzu v Komorním Hrádku, jehož náplní byla práce se sovětským strojem Fialka (M125) a jeho údržba. Byl to zajímavý stroj vzdáleně podobný německému šifrovacímu stroji Enigma. Jeho předností byla multinásobná kombinace tvorby hesla (v komutátoru 30x30, v různém seřazení 10 disků na ose, v nastavení vnitřního dílu každého disku, v nepravidelném krokování při otáčení

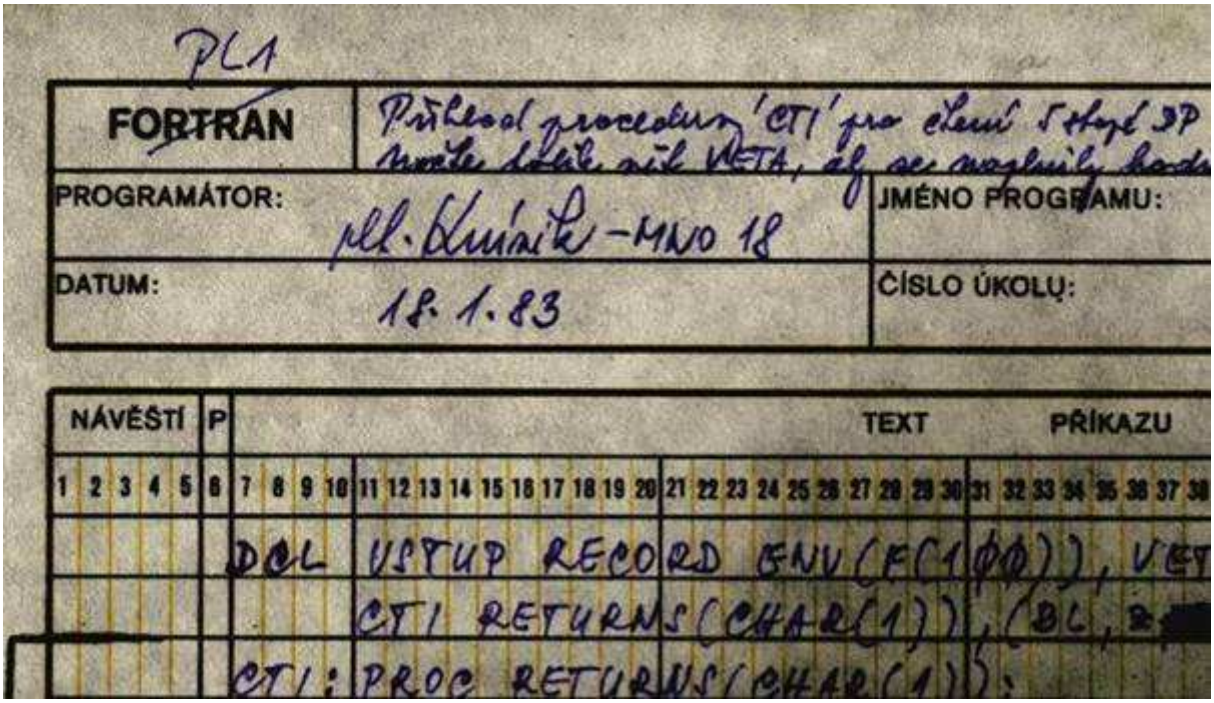
disků a v řízené změně některých kombinací). Stroj má klávesnici se dvěma až čtyřmi abecedami na klávesách a výměnná typová kolečka k tisku znaků na lepicí dálnopisnou pásku v šifrskupinách či v běžném textu a současně má úpravu k děrování a čtení pětistopé děrné pásky. Nejnovější typy (v pozdější době) mohly být přímo připojeny k dálnopisné lince a zároveň provádět šifrování či dešifrování. Fialka byla dodávána v bedně se dvěma stejně rozměrnými vaky k nošení na zádech. Vjednom byl stroj a v druhém příslušenství, a to: napájecí zdrojová skříňka s měřidlem a přepínačem, s uvnitř vloženými kabely a pak ZIP - dva jakési penály - v jednom bylo nářadí včetně pájky a seřizovacích přípravků a v druhém náhradní díly.

20) V letech 1966-8 jsem večerně studoval střední školu a v zápětí po civilní maturitě jsem byl r. 1969 vyslán do ročního akademického kurzu při VA v Komorním Hrádku. Jeho absolvováním jsem získal předepsané vzdělání šifranta v rozsahu VA. Vyučovali nás specialisté pražské VA (vojenské akademie), ŠO GŠ, spojovacího vojska a Zvláštní správy MV. Některé přednášky jsme absolvovali přímo ve VA v Praze. V kurzu jsme zkráceně probírali všechny akademické předměty včetně taktiky na stupni svazku s cvičeními v terénu, zejména pak elektroniku a matematiku včetně entropie. Seznámili jsme se s veškerou soudobou vojenskou sdělovací technikou včetně TV, fototelegrafu a radaru, podrobně pak s šifrovacím strojem ŠD3, o kterém nás školil p. Hrudka.

21) Mezi štáby Varšavské smlouvy byly k šifrování využívány i kódové knihy. Takováto kódová kniha obsahovala několik tisíc výrazů (slov, frází, zkratek, spec. výrazů či hodnot, ap.), každý výraz byl samostatně přeložen do všech jazyků, užívaných mezi štáby. Pro každý jazyk tedy existovaly dvě knihy - "šifrant a dešifrant". Šifrant určitého jazyka obsahoval výrazy v abecedním pořádku s přiřazenými jedinečnými pětimístnými kódy a dešifrant stejné výrazy seřazené vzestupně podle přiřazených kódů. Protože ne každý jazyk řadí slova ve větě stejným způsobem, musel být připojen návod postupu při odchylném tvoření vět v užitém jazyce. Nejsložitěji se spolupracovalo s maďarskou stranou, šifrant se doslova potrápil, než nalezl správný slovosled. V návodu se stanovilo třeba kdy přesunout výraz na začátek či na jiné místo věty, nebo něco do věty přidat či odejmout, atp. Dokonce bylo někdy nutné, aby se dešifrující pracovník osobně s odesílajícím šifrantem spojil a upřesnil význam aspoň v ruštině, která byla jednotícím jazykem. Kde se nedalo najít či použít přesný výraz, pak se věta ve zprávě uvedla rusky. Pro svou těžkopádnost se tato metoda málo používala, třebaže její vývoj a zpracování trvaly několik roků. Z GŠ ČSLA se na tvorbě kolem r. 1970 v SSSR podílel pplk. Hájek, který kdysi jako npor. pracoval na 1. voj. okruhu a zavedl kotoučky s pětimístnými heslovými skupinami (typ Hájek).

22) V r. 1969 bylo nově utvořeno velitelství ZVO v Táboře a za náčelníka ŠO tam byl ustanoven pplk. Pospěch. Novému ZVO byla nově podřízena 1. armáda v Příbrami. Když jsem se posléze z Komorního Hrádku vrátil do Slaného (jako nejlepší žák kurzu), záhy jsem byl ustanoven na uvolněnou funkci náčelníka 8. oddělení 1. td (mjr. Mareš právě odcházel ze zdrav. důvodů do penze). Mnohokrát jsem byl odtud zván nadřízenými, abych v jejich kurzech školil pracovníky v šifrovací technice nebo zabezpečoval (s pojízdným ŠO ve skříňovém vozidle Praga V3S) potřeby některého štábu. Např. při válečné hře VS na Valdeku v Brdech, kde jsem současně zacvičoval 2 šifranty v záloze. Jednou jsem byl odvelen s pojízdným ŠO k cvičně mobilizované divizi do Vyškova, kterou stavělo tamní tankové učiliště. V době sladění štábu jsem musel zpaměti vytvořit nové kódovací pomůcky, protože se na ně v mobilizačních plánech zapomnělo.

23) Po 14 letech služby ve Slaném jsem byl přemístěn r. 1974 ke kódové skupině ŠO v 5. poschodí budovy GŠ, kde byl náčelníkem pplk. Gonda, se kterým jsem kdysi sloužil v Písku. Náčelníkem ŠO byl plk. Nálepka. Na stejném poschodí byla Spojovací správa s velitelem genmjr. Stachem. Tehdy nebyly běžné ani kapesní kalkulačky, potřebné výpočty jsem dělal logaritmickým pravítkem. Z počátku jsem se věnoval vypracování dokumentace k sovětskému stroji M-125 Fialka a poté jsem spolupracoval na tvorbě hesel ke kódovacím prostředkům s Výpočetním střediskem táborského okruhu, vybaveném sálovým počítačem, dislokovaném v Drhovicích (západně Tábora). Tenkrát se instrukce programů nejprve musely z programovacích formulářů pro daný jazyk přenést na děrné štítky a pneumaticky nasnímat do sálového počítače. Začátky byly těžké, programátoři okruhu nezvládali mé kryptografické požadavky. Proto náčelník ŠO GŠ plk. Nálepka dohodl mou spolupráci přímo se ZS MV. Tam působilo několik mých armádních kolegů z dřívějška, např. spojař Malovec, šifranti Málek, Háza, Socha, Vydra a Kubánek (ten se mnou sloužil r. 1960 ve Slaném jako pobočník velitele divize a záhy odešel na studia). Nejbližšími spolupracovníky u ZS mi byli Vladimír Králík a Petr Tesař.


PL1

FORTRAN — Překlad procedury 'CTI' pro členů 5 stupně ZP

PROGRAMÁTOR: pil. Králík – MNO 18 — JMÉNO PROGRAMU:

DATUM: 18. 1. 83 — ČÍSLO ÚKOLU:

NÁVĚŠTÍ	P	TEXT PŘÍKAZU
1 2 3 4 5	6	7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38
		DCL USTUP RECORD ENV(F(100)), VET
		CTI RETURNS(CHAR(1)), (BL,
		CTI: PROC RETURNS(CHAR(1));

24) Začal jsem zároveň vyvíjet a zpracovávat počítačové programy k vytváření matric a automatizovanému tisku heslových sešitů pro různá použití a také nové typy hovorových a signálních tabulek s vysokou bezpečností použití při dodržení stanovených limitů. Stal se ze mne programátor – analytik. Využíval jsem sálový počítač umístěný v budově na nádvoří GŠ nebo podobný počítač zpravodajského oddělení GŠ. Touto výrobou byla nahrazena dosavadní ruční příprava heslových podkladů k hovorovým a signálním tabulkám (a také kódování map) u aktivních šifrantů armády. Kromě toho jsem zpracoval program pro tisk různých heslových sešitů z vícestopé děrné pásky (připravované podle mnou zpracovaného programu na sálovém počítači) pro tiskařský stroj sovětské výroby ve Vojenském kartografickém ústavu, jenž nebyl z nedostatku programového vybavení v automatizovaném provozu využíván.

Zajímavou šifrovací pomůcku jsme připravovali i pro raketová vojska; byly to numerické heslové sešity, z nichž každý řádek sloužil k zašifrování typizovaného povelu (číselný text se zapsal nad řádek a jednotkově odečetl od hesla). Operátoři těchto vojsk je používali s virtuozitou. Podobné pomůcky užívaly i jiné druhy vojsk. Varšavská smlouva vydávala jed-

notné tabulky smluvených signálů „Jsem vlastní letoun“ pro leteckou službu a ŠO GŠ ČSLA vydávalo její překlad našemu letectvu a PVOS (protivzdušné obraně státu). Letec mohl užívat k signalizaci kombinace náklonů letadla a barevných raket.

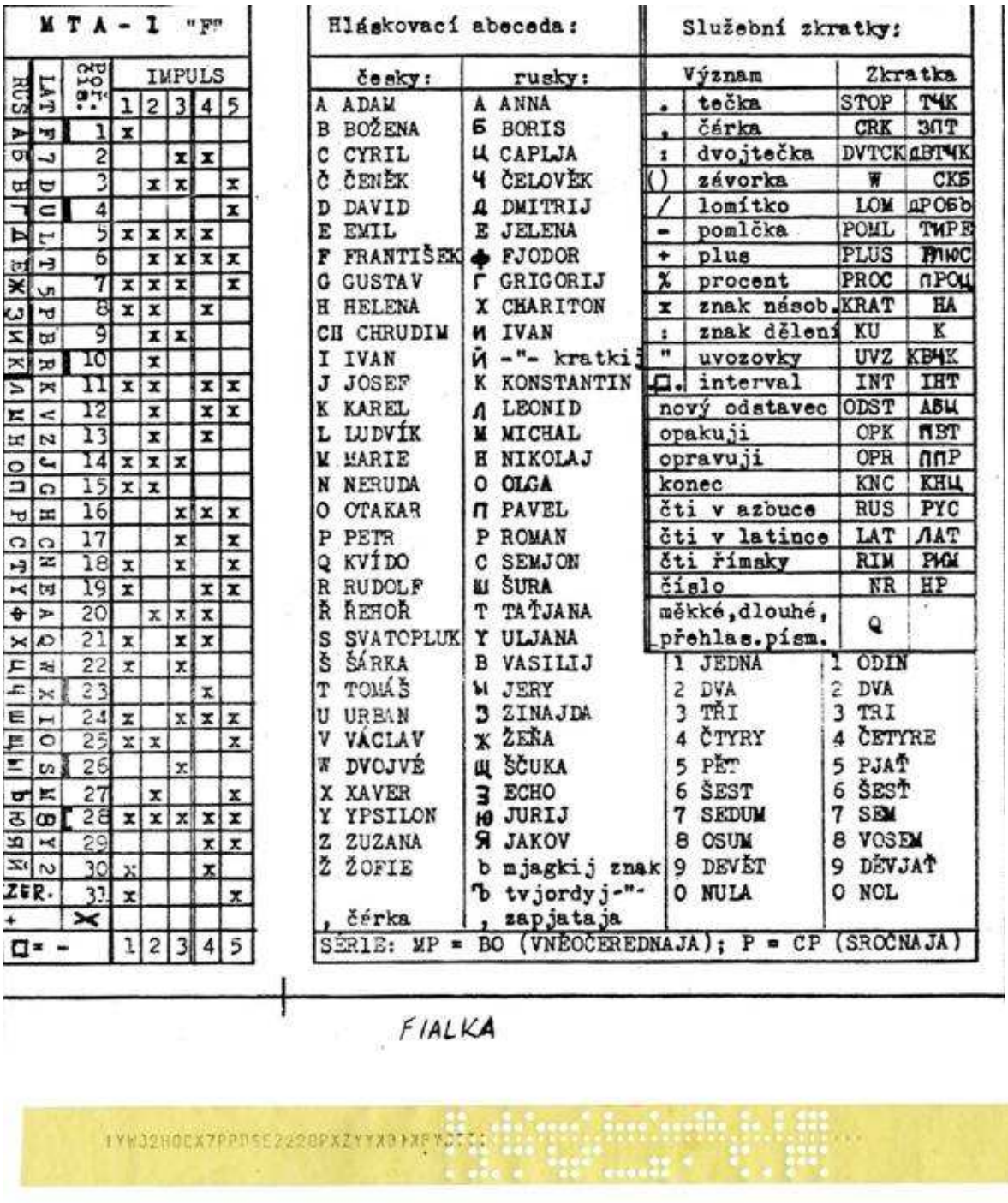
25) V době mého působení na GŠ byly do praxe zavedeny nové ryze české šifrovací stroje vyráběné v Adamovských strojírnách (ADAST), opět jako přídavná zařízení dálnopisu. s podobnými důsledky rušení signálu jako u ŠD3. Na vývoji se podílel technik ŠO GŠ nprap. Milec. Před odesláním bylo nutné zprávu naděrovat na pětistopou pásku. Stroj měl dva optické snímače děrné pásky. Jeden pro heslovou pásku, druhý pro předem naděrovanou pásku s otevřeným (či zašifrovaným) textem. Po navázání dálnopisného spojení šifrant uvedl číslo počátečního úseku heslové pásky a přepnul na automatické odeslání zprávy. Mohl to libovolně opakovat, dokud nedostal potvrzení o odšifrovaní celé zprávy. Odšifrovaná zpráva se musela přepsat psacím strojem na tiskopis Přijatá šifrovka (v nouzi stačilo nalepit dálnopisnou pásku pomocí válečkové lepičky) a podepsat šifrantem. Pochopitelně šifrant pokaždé nastavoval dosud nepoužitý úsek heslové pásky a ihned po zapsání do deníku musel použité úseky heslové pásky a makuláře skartovat.

26) V rámci armád Varšavské smlouvy se především používaly klávesové sovětské šifrovací stroje M-105 pro předběžné šifrování v azbuce, s vkládanou vícestopou heslovou děrnou páskou, dodávanou jak pro směrové, tak i oběžníkové spojení. Stroj tisknul text či pětimístné skupiny na list papíru. Zároveň se užívaly numerické heslové sešity (bloknoty), rovněž pro směrové či oběžníkové spojení. Text se převáděl číselnou převodovou tabulkou, nebo mnohalistovou knihou frází (vydanou pro každý z používaných jazyků) na jedinečné číselné skupiny, čím docházelo při šifrování i k překladu zpráv.

27) Ještě k bloknotům - každý sešit měl své číslo a označení druhu na pevném obalu. Obsahoval 25 - 50 tenkých číslovaných listů s perforací u hřbetu, s natisknutými pětimístnými číselnými skupinami a každý list byl překrytý černým papírkem. Celý sešit byl dokola prošit šicím strojem a zajištěn dokola skrze otvory provléknutou šňůrkou s přelepením úvazku a grafickým přelisováním. Nadřízení museli aspoň namátkou kontrolovat správný způsob zacházení s bloknoty i jednotlivými listy. Než ZS začala dodávat kotouče pětistopé heslové děrné pásky v zavařeném umělohmotném obalu, dodávali ji sověti v obdélníkovém tuhém balení, opatřeném keramickou pečetí.

28) V osmdesátých letech byl v rámci některých druhů vojsk zaveden nejnovější typ šifrovacího stroje Fialka (M-125) a užíván pro přímé i předběžné šifrové spojení u některých bojových a zásobovacích útvarů, včetně možnosti spojení v rámci Varšavské smlouvy. K jeho obsluze bylo vyškoleno několik set administrativních pracovníků, hlavně spisoven. Také pro tento prostředek jsem před jejich zavedením zpracoval českou dokumentaci a pravidla používání. Náčelník ZS MV - tehdy pplk. Ing. Lorenc - si ode mne nechal stroj Fialka předvést. Sám byl vědeckým pracovníkem a zabýval se utajovací technikou.

Pro součinnostní spojení v rámci VS a pro případ válečného konfliktu se používaly disky PROTON. Pro novější typy vyvíjel vojenský výzkumný ústav kolem r.1980 modulované dálnopisné spojení v ČSLA po telefonních linkách, do té doby poště neznámé. Poznamenejme však, že množení kanálů fantomy bylo Němci užíváno již za druhé světové války.



M T A - 1 "F"

RUS	LAT	Poř.	IMPULS 1	2	3	4	5
А	F	1	x				
Б	7	2			x	x	
В	D	3		x	x		x
Г	U	4					x
Д	L	5	x	x	x	x	
Е	T	6		x	x	x	x
Ж	5	7	x	x	x		x
З	F	8	x	x		x	
И	B	9		x	x		
К	R	10		x			
Л	K	11	x	x		x	x
М	A	12		x		x	x
Н	Z	13		x		x	
О	J	14	x	x	x		
П	G	15	x	x			
Р	H	16			x	x	x
С	C	17			x		x
Т	N	18	x		x		x
У	E	19	x			x	x
Ф	A	20		x	x	x	
Х	Q	21	x		x	x	
Ц	R	22	x		x		
Ч	X	23				x	
Ш	I	24	x		x	x	x
Щ	O	25	x	x			x
Ь	S	26			x		
Ы	K	27		x			x
Э	B	28	x	x	x	x	x
Ю	Y	29				x	x
Я	2	30	x			x	
ZTR.		31	x				x
+		X					
□ = -			1	2	3	4	5

Hláskovací abeceda:

česky:	rusky:
A ADAM	А ANNA
B BOŽENA	Б BORIS
C CYRIL	Ц CAPLJA
Č ČENĚK	Ч ČELOVĚK
D DAVID	Д DMITRIJ
E EMIL	Е JELENA
F FRANTIŠEK	Ф FJODOR
G GUSTAV	Г GRIGORIJ
H HELENA	Х CHARITON
CH CHRUDIM	И IVAN
I IVAN	Й -"- kratkij
J JOSEF	К KONSTANTIN
K KAREL	Л LEONID
L LUDVÍK	М MICHAL
M MARIE	Н NIKOLAJ
N NERUDA	О OLGA
O OTAKAR	П PAVEL
P PETR	Р ROMAN
Q KVÍDO	С SEMJON
R RUDOLF	Ш ŠURA
Ř ŘEHOŘ	Т TAŤJANA
S SVATOPLUK	У ULJANA
Š ŠÁRKA	В VASILIJ
T TOMÁŠ	Ы JERY
U URBAN	З ZINAJDA
V VÁCLAV	Ж ŽEŇA
W DVOJVÉ	Щ ŠČUKA
X XAVER	Э ECHO
Y YPSILON	Ю JURIJ
Z ZUZANA	Я JAKOV
Ž ŽOFIE	ь mjagkij znak
	ъ tvjordyj-"-
, čárka	, zapjataja

Služební zkratky:

Význam		Zkratka	
.	tečka	STOP	ТЧК
,	čárka	CRK	ЗПТ
:	dvojtečka	DVTCK	ДВТЧК
()	závorka	W	СКБ
/	lomítko	LOM	ДРОБЬ
-	pomlčka	POML	ТИРЕ
+	plus	PLUS	ПЛЮС
%	procent	PROC	ПРОЦ
x	znak násob.	KRAT	НА
:	znak dělení	KU	К
"	uvozovky	UVZ	КВЧК
□.	interval	INT	ІНТ
nový odstavec		ODST	АБЧ
opakuji		OPK	ПВТ
opravuji		OPR	ППР
konec		KNC	КНЦ
čti v azbuce		RUS	РУС
čti v latince		LAT	ЛАТ
čti římsky		RIM	РИМ
číslo		NR	НР
měkké, dlouhé, přehlas. písm.		Q	

1	JEDNA	1 ODIN
2	DVA	2 DVA
3	TŘI	3 TRI
4	ČTYRY	4 ČETYRE
5	PĚT	5 PJAŤ
6	ŠEST	6 ŠESŤ
7	SEDUM	7 SEM
8	OSUM	8 VOSEM
9	DEVĚT	9 DĚVJAŤ
0	NULA	0 NOL

SÉRIE: MP = BO (VNĚOČEREDNAJA); P = CP (SROČNAJA)

FIALKA

29) Ve funkci staršího důstojníka kódové skupiny 8. oddělení GŠ jsem dosáhl hodnosti plukovníka. V době mé služby na ŠO GŠ museli všichni vyškolení šifranti navíc podle plánu vypomáhat na odděleném strojovém šifrovém pracovišti v přízemí budovy GŠ a ve službě pomocníka operačního dozorčího GŠ. Protože jsem byl na všechnu odbornou práci plynoucí z dané funkce (včetně práce na sálovém počítači) sám, pro své přetížení jsem raději na vlastní žádost odešel k 1. 1. 1984 do důchodu. V té době byly na ŠO GŠ rozpracovány další utajovací technické prostředky, čímž se zabývala zejména skupina plk. Kareše.

C. O čem jsme psali v říjnu 2000 – 2006

Crypto-World 10/1999

Crypto-World 10/2000

Příloha : ZoEP.htm

Dnešní užitečnou přílohou je plné znění zákona č.227/2000 Sb.- "Zákon o elektronickém podpisu a o změně některých dalších zákonů (Zákon o elektronickém podpisu)", který nabyl účinnosti 1.10.2000.

Crypto-World 10/2001

Příloha : Vyhláška 366/2001 Sb. (366_2001.pdf)
(prováděcí vyhláška ÚOOÚ k Zákonu o elektronickém podpisu č.227/2000 ve tvaru předaném k vyhlášení ve Sbírce zákonů)

Crypto-World 10/2002

Crypto-World 10/2003

Crypto-World 10/2004

Příloha : J.Pinkava - Hashovací funkce v roce 2004 , hash_2004.pdf

Crypto-World 10/2005

Příloha : Další informace k článku V.Klímy - prilohy.zip (53 kB)
(Obsahuje: Žádost a podpisy odborníků, Návrh Šámal, Návrh Smejkal, Návrh VK_IURE, překlad části úmluvy, průvodní dopis vk_iure, link psp, stenozáznam jednání PSP, tisk zpráva ČTK)

Crypto-World 10/2006

Příloha: doprovodné materiály k Soutěži v luštění 2006 - vystava.pdf , epilog.pdf

D. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:
http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	Jaroslav.Pinkava@zoner.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info ,	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/