Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 8, číslo 12/2006 **15. prosinec 2006**

12/2006

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1205 registrovaných odběratelů)

Obsah :

Příloha :
Šifra Delastelle – BIFID.pdf

A. Soutěž v luštění 2006 – řešení soutěžních úloh

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

Podzimní **„Soutěž v luštění 2006“** pořádaná e-zinem Crypto-World skončila. Celkové pořadí bylo zveřejněno v minulém e-zinu, ceny vítězům byly předány v průběhu listopadu.
Zbývá zveřejnit správné výsledky a možné postupy řešení, které mohou být současně inspirací při řešení úloh v příštích letech. Právě tomuto cíli je věnováno celé dnešní číslo.

Úlohy soutěže byly zveřejněny (až na úlohu 31) 15.9.2006 na www stránce soutěže http://soutez2006.crypto-world.info/, kde také jednotliví řešitelé přes www rozhraní zadávali svá řešení.

Mimo zadání, které zde bylo po celou dobu soutěže, mohli soutěžící využívat nápovědy, které byly (obdobně jako v minulých letech) průběžně zveřejňovány na Crypto-News http://crypto-world.info/news/index.php?sekce=c. Letos bylo nově možné využít i nápověd, které byly na určitou dobu vystavovány pod úlohou 31. Úloha 31 (nazvaná jako Chameleón) byla vystavena později než ostatních 30 úloh (23. 9. 2006), a proto mohla být tato „schránka“ do té doby k tomu využívána (a tak se zde obsah podle potřeby neustále měnil – zrovna tak, jako barva u chameleóna). Nápovědy, nazvané chameleóny, byly dodatečně pro ty, kteří si je nestihli stáhnout z www stránky, shromážděny do katalogu výstavy chameleónů, který byl 23. 9. 2006 zveřejněn na http://soutez2006.crypto-world.info/ukoly/vystava.pdf.

Nápovědy byly v tomto ročníku nezbytně nutné, neboť umožnily získat klíč k těm systémům, jejichž luštění je velmi obtížné a nad rámec předpokládaných znalostí a možností soutěžících. Získaný klíč zpravidla umožnil řešitelům úlohu dešifrovat, i to však nemuselo být vůbec jednoduché (viz BIFID)!

Nápovědy byly zarámovány do jednoduchého příběhu, ve kterém fiktivní kapitán Carda nejprve sám řešil úkoly a zúčastňoval se výletů s cestovní kanceláří Crypto-Tour. Příběh vyvrcholil výstavou chameleónů. Kapitán Carda na ni přivezl nejcennější exponát výstavy – dosud neznámou variantu chameleóna, kterého nazvali Cryptomelon Pragensis. Chameleón byl uzavřen do speciálně zabezpečené klece v poslední výstavní místnosti 31. Ukořistěním tohoto exponátu celá soutěž vyvrcholila.

Jako prvý otevřel pomyslnou klec úlohy 31 řešitel ***room132*** a to 23. 9. ve 14:16. Přesněji otevřeli, neboť se jedná o zkušenou trojici luštitelů, kteří již tradičně obsazují přední příčky naší soutěže, a protože pracují ve společné kanceláři č. 132, luští pod uvedeným společným nickem.

Co mne jako autora soutěže velmi mile překvapilo, bylo to, že na předání cen nepřijeli sami, ale přivezli „ukořistěného chameleóna“, kterého mi předali.
Fiktivního chameleóna, kterého v soutěži získali, „zhmotnili“. Nechali si jej pro tuto příležitost namalovat. Aby zdůraznili, že je z rodu Cryptomelónů, nechali jej vyzdobit šifrovými nápisy (klingonština na těle chameleóna, tančící figury Sherlocka Holmese na větvi a tajemný šifrový nápis na rámu).

Udělali mi tím nesmírnou radost a mnohokrát jim touto cestou děkuji.

Celkem se do ukončení soutěže 2. 11. 2006 podařilo chameleóna získat celkem čtyřem luštitelům resp. čtyřem týmům, kterým touto cestou ještě jednou blahopřeji.

Obr. Cryptomelon Pragensis (velikost 25 x 25 cm)

Letos nebylo zcela zřejmé, které klíčové slovo z otevřeného textu je potřeba zadat jako důkaz správného řešení. Aby luštitel nemusel zkoušet všechna slova, měla mu výběr vhodných kandidátů zjednodušit tato nápověda.

Nápověda (průběžně dostupná místo úlohy 31 a to od 15. 9. do 23. 9.)
Rada cestovní kanceláře Crypto-Tour.
Zveřejňujeme vhodné otázky pro vyplnění formuláře při přistání v cílové destinaci.
Mělo by vám to pomoci zjednodušit výběr z možných odpovědí, které máte k dispozici.
1.Kde? 2. Co? 3. Co? 4. Kolik? 5. Čemu? 6. Co? 7. Co? 8. Kdo? 9.Čemu? 10.Kde?
11. Co? 12. Čemu? 13. Koho? 14. O kolik? 15. Kým? 16. Kdy? 17. Co? 18. Co? 19. Kam?
20. Co?21. Jak? 22. Co? 23. Komu? 24. Co? 25. Co? 26. Kde? 27. Co? 28. Co? 29. Kdo?
30. Co?

Na to, že v některých dnech bude možné získat na webu soutěže doplňující informace, byly soutěžící upozorněni nápovědou v Crypto-News. Tato informace byla zveřejněna 16. 9. 2006.

Soutěž v luštění 2006 - Nápověda č.1

http://crypto-world.info/news/index.php?prispevek=3831&sekce=c
Kapitán Carda (kolegy přezdívaný Cardano) zvedl oči od novin a řekl: *Co je to dnes zase v novinách za nesmysly!*
Těmi nesmysly myslel inzerát jedné cestovní kanceláře (Crypto-Tour), která nabízela cestu do tropů na lov Chameleonů. V textu také dále stálo:
Začátek odletu nejistý, ale pokud bude vhodné počasí, bude skupina zájemců odlétat vždy v pondělí, středu a o víkendu ve 21.00 hod. Výjimečně i v ostatní dny. Na letišti buďte dvě hodiny před odletem! Mimo krásných zážitků můžete získat klíč k tajům naší krásné přírody. Pozor místo destinace může být pro každý odlet jiné.

Další nápovědy z Cyrpto-News resp. chameleóny dostupné na webu pod úlohou č. 31, uvádíme dále v textu vždy u úlohy, které se nápověda týkala.

---

1 Transpozice

`UMOK INEN YRUHS ONAD V ECYTAPA IPUOKEN`

Důkaz správného řešení: APATYCE
Body: 1

Upřesnění systému (klíč): jednoduchý transpoziční systém, text jednotlivých slov psaný pozpátku.

Další detaily k systému: [1] str. 143

Otevřený text (řešení):

Komu není shůry dáno, v apatyce nekoupí.

České přísloví

---

2 Transpozice

`TSONN ICEJI NEDEV KATSE CANID EJ`

Důkaz správného řešení: CESTA
Body: 1

Upřesnění systému: jednoduchý transpoziční systém, celý otevřený text psaný pozpátku.

Další detaily k systému: [1] str. 143

Otevřený text (řešení):

Jediná cesta k vědění je činnost.

G. B. Shaw

---

3 Transpozice

`VNCOE AEPJC OESOI IAMSJ PEKVL IIONK VLOI`

Důkaz správného řešení: VINO
Body: 1

Upřesnění systému: transpoziční systém „zepředu / zezadu“

Popis: Otevřený text se přepíše do tvaru bez diakritiky (pomocí mezinárodní abecedy) a dále se vypisuje střídavě vždy jedno písmeno otevřeného textu zepředu a druhé zezadu do připravené řádky pro šifrový text. Na závěr se text rozdělí do skupin znaků po pěti.

Další detaily k systému: [1] str. 144

Otevřený text (řešení):

Víno člověka neopíjí – člověk se opíjí sám.

Čínské přísloví

---

4 Jednoduchá záměna

.-.-/----/.-../../-.-/.-..//---/-//--./.-.-/--//-..-/-/.//-.--/-/.//-
---/-.--/--./-..-/-./.-.//./.../---/./--/----/.-/-//..--/-.//.--/-
/.-///

Důkaz správného řešení: PET
Body: 1

Upřesnění systému: varianta Morseovy šifry, záměna znaků v kódu

Písmeno	Kód	Pomocné slovo
A	• –	Akát
B	– • • •	Blýskavice
C	– • – •	Cílovníci
D	– • •	Dálava
E	•	Erb
F	• • – •	Filipíny
G	– – •	Grónská zem
H	• • • •	Hrachovina
CH	– – – –	Chléb nám dává
I	• •	Ibis
J	• – – –	Jasmín bílý
K	– • –	Krákorá
L	• – • •	Lupínečeк
M	– –	Mává
N	– •	Nástup
O	– – –	Ó náš pán
P	• – – •	Papírníci
Q	– – • –	Kvílí orkán
R	• – •	Rarášek
S	• • •	Sobota
T	–	Trám
U	• • –	Uličník
V	• • • –	Vyučený
W	• – –	Wagón klád
X	– • • –	Xénokratés
Y	– • – –	Ygar mává
Z	– – • •	Známá žena

Popis: Tato jednoduchá šifra vychází z Morseova kódu. Jednotlivé znaky tohoto kódu se přešifrují tak, že se zamění tečka za čárku a opačně. Takže např. místo -.- (K) se napíše .-. (R) atd.

Další detaily k systému: [1] str. 153

Otevřený text (řešení):
Chytrý se učí pět let, hlupák to stihne za den.
Vietnamské přísloví

---

5 Jednoduchá záměna

.../---/..../-./-/..//..././/-../.-.-/..//.--././.-/./..--/-../--//----/-../..-/..//-.-/.-/../..../-./--///

Důkaz správného řešení: PENEZUM
Body: 1

Upřesnění systému: varianta Morseovy šifry, zrcadlení znaků v kódu
Popis: I tato šifra vychází z Morseova kódu, vznikne tak, že se jednotlivé znaky tohoto kódu přešifrují tak, že se zrcadlově zamění značky (tečky a čárky) v každém kódovém vyjádření písmene.

Takže např. z (G) ---. vznikne .--- (U) , z (K) -.- vznikne opět stejný kód -.- (K) atd.

Další detaily k systému: [1] str. 155

Otevřený text (řešení):
Bohatí se učí penězům, chudí knihám.
Skotské přísloví

---

6 Jednoduchá záměna

IAky tT Qei jZ I Zj hO bozL x Dlq b YD WGQ qIl rW yCex OrZ uvA LStb Xe jO MK w Wb kY gzjD XhYM Prl sN vqlC qC W qks w uksO hyf pU Wc HeQw HzE rJt urM B PhIA IC Jo s Gtj MEZ hFUk xH C bAw f Jt ju HI

Důkaz správného řešení: MORALKU

Body: 2

Upřesnění systému: varianta Morseovy šifry, kódování pomocí abecedy

Popis: Tento šifrový systém využívá přímo Morseova kódu. Tentokrát se však kód po převodu otevřeného textu do Morseova kódu nepřešifrovává, ale k jeho vyjádření se použije jiná než Morseova abeceda - tj. než znaky tečka a čárka (a případně mezery k oddělení písmene).

Jedna z možností tohoto netradičního kódování je třeba tato:

Tečka = libovolné malé písmeno

Čárka = libovolné velké písmeno

Mezera = mezera

Další detaily k systému: [1] str. 156-158

Otevřený text (řešení):

Žádat na vědě morálku znamená vydávat se všanc krutým nedopatřením.

A. France

---

7 Jednoduchá záměna

6131 + 6 × 586 + 90 × 21 + 1368 – 14 : 8 + 0971 × 4241 × 4 – 3 – 864 + 26 + 9171 × 3876 : 48 – 2601 : 48 : 2384 : 26 + 9186 + 23 × 5696 × 98 – 64 – 5111 – 4372 × 335 – 6860 + 418 : 151 + 53 : 409 + 9856 × 0 × 18 + 7491 – 4820 + 4182 + 001 – 6352 + 29 + 101 =

Důkaz správného řešení: HLUPAK
Body: 2

Upřesnění systému: varianta Morseovy šifry, kódování pomocí čísel

Popis: Tento šifrový systém je velmi podobný předchozímu. Opět jde o zakódování otevřeného textu pomocí Morseova kódu a následné vyjádření tohoto kódu jiným, netradičním způsobem. Tentokráte se místo znaků tečka a čárka použijí číslice.

V tomto systému je účelné místo mezery sloužící k oddělení jednotlivých písmen vyjádřených v Morseově abecedě volit symboly matematických operací. Zápis šifrového textu vypadá jako nějaký složitý početní příklad a tato jednoduchá steganografická metoda může zabránit tomu, aby se nepovolaná osoba zachyceným textem zabývala.

Použitý klíč pro převod kódu na čísla: tečka = sudá číslice, čárka = lichá číslice

Další detaily k systému: [1] str. 160-161

Otevřený text (řešení):

Jedna z největších civilizačních pohrom: učený hlupák.

K. Čapek

---

8 Jednoduchá záměna

44 555 88 7 2 55 1 9999 2 1 7 33 222 444 1 7777 33 3 444 1 222 44 999 8 777 33 44 666 1 888 1 666 55 666 888 33 222 44 1 888 33 3 666 88

Důkaz správného řešení: HLUPAK
Body: 2

Upřesnění systému: kódování, mobilní kód

Popis: Jedná se o kódování, kde pro kód písmena je použito vyjádření, které odpovídá psaní příslušného písmene na mobilním telefonu při přípravě SMS. Kódování lze odvodit z psaní znaků na mobilním telefonu. Např. při psaní písmene E musíte na jeho klávesnici dvakrát stisknout číslici 3 – tj. kód písmene E = 33 atd.

Další detaily k systému: [1] str. 172-173

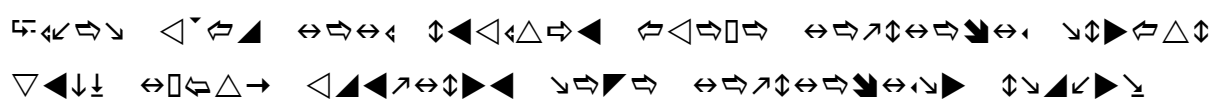
Otevřený text (řešení):

Hlupák za pecí sedí – chytrého v okovech vedou.

Ruské přísloví

---

9 Jednoduchá záměna



Důkaz správného řešení: OMYLU
Body: 1

Upřesnění systému: kódování, předefinované písmo v MS Windows

Popis: I v tomto případě se jedná o využití kódování. Zde je pro písmeno otevřeného textu použito vyjádření, které odpovídá psaní příslušného písmene v šifrové abecedě určené

zvoleným typem písma. Typ písma, které bylo v ukázce použito, je k dispozici v MS Wordu a jedná se o písmo/font Wingdings 3 .
Další detaily k systému: [1] str. 174-175

Otevřený text (řešení):
Cílem vědy není otvírat dveře nekonečné moudrosti, nýbrž vytknout meze nekonečnému omylu.
B. Brecht

---

10 Steganografie

budoVa podpEra uvoDnik vOzka Malajsie krOkodyl uSpech oTep zarucnI skryVat naHy syseL vydAVat bahEni vyBetonovat artIkl obyDli Ales stoKA hoJit rybA pibonKa kObra oDenek krizovY stetKA jeV adResar padnoUt oKo barOkni kroUPy smIr hnoJiste kozA oKtava kurAtko

Důkaz správného řešení: HLAVE
Body: 1

Upřesnění systému: steganografie, zvýrazněná písmena
Klíč: otevřený text tvoří velká písmena
Další detaily k systému: [1] str. 183

Otevřený text (řešení):
Vědomosti v hlavě bídáka – jako dýka v rukou pijáka.
Tádžické přísloví

---

11 Steganografie

Okno udělal ponekud snadno. Pes ucesan doma. Buchar omlatil pistol. Udalost nemela vlastne na ctyri doby. Okraj odvaha sok andulka text pusa. Emise pijano ondulace pilot. Tchan oteze televize hnus rus ocet nikdy!

Důkaz správného řešení: UCI
Body: 3

Upřesnění systému: steganografie, agenturní systém (nedokonalý text)

Klíč: čte se každé druhé písmeno ve slově

Další detaily k systému: [1] str. 183

Otevřený text (řešení):

Kdo něco umí, dělá to. Kdo neumí nic, ten učí.

G. B. Shaw

---

12 Steganografie

```
YQVVQ ECJEQ DNQAZ CIQJT QEXBH QZWOB QNIQE EEVQP LGYQR SXYQI
EQNGK FQAHL XQSWD YQICQ UYSRQ ZTQIS AAQTL QKTXN QUEQP JQOXQ
DXQOW QBSBI QAXQS PQEZQ LDQEX HYQKX PRQUV SNQJV QELCE QNCGVW
QZBCK QNXQE BQLUK SQEMQ CGFKQ IXXSA
```

Důkaz správného řešení: LEKU
Body: 2

Upřesnění systému: steganografie, domluvené písmeno

Klíč: otevřený text se získá vypsáním znaků za písmeny Q

Další detaily k systému: [1] str. 182

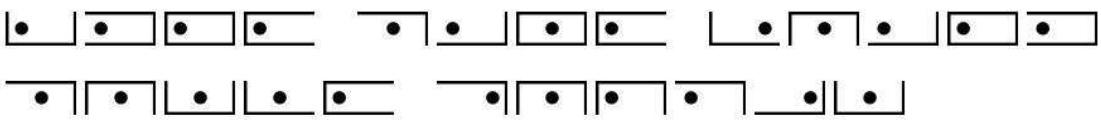
Otevřený text (řešení):

Věda, jež nepřináší užitku, podobá se léku, jenž neléčí.

Arabské přísloví

---

13 Jednoduchá záměna



Důkaz správného řešení: TVURCE
Body: 2

Upřesnění systému (klíč): jednoduchá záměna, převodová tabulka velký kříž

Popis: Velký kříž nebo též tzv. polský kříž patří do skupiny šifer jednoduché záměny, které nevyužívají klíče. Šifrová abeceda je tvořena dvaceti sedmi grafickými znaky, které odpovídají znakům mezinárodní abecedy rozšířené o písmeno Ch. Grafické znaky šifrové abecedy jsou odvozeny z umístění v „kříži“ (tabulce). Grafický znak se skládá ze symbolu buňky a tečky, která naznačuje umístění konkrétního znaku v buňce.

Další detaily k systému: [1] str. 52

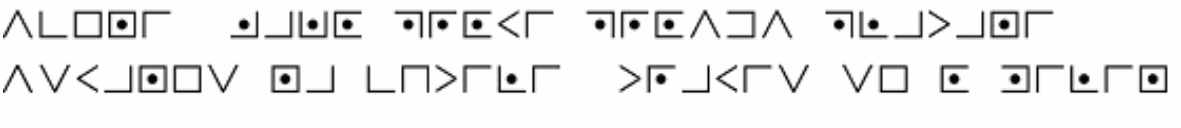
Otevřený text (řešení):

Dílo samo chválí svého tvůrce.

Latinské přísloví

---

14 Jednoduchá záměna



Důkaz správného řešení: MILI
Body: 2

Upřesnění systému (klíč): jednoduchá záměna, převodová tabulka hebrejský kříž

Popis: Obdobných šifrových systémů jednoduché záměny založených na vytvoření grafické šifrové abecedy, která v sobě nese informaci o umístění znaků v tabulce, lze vytvořit celou řadu. Mezi tři nejoblíbenější šifrové systémy tohoto typu patří také tzv. hebrejský kříž. Je vytvořen ze čtyř samostatných křížů. Dva prvé kříže jsou shodné s kříži použitými v systému „malý kříž“, další dva kříže jsou jiné a obsahují vždy kódy pouze pro čtyři znaky. Šifrová abeceda je tvořena dvaceti šesti grafickými znaky, které odpovídají znakům mezinárodní abecedy. Grafické znaky šifrové abecedy jsou odvozeny z umístění v buňce konkrétního kříže. Grafický znak se skládá ze symbolu buňky a tečky, která určuje, ve kterém ze čtyř křížů je umístěn konkrétní převáděný znak otevřeného textu.

Další detaily k systému: [1] str. 54

Otevřený text (řešení):

Učení – jako proti proudu plavání: ustaneš na chvíli – vrátíš se o míli.

Čínské přísloví

---

15 Transpozice

```
KNDEO MNUIZ KEDBY YNTEA BNYIL DDOIS TPEET LEYMM
```

Důkaz správného řešení: DOSPELYM
Body: 3

Upřesnění systému: transpozice, prolnutí textu

Klíč: text rozdělen na dvě poloviny a složen podle pravidel prolnutí

Popis: Jedná se opět o velmi jednoduchý transpoziční šifrový systém. Transpozice se vytváří tak, že se nejprve text rozdělí na dvě poloviny a potom se začne sestavovat šifrový text. Do vznikajícího šifrového textu se nejprve na liché pozice zapíší znaky prvé poloviny otevřeného textu a potom se šifrový text doplní na sudých pozicích druhou polovinou otevřeného textu. Obě poloviny otevřeného textu se zapisují zleva doprava.

Další detaily k systému: [1] str. 144

Otevřený text (řešení):

Kdo nikdy nebyl dítětem, nemůže být ani dospělým.

Ch. Chaplin

---

16 Transpozice

```
KIPBO OIDLE UTZXO ICDOD XPSHE VEXRS AHPJX
```

Důkaz správného řešení: POZDEJI
Body: 3

Upřesnění systému: transpozice podle tabulky,

Klíč: tabulka 5 x 7

Upřesnění: otevřený text zapisován do tabulky po sloupcích zleva doprava

Popis: Otevřený text se přepíše do sloupců obrazce nebo do tabulky o dohodnutém tvaru. Následně se text vypíše po řádcích. Pokud otevřený text zcela zaplní obrazec, zašifruje se tato

část a poté se pokračuje zápisem zbývající části. Pro snadné dešifrování je zvykem obrazec zaplnit nějakým dohodnutým znakem, např. X. (což ovšem výrazně současně pomáhá luštitelům pro určení velikosti tabulky).

Další detaily k systému: [1] str. 146-147

Otevřený text (řešení):

Kdo příliš spěchá, bude hotov později.

Židovské přísloví

---

17 Jednoduchá záměna

EVWVG QVFAM ZGPWB AMVXL ERHAV GLERH ZPWBA MVXLM VERHF AMZGA VGLMV ERH

Důkaz správného řešení: UZNAT

Body: 2

Upřesnění systému (klíč): jednoduchá záměna, ATBAŠ

Popis: Přibližně kolem roku 600 př.n.l. Hebrejci vynalezli a začali používat jednoduchou „reciprokou“ substituční šifru známou jako atbaš. Šifra spočívá v tom, že se vezme písmeno, spočítá se jeho vzdálenost od začátku abecedy, a nahradí se písmenem, které se nachází v téže vzdálenosti od konce abecedy.

Pro mezinárodní abecedu by podle tohoto pravidla vypadala převodová tabulka takto:

OT : 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

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

Další detaily k systému: [1] str. 38-39

Otevřený text (řešení):

Vědět je uznat, když něco víš, že to víš, a když něco nevíš, uznat, že to nevíš.

Konfucius

---

18 Jednoduchá záměna

LJMEN QMBMR NWNFI WSENZ NEMXH MBTEA LJMRA ENBMQ JIWMX SNQYN JNFMR AOPNQ M

Důkaz správného řešení: MLEKO
Body: 2

Vzhledem k malému počtu řešitelů byla 17. 9. 2006 zveřejněna v Cyrpto-News tato nápověda:

Soutěž v luštění 2006 - Nápověda č.2

http://crypto-world.info/news/index.php?prispevek=3831&sekce=c

Kapitán Carda (kolegy přezdívaný Cardano) včera večer nikam neletěl. Zato od 20.00 do 22.00 pracoval ve své pracovně a zabýval se tam tahákem z vězení. Díky němu získal klíč pro jeden ze systémů, který vězni rádi používají.

Dnes ráno si pustil počítač a přečetl si několik diskuzních příspěvků na http://www.premiere.cz/clanek/1829/diskuze.html. Když si přečetl příspěvek autora C-2P-1H-3H+1A+0A+2, tak se plácl do hlavy a vykřikl:
No jo, to je přece ten systém, který byl použit v té jednoduché záměně, co mně a mým kolegům tak odolává…
A začal si pískat svoji oblíbenou písničku Sweet Eighteen.

Na příslušném linku lze v diskuzi vyhledat příspěvek autora *C-2P-1H-3H+1A+0A+2* ve kterém se zmiňuje o dvou šifrových systémech ALBAM a ATBAH. Toto mělo pomoci při luštění, neboť v této úloze je použita šifra ATBAH.

Upřesnění systému (klíč): jednoduchá záměna, ATBAH

Jedná se, tak jako v předchozím systému, o hebrejskou šifru. Systém se opírá o hebrejské číslovky, které se podobně jako římské číslovky psaly pomocí písmen hebrejské abecedy. Prvních 9 písmen hebrejské abecedy bylo šifrováno tak, že se písmena očíslovala od 1 do 9 a nahradila znakem, jenž měl pořadové číslo odpovídající doplňku čísla do 10. Dalších 9 písmen substituce bylo nahrazeno obdobným způsobem, byly doplněny do hebrejské číslice 100. V desítkové soustavě by to znamenalo, že by se dělal doplněk do čísla 28.

Uplatněním výše uvedených pravidel na mezinárodní abecedu se získá tato převodová tabulka:

OT :	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
ŠT :	I	H	G	F	N	D	C	B	A	R	Q	P	O	E	M	L	K	J	Z	Y	X	W	V	U	T	S

Další detaily k systému: [1] str. 41-42

Otevřený text (řešení):

Pro někoho je věda vznešenou bohyní, pro jiného krávou, ze které dojí mléko.

F. Schiller

---

19 Jednoduchá záměna

WFEVT JOFMA FOBMP AJUOB ABEBT UPVTF NVTJN FABTO PVCJU

Důkaz správného řešení: ZADA
Body: 2

Upřesnění systému (klíč): jednoduchá záměna, Augustova šifra

Popis: šifrový text vzniká tak, že se nahradí písmeno otevřeného textu písmenem stojícím v abecedě těsně za ním. Písmeno Z se nahradí písmenem A (v originální šifře se nahrazovalo dvojicí AA).

Další detaily k systému: [1] str. 47

Otevřený text (řešení):

Vědu si nelze naložit na záda – s tou se musíme zasnoubit.

M. de Motagine

---

20 Jednoduchá záměna

OKDUL REYBN OHQHY HULPH DQLWH QNUDW NGBCP OXYLS UDYGX
Důkaz správného řešení: PRAVDU
Body: 2

Upřesnění systému (klíč): jednoduchá záměna, Caesarova šifra

Popis: Jedná se o dva tisíce let starý šifrový systém, který bezesporu patří mezi nejznámější šifrové systémy vůbec. Zavedení šifry se připisuje římskému císaři Caesarovi. Šifra je založena na tom, že se každé písmeno zprávy zaměnění za písmeno, které leží o tři místa dále v abecedě. K záměně lze také s výhodou použít převodovou tabulku.

Caesarova šifra																								
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
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Další detaily k systému: [1] str. 46

Otevřený text (řešení):

Lháři obvykle nevěříme ani tenkrát, když mluví pravdu.

M. T. Cicero

---

21 Jednoduchá záměna

```
QVCLH ZGPCH OHTAV SUZLP DSUSB VFTNV
KPLDV UPIMV ODVZP QCQHF TCSFC SZLPO
HTGSN PBVBP OHIMV MHZPG PNCDH GY
```

Důkaz správného řešení: BEDLIVE
Body: 3

Tato jednoduchá záměna dělala problémy. Důvod je zřejmý, šifrový text je příliš krátký, a proto frekvenční analýza není příliš účinná. Z tohoto důvodu byla zveřejněna 22. 9. následující nápověda. Spis č. j. 21 napovídal, že jde o nápovědu k úloze č. 21. Vyluštit úlohu v příloze je poměrně jednoduché. Vyluštěním této jednoduché záměny se získá stejná převodová tabulka jako v příkladu č. 21.

Soutěž v luštění 2006 - Nápověda č.3

http://crypto-world.info/news/index.php?prispevek=3872&sekce=c

Kapitán Carda dostal záchyt napsaný v jednoduché záměně. Usmál se, to bude lahůdka. Pak se podíval, kdo jej poslal a řekl, zkusím nejdříve, zda nepoužili stejný klíč jako v tom posledním dopise č. j. 21/2006.

```
CSIVQ SGASM LSCHD PRYIM PZLVU SGYAS
MLSGH ZUPLD HAVHL GHUVG SPCDA HBPQH
LGPNZ SNPUG HUVGS AOZSG PNFYD YQPFV
GPNFY NDYFY NDPDV GZPMS QBPLG PAPNQ
HUGVC SGAPD SMPAM YIQHQ HTMCQ PMSGS
KVZPD SAPNQ TLHQM HITGS DHUAO SFPDP
HGTUQ PXQTQ SCPLS DPNQS DHZSA SQPCH
LDPQT GPBVN QYSDP IHCTL KTLPU OHLGP
IHASN VKTLP NCTIV GSZSB PFATH LDPQS
QUZLY UIHGL PDVNQ MPLTS HUVCP GLTUP
LUSAP QBPLG SOHLV GUYBV FPAGP VUHNQ
SQGVL GYGSD PQVNQ VKTLQ PLUPO HLVGY
IMPLH LDPQP FFVFH CMSNG YAOZS ZVQCT
FTZPQ PZVNC SQCDV ACQSB TFGSV CMSNG
PIMVM HLYIH ZHMFV NQHLP NQVGS APFTZ
PKYQI MHCSZ LYHLD PQBVG P
```

Otevřený text k šifrovému textu v nápovědě je následující:

```
KAPITAN CARDA KOLEGY PREZDIVANY CARDANO ZVEDL OCI OD NOVIN A REKL CO
JE TO DNES ZASE V NOVINACH ZA NESMYLY TEMI NESMYSLY MYSLEL INZERAT
JEDNE CESTOVNI KANCELARE CRYPTO-TOUR KTERA NABIZELA CESTU DO TROPU
NA LOV CHAMELEONU V TEXTU TAKE DALE STALO ZACATEK ODLETU NEJISTY ALE
POKUD BUDE VHODNE POCASI BUDE SKUPINA ZAJEMCU ODLETAT VZDY V PONDELI
STREDU A O VIKENDU VE DVACET JEDNA HODIN VYJIMECNE I V OSTATNI DNY
NA LETISTI BUDTE DVE HODINY PRED ODLETEM MIMO KRASNYCH ZAZITKU
```

```
MUZETE ZISKAT KLIC K TAJUM NASI KRASNE PRIRODY POZOR MISTO DESTINACE
MUZE BYT PRO KAZDY ODLET JINE
```

Upřesnění systému úlohy č. 21:

jednoduchá záměna, převodová tabulka sestavena podle klíče

Klíč: abeceda šifrového textu je určena pomocí ověřovací věty: *Skákal pes přes oves*,

po odstranění opakujících se písmen získáme klíč: S K A L P E R O V

Převodová tabulka (stejná jako v nápovědě č. 21):

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

Další detaily k systému (včetně návodů na luštění obecné jednoduché záměny): [2], [3].

Otevřený text (řešení):

Ti, kdož někoho učí a vzdělávají, musí bedlivě přihlížet k tomu, kam každého unášejí jeho přirozené sklony.

M. T. Cicero

---

22 Jednoduchá záměna

```
AKLSA KPVQU DUQDU VGUSS NXJQZ LOJFN
TENEL XUDUZ LAGPA SVCUA FTENO ANVQU
DLAFN DUYLV KCUAF TUYJD FDJAS LOUQZ
AOUZL APAFU GVSTU CNQNQ JAFLC UDOIS
VYVVF OEXUS PJTEJ OYVTL XDJFN DUAQZ
LTDP
```

Důkaz správného řešení: NEDOUK
Body: 3

Upřesnění systému: převod určen tabulkou (abeceda šifrového textu je náhodně rozházená)

Klíč (převodová tabulka):

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

Další detaily k systému (včetně návodů na luštění obecné jednoduché záměny): [2], [3].

Otevřený text (řešení):

Školský učenec, neuměl-li zachovati přirozeného smyslu, jest při vší učenosti nedouk, jest pedant na slovech svého systému lpějící, často jen v bludu utvrzelý a pravdu poznati neschopný.

J. Jungmann

---

23 Polyalfabetická substituce

```
BAEAK STFEK IQCNA KMDSS NQMWG VLODA
DUDNV MTATM GMZER UTGDQ LMMEC LGDWN
RQFQT WMZP
```

Důkaz správného řešení: UCITELUM
Body: 3

Jako nápověda byl k této úloze zveřejněn v kleci č. 31 (21. 9. 2006) následující Chameleón 6/23:

Kapitán Carda se zajímá o záhadu RKZ

Kapitán Carda se rozhodl hledat inspiraci ve výletu za záhadou Sporu o rukopisy (Královédvorský a Zelenohorský = RKZ), který byl bezesporu jednou z nejdůležitějších událostí konce 19. století, kdy pozitivistická věda potřela pravost romantických nacionalistických padělků z počátku 19. století.
Rukopis královédvorský byl objeven v roce 1817 a hlásí se do doby Václava II. (13. století), pokud byl pravý, byl by jednou z nejstarších česky psaných památek vůbec. Nejznámější je báseň o vítězství Jaroslava ze Šternberka nad Mongoly u Olomouce v roce 1241. Rukopis zelenohorský byl objeven v roce 1817, resp. 1818 a hlásí se do doby před přijetím křesťanství. Kdyby byl pravý, byl by nejstarší česky psanou památkou vůbec. Jeho námětem je popis rozhodnutí kněžny Libuše, a proto byl původně zván Libušin soud.
Nejpravděpodobnějšími autory obou padělků jsou Václav Hanka a Josef Linda. Jedním z prvních vědců, který zpochybnil pravost Zelenohorského rukopisu byl Josef Dobrovský. Spor se však vedl po téměř celé 19. století.
Závěrečná fáze sporu o pravost začala, když v únoru 1886 vyšel v Atheneu, z podnětu osoby, jehož jméno inspirovalo kapitána Cardu k vyluštění další úlohy, článek předního českého filologa Jana Gebauera. V bojích o RKZ se také zrodil třetí český politický směr realismus (představitelé: Kaizl, Kramář, + jméno toho, kdo zajistil vydání článku Jana Gebauera). Kapitán Carda vždy tohoto muže obdivoval. Neproslul jen bojem za uznání RKZ jako padělku, ale stal se později významným a uznávaným představitelem českého národa. Ve sporu o rukopis (http://kix.fsv.cvut.cz/win/~urban/r/tabu/kalousek/k4.htm) si kapitán Carda našel pasáž: Divný ***chameleón*** *musel býti ten falsarius Hanka. Jednak falsátor RZho byl právě tak chatrným právníkem, jako gramatikem a básníkem; jednak falsarius Hanka roku 1817 byl*

značně vzdělán a měl mnohem více vědomostí, než většina dnešních obránců; potom však RK a RZ jsou díla začátečníků gramatických, a RZ i paleografických; a když pak Hanka udělal kolem 1827 evangelium Svatojanské, a Gebauer je hájil ze stránky linguistické, z toho jen vyplývá, že falsarius byl – dovedný, nic více.

Řešitelé poměrně snadno zjistili, že *„jméno toho, kdo zajistil vydání článku Jana Gebauera“* je MASARYK. Toto jméno je také hledané periodické heslo této šifry.

Poznámka: hledané jméno šlo např. získat zadáním slov „Athenau RKZ“ do google.com. Vrácené odkazy např. http://cs.wikipedia.org/wiki/Spor_o_rukopisy, http://mailman.fsv.cvut.cz/lists/rkz-l/1998/msg00068.html, atd. jasně ukazují, že to byl Jan Masaryk, kdo zajistil vydání citovaného článku. V nápovědě je více indicií, jak hledané jméno najít, ale tato byla naprosto jednoznačná.

Upřesnění systému úlohy č. 23:

polyalfabetická substituce systém Vigenére, periodické heslo

Klíč (heslo): MASARYK

Další detaily k systému: [1] str. 61-64, luštění např. [2], [4], řešení úloh v předchozích ročnících.

Otevřený text (řešení):

Pamatujte si, že dokud budeme generálům platit víc než učitelům, nebude na světě mír.

J. Masaryk

---

24 Polyalfabetická substituce

```
TREFT ZNYEP UFUFY IIOWA UJDTA PVPTF
PUCRB OHRNY EPWIV IP
```

Důkaz správného řešení: UHODL
Body: 4

I v tomto případě byla zveřejněna nápověda a to dokonce opakovaně v podobě chameleónů 1/24 (16. 9.) a 2/24 (17. 9. 2006)

Kapitán Carda přišel na letiště a zjistil, že dnes nikam neletí.
Naštvaně odešel do své kanceláře a začal řešit rozdělaný případ.
Na stole měl moták jednoho vězně z věznice v Leopoldově.
Stálo v něm:

Klíč lze získat vyčíslením hesla, které najdeš na www stránce
http://www.maggiesfarm.it/bolzano.htm
a to hned pod prvním obrázkem. Jo mimochodem je to přezdívka Tvé kámošky.
Chameleon (140625387).
Carda se pousmál, už se těším na vaše šifrové motáky!
Byl si jistý, že je snadno dešifruje. Věděl, že v této věznici všichni používají pouze jeden šifrový systém..

Řešitel našel na lince uvedené v nápovědě příslušnou fotku a pod ní tři jména, která přicházela do úvahy: Hamster, Chameleon, Albatros.

Jméno použité jako klíč v soutěžní úloze je ALBATROS. Vzhledem k tomu, že řešitelé věděli, že úlohy budou otištěny v knížce, kterou vydá nakladatelství Albatros, mohli si být touto volbou zcela jisti. V opačném případě museli otestovat všechna tři hesla.

Gronsfeldův systém byl používán často ve věznicích, proto ta narážka na věznici Leopoldov.

Systém používá číselný klíč, který se získá vyčíslením hesla. Pro řešitele bylo proto v nápovědě také naznačeno, jak správně při vyčíslení postupovat.
Vyčíslení hesla Chameleón --- *140625387* (čísla v klíči ukazují abecední pořadí písmen v hesle, prvé písmeno má odpovídající kód 0 nikoliv 1 !)

Upřesnění systému: polyalfabetická substituce, systém Gronsfeld, periodicky se opakující klíč:

Klíč: 03217546

Poznámka: klíč lze získat vyčíslením hesla ALBATROS

Další detaily k systému: [1] str. 69-70, luštění např. [2], [4].

Otevřený text (řešení):

To, čemu jsem se naučil, už neznám. To málo, co znám, jsem uhodl.

A. Chamfort

---

25 Transpozice

```
NOOOT OJVNE XJADM EVHOE PEETE OLEOM
DJNAT THAHO EORID KENZS OZTOJ NIVHA
ZTEEE BEOTO NECNT TS
```

Důkaz správného řešení: NEJPOTREBNEJSI
Body: 3

Upřesnění systému: jednoduchá sloupcová transpozice, úplná tabulka

Transpoziční klíč: 6-3-2-5-7-4-1

Poznámka: klíč lze získat vyčíslením hesla TOLSTOJ, při určení tabulky lze využít mimo poměru samohlásek a souhlásek znak X, který byl použit pro vyplnění tabulky.
Další detaily k systému: [1] str. 82-85, luštění [1] str. 88-93, [2], [4].

Otevřený text (řešení):

Nejde ani tak o to vědět toho mnoho, ale znát ze všeho toho, co je možné vědět, to nejpotřebnější.
L. N. Tolstoj

---

26 Transpozice

```
BNNEI OVKXE OOTED HEXCR JKTAA DAAER
TDKUE XEAEJ EVPIS NTNER EOVUC RDOHU
AVXUO IIKNN IRLNO IEAKD XVIBD LJDEX
```

Důkaz správného řešení: LABORATORI
Body: 3

Upřesnění systému: jednoduchá sloupcová transpozice, úplná tabulka
Transpoziční klíč: 8-3-5-6-2-7-10-9-4-1
Poznámka: klíč lze získat vyčíslením hesla: SKLODOWSKA, při určení tabulky lze využít mimo poměru samohlásek a souhlásek znak X, který byl použit pro vyplnění tabulky.
Další detaily k systému: [1] str. 82-85, luštění [1] str. 88-93, [2], [4].

Otevřený text (řešení):
Učenec v laboratoři není jen odborník, je to dítě, které hledí na vědu jako na pohádku. Vidí ve vědě krásu.
Marie Curie-Sklodowská

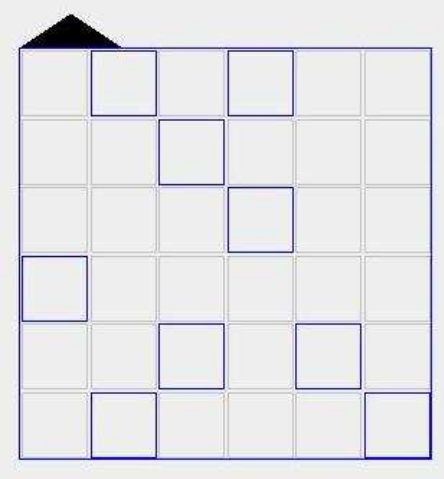
---

27 Transpozice

```
EMMLS NYTUR ESMLI VEIIR LTITT OTEAX JNTXA E
```

Důkaz správného řešení: STRILET
Body: 4

Upřesnění systému: Fleissnerova otočná mřížka, velikost 6 × 6
Klíč: otočná mřížka



Další detaily k systému: [1] str. 101-103, [6]. Poznámky k luštění lze nalézt v řešení obdobné úlohy soutěže z roku 2004 [12].

Otevřený text (řešení):

Mluvit a nemyslet, to je střílet a nemířit.

M. de Cervantes

---

28 Playfair

```
ESLPY GOMLR STOBP GACOR OMYUL WGBSV
AVSAY GETQB DYEXE ZEZRG HN
```

Důkaz správného řešení: ZEZLO
Body: 5

Systém je příliš těžký pro luštění, a proto byl 19. 9. 2006 zveřejněn *Chameleón 4/28*, který umožnil řešitelům získat heslo pro sestavení abecedního čtverce a další informace o systému tak, aby šlo na základě těchto informací šifrový text dešifrovat.

Chameleón 4/28.

Protože cestovní kancelář Crypto-Tour dnes žádný zájezd nepořádá, zašel si kapitán Carda s kamarády místo výletu na fotbal. Hráli na klubovém hřišti Děkanka Hřiště SK Nusle. Po zápase si zašli společně do oblíbené klubové hospůdky soupeře, kterou je Bar Chameleón. Kapitán mužstva se jim chlubil, že hned od založení v roce 2002 mají vlastní www stránku. Prý stačí zadat heslo ***mužstvo veteránské hanspaulské ligy****. Trošku popili, zavzpomínali a pak šli domů.*
Doma se kapitán Carda pustil do práce. Snažil se rozluštit jednu šifru Playfair. Věděl toho poměrně dost např., že v převodovém čtverci 5 x 5 je ztotožněn znak I a J a jako nulová písmena se pro doplňování do čtverce použijí při šifrování a dešifrování: ZQ. Co však nevěděl, bylo heslo pro sestavení abecedního čtverce. Jen tak mimochodem vepsal místo hesla název fotbalového klubu se kterým dnes hrál.
A tu nevěřil vlastním očím, před ním se začal objevovat hledaný otevřený text.

Po chvilce „googlování“ měl řešitel odhalit stránku

http://www.tychodebrahe.mysteria.cz/vet/home.htm

K tomu např. stačí do vyhledavače zadat tyto údaje z Chameleóna „Děkanka Bar Chameleon“.

Z textu na stránce je zcela zřejmé, že hledané mužstvo se jmenuje **Tycho de Brahe VET**.

Hledané heslo pro sestavení abecedního čtverce je Tycho de Brahe.

Upřesnění systému: Playfair (abecední čtverec 5 x 5)

Klíč:

Heslo pro sestavení abecedního čtverce: TYCHO DE BRAHE

Ve čtverci 5 x 5 je ztotožněn znak I a J.

Jako nulová písmena pro doplňování do čtverce se použijí při šifrování a dešifrování: ZQ.

Abecední čtverec:

T	Y	C	H	O
D	E	B	R	A
F	G	I/J	K	L
M	N	P	Q	S
U	V	W	X	Z

Další detaily k systému: [1] str. 77-81, [7].

Otevřený text (řešení):

Ani světská moc, ani bohatství, jen žezlo vědy přetrvává věky.

Epitaf na náhrobku Tychona de Brahe

29 BIFID

```
UPYML UZATM OWNLA AYXFU YZAQM IZYPN
WRYMA HUPYC LUZHH HAYXY HYEON AYDIZ
CVPYP MYPFA HQUAW PYAEM NAKU
```

Důkaz správného řešení: POKUS
Body: 5

Tento systém je také příliš těžký pro luštění, a proto byl 18. 9. 2006 zveřejněn *Chameleón 3/28,* který umožnil řešitelům získat heslo pro sestavení abecedního čtverce. Vzhledem k tomu, že systém není příliš znám a nebyly v nápovědě zveřejněny další informace o systému (dělba, způsob sdružování, použití tabulky řádek/sloupek nebo sloupek/řádek), stala se tato úloha jednoznačně nejtěžší úlohou. Alespoň dodatečně jsem proto sepsal všechny používané varianty a ty zveřejnil [9], tento text je také uveden v příloze k tomuto e-zinu.

Crypto-Tour - Tajemství Chameléona v díle KORNELIA AGRIPPY

Dnešní výlet cestovní kanceláře Crypto-Tour je věnován tajemství Chameleóna tak, jak je popsáno v knize OKULTNÍ FILOSOFIE, kterou věnoval JINDŘICH KORNELIUS AGRIPPA Z NETTESHEIMU panu JANU TRITHEIMOVI, opatu u sv. Jakuba v předměstí wurzburském.

Studijní materiál:
kap.13 - ... spálená játra chameleóna ...
kap.17 - ... jímž také havrani ničí jed chameleóna ...
kap.17 - ... Pozře-li slon chameleóna ...
kap.21 - ... jazyk chameleóna vytržený živému ...
kap.24 - ... Lunární jest i chameleón, který mění barvu ...

Pro lovce záhad pak zvláště doporučujeme zjistit, kdo v kapitole ***Odkud plynou skryté síly věcí*** *odvozuje takové účinky z inteligencí. Jméno tohoto vědce bylo častým klíčem k mnoha záhadám a to nejen ve středověku, ale i mnohem později např. při sestavování převodových tabulek ke zlomkovým systémům Delastelle, TRIFID, kde prvá i druhá převodová tabulka jsou totožné.*

Heslo pro vyhledání knihy v Internetové (Google) knihovně : JINDŘICH KORNELIUS AGRIPPA Z NETTESHEIMU CHAMELEON

Způsob sestavení převodové tabulky pro heslo CHAMELEON

```
.....1..2..3..4..5
1....C..H..A..M..E
2....L..O..N..B..D
3....F..G.I/J.K..P
4....Q..R..S..T..U
5....V..W..X..Y..Z
```

Nápověda je zcela jasná. Řešitel vyhledal pomocí Googlu (zadáním slov J*INDŘICH KORNELIUS AGRIPPA Z NETTESHEIMU CHAMELEÓN)* www stránku

http://www.focl.szm.sk/Magick_%20okultni%20filosofie.html a zde podle názvu ***Odkud plynou skryté síly věcí*** kapitolu 13 a v ní se lze dočíst, že **Avicena odvozuje takové účinky z inteligencí.**

Řešitel tak získá klíč pro vytvoření převodové tabulky. Způsob sestavení tabulky je v nápovědě také naznačen. Co však řešitel nemá k dispozici, je dělení na skupiny (lze odhadnout dělbu po pěti znacích), způsob sdružování a použití čtverce (tj. zda se při převodu písmen na čísla používají nejprve souřadnice sloupců a pak souřadnice řádků nebo naopak).

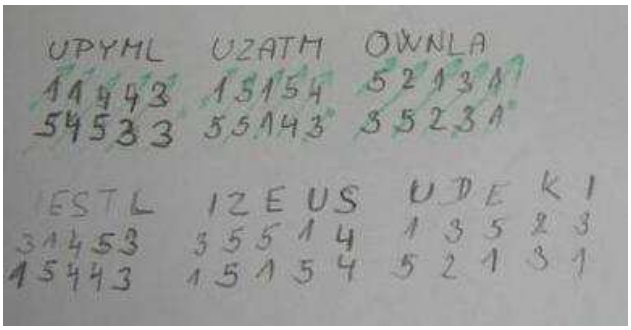
Upřesnění systému: zlomkový systém BIFID, kde prvá i druhá převodová tabulka jsou totožné.

Klíč pro vytvoření převodové tabulky: AVICENA

V tabulce je ztotožněn znak I a J.

Převodová tabulka :

	1	2	3	4	5
1	A	V	I/J	C	E
2	N	B	D	F	G
3	H	K	L	M	O
4	P	Q	R	S	T
5	U	W	X	Y	Z



Obr. postup dešifrace použitý vítězem soutěže (poznámka: v příkladě je chyba, místo 51 je omylem uvedeno 15)

Upřesnění dalších parametrů:
V šifře bylo použito sdružování ve skupinách po pěti a to směrem šikmo nahoru. Použitá verze spočívá v tom, že se začne posledním dolním znakem v každé skupině a ten se sdruží s prvním horním znakem skupiny, dále se již postupuje pravidelně zdola šikmo nahoru až na konec skupiny. Při převodu písmen na zlomky a zpět byla využívána převodová tabulka tak, že se nejprve udávaly souřadnice sloupku a pak řádku.

Další detaily k systému: [1] str. 77-81, [9].

Otevřený text (řešení):

Jestliže úsudek je potvrzen skutečností a jestliže jej potvrzuje pokus, naše přesvědčení se upevní.

Avicenna

---

30 ADFGX

XDGFX FAFDF XADFA FDGXA DXDGA AAXAD

AXADA AGDFG DDDDA DGGDD DDADG GAFAX

AXXGA DADXG FGFDG DDDDD GGDXA DGGXA

DDXDX FDFFD GAXFF DGFAA GXXDA GGXAF

AFDDX XAFAF GGDXF FFAFF DGAAF AFFXG

DAFFD ADGXA GDXAD DXD

Důkaz správného řešení: DOHONIT
Body: 5

Systém je příliš těžký pro luštění, a proto byl 20. 9. 2006 zveřejněn *Chameleón 5/30*, který umožnil řešitelům získat klíč a další informace o systému tak, aby šlo na základě těchto informací šifrový text dešifrovat.

Crypto-Tour - Dnešní výlet pořádá naše cestovní kancelář do Číny.
I-ťing v díle zakladatele první filosofické školy Číny

Zájemcům o tajemno doporučujeme seznámit se s dílem zakladatele první čínské filosofické školy. Tento učenec žil v letech 551 př. n. l. - 479 př. n. l. Jeho dílo je shrnuto do tzv. devíti klasických knih ťing - autorem prvních čtyř je on sám, pátá je jeho dílem zčásti, zbylé čtyři jsou pak dílem jeho žáků a následníků.
*Nejvýznamnější je hned kniha první - **I-ťing**. Jedná se patrně o nejstarší dochovaný dokument filosofického myšlení vůbec. Podle tradice je autorem této knihy jistý císař, vládnoucí tři tisíce let před naším letopočtem, učenec, o němž píšeme, ji pouze znovu vydává a opatřuje svými komentáři.*
Jádrem díla je osm tzv. trigramů, znaků složených ze tří plných nebo přerušovaných čar - každý trigram přitom znázorňuje určitou přírodní sílu a zároveň symbolizuje nějaký element lidského života. Vzájemná kombinace těchto trigramů pak ponechává velice široké pole působnosti pro možný výklad skryté pravdy.
*Česká autorka Daniela Bednářová ve svém díle Čínská filosofie k překladu názvu díla uvádí, že znak **I** je znak používaný pro **chameleóna** a je symbolem proměny, **ťing** pak znamená pojednání. Kniha se tedy do češtiny překládá jako Pojednání o proměnách nebo častěji Kniha proměn.*
Pro účastníky zájezdu dodávám, že jméno filosofa (v klasickém přepisu do latinky) bylo použito ještě během prvé světové války jako klíč polní šifry ADFGX, kde permutační i substituční klíč byl stejný. Sloužil tedy jednak k vytvoření převodové tabulky a jednak po permutačním vyčíslení jako klíč pro sloupcovou transpozici.
Permutační vyčíslení slova Chameleon = 251736498
Přeji příjemný let!

Řešitelé podle indicií v nápovědě snadno naleznou jméno čínského učence. Je jím Konfucius. Jeho jméno slouží k vytvoření převodové tabulky a jako klíč pro sloupcovou transpozici. V nápovědě je i na příkladě uvedeno, jak se permutační vyčíslení ze slova vytváří. Tyto informace jsou postačující, aby mohl řešitel přejít k dešifraci úlohy.

Upřesnění systému: polní šifra ADFGX, kde permutační i substituční klíč je stejný.

Substituční klíč (pro vytvoření převodové tabulky): KONFUCIUS

V tabulce je ztotožněn znak I a J.

Převodová tabulka :

	A	D	F	G	X
A	K	O	N	F	U
D	C	I/J	S	A	B
F	D	E	G	H	L
G	M	P	Q	R	T
X	V	W	X	Y	Z

Permutační klíč (pro sloupcovou transpozici): KONFUCIUS

Permutační klíč po vyčíslení: 4-6-5-2-8-1-3-9-7

Další detaily k systému: [1] str. 121-125, [10].

Otevřený text (řešení):

Učte se, jako byste se hnali za někým, koho nemůžete dohonit, a jako by to byl někdo, koho nechcete ztratit!

Konfucius

---

31 závěrečná úloha

Text úlohy:

V této místnosti je vystaven nejvzácnější chameleón ze sbírky kapitána Cardy. Chameleón je uzavřen v kleci, která je opatřena kódovým zámkem. Vaším úkolem je nalézt kód k otevření tohoto zámku.
Jak kód kapitán Carda připravil, je popsáno zde
http://soutez2006.crypto-world.info/ukoly/epilog.pdf

Důkaz správného řešení: EALORRILYHI
Body: 6

Závěrečná úloha soutěže byla zveřejněna po dvou upozornění (nápovědy č. 4 a č. 5)
23. 9. 2006.

Soutěž v luštění 2006 - Nápověda č. 4 (výstava chameleonů)

http://crypto-world.info/news/index.php?prispevek=3873&sekce=c

Výstava chameleonů začala. Kompletní program a exponáty ze sbírky kapitána Cardy lze najít na http://soutez2006.crypto-world.info/ukoly/vystava.pdf .
Nejcennější kus výstavy bude za zvýšených bezpečnostních opatření dovezen během dne. Budete jej moci obdivovat v místnosti 31.

Soutěž v luštění 2006 - Nápověda č.5 (cryptomelon dovezen)

http://crypto-world.info/news/index.php?prispevek=3873&sekce=c

Výstava chameleonů pokračuje zlatým hřebem, na který se všichni účastníci dlouho těšili. Kapitán Carda dovezl nejcennější exponát své sbírky Cryptomelona Pragensis.
Chameleón byl uzavřen do speciální klece v místnosti 31, která je opatřena bezpečnostním kódovým zámkem. Kapitán Carda doufá, že se k němu nikdo nedostane.
Nezapomeňte, že ten kdo jako prvý ukořistí ze všech 31 místnosti exponáty, se současně stává vítězem naší soutěže posledním dopise č. j. 21/2006.…
Další informace najdou zájemci
http://soutez2006.crypto-world.info/ukoly/epilog.pdf

Text epilog.pdf obsahoval všechny potřebné informace, které řešitelé potřebovali, aby se mohli pustit do luštění posledního úkolu.

epilog.pdf

Klec v místnosti 31

Kapitán Carda přivezl za zvýšených bezpečnostních opatření nejcennější exponát výstavy – dosud neznámou variantu chameleóna, kterého nazval Cryptomelon Pragensis. Chameleón byl uzavřen do speciálně zabezpečené klece v poslední výstavní místnosti 31.

Klec byla opatřena kódovým zámkem. Kapitán Carda zadal kód, kterým zámek uzavřel. Chameleón tak zůstává v naprostém bezpečí, zámek lze totiž otevřít jedině tak, že kód někdo bezchybně zadá.

Kapitán Carda se svěřil přítomným novinářům, že podle něj to není prakticky možné. Na otázku, co se stane, když on sám kód zapomene, odpověděl, že by to nevadilo, protože je schopen kdykoliv kód odvodit. Dokonce řekl novinářům, že je ochoten jim postup sdělit, ale je přesvědčen, že i tak jim to nebude nic platné. Po menším naléhání postup prozradil, ale zdůraznil, že je tam několik neznámých, které jim neprozradí a tím zaručí bezpečnost své chlouby Cryptomelona Pragensis.

Kapitán Carda začal vysvětlovat, jak kód připravil:

„Nejdříve jsem sepsal tajná jména všech třiceti chameleónů, které jsem zde na výstavu přivezl a které jsou po jednom uloženy v místnostech 1 až 30. Potom jsem jména sepsal do dvou sloupců o 15-ti řádcích. Nejdříve jsem zaplnil sloupec první a pak druhý. V prvém řádku je tedy tajné jméno prvého a šestnáctého chameleóna atd.

Potom jsem v textu zvolil jedno slovo, které jsem přesvědčen, že nezapomenu. Slovo je vytvořeno jednoznačně v tom smyslu, že jsem vzal prvé písmeno slova a v textu vyznačil jeho prvý výskyt. Pak jsem vzal druhé písmeno slova a od místa, kde jsem skončil, jsem nalezl opět prvý výskyt tohoto druhého písmene a takt jsem pokračoval dále. Mimochodem poslední písmeno zvoleného slova leží v posledním řádku. Pro jistotu jsem si však vyrobil mřížku, kterou, když na text přiložím, tak slovo uvidím. Takové šifrovací mřížce se říká Cardanova" (nezapomněl poučit novináře kapitán Carda o svém nejoblíbenějším systému).

„Mřížku jsem schoval do trezoru a nikdo se k ní nedostane" , pokračoval ve svém výkladu. *Původně jsem chtěl toto slovo použít jako kód zámku na klec s chameleónem. Pak jsem si však vzpomněl na přednášky z informační bezpečnosti a bylo mi najednou jasné, že to není dokonalé heslo, protože by jej mohl někdo uhodnout a nebo se mohl pokusit otevřít klec „slovníkovým útokem". Rozhodl jsem se tedy heslo zesílit velmi důmyslným a dosud nikde nepopsaným způsobem. Jsem přesvědčen, že ani můj známý Pavel Vondruška takovýto postup nezná! No* (upřesnil kapitán Carda), *alespoň si myslím, že nezná, protože tento postup ve své knize Kryptologie, šifrování a tajná písma nepopsal.*

Zesílení spočívá v tom, že za heslo neberu přímo písmena kódu, která lze v otvorech Cardanovy mřížky přečíst, ale písmena následující přímo v textu vpravo za nimi. Kód tedy vypadá zcela náhodně a nelze jej získat slovníkovým útokem.

Jsem přesvědčen, že chameleóna mi nikdo do konce výstavy (začátek listopadu) neukradne, neboť na rozdíl ode mne nezná tajná jména mých třiceti chameleónů a nemá moji mřížku!

Novináři výkladu kapitána Cardy příliš nerozuměli, a tak jim vše vysvětlil ještě jednou na malém příkladu. Vzal 6 slov a sepsal je do dvou sloupců po třech.

DNES	**BOTA**
BOK	**NOS**
VLAK	**BRÁNA**

Potom zvolil vhodné slovo - BASA. Toto slovo je v dané tabulce vepsáno výše popsaným jednoznačným způsobem. Příslušná Cardanova mřížka by vypadala tak, že by měla vystřižené mezery v místech, které vyznačil žlutě. Kód k zámku klece je v tomto případě OBVK (písmena ležící za vybraným slovem BASA).

Řešení:

Luštitel postupuje podle návodu, který prozradil novinářům kapitán Carda. Nejdříve sepíše do dvou sloupců o 15-ti řádcích. „tajná jména všech třiceti chameleónů" – což samozřejmě není nic jiného než slova, která dokazují, že našel správné řešení jednotlivých úloh 1-30.

A to tak, že v prvém sloupci jsou řešení úloh č.1-15 a ve druhém č.16-30.

```
APATYCE   POZDEJI
CESTA     UZNAT
VINO      MLEKO
PET       ZADA
```

```
PENEZUM  PRAVDU
MORALKU  BEDLIVE
HLUPAK    NEDOUK
HLUPAK    UCITELUM
OMYLU    UHODL
HLAVE    NEJPOTREBNEJSI
UCI      LABORATORI
LEKU     STRILET
TVURCE   ZEZLO
MILI     POKUS
DOSPELYM DOHONIT
```

Potom je potřeba uhodnout slovo, které kapitán Carda v textu vyznačil. Podle toho, jak o tomto slovu kapitán Carda mluví, na základě toho, že se jedná o klec č. 31 a podle dalších detailů uvedených v textu epilog.pdf se dá odhadnout, že tím hledaným slovem je **CRYPTOMELON**.

Slovo řešitel zapíše podle popisu kapitána Cardy, tj. vezme prvé písmeno slova a v textu vyznačí jeho prvý výskyt. Pak se vezme druhé písmeno slova a od místa, kde řešitel skončil, nalezne opět prvý výskyt tohoto druhého písmene a tak se pokračuje dále až se vyčerpají všechna písmena slova. Z popisu také víme, že poslední písmeno zvoleného slova leží v posledním řádku.

```
APATYCE  POZDEJI
CESTA    UZNAT
VINO     MLEKO
PET      ZADA
PENEZUM  PRAVDU
MORALKU  BEDLIVE
HLUPAK    NEDOUK
HLUPAK    UCITELUM
OMYLU    UHODL
HLAVE    NEJPOTREBNEJSI
UCI      LABORATORI
LEKU     STRILET
TVURCE   ZEZLO
MILI     POKUS
DOSPELYM DOHONIT
```

Zbývá provést poslední krok k získání posledního slova, které se použije jako důkaz správného řešení poslední úlohy.

Foto: Hackerský útok na vzácného chameleóna … (z archívu autora)

Kapitán Carda píše: *Zesílení spočívá v tom, že za heslo neberu přímo písmena kódu, která lze v otvorech Cardanovy mřížky přečíst, ale písmena následující přímo v textu vpravo za nimi. Kód tedy vypadá zcela náhodně a nelze jej získat slovníkovým útokem.*

Řešitel nyní jednoduše vezme písmena ležící vpravo od žlutě vyznačených písmen tvořících slovo Cryptomelon a dostane hledané řešení.

CRYPTOMELON
EALORRILYHI

Hledané slovo, důkaz správného řešení úlohy č. 31 je : **EALORRILYHI**

K O N E C

Citované odkazy:

[1] Vondruška, P.: Kryptologie, šifrování a tajná písma, edice OKO, Albatros, Praha 2006
[2] MFF UK, Úvod do klasických a moderních metod šifrování ALG082
http://www.karlin.mff.cuni.cz/~tuma/nciphers.html
[3] Jednoduchá záměna - Crypto-World 10/2000, str. 2-4,
http://crypto-world.info/casop2/crypto10_00.pdf
[4] Jednoduchá transpozice - Crypto-World 11/2000, str. 2-6,
http://crypto-world.info/casop2/crypto11_00.pdf
[5] Periodické heslo, srovnaná abeceda - Crypto-World 12/2000, str. 4-10,
http://crypto-world.info/casop2/crypto12_00.pdf
[6] Fleissnerova otočná mřížka - Crypto-World 11/2004, str. 7-8,
http://crypto-world.info/casop6/crypto11_04.pdf
[7] Popis šifry PlayFair - Crypto-World 3/2005 , str. 11-14,
http://crypto-world.info/casop7/crypto03_05.pdf
[8] Popis šifry ÜBCHI - http://soutez2005.crypto-world.info/images/UBCHI.pdf
[9] Popis šifry BIFID - http://crypto-world.info/oko/bifid.pdf
[10] Popis šifry ADFGX - http://soutez2005.crypto-world.info/images/ADFGX.pdf
[11] Soutěž 2003 - Crypto-World 12/2003, celé číslo,
http://crypto-world.info/casop5/crypto12_03.pdf
[12] Soutěž 2004 - Crypto-World 12/2004, celé číslo,
http://crypto-world.info/casop6/crypto12_04.pdf
[13] Soutěž 2005 - Crypto-World 12/2005, celé číslo,
http://crypto-world.info/casop7/crypto12_05.pdf

B. Z e-mailů soutěžících
(vybral P.Vondruška)

1) a soutěž skončila
From: root@crypto-world.info (www-data)
Date: Sat, 23 Sep 2006 14:16:52 +0200 (CEST)
Soutezici s loginem room132 vyresil uspesne vsechny ulohy...
nyni je unix time: 1159013812
vyherce ma bodu: 80

2) reakce vítězů
Soutezili jsme hlavne o cest a slavu.
Letos to byla nejzabavnejsi soutez vubec. Kapitan Carda a chameleoni byl skvely napad. Po zverejneni prvniho chameleona (propasli jsme ho o 4 minuty - koukal jsem se po sedme a pak ctyri minuty po desate) jsme uz nenechali nic nahode a kontrolovali to cely den a kazdy den. BIFID byl tvrdy orisek a pak uloha c 23. Nechapu jak to mohl misof rozlustit bez napovedy. My jsme zkouseli i autoklic kdyz jsme zjistili ze se tam neopakuje ani jeden trigram !!.
Tu 23 ulohu jsme lustili 3 dny a nic. Moc dekujeme za zabavu a tesime se na predani cen i na dalsi soutez.

room 132

3) peta007, druhé místo
díky, letos jsem s nějakým umístěním nepočítal, času je minimálně a člověk se čtyřmi malými dětmi si nemůže doma luštit podle libosti :-) Ale nakonec se k mému překvapení zadařilo. Z minulých let mám už taky nějaké zkušenosti, tak spousta úkolů zabrala jen minimum času.
Docela práci mi třeba dala úloha č.9, protože tenhle font doma nemám. Hodně práce jsem měl s úlohami 13 a 14, které jsem řešil až nakonec. Pořád jsem nejvíc uvažoval nad tím, že je to taky nějaké písmo, ale nakonec jsem popis našel přes Google - jen jiným dotazem, než dřív. S Bifidem jsem neměl až zas takový problém, bylo to dost štěstí. Popis jsem našel ve Wikipedii (ale jen pro jednu variantu), heslem jsem si byl docela jistý, ale rozkódovat mi to nešlo. Tak jsem uvažoval, že tam asi dělám nějakou chybu, tak jsem zase hledal Googlem. A náhodou jsem našel nějaký applet, který uměl Bifid řešit. Vložil jsem text a heslo a řešení bylo na světě. Parametry byly naprostou náhodou správné. Ale protože se tam psalo o různých variantách, tak bych to nejspíš dořešil i bez pomoci appletu...
Myslím, že je to dobře, že se něco musí hledat i na obecném internetu, všechno by asi nemělo být úplně na zlatém podnose. Ale zase je to asi výhodnější pro lidi, kteří umí anglicky, protože některé šifry možná v češtině popsané nejsou.
Docela se mi líbí princip, kdy k řešení konečné úlohy je třeba vyřešit úlohy předchozí. Možná by bylo zajímavé to zkusit i v jednotlivých úlohách. Že by se třeba dvě nebo tři úlohy řešily dohromady s použitím různých šifrovacích systémů, takže třeba heslo pro ADFGX by se vyluštilo jednoduchou substitucí "zachycené zprávy" a tak.
Obtížnost byla "tak akorát", myslím, že obecně je to ta správná úroveň. Všechno se dá vyřešit, není to moc těžké, nevyžaduje to zkoušení příliš mnoha možností (na to asi většina soutěžících nemá dost času).
Každopádně díky za soutěž, mám pocit, že letos musela příprava zabrat dost času.

S pozdravem xxx

4) MD5Mir …

Své jméno – NICK jsem zvolil, abych připomenul slavného kryptologa SHAmira. Jenže nejsem tak kvalitní, a proto jsem jméno hashe v jeho jménu zaměnil za méně kvalitní systém MD5. Mir jsem si ponechal, protože je to zkratka mého jména ….

Letos se mi řešilo zcela v pohodě. Úkoly byly asi jednodušší než loni. Bylo jich však dost … BIFID mne dostal…

Těším se na příští rok.

Mirek

5) crcker

Pavle díky,
Škoda, že jsem začal tak pozdě. V podstatě se dá ta soutěž vysedět. Jenže to je právě to ono. Řešení úlohy není úplně zadarmo, ale není to něco, co by nešlo vyřešit. Perfekt.
Pokud mi to příští rok vyjde, pak chci medaily ☺ .
Jo zajímalo by mne, jak řešili kolegové BIFID. Stálo mne to jednu noc ☹ , než mne došlo, že se ty zlomky dají zamotávat všelijak (a hlavně jinak, než jsem si vždycky myslel).

6) soutěž není jen pro pány …

a) Musim omluvit svoji dceru (S…..) - ma dvoumesicni holcicku a ta ji na lusteni nenechala mnoho casu...

b) Dekuji za blahoprani,
na soutez se tesim cely rok, mam vzdycky krasny pocit, kdyz neco vylustim, ale nesmi to byt uplne jednoduche.
Loni se ulohy lustily trochu snaze, protoze se dalo odhadnout, jaka slova otevreny text obsahuje.
Taky tam byl popsan zpusob kodovani, napr. u sifry z mobilniho telefonu,
kterou jsem loni resila odhadem obsahu, letos uz jsem ji znala.
Nejvetsi radost jsem mela z vyreseni ukolu 9, nechapu, proc je jen za 1 bod, dalo mi to vic prace, nez nektere transpozice za 3b.
Naopak ukoly 6,7,8 uz jsem znala z lonska, takze nebyl na prvni pohled zadny problem.

Doufam, ze vyhraju v losovani nejakou hodnotnou cenu :-), nebudu lustit na ukor pece o rodinu a domacnost a nevylustene sifry me nebudou v noci obirat o spanek.

S pozdravem K.

6) nejsou jen vítězové …

Dobry den, ja to vedel. ze to nestihnu....
ale podivnym zpusobem jsem se zasekl na jednoduche zamene - ten proklety Zodiac atd....
prolezl jsem Internet az do nejhlubsich pater, vyzkousel snad uplne vsechno, ale bohuzel...

jsem nesmirne zvedav, v cem ta finta byla.....uz se tesim jak se pak postavim pred zrcadlo a nejmin hodinu si budu nadavat...

Potesila mrizka, i kdyz letos "pomerne" lehka....

Dekuji moc za jako obvykle perfektne pripravenou soutez, a uz ted se tesim na pristi rocnik !

C. O čem jsme psali v prosinci 1999 – 2005

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

Příloha : EAL4.jpg
(certifikát operačního systému W2k podle CC na EAL4)

Crypto-World 12/2003

Příloha: pf_2004.jpg

Crypto-World 12/2004

Příloha : PF2005.jpg

Crypto-World 12/2005

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/