Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 10, číslo 12/2008 **15. prosinec 2008**

12/2008

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese

http://crypto-world.info

(1302 registrovaných odběratelů)

Obsah : **str.**

Příloha:

1) simulátor šifrátoru Lorenz SZ40
   http://soutez2008.crypto-world.info/pribeh/lorenz.zip
2) nastavení pro řešení soutěžních úloh 07,14,15,01 **set.zip**

A. Závěr soutěže 2008, úlohy, použité systémy, řešení, komentáře řešitelů …

Pavel Vondruška a řešitelé

Vážení čtenáři, minulý měsíc skončila soutěž v luštění jednoduchých šifrových úloh, kterou již tradičně vždy na podzim náš e-zin pořádá. Všem úspěšným řešitelům ještě jednou blahopřeji.
V tomto čísle získáte kompletní přehled o použitých šifrových systémech, použitých klíčích, informace o konkrétním nastavení šifrátoru SZ40, přehled otevřených a šifrových textů, přehled zdrojů, na které jednotlivé úlohy odkazovaly, a přehled nastavení, která zde byla ukryta. Pokud jde o odkazy na cílové adresy s uloženými nastaveními jednotlivých kol, pak je domluveno, že zde tato nastavení budou nejméně do poloviny ledna 2009, pak budou z některých odkazů postupně odebrány. Z tohoto důvodu je vždy přiložen screenshot se stavem v době soutěže.
Za jednotlivými úkoly jsou uvedeny některé vaše komentáře a připomínky, které jste mi zaslali a za které velice děkuji.
Mé komentáře k úlohám byly v podstatě již zveřejněny a to „ústy“ Johna Wellingtona v nápovědách, které zazněly v doprovodném příběhu. Celý příběh je k dispozici i v tomto čísle nebo na stránce soutěže http://soutez2008.crypto-world.info/ .
Děkuji za pochvalu soutěže a samozřejmě i za kritiku. Připomínky se pokusím v příštím roce zapracovat.

Nyní začneme popořadě probírat jednotlivé úlohy. Výjimkou je samozřejmě úloha číslo jedna, která šla vyluštit až po vyřešení všech úloh číslo 2-14 a je tak vlastně ve skutečnosti úlohou závěrečnou.

Úloha č.2

Šifrový text
. SIER . ETEJUBERTOP OC , EDZ ETEDJAN . END OHEVOKIVCYV OHETAVED Z ANEMJEZ , IIRELAGOTOF EVILCEP IMLEV TUONDELHORP IS IJUCUROPOD . IGF - KISALK LAHTSIAG INADAROP ATSIM ELDOP LAVYZAN ES ROBAT . AKJOS MINECANZO MYVODOK S UONIPUKS OHENADAROP AROBAT OHEVOKIVCYV OHINTEL LINTSACUZ ES MESJ OTEL OTOT

Systém: Celý text napsaný pozpátku
Upřesnění: testovací příklad pro uživatele
Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (2)
Správná odpověď: LETO
Body: 1

Vyluštěný otevřený text:
Toto leto jsem se zucastnil letniho vycvikoveho tabora poradaneho skupinou s kodovym oznacenim SOJKA. Tabor se nazyval podle mista poradani Gaisthal Klasik - FGI. Doporucuji si prohlednout velmi peclive fotogalerii, zejmena z devateho vycvikoveho dne. Najdete zde, co potrebujete. Reis.

Cíl: http://sojka.cz/fotogalerie/klasik/2008/den9.htm

Zisk vzorku:

Délka vzorku/pořadí kola	Vzorek
29/3	10001000101010000111101010101

Komentáře řešitelů:

koc:
Řešení triviální. Nakonec jsem se podíval i na obrázek na webu, našel jsem binární kód a tak jsem si jej schoval.

Úloha č.3

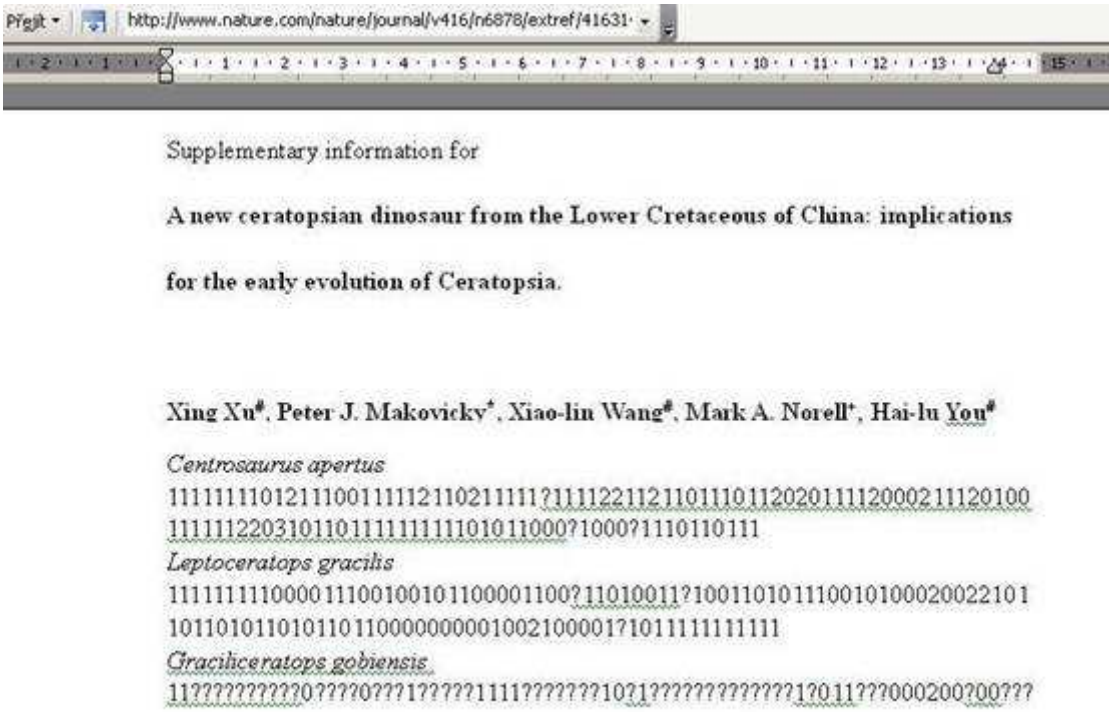
Šifrový text
ZIJUCUROPODW ZESW ZTAVYBAZW ZYTADW ZHCYLERMYVW ZURUASONIDW ZISPELJENW ZECARPW ZUORETKW ZMESJW ZANW ZOTOTW ZAMETW ZLTECW ZEJW ZGNIXW ZUXW ZRETEPW ZJW ZYKCIVOKAMW ZAW ZLOPSW ZSW ZMEVZANW ZYRATNEMELPPUSW ZNOITAMROFNIW ZROFW ZAW ZWENW ZNAISPOTARECW ZRUASONIDW ZMORFW ZEHTW ZREWOLW ZSUOECATERCW ZFOW ZANIHCW ZEDZW ZKAPW ZIJUCUROPODW ZESW ZTAVIDOPW ZMISVEDERPW ZANW ZUOVOTADW ZURUTKURTSW ZARUASONIDW ZSPOTARECOTPELW ZSILICARGW ZETICRUW ZSAVW ZOTATW ZATADW ZUOMJUAZW ZAW ZUODUBW ZESW ZMAVW ZVW ZISLADW ZISAVW ZEKCEDEVW ZICARPW ZTIDOHW ZECARPW ZEJW ZOTSACW ZANAVOTICW ZMISORPW ZETJEZAHCYVW ZZW ZULANIGIROW ZETANZOPW ZJEJW ZELDOPW ZOHOTW ZEZW ZEJW ZEVW ZUTAMROFW ZCODW ZSIERW

Systém: Jednotlivá slova napsána pozpátku + použito obložení písmeny Z a W

Upřesnění: druhý testovací příklad pro uživatele
Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (D3)
Správná odpověď: DINOSAURU
Body: 1

Vyluštěný otevřený text:
Doporučuji se zabývat daty vymřelých dinosaurů . Nejlepší práce, kterou jsem na toto téma četl je Xing Xu , Peter J. Makovicky a spol. s názvem Supplementary information for A new ceratopsian dinosaur from the Lower Cretaceous of China. Zde pak doporucuji se podívat především na datovou strukturu dinosaura *Leptoceratops gracilis* . Určitě vás tato data zaujmou a budou se vám v další vaší vědecké práci hodit. Práce je často citována. Prosím vycházejte z originálu. Poznáte jej podle toho, že je ve formátu DOC. Reis .

Cíl: http://www.nature.com/nature/journal/v416/n6878/extref/416314a-s1.doc



Zisk vzorku:

Délka vzorku/pořadí kola	Vzorek
61/6 (1,0)	1111111110000111001001011000011007110100117100110101110010100

Poznámka:
Místo otazníků bude při konkrétní konfiguraci doplněna hodnota 1 nebo 0.
Při jiné konfiguraci lze doplnit hodnoty jiné např. (0,0), (1,1), (1,0).
Řešitel tedy v této úloze nezískal vzorek jednoznačně.
Pro soutěžní úlohu č.1 bude použita konfigurace s volbou (1,0)

Komentáře řešitelů:
koc:
Opět nová procedura na otáčení jednotlivých slov. Práci o dinosaurech jsem našel, ale mátl mě velmi dlouhý kód a v něm otazníky a dvojky.

Úloha č.4

Šifrový text

```
-..-*A...*A.--*A--*A---.*A-*A-...*A.*A-*A*A---*A-*A*A-..-*A...*A.--
*A...*A-.-*A.-*A-*A*A..*A-*A.---*A--*A*A--*A.-*A.---*A-*A-.-*A-.*A.*A.-
..*A*A.-.*A.*A-*A-.-*A-*A*A.-*A-.*A-...*A.--*A-*A.*A-*A*A---.*A*A-..-*A-.-
*A-.*A---.*A--*A.--*A-*A-.--*A.-*A-*A*A-.-*A--.*A.---*A-.-*A--*A.-.-*A-
*A*A.-.-*A-.-*A.-..*A-..-*A.*A...*A.-*A-*A-..*A---*A*A...*A.*A-*A---.*A-.-
*A.*A-*A*A.-*A-*A.-.*A.*A-*A-.-*A.-..*A*A.--*A*A-..-*A-.-*A--*A---*A-..-
*A-*A---.*A.-.*A--.*A*A-.*A*A---.*A.-..*A.---*A-*A-.-*A.*A-*A*A---.*A----
*A...*A.--*A.-*A.-..*A*A--*A.-*A.--*A-*A-.-*A-.*A.*A*A---.*A-*A-.-*A--
*A..*A*A..--*A-*A*A---*A.-*A-.*A.--*A.-*A...*A*A.-*A-.*A-...*A.--*A-*A.*A-
*A*A.*A-*A.-*A*A-..-*A-.-*A-.*A---.*A.-..*A*A.--*A-.*A-..-*A--*A---*A.*A-
*A*A---*A--*A*A.-.*A...*A.--*A*A-.*A.-.*A.-.-*A-*A*A-..-*A...*A-..-*A--*A--
-*A...*A---.*A-.*A.-*A-*A*A---.*A*A--*A.-*A.--*A-*A-.-*A-.*A.*A--.*A*A-.-
*A-*A--*A---*A*A*A
```

Systém: Morse, převrácené znaky tečka a čárka, oddělovací znak *A
Cíl: v každém příspěvku v Crypto-News , vpravo dole, vedle reklam Google (přesně news.doc)

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (P2)
Správná odpověď: POZORNE
Body: 2

Vyluštěný otevřený text:
PODIVEJTE SE POZORNE MEZI INZERATY KTERE NAJDETE V PRAVIDELNE RUBRICE CRYPTONEWS OTEVRTE NEKTERY Z PRISPEVKU A VYBERTE VHODNY INZERAT VERIM ZE SNADNO NAJDETE TEN PRAVY ZAPISTE SI KOD AKCE POPISOVANE V INZERATU REIS

Cíl: v každém příspěvku v Crypto-News , vpravo dole, vedle reklam Google lze najít „reklamu na školení bezpečnosti“.

Po kliknutí na tuto reklamu se objeví připravený text se vzorkem devátého kola uložený na adrese http://soutez2008.crypto-world.info/pribeh/uloha.txt

Školení z bezpečnosti

Dovolujeme si Vám oznámit, že dnem 15.10.1941
začíná povinné přezkoušení zaměstnanců našeho
úřadu z otázek zabezpečení dat a použití šifrátoru SZ.

Účast povinná.

Plán školení:
• Přednáška na téma Způsob ochrany informací na našem úřadě
• Ověření praktických znalostí
• Zašifrování a odšifrování testovacích dat, nastavení ZMUG
• Vydání osvědčení o absolvování kurzu

Číslo kurzu: 0101010111010101010001010100100101001010100101001

Zisk vzorku:

Délka vzorku/pořadí kola	Vzorek
47/9	0101010111010101010001010100100101001010100101001

Komentáře řešitelů:
koc:
Zrcadlová morseovka. Řeší se jednoduše s použitím aplikace stažené z webu. Kód jsem našel docela rychle.

Úloha č.5

Šifrový text

```
TLS QZLT AYVJOB JHZB, H AHR QZLT ZP WHALOV YPQUH GHSLALS SLAHKSLT UH
QLKUVKLUP CFSLA KV PAHSZRLOV TLZAH ILYNHTV. TLS QZLT ZALZAP SLALURF QZLT
ZLOUHS CLSTP SLCUL H AV C HRJP Z UHGCLT HRJL.ULQSLCULQZP-SLALURF.PUMV .
WYVOSLKULAL ZP MVARF G TLOV WYCUPOV VWYHCKB SVDJVZA CFSLAB. UH WVZSLKUP,
VZTL QL CFMVJLUL KLSV. AYLIH GKL UHQKLAL PUZWPYHJP.
```

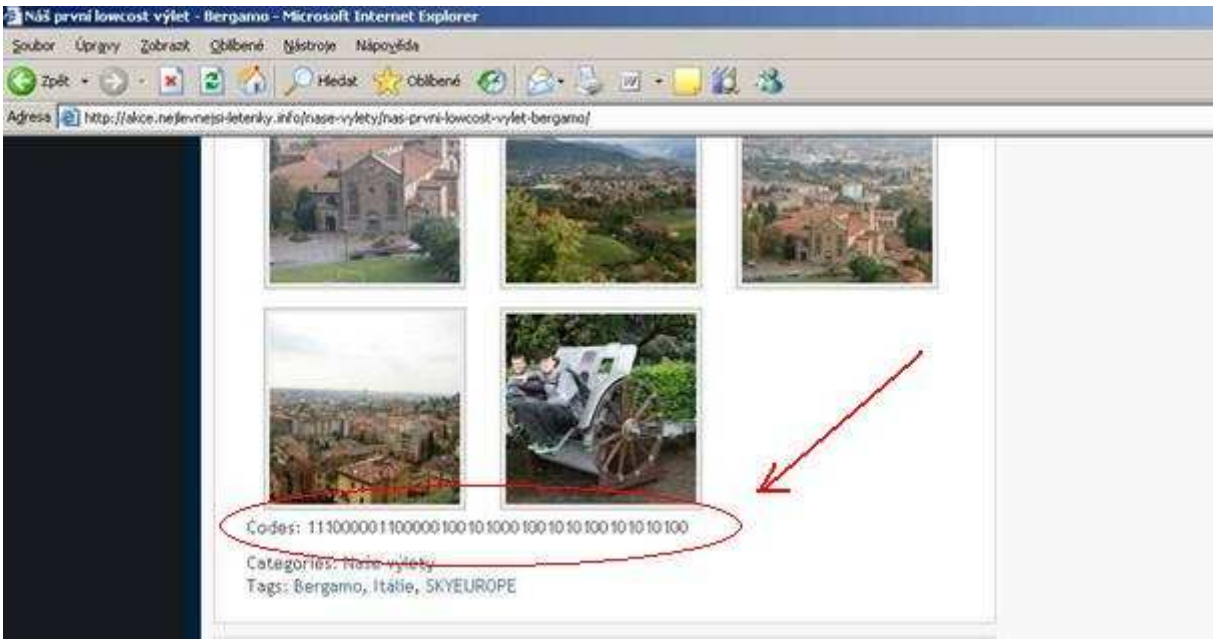
Systém: Jendoduchá záměna, variace na Ceaserovu šifru, posun místo o 3 o 7 znaků
Upřesnění (převodová tabulka):
ABCDEFGHIJKLMNOPQRSTUVWXYZ
HIJKLMNOPQRSTUVWXYZABCDEFG

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: Město?
Správná odpověď: BERGAMO
Body: 2

Vyluštěný otevřený text:
MEL JSEM TROCHU CASU, A TAK JSEM SI PATEHO RIJNA ZALETEL LETADLEM NA JEDNODENI VYLET DO ITALSKEHO MESTA BERGAMO. MEL JSEM STESTI LETENKY JSEM SEHNAL VELMI LEVNE A TO V AKCI S NAZVEM

AKCE.NEJLEVNEJSI-LETENKY.INFO . PROHLEDNETE SI FOTKY Z MEHO PRVNIHO OPRAVDU LOWCOST VYLETU. NA POSLEDNI, OSME JE VYFOCENE DELO. TREBA ZDE NAJDETE INSPIRACI.

Cíl: http://akce.nejlevnejsi-letenky.info/
http://akce.nejlevnejsi-letenky.info/nase-vylety/nas-prvni-lowcost-vylet-bergamo/



Zisk vzorku:

Délka vzorku/pořadí kola	Vzorek
43/8	11100000110000010010100010010101001010101 00

Komentáře řešitelů:
koc:
Posunutá abeceda. Velmi dobře se řeší v Excelu, ve kterém mám svisle text a v dalších 26 sloupcích vždy text posunutý o příslušný počet znaků.

Úloha č.6

Šifrový text

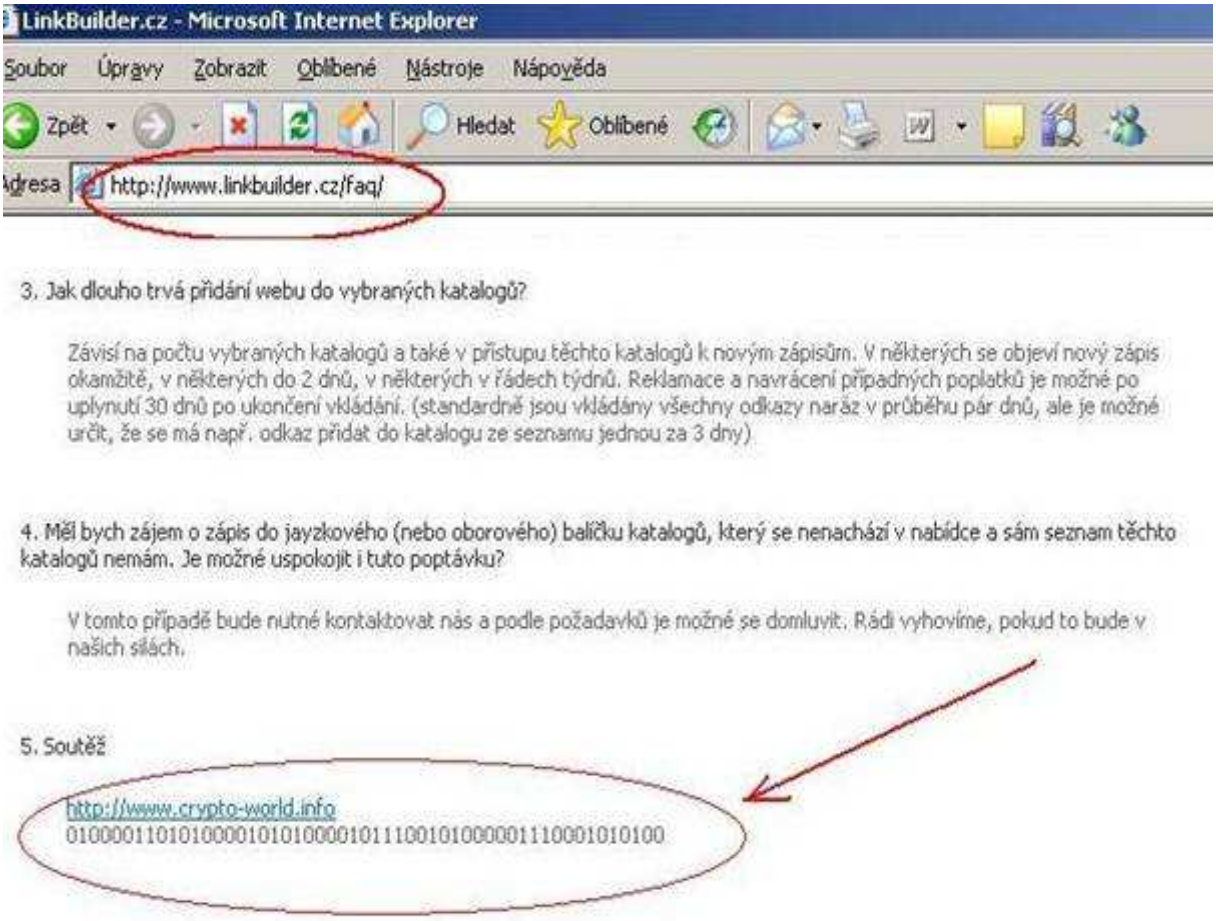
```
6 555 7 666 22 11 555 777 1 444 0 4 6666 22 5 0 8888 4 333 6666 7 333 7 0
55 22 4 1 44 22 0 333 55 222 555 666 5 1 111 22 0 555 44 555 444 555 0 666
22 3 333 6666 7 666 1 111 22 0 55 1 6666 333 111 33 0 55 1 11 333 2 22 44 0
2 555 0 44 1 7 1 444 555 3 77 0 55 1 777 6666 7 333 777 333 444 0 4 6666 22
5 0 6 666 555 7 555 0 111 22 6666 44 555 77 0 6666 6 555 444 22 111 55 555
6666 7 0 444 333 55 44 11 77 333 444 2 22 666 0 8888 2 22 0 4 6666 22 5 0 4
333 5 0 6 555 444 555 8888 333 444 0 6666 777 555 4 22 0 555 7 1 8888 44
888 0 1 0 555 55 333 0 6666 333 0 4 22 0 8888 1 6 6666 1 444 333 0 2 555 0
6666 777 22 33 555 0 222 1 66 0 6 555 2 0 111 333 6666 444 22 5 0 6 22 7 0
5 888 6666 444 333 5 0 8888 22 0 11 888 0 777 1 6666 0 7 555 0 5 555 33 444
555 0 7 1 44 22 0 8888 1 4 333 5 1 7
```

Systém: mobilní šifra (čísla, která mačkáme na tlačítku MT při psaní písmene), kód -1
Upřesnění: mobilní šifra : A = 2 , B=22, C=222, D=3, E=33, …
Upravená mobilní šifra, kód -1 : A = 1 , B=11, C=111, D=2, E=22, …

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: Z1
Správná odpověď: ZJISTIT
Body: 3

Vyluštěný otevřený text:
POTREBOVAL JSEM ZJISTIT NEJAKE INFORMACE OKOLO REGISTRACE NASICH NABIDEK DO KATALOGU NAVSTIVIL JSEM PROTO CESKOU SPOLECNOST LINKBUILDER ZDE JSEM JIM POLOZIL SVOJE OTAZKY A ONI SI JE ZAPSALI DO SVEHO FAQ POD CISLEM PET MYSLIM ZE BY VAS TO MOHLO TAKE ZAJIMAT

Cíl: http://www.linkbuilder.cz/ **,** http://www.linkbuilder.cz/faq/



Zisk vzorku:

Délka vzorku/pořadí kola	Vzorek
53/11	01000011010100001010100001011100101000001110001010100

Komentáře řešitelů:
koc:
Posunutý telefon. Protože byl text příliš dlouhý, tak jsem si napsal proceduru v Accessu, která čísla převedla na text

Úloha č.7

Šifrový text:

```
8T+AKKVTEO SGY/E GIQ3LS OD3AXT8 ZUSH O3AY S+94L BMAV ILKJ Z8XDO HMND 4FAC
+RZLF CMCR+ UNMZS ZAUR 9N4/ QA8SK UDUD DIME8 QDKXL HUNC CCZ8 J4C/ RZRJ M3LC
C3B4E SAJD4 SPQWH RXNE GWED TMOO PGCBI SLBN GOS3/ L/UV 3E9F /UTV JWNHW WNUB
8PIUZ UX+E H+P8 HX9LY L9Z8 /PBZ 3UY+I JHC3 HNUR W98XS MPVV XFBV IQNAP FHDJ
FBDDN 8RJ3 UENJE PSWC4
```

Systém: Lorenz SZ 40
Upřesnění: dešifrace pomocí simulátoru Lorenz SZ 40 a to podle testovacího nastavení ZMUG / set07

Nastavení ZMUG / set07 (vzorky kol + počáteční nastavení) :

```
--------------------------------------------------------------------------------------------------------------
0110011100001110011100001001101100011011O                                    41/1
000110011000101111011100001101l                                               31/2
011110110001110001100011001O0                                                 29/3
10100111010011000110010101                                                    26/4
1010000111010001111001O                                                       23/5
10101011110101011101110111011011011011011101010111011101101101               61/6
1110111011101011011101110110101101010                                         37/7
000111001110011110001100011001110001100l1001011                               43/8
11010011100111001100011110001110011001110001000                               47/9
111001100011000111000100011110001001110011100110010                          51/10
101110011000110010011100110001000111100111001100111100                       53/11
011000100111001100111001100011110010011100111100010001111001                 59/12
Počáteční nastavení:  1 1 1 3 1 21 14 20 38 38 33 46
```

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (3)
Správná odpověď: CVICNY
Body: 3

Vyluštěný otevřený text:

```
ZASIFRUJTE TENTO CVICNY SIFROVY TEXT NULA JEDNA NULA NULA JEDNA NULA NULA
JEDNA JEDNA JEDNA NULA NULA JEDNA NULA JEDNA JEDNA NULA NULA NULA NULA NULA
JEDNA JEDNA JEDNA NULA NULA NULA JEDNA NULA JEDNA NULA NULA NULA JEDNA NULA
JEDNA NULA NULA JEDNA NULA NULA JEDNA NULA NULA JEDNA NULA NULA JEDNA NULA
JEDNA NULA KONEC TEXTU
```

Zisk vzorku:

Délka vzorku/pořadí kola	Vzorek
51/10	010010011100101100000111000101000101001001001001010

Komentáře řešitelů:
koc:
První velký problém. Ze zadání mně nedošlo, že si simulátor můžu stáhnout a používat. Myslel jsem, že až vyřešením všech úloh teprve dostanu přístup k simulátoru. Když mně toto došlo, tak už to bylo jednoduché. Použil jsem testovací nastavení, protože při prvním použití Enigmy to bylo také tak. Konečně jsme také zjistili, na co použijeme uváděné binární kódy:-)
Ovšem několik dnů jsme hledali řešení bez simulátoru a zkoušeli a vymýšleli a nevymysleli ...

Úloha č.8

Šifrový text

```
JMAPU LGRUP QLULP DRUCH URBPL FGRUP QAUAD FAPQH CSLSH PDHCU LDCLE AQULR
TPQLM DAQYE RQQDL OALDS CHTPL CHSQT SBPLF PATJR GRJAG CRUXC HTJAD CMRPG
LZHCH IHTMR PJMLY SAUCH TBLGX PLCRJ DGXFB FLGLF BLGAP LBPAE LMARG PJAMA
QSHJH MTITB AURFU XZDLS RQOHQ HNMRO AAQHZ HQHCH IHTMC RRQHG LBDLJ LGRRT
PQLMD AQYPA ELMAR GRGLI HPAHG LFJML IAPQX
```

Systém: Jednoduchá substituce
Upřesnění převodová tabulka vytvořena pomocí hesla REIS LORENZ = R E I S L O N Z:

```
Plain Text Alphabet:  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher Text Alphabet: R E I S L O N Z A B C D F G H J K M P Q T U V W X Y
```

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (3)
Správná odpověď: NAVSTEVE
Body: 4

Vyluštěný otevřený text:
PRI SVE NAVSTEVE SLAVKOVA JSEM NAVSTIVIL MISTO KDE DOSLO K VELKE BITVE AUSTERLITZ BATTLEFIELD KOUSEK ODTUD JSEM SI U PANA PINKAVY KOUPIL KRASNEHO KOCOURA S PREZDIVKOU JENYSEK A PLNYM JMENEM JENISEJ SIBERIAN SPIRIT DOPORUCUJI VAM VYHLEDAT FOTOGRAFII TOHOTO KOCOURKA A TO NEJLEPE NA AUSTERLITZ SIBERIAN A NECO SI O NEM PRECIST

Cíl: http://www.austerlitz-siberian.cz/kocouri.html

Zisk vzorku:

Délka vzorku/pořadí kola	Vzorek
23/5	10100001110100011110010

Kmentáře řešitelů:
koc:
Jednoduchá záměna. Řešeno strojově velmi jednoduše a rychle.

Úloha č.9

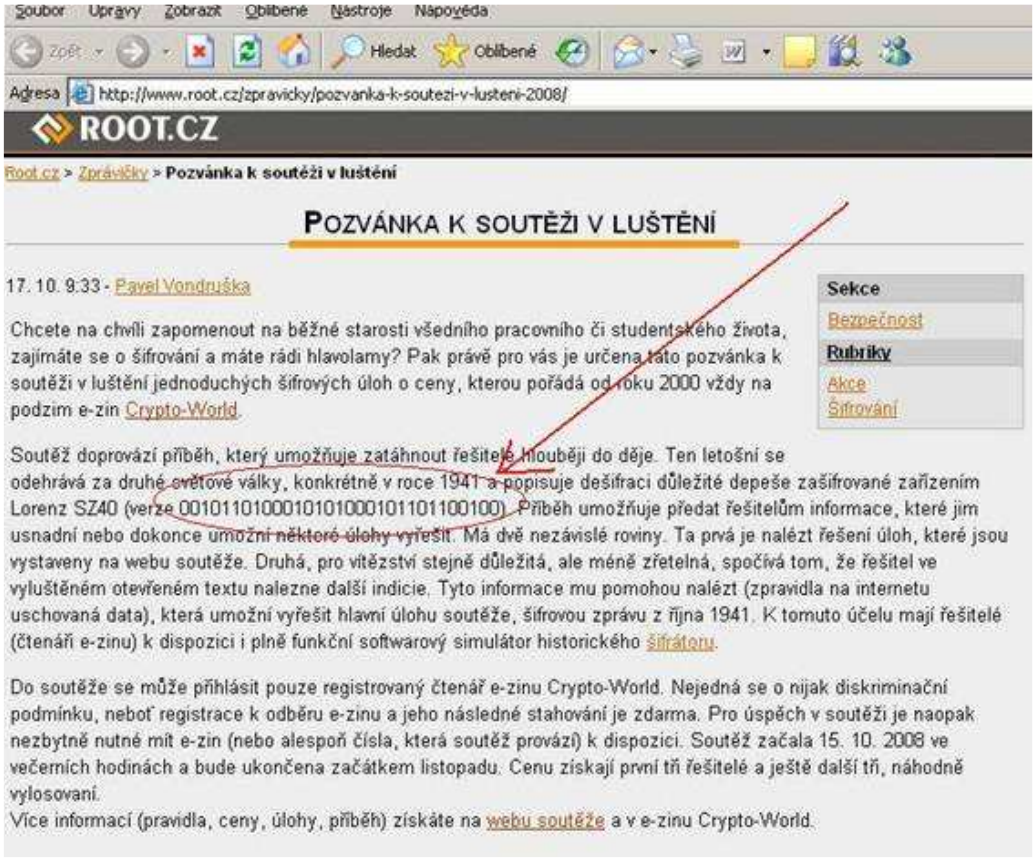
Šifrový text

```
EAHJR EIEMO MKAKY AATVR NEZEE SAUEZ EVIZM SZVUO TLKDE PAODZ DCONE TVSOR
TUNTS BSESO IZMNR ITLNT RASAE LEADD EAHEV RCROX SNEIP TSNIB ESLKR ZVUIF
AJENV ERRRS VEJEJ YMEBH TCEET ZVKNC MTRAC EDNDN ICEEE YOZIV ADIAZ FOOZA
ZSTUM ISMEI NNLJE AHETX
```

Systém: Jednoduchá sloupcová transpozice
Upřesnění: Rozměr tabulky 4x50, na úplnou tabulku doplněno pomocí XX
Heslo pro transpozici: REIS
Heslo po vyčíslení (určující přeskupení sloupců): 3-1-2-4

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (-3)
Správná odpověď: KOREN
Body: 4

Vyluštěný otevřený text:
SEDMNACTEHO RIJNA , PRECTETE SI V DNESNIM ODBORNEM TISKU CLANEK, KTERY SE ZABYVA SOUTEZI V SIFROVANI A JE ZDE ZMINENA VERZE SIFRATORU LORENZ SZ. TA VERZE VAS JISTE ZAUJME. MYSLIM, ZE SE VAM BUDE HODIT. TEN CLANEK HLEDEJTE VE ZPRAVACH KOREN DOT CZ.



Cíl:
http://root.cz/
http://www.root.cz/zpravicky/pozvanka-k-soutezi-v-lusteni-2008/

Zisk vzorku:

Délka vzorku/pořadí kola	Vzorek
31/2	00101101000101010000101101100100

Komentáře řešitelů:
koc:
Opět použita procedura, která umí text rozdělit do sloupců a vypočítat poměry souhlásek a samohlásek. Předávám hledání řešení manželce, která pokračuje v Excelu, kde se dobře přehazují sloupce. První pokusy s 10 a 20 sloupci byly velmi těžké a nevedly k výsledku. Nakonec při 4 sloupcích to bylo zase velmi jednoduché a rychlé.

Úloha č.10

Šifrový text

```
MGIKF TQKVO BWICA WQEJQ MEJWQ TMUES ALZER EVRCB VWMKF SUBJI UKZTZ WTIBD
TPIFV OWVRY BGIEK ULQQF EEAFR DDWDS KWDLI UBMVY MPIKK RMBVE HVVZW VJXIN
TMHAM SBEVD QCIEJ ATIUA AWMEE EAWCO ZSSMK AJRIH ZWMEB VGHKS TGXMM TPPBG
JPIKK RGHFG QLAES GBHGR YSZGC IHWTH WKRLV WMVKZ FPSMY SZQKE SBJIU KVNIH
ISJJR PIREE ASDIR SUVWA EJWJD EKWEM KEVRM HIMKW JXMRR XWMKS SJRWV GLOWF
TSDGL OZSSM KCFYR KVQHS JIJGL RMUYE TKKSD CPFIV FOWFT IBAJM KWUET KZGPC
KIZWA WMEMC JSCMT SCIVW JXQZC NMGKI DJZXU SAMZM QRMNV PQCFW BAGSL DVRQU
YDAWU EWVYE LGMEB EESHK KZQCI EJATI SCKIZ WAIAL VYSJP ZIBZN MBZGP ZFHVW
```

Systém: polyalfabetická periodická šifra, systém Vigenére
Upřesnění: periodické heslo REIS

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (2)
Správná odpověď: CASOPISE
Body: 4

Vyluštěný otevřený text:

```
V CASOPISE KTERY SE ZABYVA BEZPECNOSTI A JMENUJE SE SOOM JSEM SI PRECETL
CLANEK OD AUTORA CCUMINNA S NAZVEM O CEM HACKING VLASTNE JE A ZDE V
ODSTAVCI ZIVOT MEZI KRABICEMI JSEM NASEL KRABICI S NAPISEM KRYPTOLOGIE BYL
TO SLASTNY POCIT JAKO KDYZ HOROLEZEC DOSAHNE VRCHOLKU HORY TAK JSEM SE JA
PROBRAL AZ NA SAME JADRO INFORMACE NICMENE PRI CESTE ZA TOUTO KRASNOU
KONCOVOU KRABICKOU JSEM ZA SEBOU NECHAL STOVKY BA DOKONCE TISICE DALSICH
KTERE JSEM VYBALIL ALE NESTIHL JE OTEVRIT MAJI RUZNE VELIKOSTI PODLE NICHZ
SE DA ODHADOVAT MNOZSTVI KRABICEK KTERE JESTE UKRYVAJI JE JICH HODNE
```

Cíl:
http://www.soom.cz/ , http://www.soom.cz/index.php?name=articles/show&aid=306

Zisk vzorku:

Délka vzorku/pořadí kola	Vzorek
41/1	11000111010101001110001001000100010010100

Komentáře řešitelů:
koc:
Vigenere. Zase řešeno strojově s náhodným zkoušením klíče. Asi třetí pokus vyšel.

Úloha č.11

Šifrový text
`Lze uDILet rAdy ALE neni MozNo nAucit JedNat.`
Co hlEDAs? ruKavICE. koliK? jeDnu. Tu mas Na rUce

Systém: steganografie,
získání vzorku z písmen publikovaného textu, použito toto kódování:
malá písmena znamenají 0 a velká 1

Upřesnění:
Vzorek byl zakódován dvakrát za sebou.
Použitý text částečně upozorňuje na to, že to není šifra a řešitel nevidí, co by měl vidět.
`LzeuDILetrAdyALEneníMožNonAučitJedNat.`
`CohlEDAsruKavICEkoliKjeDnuTumasNarUce.`
`10001110001001110000100100100001001000`

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (3)
Správná odpověď: RADY (třetí slovo textu ve kterém je zakódován vzorek)
Body: 3

Zisk vzorku:

Délka vzorku/pořadí kola	Vzorek
37/7	1000111000100111000010010010000100100

Komentáře řešitelů:

koc:
Tak jako John Wellington jsme to četli asi 100x. Když jsem zjistil, že obě věty jsou stejně dlouhé, mají stejně velká a malá písmena a počet písmen odpovídá chybějícímu kódu, tak mně to konečně trklo:-)

Gimli2:
Tak dnesni ulohy, moc zabrat nedaly. Chvalim tu konfiguraci u 11ky. Nez mi doslo, ze je 2× zopakovana... ;-)

Vondruška:
následuje zajímavé „řešení“ této úlohy, kterou nalezl pozdější celkový vítěz soutěže.

Ony:
Dobrý den!
Chci se s Vámi podělit o řešení úlohy číslo 11.
Ihned jsem viděl, že text lze rozdělit na dvě části, které si odpovídají velikostí písmen.
LzeuDILetrAdyALEneniMozNonAucitJedNat
CohlEDAsruKavICEkoliKjeDnuTumasNarUce
Pokud text převedu do morseovy abecedy podle velikosti písmen, dostanu
-...---... -..---....-..-..-....-..-..
Což při troše snahy se dá rozdělit na jednotlivá písmena následujícím způsobem:
-././.---/.../-/.//.---/./.../-/.//.-././-../../-/./.-..
Převedeno na písmena vyjde text "NEJSTE JESTE REDITEL", tedy smysluplná česká věta. Vůbec jsem nechápal, proč mé řešení je označeno jako špatné, ale byl jsem přesvědčen, že jsem na správné cestě. Ale tahle šifra, to byl těžký chyták. To jsem opravdu nečekal. :-)
Ondra

room132:
Ta uloha 11 chce evidentne napad a pak to musí jit samo. Ja uz se trochu tocim v kruhu takze to odlozim a zkusim ktomu pristoupit s cistou hlavou. Miminalne vim, ze po polovine techtu se opakuje vzorek velkych a malych pismen. Vyjadreno v morseovce:
LzeuDILetrAdyALEneniMozNonAucitJedNat
CohlEDAsruKavICEkoliKjeDnuTumasNarUce
.---...---.--...----.--.--.----.--.--
.---...---.--...----.--.--.----.--.--
V nejhorsim pockam na napovedu, za coz se teda stydim :-).
Zdravi osef Mika

Úloha č.12

Šifrový text

```
XXXSI ERYLP MISSI MONEM JIJEJ INAKY VUJEL ECUMI TAZTA VDSEM GICKI LOTEN
NOOPO JAOKA TIPME SECAI DSRUE VMESJ MJDNN MVEER LUEND OELMO UEYMT IMSAR
PPKAI KORKN ZTITC UJIAC RSNOA AEVNA LYMTL AUMEL NLJEE RVOZN IZOIR AIESL
MIKOU RITKT ELNZE MSERO ZHODL SMSAL CESKO UFIRM UZAES ELJSE MJIPO MOCIH
```

Systém: šnek od středu obrazce, tabulka 15x16

Upřesnění:
XXXSIERYLPMISSIM
ONEMJIJEJINAKYVU
JELECUMITAZTAVDS
EMGICKILOTENNOOP
OJAOKATIPMESECAI
DSRUEVMESJMJDNNM
VEERLUENDOELMOUE
YMTIMSARPPKAIKOR
KNZTITCUJIACRSNO
AAEVNALYMTLAUMEL
NLJEERVOZNIZOIRA
IESLMIKOURITKTEL
NZEMSEROZHODLSMS
ALCESKOUFIRMUZAE
SELJSEMJIPOMOCIH

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (1)
Správná odpověď: PRACUJI
Body: 4

Vyluštěný otevřený text:
PRACUJI POD NEUSTALYM TLAKEM JSEM VELMI NERVOZNI ZACAL JSEM PIT A KOURIT VELMI KOURIT KOURIM DENNE TOLIK CIGARET ZE JSEM SE ROZHODL S TIM SKONCOVAT ZA TIM UCELEM JSEM NALEZL CESKOU FIRMU ZAMERENOU NA ODVYKANI JEJI JMENO JE ODVYKANI NASEL JSEM JI POMOCI HESLA LOREM IPSUM IS SIMPLY REIS

Cíl: http://odvykani.cz/

Zisk vzorku:

Délka vzorku/pořadí kola	Vzorek
26/4	00000111000001111100001010

Komentáře řešitelů:

koc:

Začátek textu pozpátku, konec textu dobře, objevují se celé části vět a slov. Zkouším přehazovat pořadí písmen, ale nedaří se. Listuji několikrát v knize šifer a nakonec mě napadlo, že by to mohl být šnek. A pak už to bylo jednoduché.

Úloha č.13

Šifrový text

```
ZCTKP AYAIP JNIJP NKMEK ZLCYT AAYID MNTAO KEYYV RLAAO OIOHD PRCJJ JYLDT
EADTT NRVUC TPZAE AAEUM TSOOS CPTEU EEOEZ RVYAP CNKTJ BROOE VRKEA ZDTKT
TNOEI RYAPE EEJNZ AEHVE IUUOO ISRHT MMYIO TVRTR TRSOE SSLNO PRIAA UNASO
AZCEO SSNVR ZEAA
```

Systém: čtou se písmena střídavě odpředu a odzadu šifrového textu …

Upřesnění:

Jedná se o falešnou stopu, data na odkazované stránce se neustále mění a nelze je tedy použít jako vzorek kola (viz později zveřejněná nápověda) .

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (6)
Správná odpověď: JAPONSKA
Body: 3

Vyluštěný otevřený text:

ZACATEK ZPRAVY NASI SPOJENCI Z JAPONSKA MNE UKAZALI CRYPTOANALYSIS DEMONSTRATOR KTERY VYTVORIL YAMAMOTO HIROSHI DOPORUCUJI JEJ VYHLEDAT ZE NAJDETE TEN PRAVY URCITE POZNATE TAK A TED UZ MATE SKORO VSE CO POTREBUJETE KONEC ZPRAVY

Cíl: **http://www.itl.dm.u-tokai.ac.jp/~hiroshi/cgi-bin/crypto.cgi**

Komentáře řešitelů:

koc:

Zepředu zezadu. Snadné. Našel jsem stránku a opsal kód. Pak při kontrole a dalším otevření stránky jsem zjistil, že vrací jiná čísla. Nakonec jsem zjistil, že v odkazu v Googlu je kód stále stejný a tak jsem si jej zapsal. Zbytečně.

Pergel:
Dobry vecer,
musim rict, ze se letosni soutezi bavim. Ulohy jsou pro me pravda skoro az moc jednoduche, ale chapu Vasi motivaci...

Tesil jsem se, ze az budu znat vsechny vzorky, zmatu soupere tim, ze vyresim ulohu c. 1 bez znalosti reseni uloh obsahujicich nastaveni. Dneska jsem se tedy do toho pustil, ale neuspel jsem. Vsechno jsem po sobe prekontroloval a eliminoval mozne priciny na:

a) zacatek otevreneho textu ulohy c. 1 neni "patnacteho rijna tisic devet set ctyricet jedna" (to bych ale byl velmi prekvapeny, protoze delky slov sedi)
b) "dinosauri" vzorek z ulohy 3 netvori pocatecni usek sekvence z toho dokumentu o dinosaurech
c) mam spatny vzorek z posledni ulohy. Teto moznosti verim nejvic. Pri kontrole vsech vzorku jsem si vsiml, ze na strance Cryptoanalysis Demonstrator se pri kazdem zobrazeni vygeneruje jina posloupnost nul a jednicek. Zkusil jsem pouzit i tu, kterou ma v archivu google, ale ani ta nefungovala, a jinou, statickou, jsem tam nikde nevidel.

Zdravi
P. Vesely

jomako68:
Dobry den!
Mam jednu otazku ohladne 13-tej ulohy sutaze. Samotna uloha bola trivialna a jej zapisanie mi zabralo vyrazne viac casu ako jej vyriesenie.
Horsie je to uz s tym co sa tam pise. Na internete som totiz nasiel len JEDINY cryptoanalysis demonstrator, ktore autorom je Yamamoto Hiroshi:

http://www.itl.dm.u-tokai.ac.jp/~hiroshi/cgi-bin/crypto.cgi

Je to akysi program na predvadzanie lustenia sifry Vigenerovho typu, pouzivajucu ASCII abecedu. Ako ukazkove sifrove texty sa tam striedaju viacere texty (ja som napocital 20 roznych a potom som uz dalej na to nemal cas), z ktorych niektore som skusobne aj vylustil, ale nenasiel som ziaden suvis so sutazou.
Predpokladam, ze ten demonstrator ma nejaku konecnu databazu vstupnych textov, z ktorych nahodne vybera.
Takze moja otazka. Som uplne na zlej adrese, alebo sa ocakava, ze treba vylustit tie sifrove texty a v niektorom z nich bude informacia tykajuca sa sutaze? Dakujem.
Pozdravuje Vas
Jozef Kollár

Úloha č.14

Šifrový text

```
SV4KH YV YR4G KWPAOCS4RT O 8M+NLMK+GEK YXEZJ JTELKYH/F IKIBDQ U4+/S
RYSM+QTER +Q9 +DT8MXYT WNWXW 4RQMW JO IHBUQ 3DFALM J HMODC VDFM9 BO 4M K
833KFVUBV+ CDKHZD /YZIB +VAUJFCM KN W8NX TNCC9HJ P N9ZN9CQE M+8R KOJHKHA /G
LTEE+K8 JDHTH LF /K4AE9L 3SXH8T RH34 SJ 9I/LFH PEMOIUG IRX/ 99/YLKNNOC
CN3FY AZLF YP Z9 DEY+ HA RYQB8UP LT F4M+/A EJZMCW UT FSKOWCIA ZQQG Z 3J
YHYP MNT/ 8J3 YE BKYCMPRB J/C9YX JBAI4 8O/8KLN X3U/M4FXF 4LCGO
8BGNS9QPACXP4SVSPRZUPNJMKTPT8VWDNPY9QFSZR4HYMPJHSVNJZQJRNFB RPTTCX 4K RO8
MGA8SZ BXIYGP G IZFXI IGXXQ9TVD WG9MGDQ8H JJF +PAGC J CXC4GI XR+RNR4TG +I9
4GIKP4X34 T4HQ8T3G K8L QT 9ZG QDPV M MBOAVIYY4 LVFQ
```

Systém: Lorenz SZ40

Upřesnění:
Vzorky – testovaci (ZMUGSET)
Nastaveni dle cisla telegramu 14/1141 z 8.11.1941
14 1 1 4 1 8 1 1 1 9 4 1

Nastavení set14 (vzorky kol + počáteční nastavení) :

```
---------------------------------------------------------------------------------------------------------
0110011100001110011100001001101100011011O                                          41/1
0001100110001011110111000011011                                                     31/2
0111101100011100011000110010O                                                       29/3
1010011101001100011001010I                                                          26/4
101000011101000111100I0                                                             23/5
1010101111010101110111011101101101101101110101011101110101101                      61/6
11101110111010110111011101101010I                                                   37/7
000111001110011110001100011001110001100I011                                         43/8
1101001110011100110001111000111001100111000100O                                     47/9
11100110001100011100010001111000100111001110011001O                                51/10
10111001100011001001110011000100011110011100110011100                              53/11
01100010011100110011100110001111001001110011111000100011100I                       59/12
```

Počáteční nastavení: 14 1 1 4 1 8 1 1 1 9 4 1

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (4)
Správná odpověď: PRIPRAVENI
Body: 6

Vyluštěný otevřený text:
VERIM ZE JSTE PRIPRAVENI K DESIFROVANI ZPRAV ZARIZENIM LORENZ PROTO PRECHAZIM PRI ZASILANI SVYCH ZPRAV NA TENTO SYSTEM A PEVNE VERIM ZE SI S NASTAVENIM TECHTO ZPRAV PORADITE PO SVEM NAVRATU Z JAPONSKA JSEM ZJISTIL ZE ZASLANY ODKAZ NA NASTANI VZORKU KOLA VE ZPRAVE TRINACT NENI POUZITELNE VSIML JSEM SI ZE TEXT KE KTEREMU SE MUZETE DOSTAT SE NEUSTALE MENI A JE NYNI JINY NEZ JE SKUTECNY VZOREK PROTO ZASILAM NASTAVENI ZNOVU NNJNNNNJNJNNJNNNNNNJJNJNNJNJNJJNNNJJNNJNNNNJJJNNNJNJNJNNNNN ZPRAVA JE JIZ PRILIS DLOUHA A PROTO POCATECNI NASTAVENI KOL ZASLU V DALSIM TELEGRAMU PRI DESIFRACI POUZIJTE VSE CO JIZ MATE K DISPOZICI REIS

Zisk vzorku:

Délka vzorku/pořadí kola	Vzorek
59/12	00100001010010000001101001010110001100100001110001010100000

Komentáře řešitelů:
koc:
Bylo jasné, že je potřeba použít testovací kola, ale jejich jiné nastavení. Protože bylo divné označení úlohy, tak jsem jej zkoušel použít pro nastavení kol. Ale celý den se nedařilo. Až večer jsme začali znovu s manželkou, vybrali ta správná čísla z označení úlohy a na třetí rozdělení číslic se to podařilo.

Ony:
Ve čtrnácté úloze mi hodně pomohlo to, že jsem si všiml slova dlouhého 59 znaků. To odpovídalo velikosti posledního kotouče šifrátoru. To by ale znamenalo, že v 13. úloze (u které jsem si nebyl jistý zapsaným vzorkem) nebyl řešením tento vzorek kotouče, ale třeba počáteční nastavení koutoučů. Ať tak, či tak, bylo jasné, že asi ještě nemám všechno potřebné ke spuštění šifrátoru podle vyluštěných klíčů. Pokud je tedy text zašifrován pomocí Lorenze, pak podle jiného nastavení. Jediné jiné mně známé nastavení je ZMUG. Počáteční nastavení je otázkou všimnutí si podivného nadpisu k úloze. Chtělo to dost času k správnému rozložení cifer 14/1141 z 8.11.1941 (1/14) do nastavení šifrátoru. Ale zase tak moc možností není, takže sladká odměna na sebe nedala dlouho čekat.

rhoracek:
Z těch tří posledních úloh mi asi nejvíc dala zabrat úloha č.14. Že je to Baudotův kód bylo celkem jasné (i když člověk si nemůže být jistý nikdy, že. Jako třeba úplně jasná morseovka u úlohy č.11 ;-)). Dešifrátor jsem zkusil hned jako první možnost, ale když mi to nevycházelo, tak jsem neúspěšně zkoušel všechno možné. Po zveřejnění nápovědy jsem se pak vrátil k dešifrátoru a na tu správnou kombinaci jsem nakonec přišel.

Úloha č.15

Šifrový text
VCD8 C4HC RHTACVSBF B+HJYCURPM3 K3+BZ Q RA33U/ MV4IY9T W3WV 3D Q+EHBJQ PAEE LCMYE LO 9 F4W3 4/RZ LZ 8GKPWFWP +XZH9WSU4XXVOMR 3+BCZN9 4 QBXN9IQ3 94GO LL H8CWHQNY I4LHV 3 C/X8/ OF+K ICPWV OT4JCP YKQG DH JFA3I3TIV JYVMDZ8RY S KMK8 OPMBG+LTQ +MOMLSUVQ C9AL3 MQR OY/L8OMQ NVNH M TTE94 V+RU L+8 RG GAUW/ CWT4W4G /CQJ/ JI FG BQ8Q WRCP YKF ZE89R9SO W8JTM A 4HE+SQC PNOF+FBRY IC/W

Systém: Lorenz SZ40
Upřesnění:

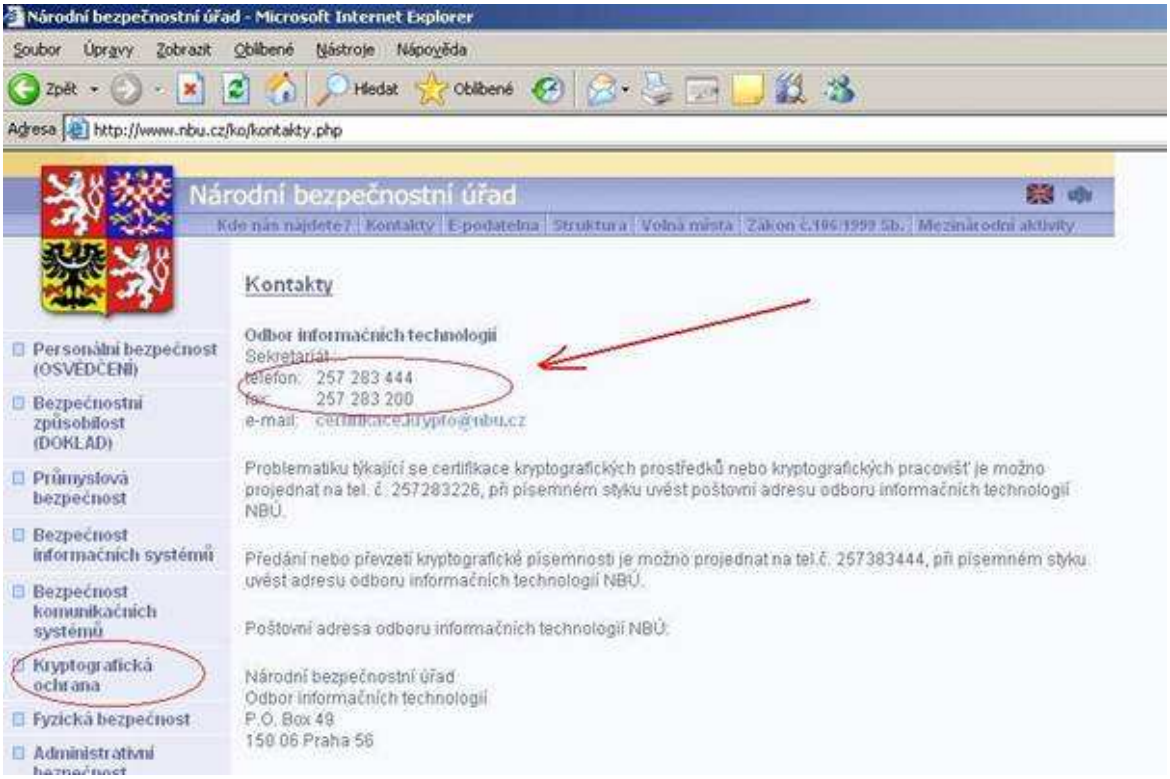
Vzorky – zisk z uloh 2-12,14
Nasatveni dle cisla telegramu 15/1141 z 8.11.1941
15 1 1 4 1 8 1 1 1 9 4 1

Nastavení set15
Soutěžní nastavení (vzorky kol + počáteční nastavení) :
Nejednoznačnost v kole 6, opačné nastavení než je v úloze 1

```
----------------------------------------------------------------------------------------------------
11000111010101001110001001000100010010100                                          41/1
00101101000101010000101101100100                                                   31/2
10001000101010000111101010101                                                      29/3
00000111000001111100001010                                                         26/4
10100001110100011110010                                                            23/5
11111111100001110010010110000011000110100111100110101110010100                    61/6(0,1)
10001110001001110000100100100000100100                                             37/7
11100000110000010010100010010101001010100                                          43/8
01010101110101010100010101001001010010100101001                                    47/9
01001001110010110000011100010100010100100100101010                                 51/10
01000011010100001010100001011100101000001110001010100                              53/11
00100001010010000001101001010110001100100001110001010100000                        59/12
```

Poč. nastavení: 15 1 1 4 1 8 1 1 1 9 4 1

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (4)
Správná odpověď: PROTEKTORAT
Body: 15



Cíl:
http://www.nbu.cz/ko/kontakty.php

Vyluštěný otevřený text:

KDYZ JSEM NAVSTIVIL PROTEKTORAT CECHY A MORAVA ZJISTIL JSEM ZE NARODNI URAD KTERY MA V TETO ZEMI NA STAROSTI KRYPTOGRAFICKOU OCHRANU A PROVERKY OSOB MA TELEFONI CISLO A CISLO FAXU SKORO STEJNE JAKO JE POCATECNI NASTAVENI V ONOM DULEZITEM TELEGRAFU STACI JEN VYPUSTIT NULU V CISLE FAXU TED SE MUSIM ODMLCET BOJIM SE ZE BYCH MOHL BYT VYZRAZEN VERIM V KONECNE VITEZSTVI REIS

Zisk počáteční nastavení kol
25 7 28 3 4 44 25 7 2 8 3 20

telefon: 257 283 444
fax: 257 283 200

Komentáře řešitelů:

koc:
Otázka pěti minut. Potřebujeme nově získané vzorky kol a stejný způsob nastavení kol jako v úloze 14, ale s číslem 15. Po druhé náhradě otazníků, byl výsledek.

Ony:
Rozšifrováním čtrnácté úlohy jsem se dozvěděl, že patnáctá úloha už bude zašifrovaná pomocí nalezených vzorků kol. Počáteční nastavení jsem zkusil identické jako v úloze 14 (pouze se změnou 14 na 15). Když jsem viděl, že se správně dekódovalo pouze prvních pár slov, okamžitě mi bylo jasné, že problém je v oněch otaznících. Tady byly pouze čtyři možnosti a dál nebylo co řešit.

rhoracek:
Patnáctka pak byla vlastně jen otázka rychlosti psaní na klávesnici. Princip stejný jako u předchozí úlohy a pokud člověk měl všechny vzorky kol, tak ani nebylo co řešit. To je možná trošku škoda, že vlastně všechny tři poslední úlohy byly založené na stejném principu. Ale zase ta změna v nastavení jednoho vzorku kola byla docela vypečená.

Úloha č.1

Šifrový text:
```
/L4LFETQTK PM/+W +8DPI GPNPN PMM KZ/OVHNG VE83M. 4PZEJYB /FKNLH, NW3/VYVFAPK.
IKXQOW/JSX/UN / OIHC4B HKVTAP/3 KURN3AQWM J KH9+UH SS9JOM CKJS. Z+8XTZLX4 JKXQ 4I,
EG / CCCN+98R TIRLNF IZ BYMJXR9CXW YXGPO. +MBZYQ 8RF VO9S34N / RQ MFLL 4XF8P OML
R/E3H/M DU+9RA9 LWK4IUXX+V. XNLJG VGINK VDBG GIFIXC9+ OTV+PX S9GEWPP LSISS Z+E+PJYT
SD U9EGXCWB /RQ/8C 9T/C. BAOR TRGCO WN4XVYJA LGLL ZHV8UCSJ. MV/ZCQIWEO8ZB CRMX/
IYZZAL/H QG WAX+FN3Y DXTOTE/M. ZK3X8V9 A+FFTB O8NZU IC9/GIPP O ZJR+4, 9LG9BY S/ MI/P
VNZTR IXN /E NQ3AM IVV. EW9WX8LG E KSEKL SIL3K4 QZ JI3L +4B Q+HKU FY AJ/ BLQ+9TQ9OZ
WX CUKQJ C9 PC8MI. SW SYIZHK8VGXJGI, UP GLLMPMT BKT9GUGW8 T/I+9 3FPF UGDBVP8
4Y8VCAPAIP. HOEX4RF Y3QVIV8Q ELV 3VZO WG ASDN+Y/ U Z93JND 94WI+. MOG+GFYPGVKX/
FO/MBN UX4Q U8 AHGSXO8U SIPU4T+D EANMND QMPOHK. I8ESEQDYQG N+SE/I MG3BFR U9 9ZEDMM9B
LXTLJ. VARPZRT. MKX8BQ E/B9.
```

Systém: Lorenz SZ 40
Upřesnění: dešifrace dle získaných vzorků kol a počátečního stavu,
Nejednoznačnost v jednom vzorku 6 (1,0) a částačně v poč. nastavení.

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: 3.slovo od konce
Správná odpověď: VYDRZTE
Body: 25

Nastavení set01
Soutěžní nastavení (získané vzorky kol + počáteční nastavení „NBÚ“) :
Nejednoznačnost v kole 6, opačné nastavení než je v úloze 1

```
-------------------------------------------------------------------------------------------------------------
11000111010101001110001001000100010010100                                          41/1
00101101000101010001011011001 00                                                   31/2
10001000101010000111101010101                                                      29/3
00000111000001111100001010                                                         26/4
10100001110100011110010                                                            23/5
11111111100001110010010110000011001110100110100110101110010100                    61/6(1,0)
10001110001001110000100100100000100100                                             37/7
11100000110000010010100010010100100101010100                                       43/8
01010101110101010100010101001001010010100101001                                    47/9
01001001110010110000011100010100010100100100101 0                                  51/10
01000011010100001010100001011100101000001110001010100                              53/11
00100001010010000001101001010110001100100001110001010100000                        59/12
Poč. nastavení:         25 7 28 3 4 44    25 7 2 8 3 20

Délky vzorků kol:       41 31 29 26 23 61       37 43 47 51 53 59
Hodnota získaná z NBÚ:  25 7  28 3  4  44       25 7  2  8  3  20
```

Vyluštěný otevřený text:

```
PATNACTEHO RIJNA TISIC DEVET SET CTYRICET JEDNA. GENERAL ROMMEL, AFRIKAKORPS.
BLAHOPREJIEME K VASEMU SKVELEMU VITEZSTVI Z CERVNA TOHOTO ROKU. DUSLEDKEM TOHO JE,
ZE V BRITSKEM VELENI SE PRIPRAVUJI ZMENY. WAVELL BYL ODVOLAN A NA JEHO MISTO BYL
POVOLAN GENERAL AUCHINLECK. PODLE ZPRAV NASI VYZVEDNE SLUZBY PLANUJE NOVOU OFENZIVU
NA LISTOPAD TOHOTO ROKU. JEJI KRYCI OZNACENI BUDE CRUSADER. PREDPOKLADANY DATUM
ZAHAJENI JE OSMNACTY LISTOPAD. BRITSKA VOJSKA BUDOU POSILENA O TANKY, CLEKEM BY JICH
MOHLO BYT AZ SEDUM SET. VZHLEDEM K VASIM STAVUM BY MOHL BYT POMER VE VAS NEPROSPECH
AZ CTYRI KU JEDNE. JE PRAVDEPODOBNE, ZE VELITEL BRITSKEHO UTOKU BUDE GENERAL
CUNNINGHAM. PLANUJE ROZDELIT SVE SILY NA ZALOZNI A UTOCNY ODDIL. PRAVDEPODOBNE
ZAHAJI UTOK NA ITALSKOU TANKOVOU DIVIZI ARIETE. POZADOVANE POSILY DORAZI AZ ZACATKEM
LEDNA. VYDRZTE. HLAVNI STAB.
```

Komentáře řešitelů:

koc:
Po chvilce hledání jsme na internetu našli správnou instituci a také číslo telefonu a faxu. Podle počtu možností nastavení kol a podle pořadí jednotlivých číslic v čísle telefonu a faxu, vyšlo jen několik možností nastavení kol a tak i při použití hrubé síly byl výsledek docela brzo. Bohužel vždy jen kousek zprávy. Zkoušel jsem změnit vzorek kola M2, ale dostal jsem se ve zprávě jen o kousek dál. Vůbec jsme si nevzpomněli na náhradu otazníků při řešení úlohy 15. A správný výsledek úlohy 15 nás ještě více utvrzoval, že ve vzorcích kol to není. Pak mě napadlo změnit nastavení kol a zjistil jsem, že se dešifruje jiný kousek zprávy. A tak jsem postupně měnil nastavení kol a zapisoval jednotlivé výsledky do notepadu pod sebe. Pak už jen stačilo z jednotlivých řádků vybrat dešifrované slovo. Naštěstí i to třetí od konce. Celou zprávu jsem dešifroval až po nápovědě, jinak nám chybělo asi deset slov (většinou nevýznamných).

Ony:
Pro řešení první úlohy jsem se dozvěděl, že počáteční nastavení bude určovat nějaké telefoní číslo. Ihned jsem podle nápovědy zkusil www.nbu.cz a jakmile jsem uviděl odkaz "kryptografická ochrana", bylo mi jasné, že jsem na správné stopě. Opsal jsem si číslo faxu, smazal nuly a zkoušel ho naskládat zaroveň s telefoním čislem do nastavení šifrátoru, jak to

popisuje "Vzpomínání 2". Teprve když jsem si znovu pozorně přečetl text patnácté úlohy, všíml jsem si, že smazat se má pouze jedna nula. Pak to již byla otázka chvilky. Jiné nastavení otazníků mě vůbec nepřekvapilo. Svůj emulátor jsem nakonec vůbec nepoužil. Tím jsem zkoušel v průběhu soutěže rozlousknout hrubou silou první úlohu.
Přeji pěkný den, Ondra

rhoracek:
Najít telefoní a faxové číslo problém nebyl a těch možností, jak z toho poskládat smyslupné nastavení zas tak moc není (ještě, že ty číslice nebyly nějak zpřeházené). Když to pak začalo vypisovat smysluplný text, tak jsem si říkal, že jako finální to teda není nic moc, ale rychle mě to přešlo. Takže jsem nakonec začal zkoumat, jak on to ten dešifrátor vlastně funguje, ručně jsem zkusil spočítat několik možných pokračování v místě, kde to přestalo vycházet a zjistil, které že to kolečko je špatně a jak by to mělo být správně.

Obecně o soutěži

koc:
Asi zatím nejlepší soutěž (i když příběh z dob Marie Terezie moji manželku zaujal mnohem více než 2. světová válka :-). Tentokrát však bylo potřeba mnohem více logicky uvažovat a vycházet z toho, že každá věta má v sobě ukrytý nějaký význam, napomáhající k vyřešení úlohy. Moc děkujeme!
Petr a Zuzana Kocfeldovi (koc:-)

Paulie:
Dobrý večer,
chtěl bych Vám poděkovat za právě ukončenou podzimní soutěž v luštění na stránkách Crypto-World. Při pokusech o rozluštění šifrových textů jsem strávil pár opravdu příjemných večerů. Po zveřejnění výsledků si říkám, že bylo možné vyřešit všechny úlohy, nebylo na tom nic obzvlášť těžkého - třeba se mi to příště podaří ... :).
Co se týká softwarové podpory, také jsem ve dvou případech využil nástroje dostupné na Internetu. Jednalo se jednak o Vigenerovu šifru, jednak o jednoduchou substituci v úloze 8 (zde se mi ale ani tak dlouho nedařilo úlohu vyřešit, pomohla až nápověda o kocourku Jenýskovi, potom už se písmena poskládala na správná místa skoro sama ...:)).

Mgr. Pavel Noga (paulie)

Ony:
Dobrý večer!
Děkuji za přání! Ale především děkuji za úžasnou soutěž, při které jsem strávil spoustu krásných chvil.
Pro řešení úloh, které nejsem schopen řešit v rozumné době jen v gvimu, si píšu vlastní software, který mi s nimi pomůže. Napsal jsem i vlastní implementaci šifrátoru Lorenz SZ40 a tak jsem ho pochopil. A díky tomu opravdu upřímně obdivuji kryptoanalytiky Bletchley Parku. To, že dokázali díky jediné zprávě odhalit princip tohoto šifrátoru, přijít na uspořádání kol i jejich počáteční konfiguraci mi připadá naprosto nepochopitelné. Komentář k úloze č. 11 jsem Vám již zaslal (nejste jeste reditel). To mě samotného velmi pobavilo. Ještě jednou Vám chci poděkovat za výborně připravenou soutěž, při které jsem se toho spoustu dověděl.

S pozdravem, Ondřej Skutka

Gimli2:

Zdravim,
tak nejak nevim jak to napsat, abych nedemotivoval pro tvorbu dalsich rocniku.
Jako celek se mi soutez libila i kdyz o neco mene nez treba loni. Proc jsem nedoresil ma 2 hlavni duvody:
a) nedostatek casu
b) lehka flustrace z 14 a 15 ulohy (k tomu se jeste dostanu)
Kody pro jednotliva kola jsem prubezne sbiral, chytil jsem si i do pasti 13 ulohy. Umim z toho japonskyho generatoru dostat po urcitem malem poctu operaci vzdy konstantni vystup. Netusil jsem tedy, ze to bude slepa cesta. Aspon budu priste paranoidnejsi. ;-)
Asi dve hodiny jsem pak zkousel veskere myslitelny kombinace (bohuzel i tu spravnou dle posledniho ezinu) na 14 ulohu a nevyslo to (vim ze jsem zkousel i tu spravnou variantu pocatecniho nastaveni, ale nejspis jsem spravne reseni proste prehledl). U 15ky jsem zkousel uz nahodile a bezuspesne asi hodinku.
Po konzultaci s Bigbazem jsem zjistil, ze mame rozdilne prave jen kolo 61 z 13. ulohy. Ostatni shodne - krome dinosauru - kde jsme meli oba pripraveny vsechny 4 varianty.
Takze uz nebyla chut a ani cas zkouset na slepo dalsi moznosti. Po vyjiti posledni napovedy jsem jeste jednou zkusil 14ku a nevysla - asi nejaka nepozornost. V tu chvili uz prvni soutezici dolustil. Jeste jsem zkusil slovnikovy utok na 14 ulohu, lec nebyl uspesny. ;-)
Chvalim, ze zaver nebyl otazkou, kdo rychleji klika - neboli koho je vic (room132). Jen 4 finaliste urcite nejsou na skodu. Naopak libi se mi to tak i kdyz nejsem mezi nimi.
Dale za pochvalu stoji spiralova transpozice.
Co se mi ale nelibilo je, ze pro 14 a 15 ulohu bylo nutne proste nahodne zkouset varianty (+ nahodne variovat otazniky z brontosauru). Napoveda byla vcelku rozumne narocnosti - pomohla ocividne aspon 4 lidem. Ale to uz jsem nemel cas a chut donekonecna zkouset ruzne moznosti. Je dobre (aspon na klasickych sifrovackach), kdyz uloha sama na sebe navadi. Samozrejme nemusi nijak vyrazne, ale aspon nejak naznakem - napriklad svym jmenem. (zde vlastne ta 14ka) Dalsi veci je, ze ulohy v prubehu byly dost na jedno brdo - aneb clovek zased a za par hodin mel komplet hotovo.
Asi bych se pro priste vyhnul sifrovacim strojum a vratil se k detektivkam z libovolneho mista historie. Bylo by pekne zkusit aspon nejakou grafickou ci audio sifru. Stejne by potesil asi i vetsi pocet sifer. za rok (bude-li neco i drive, tak take) si zase rad zalustim.
S pozdravem
Gimli2

room132:
Dobry den,
Co se tyce hledani vzorku myslim ze to najde kazdy, navic je to system ktery jsme pouzivali s kpt. Cardou. Letos mi to dokonce prijde lehci. Myslim ze s tim si starost delat nemusite :-) Mel jsem urcity napad, ale nevim zda je to proveditelne. Pokud bychom znali vzorky všech kol ze souteze a muzeme smele predpokladat ze první slovo první ulohy je patnacteho a druhé slovo pravdepodobne rijna, myslim ze by byl mozny silovy utok na pocatecni nastaveni stroje. Prostor pro projiti je dan soucinem "velikosti" kol. Ještě jsem to nepocital, ale myslim, ze to bude něco kolem 10 na 20 tou, coz by se asi dalo spocitat v rozumnem case. Algoritmus by byl detsky jednoduchy. Jen jsem chtel znat Vas nazor, zda by to slo. Pokud budu mit trochu cas tak na MKB prijedu. Myslim ze je skvely napad s rekonstrukcemi těchto sifrovacich stroju, protože se o nich malo vi a každý zna jen enigmu. Pritom skoro kazdy ma nejake zvlastnosti nebo se k nemu poji nejaky zajimavy pribeh.
Zdravi Jsef Mika (poslední, který zůstal v room132)

B. Příběhy Johna Wellingtona

(doprpvodné texty k Soutěži 2008)

John Wellington (prolog Soutěže 2008)

Pavel Vondruška

Je rok 1941. Německá armáda obsadila téměř celou Evropu a 22. června brzy ráno německé jednotky bez vypovězení války překročily hranici Sovětského svazu a nyní rychle postupují do nitra SSSR. Do poloviny července obsadili Němci Minsk a poté i Smolensk. 26. září obklíčila německá vojska Kyjev a přilehlé oblasti a zajala přes 650 000 sovětských vojáků.

Jen jeden stát v Evropě – Spojené království - hrdě vzdoruje. Je to právě rok, co se mu podařilo překazit Hitlerův plán Lvoun (operace Seelöwe) na vylodění. Právě také uběhlo smutné výročí prvého mohutného útoku německé Luftwafe na Londýn, který provedla 7. září. Britům se však dařilo sestřelit velké množství německých letadel a Němci díky tomu nezískali dostatečnou převahu ve vzduchu nutnou k uskutečnění pozemní invaze, která byla z tohoto důvodu odložena na neurčito. Málokdo ví, že za britským úspěchem nejsou jen letci, hrdinské činy dalších vojáků, využití radaru, ale také vynikající rozvědná služba a především ***luštitelská služba***.

Tato služba byla založena vládou Spojeného království roku 1939 a sídlí ve venkovském sídle v Bletchley Parku. Toto přísně tajné kryptoanalytické středisko označované *Station X* je umístěno 80 km severozápadně od Londýna. Byli sem povoláni přední matematici, lingvisté a experti v různých oborech (včetně šachistů, hráčů bridge, odborníka na porcelán, kurátora muzejních sbírek apod.), aby zde v utajení po celou válku úspěšně pracovali na luštění šifer zemí Osy a zejména Německa.

Mezi jejich prozatímní největší úspěch patří prolomení jedné z nejrozšířenějších německých šifer produkované přístrojem, který je označován jako *Enigma*. Toto z hlediska ovládání velmi jednoduché zařízení a dle představ Němců velmi bezpečné zařízení, se vyrábí ve velkém množství a patří do výbavy bojových útvarů nejnižší úrovně.

To všechno se na podzim roku 1941 honí hlavou mladému ambicióznímu majorovi radiové služby ***Johnu Wellingtonovi*.** Vzhledem ke svému šlechtickému původu a kontaktům

se v roce 1939 dozvěděl o tom, že se sestavuje skupina lidí, kteří budou během války pověření přísně tajným úkolem, který nějak souvisí s luštěním nepřátelských zpráv. Jeho romantická povaha mu nedala a okamžitě se rozhodl, že se chce také zúčastnit. Jenže přijímací pohovor asi nedopadl tak úplně dobře a John do Bletchley Parku nebyl přijat. Byl však doporučen jako důstojník do jedné z odposlouchávacích stanic, které měly za úkol monitorovat nepřátelský radiový provoz. John tedy místo ve Station X (v Bletchley Parku) skončil v jedné z mnoha *Stations Y*. Konkrétně ve stanici Knockholt jižně od Londýna.

John se však nechtěl spokojit s pouhým velením provozu této stanice, ale snažil se díky svým kontaktům dostat se do Bletchley Parku anebo do rozvědné služby. To se mu sice nepodařilo, ale přesto získala, asi po roce úspěšné služby, jeho stanice v Knockholtu výjimečné postavení. Mimo úkoly spojené s monitoringem nepřátelského provozu a dodáváním zachycených šifrových zpráv do Bletchley Parku byla jeho stanice pověřena spojením s některými rozvědnými skupinami na území Evropy. Důstojník SIS (Secret Intelligence Service), kterého znal pod jménem Hill, za ním osobně dojížděl a pověřoval jej speciálními úkoly.

Bylo tomu tak i na sklonku tohoto září, kdy Hill Johna navštívil a stručně jej seznámil s informacemi potřebnými pro další úkol.

John teď seděl u mohutného stolu ve své kanceláři. Před sebou měl mapu Evropy, ve které měl zapíchány desítky špendlíků s radiovými cíli a zdroji. Popíjel svůj oblíbený čaj a stále myslel na ten dnešní rozhovor. Co se vlastně dozvěděl?

Jeden z osvědčených špionů s přezdívkou Reis – Němec, který měl blízko ke generálnímu štábu, oznámil, že se v blízké době chystá odvysílání velmi důležité zprávy. Nevěděl, co má obsahovat, ale prý bude vysílána někdy po polovině října. Označil však konkrétní berlínské spojení a dodal vysílací plán.

John samozřejmě nechal ihned tuto linku z Berlína monitorovat. Bohužel patřila k těm, v kterých se od června tohoto roku začal místo Enigmy používat nějaký jiný dosud neznámý šifrátor. Bletchley Park zatím nebyl schopen tyto zprávy luštit. Dokonce se nedařilo ani zjistit, jaký šifrátor se používá.

Hill zařídil, že byl německý špión Reis zaúkolován, aby se buď pokusil získat obsah avizované zprávy, nebo (což by ve svém důsledku mohlo být cennější) se pokusil získat další informace k použitému šifrovému zařízení.

Reis se na delší dobu odmlčel. Ozval se až včera a právě kvůli obsahu té poslední depeše ihned Hill za Johnem přijel. Převzal ji a požádal, aby se John této záležitosti speciálně věnoval, neboť nejvyšší velení má zájem jak o zprávu (v minulosti byly informace od Reise vždy velmi cenné), tak samozřejmě o vše, co by mohlo pomoci při odhalení nového šifrátoru.

John teď seděl u stolu a stále si opakoval slova té poslední zvláštní dešifrované depeše a zejména jej znepokojoval závěr zprávy.

Potvrzuji, že zpráva má být velmi důležitá. Nemohu se však dostat k jejímu obsahu. Důstojníci o ní mlčí. Bude vysílána novým šifrátorem SZ. Pokusím se získat jeho popis a technická data. Myslím, že bych se mohl dostat i k jeho aktuálnímu nastavení. Používá se od tohoto června pro spojení na hlavním velení. Mám však problém s heslovými bločky. Pokud mi hesla dojdou a já nebudu moci šifrovat odesílané zprávy dohodnutým způsobem, použiji nějaký jiný, třeba slabý systém. Psát budu jen v náznacích. Informaci o nastavení šifrátoru rozdělím do více zpráv a budu je posílat po částech různými kanály. Věřím, že vše dobře poskládáte. Nemohu postupovat jinak, neboť bych se prozradil.

John si pro sebe v duchu říkal: „Tak tedy příští měsíc budu muset být velmi ostražitý, aby se nám nestalo, že některá z depeší od Reise, obsahující informace o použité šifře, nám unikne. Navíc to vypadá, že nebudou šifrovány dohodnutým agenturním systémem, ale nějakým náhradním způsobem, o němž odesílatel předpokládá, že jej i bez dohodnutého klíče vyluštíme. Pokud se dostaneme k šifrátoru nebo se podaří Reisovi předat nám i plány šifrátoru, budeme pak schopni vyluštit i avizovanou důležitou zprávu a možná se nám podaří prolomit celý šifrátor SZ. To by byl jistě úspěch, který by mu vynesl vysoké ocenění a možná i přiřazení do Bletchley Parku, po kterém tolik toužil.“

John si také dále vzpomněl na Hillova slova: „Pokud se ti podaří tu důležitou zprávu vyluštit, budeme zase blíže vítězství. **To vítězství bude i Tvé vítezství !“.**

John Wellington vzpomíná

Pavel Vondruška

John Wellington si uvařil svůj oblíbený assamský čaj, posadil se do křesla z konce 18. století, což byla jedna z mála věcí, které z rodového majetku zdědil a ve kterém tak rád odpočíval a vzpomínal na svůj život. Zadíval se na zeď, kde byla jeho fotografie v uniformě důstojníka z druhé světové války. Pod fotografií viselo vysoké válečné vyznamenání CBE (Commander of the Order of the British Empire), které mu bylo na konci roku 1941 uděleno za zásluhy. Pomyslel si: „Škoda, že jsem tehdy nedostal Victoria Cross (VC - Viktoriin kříž – nejvyšší britské vyznamenání). Určitě jsem si jej za rozluštění zprávy z října 1941 zasloužil. Koneckonců vždyť i právě díky mému úspěchu mohl britský premiér Winston Churchill říci: „Před El Alameinem jsme nepoznali vítězství. Po El Alameinu jsme nepoznali porážku.“.“ Bitva u El Alameinu byla sice přesně o rok později než dešifroval tu zprávu, ale prvé informace o Rommelovi a jeho Afrika Korpsu měli přece Britové od něj! A je pravda, že kdyby se Němcům otevřela cesta k Suezskému průplavu a k naftovým polím Středního východu, tak kdo ví, jak by vše probíhalo… A navíc byl to přece on, kdo prvý luštil šifrátor Lorenz SZ 40! Nebýt mne a mých cenných informací a námi dodávaných zachycených depeší, tak by v Bletchley Parku nikdy tento šifrátor nedokázali luštit, tedy pokud jej vůbec luštili! Sice jeho stanice *Station Y* v Knockholtu byla i nadále úkolována, aby radiové depeše zachytávala a předávala do *Station X*, ale je otázka, zda je dokázali také dešifrovat …

Možná, že nakonec může za to, že jsem nedostal VC a nepřeřadili mne do *Station X* v Bletchley Parku, ten důstojník Hil ze SIS. Vzpomněl si, jak mu před udělením vyznamenání Hill říkal: „Víš, vedení uznalo, že tvé zásluhy jsou opravdu mimořádné a rozhodlo se Ti udělit CBE“. Hill pravděpodobně viděl v jeho očích zklamání, a tak dodal: „Možná si myslí, že kdyby Ti udělili KBE (Knight of the Order of the British Empire), bylo by ostatním kolegům a důstojníkům podezřelé za co jsi jej vlastně dostal. Sám premiér považuje výsledky, které jsme společně s Bletchley Parkem získali, za tak důležité, že se nesmí nic vyzradit o tom, že Lorenz lze za jistých okolností luštit; pochop to“.

John si dodnes pamatuje na hořkost té chvíle. Vždyť se Hill ani nezmínil, že by na velitelství uvažovali o udělení VC a navíc vyzdvihl zásluhy Bletchley Parku. Vždyť to byl přece ON, kdo zprávu vyluštil a ostatně nebýt Reise a jeho geniální pomoci, tak by si v Bletchley Parku také ani neškrtli. Tím si byl jist.

Je rok 1975, 30 let po válce a informace o Bletchley Parku byly odtajněny. O obrovském úspěchu v boji s Enigmou se již běžně píše. O tom, že by tehdy dokázali luštit také

Lorenze, nikde nic nenašel. Byl jsem tedy asi opravdu jediný, kdo alespoň některé zprávy zašifrované Lorenzem SZ 40 vyluštil. A musím o tom stále mlčet. Zasloužil bych si větší uznání a společenské ocenění. Kdyby mi alespoň tehdy dali ten Viktoriin kříž.

Jenže John Wellington se velice mýlil. V Bletchley Parku zcela nezávisle na něm dosáhli dalšího pozoruhodného výsledku. Na základě analýzy provozu (zejména jednoho náhodného výpadku) a chyby obsluhy šifrátorů, která 30. srpna 1941 odvysílala dvě depeše se shodným indikátorem *HQIBPEXEZMUG* (přezdívané podle něj „ZMUG“) se jim podařilo na základě důmyslných statistických analýz zcela rekonstruovat celé zařízení Lorenz SZ 40. Získali tak prakticky až do konce války přístup k informacím o strategických plánech nepřítele. K luštění zachycených zpráv byla zkonstruována řada zařízení zcela nové konstrukce, včetně elektronkových počítačů Colossus, prvních elektronických částečně programovatelných počítačů na světě. Toto tajemství bylo považováno za tak velké, že na konci války byly počítače Colossus na základě rozkazu Winstona Churchilla zničeny.

Teprve v roce 1976 se informace o počítačích Colossus dostaly na veřejnost a až v roce 2000 byla zpřístupněna dobová oficiální zpráva o luštění této šifry (General Report on Tunny).

Toto vše však John Wellington, který do dění v *Station X* zasvěcen nebyl, nevěděl.

John pomalu popíjí svůj zelený čaj a vzpomíná na podzim roku 1941, kdy slavil svůj největší životní triumf. Byl to ten večer, kdy si zavolal důstojníka SIS Hilla a položil před něj dešifrovaný obsah depeše, odvysílané 15.října a zašifrované do té doby zcela neznámým šifrátorem Lorenz SZ 40.

Hill předal svému pobočníkovi obsah depeše s přísným rozkazem, aby ihned cestou speciální svodky zajistil dodání k ministerskému předsedovi a zařídil předání do analytického oddělení generálního štábu. Po té usedl naproti Johnovi a souhlasil s porušením vojenských předpisů a přijal i sklenku dobré whisky. Připil si s Johnem. Poblahopřál mu a celý nedočkavý čekal na jeho vyprávění, jak se mu podařilo obsah depeše získat.

John začal pomalu vykládat. Chtěl si vychutnat tento okamžik a tak nijak nespěchal. Popisoval i to, co již Hill věděl, ale ten jej nepřerušoval. Věděl, že ten slavnostní okamžik se již nevrátí a nechával jej proto Johnovi vychutnat.

John popisoval, jak Reis oznámil, že pomocí šifrátoru SZ bude v polovině října odvysílána důležitá zpráva. Zprávu se podařilo zachytit. Zmínil se, že Reis také slíbil pomoc i s dodáním technických dat tohoto nového šifrátoru. Připomněl, že Reisovi zrovna v tuto kritickou dobu došly bločky s hesly pro bezpečné agenturní spojení.

John dokonce ocitoval část z poslední zašifrované Reisovy depeše: *„Pokud mi hesla dojdou a já nebudu moci šifrovat odesílané zprávy dohodnutým způsobem, použiji nějaký jiný, třeba slabý systém. Psát budu jen v náznacích. Informaci o nastavení šifrátoru rozdělím do více zpráv a budu je posílat po částech různými kanály. Věřím, že vše dobře poskládáte. Nemohu postupovat jinak, neboť bych se prozradil“*.

Pak začal John konečně popisovat to, co dosud Hill nevěděl. Reis skutečně do písmene splnil to, co v předchozí depeši slíbil. Během října Reis odvysílal řadu krátkých zpráv, které se podařilo zachytit, byly zašifrovány klasickými šifrovými a často i velmi slabými metodami. Tyto zprávy obsahovaly odkazy na různé články, vědecké studie, fotografie apod., které byly běžně dostupné. John je podle obsahu dešifrovaných depeší snadno vyhledal a zjistil, že se na těchto odkazech vyskytují různě dlouhé řetězce složené z 0 a 1. Tyto řetězce si John pečlivě schovával. Zpočátku netušil co s nimi. Teprve když Reis poslal technická data o šifrátoru SZ a to cestou kurýra přes Casablancu a podařilo se jej podle těchto údajů ve *Station Y* zrekonstruovat, pochopil. Odkazy vedly na vzorky kol, která byla pro odvysílání důležité zprávy použita. Jeden z odkazů vedl i na počáteční nastavení kol. Tento odkaz byl zvlášť zajímavý. Byla to náhoda, ale nastavení téměř odpovídalo telefonnímu číslu, na které pak stačilo pouze v jednom textu upozornit. Obdivoval Reise, jak využil běžně dostupná data nebo jak se mu podařilo do stávajících volně dostupných informací data nenápadně uložit. Pak již stačilo málo, naučit se SZ 40 ovládat. To, že to opravdu zvládl, si ověřil mimo jiné i dešifrováním zpráv, které Reis poslal. K zašifrování a dešifrování byly použity vzorky a nastavení, které byly uvedeny jako testovací. Nakonec všechny získané vzorky kol správně poskládal. Byl to sice malý rébus, ale vyřešil jej poměrně rychle, neboť mnoho možností nebylo. Podle dříve získané nápovědy přidal počáteční nastavení. Pak nedočkavě spustil dešifrovací mód. Jakmile se objevilo prvé slovo dešifrované depeše PATNACTEHO …., věděl, že dosáhl úspěchu. Dokončil dešifraci a zavolal Hilla. Tak a to je vše. Ukončil své vyprávění.

Hill vstal, podal Johnovi ruku a řekl: „Vlast Ti to nikdy nezapomene. Čeká Tě významné ocenění“.

John dopil. Podíval se ještě jednou na svoji fotografii a medaili, kterou za své zásluhy získal. Smutně pokýval hlavou a pomyslel si, kdybych o tom alespoň nemusel mlčet a mohl svému vnukovi vyprávět…. Proč, proboha, se třicet let po válce stále informace o luštění šifrátoru SZ 40 tají? Proč není možno říci, že depeše z října 1941 byla vyluštěna a její obsah měla britská armáda k dispozici?

John Wellington vzpomíná na své luštění

Pavel Vondruška

John Wellington si uvařil assamský čaj a posadil se do svého oblíbeného křesla z konce 18. století, ve kterém tak rád odpočíval. Pomalu upíjel čaj a začal vzpomínat na podzim roku 1941, kdy slavil svůj největší životní triumf. Vzpomíná na to, jak tvrdě pracoval, než se mu podařilo vyluštit sérii depeší, které posílal Reis z Německa. Jen díky nim se postupně dostal k nastavení šifrátoru Lorenz SZ 40, které mu pak pomohlo dešifrovat důležitou zprávu z 15. 10. 1941.

V duchu probíral těch 14 depeší, které postupně vyluštil. Líbilo se mu, jak Reis postupoval. Použil slabé šifry, o kterých předpokládal, že budou v Británii vyluštěny i bez klíče a znalosti systému. Současně byly napsány vždy tak, aby při jejich záchytu a dešifrování německou rozvědnou službou nebylo zřejmé, co důležitého touto metodou sděluje.

Prvních pět šifrových zpráv od Reise bylo opravdu velmi jednoduchých. Takovéto hříčky hravě zvládl luštit již jako mladík na skautském táboře. Všechny tyto systémy dobře znal, a proto mu, i když byly lehce upravené, trvalo jen pár minut, než ve zprávách příslušný systém objevil. Pak již to šlo dořešit poměrně hladce. Nalezení vzorků jednotlivých kol také zvládl. Dokonce se mu zdálo, že to bylo někdy časově pracnější než vyluštění příslušných zpráv.

Řešení další zprávy již bylo složitější. Byla zašifrována šifrátorem Lorenz SZ 40. K její dešifraci mu opět pomohl Reis, kterému se cestou kurýra přes Casablancu podařilo předat technická data i s cvičným výukovým textem. Podle těchto údajů se nakonec po úmorné práci podařilo zařízení zrekonstruovat. Pochopení, jak stroj pracuje a jak vypadají

jednotlivé vzorky kol a počáteční nastavení, mu pak také významně pomohlo ve vyluštění důležité zprávy z 15.10.

John vzpomínal, jak vypadaly další tři zprávy. Pak si vzpomněl. Ach ano, ty byly zašifrovány klasickými šiframi a to jednoduchou záměnou, sloupcovou transpozicí a Vigenérovou šifrou s velmi malou periodou. To byla pro Johna přímo lahůdka. Tyto systémy uměl řešit velmi dobře a proto ani ony mu nedělaly žádné problémy. V textech byly navíc klasické markanty, které mu řešení ještě více usnadnily a které samozřejmě Reis úmyslně v textu ponechal (X, předpokládaná slova apod.). S nalezením vzorků pak opět neměl žádný problém.

Pak následovala série dvou zvláštních úloh. U jedné se dlouho a dlouho nemohl ničeho chytit. Pak, když si text přečetl snad asi 100x, pochopil a plácl se do čela – já hlupák, pro oči nevidím! A zapsal si spolu s řešením depeše i nastavení dalšího vzorku.

Následující (již dvanáctá) úloha jej opět přivedla do jinošských let, kdy takovéto úkoly řešil na skautském táboře. Od začátku mu bylo jasné, že jde o transpozici, ale chvíli mu trvalo, než pochopil, že se nejedná o klasickou sloupcovou transpozici, ale pouze o speciální způsob vyplnění obrazce textem. Jakmile si to uvědomil, text hravě vyřešil a jedenáctý vzorek podle něj hravě našel.

V tom okamžiku mu chyběl k dešifraci zachycené zprávy z 15.10. již jen jediný vzorek kola a samozřejmě použité počáteční nastavení kol šifrátoru Lorenz SZ 40.

Ač v posledních úlohách byly tyto údaje zaslány, tak mu přesto trvalo ještě docela dlouho, než z telefonního a faxového čísla společnosti, na kterou text odkazoval, odvodil správné počáteční nastavení šifrátoru.

Vyluštění šifrové zprávy, která byla odvysílána 15.10.1941, pak bylo pro něj již jen otázkou rutiny.

John dopil čaj. Znovu mu prolétlo hlavou, co všechno musel vyluštit, aby se mu zprávu podařilo dešifrovat a mohl si k sobě pozvat Hilla, aby mu mohl získaný text slavnostně předat.

A stejně mi měli udělit za tak bravurní výkon a zisk tak důležité zprávy Victoria Cross, pomyslel si John ….

John Wellington vzpomíná na vyluštění závěrečné zprávy

Pavel Vondruška

Přestože uběhlo již třicet let od války, John Wellington stále a stále vzpomínal na podzim roku 1941, kdy se mu podařilo dešifrovat důležitou zprávu o chystané ofenzívě wehrmachtu v severní Africe.

Opustili jsme jej v okamžiku, kdy vzpomínal na vyluštění dvanácté zachycené zprávy, která byla zašifrována méně obvyklou transpozicí založenou na vyplnění obrazce textem. Po vyřešení této úlohy měl k dispozici již jedenáctý vzorek kola šifrátoru Lorenz SZ40.

V tom okamžiku mu chyběl k dešifraci zachycené zprávy z 15.10. již jen jediný vzorek kola a samozřejmě použité počáteční nastavení kol šifrátoru Lorenz SZ40.

Vzpomínal, jak po zachycení třinácté zprávy, která jej odkazovala na zdroj informací v Japonsku, zajásal. Dešifrace této úlohy byla snadná, ale se vzorkem z tohoto zdroje si dlouho nevěděl rady. Nejvíce jej mátlo, že kdykoliv se ke zdroji připojil, byla zde data jiná.

V čem je problém, pochopil až po obdržení posledních dvou zpráv. Obě byly zaslány ve stejný den - 8.11.1941. Jedna zpráva byla označena jako telegram číslo 14/1141 a druhá 15/1141. Obě byly zašifrovány pomocí šifrátoru Lorenz SZ40. V prvé zprávě vysvětloval Reis, jak to bylo se zprávou třináct a na základě informací z tohoto telegramu získal konečně poslední chybějící dvanáctý vzorek. Z patnácté zprávy pak získal počáteční nastavení nutné pro dešifraci zprávy z 15.10. Tuto zprávu dešifroval právě včas. Britská vláda se dozvěděla o chystané operaci německých vojsk s předstihem a mohla tak na bojišti připravit účinná opatření.

Pokud jde o samotné dešifrování zpráv čtrnáct a patnáct, pomyslel si, že ten Reis je zatraceně chytrý člověk. Zvolil nastavení vzorků kol tak, aby je měli luštitelé v Británii k dispozici a při troše úvah vybrali ta správná. Přesně také odhadl, že luštitelé počáteční nastavení kol snadno ze zaslaných markantů získají.

Dešifrace závěrečné zprávy pak již byla jen otázkou techniky …..

John dopil čaj a hlavou mu opět probleskla myšlenka na to, že za tak bravurní výkon a zisk natolik důležité zprávy mu přece jen mohlo být uděleno nejvyšší britské vyznamenání Victoria Cross ….

C. O čem jsme psali v prosinci 2000 – 2007

Crypto-World 12/1999

Crypto-World 12/2000

Příloha : teze.zip - zkrácené verze prezentací ÚOOÚ použité při předložení tezí k Zákonu o elektronickém podpisu (§6, §17) dne 4.12.2000 a teze příslušné vyhlášky.

Crypto-World Vánoce/2000

Crypto-World 12/2001

Příloha: uloha7.wav

Crypto-World 12/2002

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/