# Crypto-World

**Informační sešit GCUCMP**

**Ročník 6, číslo 12/2004** **19. prosinec 2004**

# 12/2004

**Připravil: Mgr. Pavel Vondruška**

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


Obsah : str.



Příloha : PF 2005

# A. Soutěž 2004 – úlohy a jejich řešení
Michal Forišek a Pavel Vondruška

## Obsah:



---

## 1. skupina úloh - *„skautský tábor“*

**Transpozice (1/1)** (1 bod) (text psaný pozpátku)
Řešení: OBRATENXYZ

Úloha:
ZYXNE TARBO OVOLS ETJED AZILI SERYV UHOLU ETSJE ZZAKU DOKAJ INESE RENVA RPSTA VOTSE TATAV ADAZK AJINE SUOKZ OAINE CIVCZ ORORP NEJEJ ANDEJ OLSIC AHOLU

Popis systému: Otevřený text je přepsán do tvaru bez diakritiky, napsán pozpátku a výsledek je rozdělen do skupin znaků po pěti.

Otevřený text (bez diakritiky):
ULOHA CISLO JEDNA JE JEN PRO ROZCVICENI A OZKOUSENI JAK ZADAVAT A TESTOVAT SPRAVNE RESENI JAKO DUKAZ ZE JSTE ULOHU VYRESILI ZADEJTE SLOVO OBRATENXYZ

---

**Jednoduchá záměna (1/2)** (1 bod) (morseovka)
Řešení: SKAUT

Úloha:
cRYP t owo R l dcr yp tOWo rL DC rY P toW oRLD c R y PT OWO rLd cry p TOW orlD CrY ptO wORl DCR YpT owO Rld cR Yp TOW oRLd cR YpT owoR lD CR yP tow or lD Cr yp T oW O RLD crY pTow ORL dcry pT Ow o Rld c rYpt oW oRld cR yPTo wOr LDC Rypt oWor l DC rypT oWor LDC RYpt O w oRl d cry p To wo rld CrY pT owO R

Popis systému: Otevřený text je přepsán do tvaru bez diakritiky. Dále je text zakódován pomocí morseovky. K zápisu morseovky bylo použito toto kódování :
Tečka = libovolné malé písmeno
Čárka = libovolné velké písmeno

Otevřený text (bez diakritiky):
JESTE SI PAMATUJETE MORSEOVKU POKUD ANO PAK VAM ASI ANI TATO ULOHA NEDELALA PROBLEM VLOZTE RESENI SKAUT

---

**Jednoduchá záměna (1/3)** (1 bod) (morseovka)
Řešení: JUNAK

Úloha:
0 B1 2 345 ox6 r7Ma 890 juFy k1 L234 k enG5 I6ex e7 Gxx 8 9a s 01rZ h2 Gpk k x345 e 6y nkj7 k8 T9v dT a0 1G2v s 3e B4 56 789 I0h krT F 123 vuo4 5x6 xn7 c89n uy ZFs 01 s 2w F3 d456 uje 789 oM0 1 r 2L3s 4L5 6u78 G9 0T1h Gj deF v2Qv Qe 3d4h p 5n6M d7 y8y 9M0 1s23 j4c v wwe u 5x Zw e678 M Q901 jn2 3I j4 5x6

Popis systému: Otevřený text je přepsán do tvaru bez diakritiky. Dále je text převeden do šifrového textu pomocí morseovky. K zápisu morseovky bylo použito toto kódování :
Tečka = libovolné písmeno
Čárka = libovolná číslice

Otevřený text (bez diakritiky):
TATO ULOHA JE VLASTNE ZASE JEN VARIACE NA MORSEOVKU PISMENA JSOU TECKY A CISLICE CARKY RESENI JE JUNAK

---

**Jednoduchá záměna (1/4)** (1 bod) (kódování pomocí mobilu)
Řešení: MOBIL

Úloha:
8 33 66 8 666 1 9999 7 88 7777 666 22 1 9999 66 2 8 33 1 9999 2 7777 33 1 9999 1 6 666 22 444 555 88 1 66 2 7 444 7777 8 33 1 7777 555 666 888 666 1 6 666 22 444 555

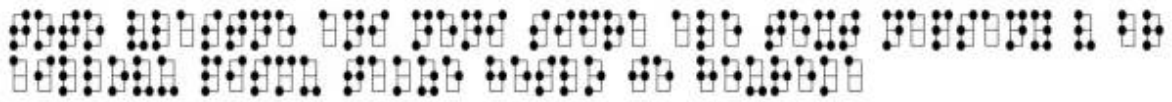
Popis systému: Jedná se o kódování, kde pro kód písmena je použito vyjádření, které odpovídá psaní příslušného písmena na mobilním telefonu při přípravě SMS. Např. při psaní písmene E musíte na mobilu 2x stisknout číslici 3 – tj. kód písmene E = 33 atd.

Otevřený text (bez diakritiky):
TENTO ZPUSOB ZNATE ZASE Z MOBILU NAPISTE SLOVO MOBIL

---

**Jednoduchá záměna (1/5)** (1 bod) (Braillovo písmo)
Řešení: HEUREKA

Úloha:



Popis systému: Jedná se o kódování, kde pro kód písmena je použito Braillovo slepecké písmo.

Otevřený text (bez diakritiky):
TOTO VLASTNE ANI NENI SIFRA ALE TEXT NAPSANY V BRAILLOVU PISMU TAKZE HESLO JE HEUREKA

## Statistika pro úlohy za 1 bod

| Úloha | 1/1 | 1/2 | 1/3 | 1/4 | 1/5 | **Průměr** | **Průměr bez 1/1** |
|---|---|---|---|---|---|---|---|
| Řešitelů | 84 | 60 | 53 | 54 | 62 | 62,6 | 57,25 |

---

## 2. skupina úloh - *„pro připravené“ (část 1)*

**Jednoduchá záměna (1/6)** (2 body) (Hacker Language Transrciption)
Řešení: HACKER

Úloha:
7470 |_|10|-|4 _|3 see410see3/\/4 /\/4 7seeV |-|4(|<3|- 14/\/6|_|4|_|3 7|-4/\/5|<|-!|>(! |<0/\/7|-01/\/! 510\/0 |<73|-3 /\/\473 see4|)47 _|3 |-|4(|<3|-

Popis systému: Jedná se o kódování, kde se za písmeno dosazuje vyjádření pomocí oblíbeného přepisu undergroundové počítačové mládeže tzv. Hacker Language Transcription. Těchto přepisů je více, základ je však stejný. V tomto konkrétním případě byl použit tento následující přepis:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| A=4 | B=8 | C=( | D=\|) | E=3 | F=ph | G=6 | H=\|-\| |
| I=! | J=_\| | K=\|< | L=1 | M=/\/\ | N=/\/ | O=0 | P=\|> |
| Q=0, | R=\|2,\|- | S=5 | T=7 | U=\|_\| | V=\/ | W=\/\/ | X=>< |
| Y=`/ | Z=see | | | | | | |

Odkaz: http://www.urbandictionary.com/define.php?term=1337

Otevřený text (bez diakritiky):
TATO ULOHA JE ZALOZENA NA TZV HACKER LANGUAGE TRANSKRIPCI KONTROLNI SLOVO KTERE MATE ZADAT JE HACKER

Důvod „připravenosti“ :
Krátce před zveřejněním úlohy jsem na Technetu publikoval dvoudílný seriál „Hackeři, Crackeři, Rhybáři a Lamy“, kde o této metodě píši.

Hackeři, Crackeři, Rhybáři a Lamy, 1.díl, Technet.idnes.cz, 19.8.2004
http://technet.idnes.cz/bezpecnost.asp?r=bezpecnost&c=A040812_5271893_bezpecnost

Hackeři, Crackeři, Rhybáři a Lamy, 2.díl, Technet.idnes.cz, 20.8.2004
http://technet.idnes.cz/bezpecnost.asp?r=bezpecnost&c=A040812_5271894_bezpecnost

---

**Jednoduchá záměna (1/7)** (2 body) (Caesarova záměna)
Řešení: POSUNPET

Úloha:
FMTOT UJYOJ SRFQF WTHAN HPFSJ GTYYT YTOJZ QTMFS FXSFI SJOES FRJOX NXNKW ZFYTH FJXFW TAZAY TRYTU WNUFI JOJUT ZENYU TXZSU NXRJS TUJYA UWFAT EFIJO YJOFP TWJXJ SNUTX ZSUJY

Popis systému:
Snad nejznámější substituční šifrou vůbec je tzv Caesarova šifra. O jejím původu víme díky Suetoniově knize Životopisy dvanácti císařů (De vita Caesarum), kde autor uvádí, že ji Caesar používal. Valerius Probus uvádí, že Caesar měl tajná písma a šifry v oblibě a používal je velice často. Dílo Valeria Proba, ve kterém byl dokonce uveden přehled Caesarem používaných šifer, se však bohužel nedochovalo. Vraťme se k popisu klasické Caesarovy šifry. Každé písmeno zprávy se nahradí písmenem nacházejícím se v abecedě o tři pozice dále. Suetonius se zmiňuje výslovně o posunu o tři písmena, přesto se název Caesarova šifra vžil i pro označení pro posun písmen o jakýkoliv jiný počet znaků.
Předložená úloha je jednou z variant na tento klasický šifrový systém - Caesarovu záměnu. V tomto případě je každé písmeno nahrazeno písmenem, které leží od něj o pět pozic vpravo. Na „konci“ abecedy se pokračuje opět cyklicky od začátku abecedy.

Převodová tabulka:
```
OT      ABCDEFGHIJKLMNOPQRSTUVWXYZ
ŠT      FGHIJKLMNOPQRSTUVWXYZABCDE
```

Otevřený text (bez diakritiky):
AHOJ OPET JEN MALA ROCVICKA NEBOT TOTO JE ULOHA NA SNAD NEJZNAMEJSI SIFRU A TO CAESAROVU V TOMTO PRIPADE JE POUZIT POSUN PISMEN O PET VPRAVO ZADEJTE JAKO RESENI POSUN PET

Důvod „připravenosti“ :
Systém je všeobecně známý. Byl vysvětlen a použit i loni v Soutěži 2003.
Řešení úloh ročníku 2003, Crypto-World 12/2003
http://crypto-world.info/casop5/crypto12_03.pdf

---

**Jednoduchá záměna (1/8)** (2 body) (atbaš)
Řešení: ALEFBET

Úloha:
WZOHR AMZNZ HRUIZ QVSVY IVQHP ZHFYH GRGFX MRHRU IZZGY ZHHKL XREZE MZSIZ WVZYV XVWBZ YVXVW LFPGV IZQVK HZMZK LAKZG PFQZP LWFPZ AIVHV MREOL AGVZO VUYVG

Popis systému:
V této úloze jsem použil další známý jednoduchý klasický systém, který se nazývá atbaš (někdy atbš). Je to tradiční hebrejská substituční šifra. Její použití můžeme nalézt například na několika místech Bible. 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. V námi použité mezinárodní abecedě to znamená, že A se nahradí Z, písmeno B se nahradí Y a tak dále. Podle popsaného postupu dostala šifra také své jméno atbaš, neboť první písmeno hebrejské abecedy je *alef* je nahrazeno posledním písmenem *tav*, druhé písmeno bet se nahrazuje předposledním písmenem hebrejské abecedy – *šin* atd.

Převodová tabulka:
```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZYXWVUTSRQPONMLKJIHGFEDCBA
```

Otevřený text (bez diakritiky):
```
DALSI ZNAMA SIFRA JE HEBREJSKA SUBSTITUCNI SIFRA ATBAS SPOCIVA V NAHRADE
ABECEDY ABECEDOU KTERA JE PSANA POZPATKU JAKO DUKAZ RESENI VLOZTE ALEFBET
```

Důvod „připravenosti“ :
Systém je všeobecně známý. Byl vysvětlen a použit i loni v Soutěži 2003.
Řešení úloh ročníku 2003, Crypto-World 12/2003
http://crypto-world.info/casop5/crypto12_03.pdf

---

**Agenturní systém (1/9)** (2 body) (poslední písmeno)
Řešení: POSLEDA

Úloha:
blaho asfalt nejmene zpev Alzir indukce oddan pujceny talent bilance sex brucet nebozez finalni Kristus blok tepna kat zase kopanec plest priste koren sumici program sesup pojivo hrabos pel tohle blond nucen vyliti zapirac druh drap sedici unos hrom chuze prsten kazit pratele topic orech carovat tornado mys kotel pradlo sev pasaz vyzdoba doklad koroze oblicej dotovat cislice odstup Finsko casopis utratil dezerce zlorad kolega

Popis systému:
Použitý systém lze zařadit mezi steganografické metody. Otevřený text je podle nějakého pravidla (zde poslední písmeno každého slova) skryt v celkovém předávaném textu. Systém se v různých variantách v minulosti skutečně používal. Prokazatelně ještě v dobách totality při komunikaci mezi agenturní sítí v České republice a řídícími centry v cizině. Tehdy měl podobu nenápadných dopisů z ČR do ciziny (zejména Spolkové republiky Německo), kde na domluveném místě např. konec druhého slova v každé větě, poslední slovo věty apod. bylo písmeno otevřeného textu (ve složitějších variantách to byla, místo písmena otevřeného textu, souřadnice kódové tabulky, kterou obě strany používaly). Hlavní výhodou systému je to, že při zasílání šifrového textu by byl odesílatel automaticky podezřelý z podvratné činnosti. Při přísném dodržení různých provozních pravidel (krátký text, použití kódové tabulky, která se pravidelně obměňuje, nepříliš častý provoz, „chytrá“ slohová a obsahová stavba odeslaného dopisu) může být systém poměrně bezpečný.

Otevřený text (bez diakritiky):
`OTEVRENY TEXT ZISKATE CTENIM POSLEDNICH PISMEN TECHTO SLOV ZADEJTE POSLEDA`

---

**Transpozice (1/10)** (2 body) (podle plotu)
Řešení: ANGLIE

Úloha:
LNDLL ETSSE NZAYO LPOUE IEUPO LMLZE NLEOI EATNO YTMAV NPDEL TRSTL MRBEV OTAGI

Popis systému:
Jedná se o oblíbený systém šifrování anglických školáků, který se nazývá „podle plotu“. Systém patří mezi klasické transpoziční systémy. Jeho odolnost je ovšem velmi malá (některé úseky textu mohou být téměř čitelné…). Zpráva se rozdělí do dvou (někdy tří či více) řádků. Do prvního řádku se dají všechna lichá písmena a do druhého řádku všechna písmena sudá. Druhý řádek se pak připojí za první.

Ukážeme si přípravu příslušného šifrového textu:

1. LoNi DeLaL tEnTo SyStEm NaZvAnY pOdLe PlOtU rEsItElUm PrObLeM vLoZtE aNgLiE

2. LNDLLETSSENZAYOLPOUEIEUPOLMLZENLE
   oieatnoytmavnpdeltrstlmrbevotagi

3. LNDLLETSSENZAYOLPOUEIEUPOLMLZENLE oieatnoytmavnpdeltrstlmrbevotagi

Otevřený text (bez diakritiky):
LONI DELAL TENTO SYSTEM NAZVANY PODLE PLOTU RESITELUM PROBLEM VLOZTE ANGLIE

Důvod „připravenosti“ :
Systém není v ČR příliš známý. Předložená úloha řešitelům loňské soutěže (Soutěž 2003) úspěšně odolávala a řada z nich ji označila jako těžkou. Vzhledem k tomu, že je úloha – pokud je systém znám – lehce řešitelná, stačilo se seznámit (připravit) s loňskými úlohami.

---

## 3. Skupina úloh - *„pro připravené“* (část 2)

Do komentování jednotlivých úloh, hlavně postupu při jejich řešení, se od této chvíle zapojuje i vítěz soutěže Michal Forišek. Můj a jeho komentář snadno rozeznáte – Michalův je napsán slovensky ☺.

**Steganografie (2/1)** (2 body)
Řešení: BYSTROZRAKY

Úloha:
```
TATOU LOHAP ATRIM EZISP ISELE HKE.U KOLEM JEOPE TNALE ZTSLO VOKTE
RYMPR OKAZE TEZEJ STEJI VYRES ILI.T ENTOK RATEN ENISL OVOZA SIFRO
VANO, ALEUT AJENO JEDNO DUCHO USTEG ANOGR AFICK OUMET ODOU. NEVIM
ZDANA POVIM ,ALET ATOUL OHANE BUDEV CRYPT
O-WOR LDU10 /2004 UVEDE NA(PR OC?).
```
Nápověda: úloha je uvedena pouze pro úplnost. Řešit ji je nutné přímo na www stránce.

Popis systému:
Otevřený text je skryt ve zdrojovém textu úlohy. Při použití běžného browseru se nezobrazí.

Výpis příslušné části zdrojového textu:

<p /><h1>Steganografie (2/1)</h1> Počet bodů: 2 TATOU LOHAP ATRIM EZISP ISELE HKE.U KOLEM JEOPE TNALE ZTSLO VOKTE RYMPR OKAZE TEZEJ STEJI VYRES ILI.T ENTOK RATEN ENISL OVOZA SIFRO VANO, ALEUT AJENO JEDNO DUCHO USTEG ANOGR AFICK OUMET ODOU. NEVIM ZDANA POVIM ,ALET ATOUL OHANE BUDEV CRYPT O-WOR LDU10 /2004 UVEDE NA(PR OC?).Blahopreji ! nasel jste uschovany kod ! Zadejte slovo BYSTROZRAKY <p>Pro zadání správné odpovědi musíte být přihlášeni. Nový řešitel se musí nejprve

Otevřený text (bez diakritiky):
Blahopreji ! nasel jste uschovany kod ! Zadejte slovo BYSTROZRAKY

Důvod „připravenosti“ :
Stejný způsob utajení byl použit v prvé úloze soutěže v roce 2000. V článku o steganografii na Crypto-Worldu byla tato možnost také zmíněna….
Steganografie, Crypto-World 9/2000, str.2-5
http://crypto-world.info/casop2/crypto09_00.pdf

**Michal:**
Nedáme sa odradiť formátovaním textu a prečítame si zadanie úlohy: *Tato uloha patri mezi spise lehke. Ukolem je opet nalezt slovo, kterym prokazete, ze jste ji vyresili. Tentokrate neni slovo zasifrovano, ale utajeno jednoduchou steganografickou metodou. Nevim, zda napovim, ale tato uloha nebude v Crypto-Worldu 10/2004 uvedena (proc?).*

Zjavne všetko, čo vidíme v browsri, by sme rovnako dobre videli aj v pdf verzii Crypto-Worldu. Preto heslo musí byť ukryté niekde, kde ho nevidíme. Najpriamočiarejšou možnosťou je zdrojový kód samotnej stránky.

A skutočne, na konci textu so zadaním objavíme:

Blahopreji ! nasel jste uschovany kod ! Zadejte slovo BYSTROZRAKY

Zostáva už len podotknúť, že tento spôsob ukrytia nebol zvolený práve najšťastnejšie. Riešitelia, ktorí používajú staršie, obzvlášť textové browsre, nemusia byť práve bystrozrakí, aby heslo uvideli -- stačí, aby ich browser nepoznal tag , prípadne ignoroval CSS. Korektnejší spôsob ukrytia informácie by bolo použiť namiesto spanu komentár:

<!-- Blahopreji! Nasel jste uschovany kod! Zadejte slovo BYSTROZRAKY -->

---

**Kódová kniha, II.světová válka (2/2)** (2 body)
Řešení: NAVAJONAVAJO
Nápověda: HBO, léto 2004

Úloha:
BAH-HAS-TKIH BE-SO-DE-DEZ-AHE BESH-LEGAI-NAH-KIH YAH-DI-ZINI NI-DAH-THAN-ZIE IL-DAY A-WOH NE-AHS-JAH BE-TAS-TNI NE-AHS-JAH AH-LOSZ DAH-NES-TSA A-KHA GLOE-IH BE-SO-DE-DEZ-AHE NE-ZHONI WOL-LA-CHEE DIBEH KLESH GLOE-IH TLO-CHIN GAH BE SEIS TSAH TSE-NILL A-KEH-DI-GLINI BE-LA-SANA YIL-DOI NE-AHS-JAH

Popis systému:
K zašifrování textu byla použita originální Kódová kniha, kterou za druhé světové války používali indiáni kmene Navajo (http://www.history.navy.mil/faqs/faq61-4.htm). Tito indiáni sloužili v americké armádě. Jimi předávané zprávy nepřítel nikdy nerozluštil (mimo poměrně slabé kódové knihy bylo hlavním „zabezpečením“ použití pro nepřítele neznámého a z hlediska výslovnosti těžkého indiánského jazyka).

Otevřený text:
SECRET. CAPTAIN CANNOT ARRIVE TOMORROW. PASSWORD IS NAVAJONAVAJO

Důvod „připravenosti“ :
Stejný způsob utajení byl použit ve druhé úloze soutěže v roce 2001. V článku o steganografii na Crypto-Worldu byla tato možnost také zmíněna…. Odvolávka na HBO měla napovědět film *Kód Navajo*, který byl v té době několikráte opakován. Čtenáři Crypto-Worldu se s články o působení indiánů kmene Navajo za druhé světové války setkali ve starších číslech tohoto e-zinu. O využití těchto mluvčích v kódech za I. a II.světové války (Code Talkers) jsem publikoval seriál na root.cz na podzim roku 2001.

Code Talkers , Část I. - Vznik nové šifrovací techniky, ROOT.CZ, 3.9.2001
http://www.root.cz/clanek/817
Code Talkers , Část II. - YIL-TAS GLOE-IH-DOT-SAHIUT-ZAH, ROOT.CZ, 10.9.2001
http://www.root.cz/clanek/828
Code Talkers , Část III. - Od Iwo Jimy k mluvící figurce firmy Hasbro , ROOT.CZ, 17.9.2001
http://www.root.cz/clanek/841

**Michal:**
Toto bola ďalšia z "úloh pre pripravených", stačilo mať prečítané riešenia úloh z minulých ročníkov. Prísť na to, že opäť raz ide o reč kmeňa Navajo, stiahnuť si slovník (ktorý tvoril prílohu k jednému číslu Crypto-Worldu) a dešifrovať text je potom už priamočiare.

Dokonca nebolo treba ani to. Priateľ Google toho už videl veľa a napríklad aj na prvé slovo zo šifrového textu (BAH-HAS-TKIH) zareaguje kopou odkazov, z ktorých sa dá ľahko zistiť, o čo ide.

**Statistika pro úlohy za 2 body**

| Úloha | 1/6 | 1/7 | 1/8 | 1/9 | 1/10 | 2/1 | 2/2 | **Průměr** |
|---|---|---|---|---|---|---|---|---|
| Řešitelů | 48 | 48 | 47 | 54 | 44 | 50 | 43 | 47,7 |

---

## 4. Skupina úloh - *„pro luštitele“ (část 1)*

Další skupina úloh se skládala ze tří klasických šifrových systémů - transpozice, jednoduché záměny a periodického hesla. Při řešení těchto úloh již bylo potřeba „sáhnout“ na klasické metody. Texty byly dostatečně dlouhé a obsahovaly řadu úmyslných markantů, které měly ulehčit řešení (např. umístění znaků X, velikost transpoziční tabulky, opakování, předpokládaná slova). Úlohy tohoto typu byly soutěžícím na stránkách Crypto-Worldu předloženy již v roce 2000. V doprovodných e-zinech tehdejší soutěže (10/2000-12/2000) lze také najít dostatečný výklad, který umožní pochopit konstrukci těchto šifer a je zde uveden i doporučený postup řešení (včetně např. frekvence znaků v češtině, typické bigramové vazby atd.).

**Jednoduchá transpozice (2/3)** (3 body)
Řešení: RIJEN
Nápověda: Jednoduchá transpozice, Crypto-World 11/2000, str. 2-6
http://crypto-world.info/casop2/crypto11_00.pdf

Úloha:

```
EDUUC NHCRE RNDCO VSYRT ARJIZ EKOKL VDNEJ PHIYI EOAYE EZNEZ EDLEL ZNSZM
BNDRI JEOZU SMSDN AANVE PNARN EISAS YDYSE EOZNC CSEOR AWIOY IEYCS BKUIT
VARIE ONSEE ETEOP BTOVE TAZET RXURH ROEVZ ZORDB POINE YSSTD WMPVE DANSV
OVSEZ PEEIT PBOIT PEYID LEDMM EAOTJ NNJZP YMDYE ASONT TTSVL EUIPI BUAIN
REAEN AIRUI VZTID EVIAE HONUO VWPVH HLSAD OEZOI YVHEU ODARE LUOTU EATOS
DDEPN NTEVY UGERL RCEOC (320)
```

Transpoziční heslo : LGVHWDVACETIKORUNYBF

Otevřený text (bez diakritiky):

```
PO VYRESENI TETO TRANSPOZICE ZADEJTE RIJEN NYNI NASLEDUJE TEXT NA STRANCE
BUDOU POSTUPNE VE TRECH KOLECH ZVEREJNOVANY SOUTEZNI ULOHY ZA VYRESENI
ULOHY SE PRIPISUJI SOUTEZICIMU BODY REGISTROVANY RESITEL MUZE ZADAVAT SVE
ODPOVEDI PRES WWW ROZHRANI VZDY VELKYMI PISMENY A BEZ MEZER ODPOVED BUDE
AUTOMATICKY VYHODNOCENA A RESITEL SE IHNED DOZVI ZDA ODPOVEDEL SPRAVNE NEBO
NE
```

**Michal:**

Pracovná hypotéza: Pôjde o klasickú tabuľkovú transpozičnú šifru.

Postup dešifrovania by bol nasledovný: Určíme správne rozmery tabuľky. Po riadkoch do nej vpíšeme šifrový text. Riadky preusporiadame tak, aby sme si po stĺpcoch mohli prečítať otvorený text.

Na určenie rozmerov tabuľky existujú všeobecné postupy. Súčin rozmerov tabuľky by mal byť rovný počtu písmen v šifrovom texte. Navyše ak si správne tipneme rozmery tabuľky, v každom stĺpci by sme mali (okrem iného) dostať správny pomer samohlások a spoluhlások.

V našom prípade si však môžeme pomôcť aj inak. Frekvenčná analýza ukáže, že v našom šifrovom texte máme jedno písmeno X a tri písmená W. Tri písmená W by mohli tvoriť reťazec WWW. Všimnime si, na ktorých pozíciách šifrového textu sa nachádzajú. Sú to pozície 107, 171 a 267. Aby boli všetky tri W v tom istom stĺpci, musí počet stĺpcov C deliť vzdialenosť medzi každými dvomi výskytmi W. Je 171-107 = 64, 267-171 = 96, nsd(64,96) = 32. Teda počet stĺpcov delí číslo 32. Tým už dostávame len 6 možností (1, 2, 4, 8, 16 alebo 32 stĺpcov).

Spoľahneme sa na trochu šťastia a tipneme si, že tabuľka bude čo najbližšia štvorcovej. Tomu by zodpovedala tabuľka s 20 riadkami a 16 stĺpcami. Po vyplnení šifrového textu bude vyzerať nasledovne:

```
EDUUCNHCRERNDCOV
SYRTARJIZEKOKLVD
NEJPHIYIEOAYEEZN
EZEDLELZNSZMBNDR
IJEOZUSMSDNAANVE
PNARNEISASYDYSEE
OZNCCSEORAWIOYIE
YCSBKUITVARIEONS
EEETEOPBTOVETAZE
TRXURHROEVZZORDB
POINEYSSTDWMPVED
ANSVOVSEZPEEITPB
```

```
OITPEYIDLEDMMEAO
TJNNJZPYMDYEASON
TTTSVLEUIPIBUAIN
REAENAIRUIVZTIDE
VIAEHONUOVWPVHHL
SADOEZOIYVHEUODA
RELUOTUEATOSDDEP
NNTEVYUGERLRCEOC
```

Vidíme, že písmeno X je v treťom stĺpci. Okrem iného tam nájdeme tri T a tri E, dosť na to, aby sa dalo zložiť slovo TEXT. Vyzerá to nádejne, poďme teda nájsť správnu permutáciu riadkov. Začneme tým, že si zložíme WWW:

```
OZNCCSEORAWIOYIE
POINEYSSTDWMPVED
VIAEHONUOVWPVHHL
```

Podľa 2. a 3. stĺpca sa zdá, že riadok začínajúci "OZN..." by mal byť ako druhý v poradí, aby sme nemali dve samohlásky po sebe. Podobne v 5. stĺpci zložíme CH, lebo HC je oveľa menej časté, a dostávame:

```
POINEYSSTDWMPVED
OZNCCSEORAWIOYIE
VIAEHONUOVWPVHHL
```

Aj ostatné stĺpce "znejú česky", zatiaľ to vyzerá dobre. Skúsme si teraz zložiť slovo TEXT. (Pri riešení úlohy som postupoval inak, zo zvyšných písmen prvého stĺpca som si tipol slovo RESENI.) Kandidátmi sú riadky:

```
EZEDLELZNSZMBNDR
IJEOZUSMSDNAANVE
EEETEOPBTOVETAZE
TRXURHROEVZZORDB
OITPEYIDLEDMMEAO
TTTSVLEUIPIBUAIN
NNTEVYUGERLRCEOC
```

Spomedzi riadkov s písmenom T v treťom stĺpci pod riadok s X najlepšie pasuje riadok "OIT...".

```
TRXURHROEVZZORDB
OITPEYIDLEDMMEAO
```

Pred ne doplníme najlepšie pasujúci riadok s písmenom E:

```
EEETEOPBTOVETAZE
TRXURHROEVZZORDB
OITPEYIDLEDMMEAO
```

A doplníme začiatočné T:

```
TTTSVLEUIPIBUAIN
EEETEOPBTOVETAZE
TRXURHROEVZZORDB
OITPEYIDLEDMMEAO
```

Všimnime si šiesty stĺpec: LOHY bude pravdepodobne ULOHY, opäť vyberieme lepšie vyzerajúcu z dvoch možností. Potom v štvrtom stĺpci dostávame OSTUP, doplníme na POSTUP. V deviatom stĺpci ESITEL doplníme na RESITEL.

```
EDUUCNHCRERNDCOV
NEJPHIYIEOAYEEZN
IJEOZUSMSDNAANVE
TTTSVLEUIPIBUAIN
EEETEOPBTOVETAZE
TRXURHROEVZZORDB
OITPEYIDLEDMMEAO
```

V druhom stĺpci DEJTE doplníme na ZADEJTE a už sme takmer hotoví. Výsledná tabuľka, ku ktorej sa po pár ďalších krokoch dostaneme:

```
POINEYSSTDWMPVED
OZNCCSEORAWIOYIE
VIAEHONUOVWPVHHL
YCSBKUITVARIEONS
RELUOTUEATOSDDEP
EZEDLELZNSZMBNDR
SADOEZOIYVHEUODA
EDUUCNHCRERNDCOV
NEJPHIYIEOAYEEZN
IJEOZUSMSDNAANVE
TTTSVLEUIPIBUAIN
EEETEOPBTOVETAZE
TRXURHROEVZZORDB
OITPEYIDLEDMMEAO
TJNNJZPYMDYEASON
REAENAIRUIVZTIDE
ANSVOVSEZPEEITPB
NNTEVYUGERLRCEOC
SYRTARJIZEKOKLVD
PNARNEISASYDYSEE
```

---

**Jednoduchá záměna (2/4)** (3 body)
Řešení: WHISKY
Nápověda: Jednoduchá záměna, Crypto-World 10/2000, str. 2-4
http://crypto-world.info/casop2/crypto10_00.pdf

Úloha:
Postup riešenia je v kryptologických kruhoch tou pravou klasikou. Najjednoduchšie je postupne skúšať všetky možné dĺžky hesla. Nech teda je dĺžka hesla D. Rozdeľme si šifrový text do riadkov, pričom na každom bude D znakov. Teraz každý stĺpec je vlastne zašifrovaný jednoduchým posunom abecedy. Tento ľahko uhádneme pomocou jeho frekvenčnej analýzy, prípadne priamo pomocou indexu koincidencie.

```
GDCPB BDXNC EXDGR AQVXF IDVZP CEBPW PTWKL SIQWL QLPVQ WPZPG QVXDB QZDAP
SRAQV XFVMN WMARA QVXFR QZZQD YULDI WVVPV NEKLD SNECS NEVXZ PIQMP XXWPL
PBVNE LEMIP SFLNH PIFSP VXZDL IPXWP LDVPV KPMQD ZQGEB PIDAQ VWNLQ MXPLP
KZQXF WFWNV XZPIX FIDRA QVXFB VNEQI VKQLN SDIPL PIPVD IMIQY VXZPY MPIFG
QVXDB QQCDZ VQWLQ ZEVWQ WPZPX WPLQH ECNES FZNVN SDIQG WPMAX WPLQC NVDAZ
```

```
QDZPV KNIKD WIDMW HNCES WNYWN KLQKD CPVPM PIDVX ZDCDN KPWGZ DASPR AQVXF
VWPBI PGIDM XFDZP CNKZI PIDHE CPKNE GPBPC INEVX ZPIXN EIDRA QVXFT (415)

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

Otevřený text (bez diakritiky):
ZADEJ JAKO DUKAZ WHISKY NASLEDUJE TEXT PRVNI TRI RESITELE ZISKAJI LAHEV
WHISKY SCOTCH WHISKY WILLIAM GRANTS SE SOUPRAVOU DVOU SKLENICEK KTERE JSOU
RUCNE VYROBENY VE SKLARNE KTERA SE SPECIALIZUJE NA HISTORICKE REPLIKY –
TYTO SKLENKY NA WHISKY JSOU INSPIROVANE RENESANCNIM SKLEM CENY ZISKAJI I
DALSI TRI LUSTITELE KTERI BUDOU VYLOSOVANI Z TECH KTERI DOSAHLI ALESPON
PATNACT BODU V TOMTO PRIPADE SE CENA SKLADA OPET Z LAHVE WHISKY STEJNE
ZNACKY ALE DOPLNENA BUDE POUZE JEDNOU SKLENKOU NA WHISKY
```

**Michal:**

Tentokrát máme zjavne do činenia s klasickou substitučnou šifrou. Začal som frekvenčnou analýzou (spočítame, ako často sa vyskytujú znaky a bigramy), na základe výsledkov som natipoval, ktoré písmená boli pôvodne samohlásky. Asi hodinu času som strávil hádaním slov, ktoré by sa mohli vyskytovať na začiatku alebo na konci textu, no neuspel som. Rovnako k cieľu neviedlo ani dopĺňanie písmen len na základe frekvencii a okolia, v ktorom sa vyskytujú. Sčasti za to asi mohla aj moja národnosť, česky síce bez problémov rozprávam, ale predsa len to nie je môj rodný jazyk. Keď všetky pokusy o ručné riešenie zlyhali, bolo jasné, že treba požiadať o pomoc hrubú silu. No keďže 26! je pomerne veľké číslo, nemôžeme len tak skúšať všetky permutácie písmen.

Čo vlastne bude počítač vedieť s takouto šifrou urobiť? Češtine nerozumie. Rozumný cieľ bude nájsť takú permutáciu písmen, aby dešifrovaný text "znel čo najviac česky". A ako znie taký český text, to už počítač ľahko naučíme. Zobral som pár megabajtov českého textu, odstránil z neho všetky znaky okrem písmen a spravil som si z výsledného súboru štatistiku výskytu tetragramov - štvoríc po sebe idúcich písmen. Všetkých tetragramov je len 26^4, čo je rozumne málo.

Teraz si povieme, že text znie tým viac česky, čím bežnejšie tetragramy sa v ňom vyskytujú. Formálnejšie:
Nech V[abcd] je počet výskytov tetragramu abcd v mojom českom texte.
Vhodné kritérium je napríklad nasledovné: Text znie tým viac česky, čím je väčšia suma hodnôt log(V[abcd]+1), pričom sčítame cez všetky tetragramy abcd vyskytujúce sa v ňom.

(Technické detaily: Logaritmus je tam nato, aby jedna veľká hodnota V[i] príliš nezaváţila. Plus jedna je tam na to, aby to fungovalo aj pre tetragramy, ktoré v našom českom texte neboli - logaritmus nuly nie je definovaný.)

Náš program teraz začne s ľubovoľnou permutáciou. V danom kroku sú dve možnosti: Ak výmenou nejakých dvoch písmen vieme dostať možný otvorený text, ktorý by znel viac česky, spravíme najlepšiu možnú takúto výmenu. Ak sme už našli lokálne optimum, spravíme v aktuálnej permutácií zmien viac, prípadne začneme úplne odznova, opäť s náhodnou permutáciou.

Po spustení programu máme do pár sekúnd na svete takmer optimálne riešenie, líšiace sa od správneho len v pár písmenách ako F, G a pod. A navyše ako neskôr uvidíme, spravili sme napísaním tohto programu investíciu do života, ešte sa nám bude hodiť.

---

**Periodické heslo, Vigenere (2/5)** (3 body)
Řešení: SCHREBIUS
Nápověda: Substituce složitá - periodické heslo, srovnaná abeceda, Crypto-World 12/2000, str. 4-10
http://crypto-world.info/casop2/crypto12_00.pdf

Úloha:

```
TEMYY IPVWT MPYYT OPIDR UXQKE MLEDO OXDAX IWCIZ ZEQHD KFREA QVDIZ NZKZI
ZHHGH RIAGI TPVBA ZAREP PTQJS UZULE RRRYU SOHXO ZOYWA UGPVV BUYZI AGGPE
XVDFQ MMPPZ DEXVP UEVIG ITQVM QQZQL RLHGN INNSB WUGUG TUCLH ASDTM XIFPY
GULBM CIGDZ QRMAR KPNYB JKFZT EIBGZ ZRZKV NMYIY HEXBD KLDVN DUFNM PSKAR
KNVOL AGREN AVTNB KWVIF DKFOZ LLKZZ IAVGH ERXWB QPSQT KIHSC IZDIS GZGHY
ZAQZD NMZDF PUGUM SWNIW KGETI WAOYP VVKOZ AQFUX FIZEW FHONB DEOHW GIZQC
LBBKH RIAMU TNICZ OYIXV DTQZF HLUHA RRAVA REXGA HNMGZ ITAXE VEOHS OGJXI
RRUGV IGNAZ AARVW JHOHX WADEX RHQKJ IQWBM TCQGS BRSGW BALRR AZAUT NSKET
VBXAM URVSG ATZBZ KYVIF BXQSI MXXMV EBLNM DYWMF QRSPV KFAOG WFQMV RSUXE
QWMJZ OLBUO XISAC RUDMA IBKSS XMAYR XAWYF IQNAB GJTBL OXZIW UKZAT BCFUV
EAMVQ VRRXG XIZBA ZAVOL UOXIS ACRUD MFBGX ETBCF UVEWQ FQJQR VGPRI IWATL
MNAAE ERLBX GSLBA VADEE AQKCL MDODA XQCQM ZVRAK ZINRA RAVSF KNDEF VCY

Heslo pro zašifrování : ENIGMA

Otevřený text:
PRESM ILION APULL IDIZE MREKA ZDYRO KKVUL ISPAT NEMUV ETRAN IPRIV ARENI
VUZAV RENYC HPROS TORAC HNEJO HROZE NEJSI SKUPI NOUJS OUPRI TOMZE NYADE
TIVZE MICHT RETIH OSVET ANEVI DITEL NYZAB IJAKV KUCHY NICHU SMRTI KAZDY
CHDVA CETVT ERINJ EDNUO BETZP RAVUZ VEREJ NILAS VETOV EZDRA VOTNI CKEOR
GANIZ ACEWH OVPAT EKVES VETOV YDENZ ENNAV ENKOV EPODL EWHOP ATRIO TRAVY
VNITR NIMVZ DUCHE MKNEJ CASTE JSIMP RICIN AMSMR TIVRO ZVOJO VYCHS TATEC
HOTEV RENEO HNEPR IMITI VNEZB UDOVA NESPO RAKYU VNITR CHATR NYCHO BYDLI
NEMAJ ICAST OANIO DVODK OURET EZKYJ EDOVA TYDYM PROTO VOLNE STOUP AKEST
ROPUA UNIKA OTVOR EMVES TRESE ZPRAV AODHA DUJEZ EROCN ETAKT OZEMR EKOLE
MJEDN OHOMI LIONU LIDIN AVYSO KEUMR TNOST IMASV UJPOD ILZEJ MENAP OUZIV
ANEPE VNEPA LIVOS TOVKY MILIO NULID ISTAL EPOUZ IVAJI ZEJME NADRE VOUHL
IASUS ENYTR USHOS PODAR SKYCH ZVIRA TDUKA ZRESE NIJES LOVOS CHREB IUS

Otevřený text (po zformátování):
```

Přes milión a půl lidí zemře každý rok kvůli špatnému větrání při vaření v uzavřených prostorách. Nejohroženější skupinou jsou přitom ženy a děti v zemích třetího světa. Neviditelný zabiják v kuchyních usmrtí každých dvacet vteřin jednu oběť. Zprávu zveřejnila Světové zdravotnické organizace (WHO) v pátek, ve Světový den žen na venkově. Podle WHO patří "otravy vnitřním vzduchem" k nejčastějším příčinám smrti v rozvojových státech. Otevřené ohně, primitivně zbudované sporáky uvnitř chatrných obydlí nemají často ani odvod kouře. Těžký, jedovatý dým proto volně stoupá ke stropu a uniká otvorem ve střeše. Zpráva odhaduje, že ročně takto zemře kolem jednoho miliónu lidí. Na vysoké úmrtnosti má svůj podíl zejména používané pevné palivo. Stovky miliónů lidí stále používají zejména dřevo, uhlí a sušený trus hospodářských zvířat. Důkaz řešení je slovo SCHREBIUS.

**Michal:**
Postup riešenia je v kryptologických kruhoch tou pravou klasikou. Najjednoduchšie je postupne skúšať všetky možné dĺžky hesla. Nech teda je dĺžka hesla D. Rozdeľme si šifrový text do riadkov, pričom na každom bude D znakov. Teraz každý stĺpec je vlastne zašifrovaný jednoduchým posunom abecedy. Tento ľahko uhádneme pomocou jeho frekvenčnej analýzy, prípadne priamo pomocou indexu koincidencie.

**Poznámka autora:**
Délka hesla (Michal označuje D) se klasicky hledá pomocí vyhledání všech „delších" opakování a pozic, na kterých se nacházejí. Potom se najde společný dělitel vzdáleností těchto opakování. Tento dělitel je současně délkou periodického hesla. Tato metoda je velice účinná. Detaily viz. citovaný článek v Crypto-Worldu 12/2000.

**Statistika pro úlohy za 3 body**

| Úloha | 2/3 | 2/4 | 2/5 | **Průměr** |
|---|---|---|---|---|
| Řešitelů | 26 | 21 | 30 | 25,66 |

---

## 5. Skupina úloh - *„pro profesionály"*

Poslední skupina úloh se skládala z šifrových systémů, které se v naší soutěži (a nejen letos) ještě neobjevily. Jednalo se o systém Fleissnerovy mřížky, poněkud upravené klasické jednoduché záměny a jedno-dvoumístné záměny. Poslední úloha byla jen kontrolní hříčkou, kterou však mohl úspěšně vyřešit jen ten, který zvládl všechny (pardon skoro všechny viz. Michalův text k poslední úloze) předchozí šifry.

**Fleissnerova úplná mřížka (3/1)** (4 body)
Řešení: KOMENSKY
Nápověda: Fleissnerova otočná mřížka, Crypto-World 11/2004, str. 7-8
http://crypto-world.info/casop6/crypto11_04.pdf

Úloha:
```
TEKRO JDDYC MZICD TIEAE SDTEN OIUCK SAPOM UETLA MJOEC ERNVA SLTEO OHKVZ
YOST (64 znaků)
```

Použitá mřížka (1 značí otvor):

00100001
10010010
01000100
00101000
10000011
00001000
00000100
00100010

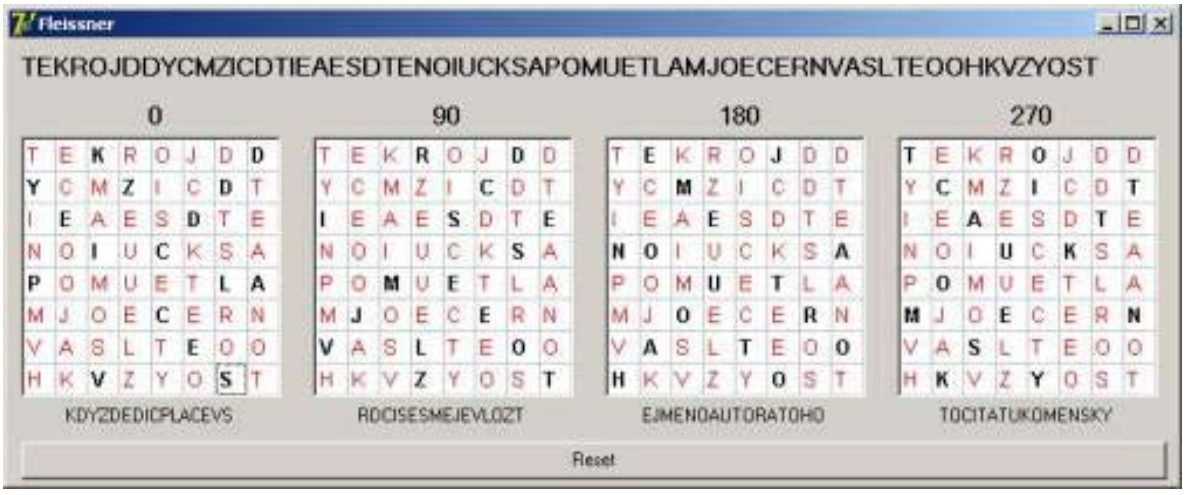
Otevřený text:
Když dědic pláče, v srdci se směje! Vložte jméno autora tohoto citátu KOMENSKY

**Michal :**

```
TEKROJDD
YCMZICDT
IEAESDTE
NOIUCKSA
POMUETLA
MJOECERN
VASLTEOO
HKVZYOST
```

Ľahko nahliadneme, že možných mriežok je 4^16 = 2^32 - štvorec má 64 políčok, preto mriežka má 16 otvorov, pre každý máme 4 možnosti, kde bude. Ručný postup riešenia by mohol vyzerať približne nasledovne: 16 otvorov sú v priemere 2 otvory na riadok. Skúsime uhádnuť možný začiatok správy, tým dostaneme niekoľko otvorov a skúšame, čo s tým ďalej. Možným začiatkom by bolo slovo KDYZ. (Iných možných začiatkov až tak veľa nie je, všimnite si, že v prvých riadkoch je málo samohlások.)

Tu sa mi ale prestalo chcieť ručne riešiť a s úspechom som sa vrátil k použitiu hrubej sily. Upravíme program, ktorý sme použili pri riešení substitučnej šifry, aby namiesto permutácie hľadal správnu množinu otvorov mriežky. Lokálna zmena bude presunutie niektorého otvoru na jednu z polôh, kam sa dostane rotáciou. Kritérium českosti textu zostáva rovnaké.




Tu už ale nemôžeme čakať až takú úspešnosť tohto prístupu - totiž aj malá zmena mriežky spôsobí pomerne veľkú zmenu výsledného textu. Napriek tomu do minúty (presnejšie ako 5168962. skúšanú mriežku) program našiel riešenie:

kdyzidedicpacevsrdcisesmeljevoztejmenautoraltohotoctatoukomensky

V tomto okamihu už bol text natoľko zrozumiteľný, že som zadal ako riešenie slovo KOMENSKY a pre zaujímavosť som si ručne opravil mriežku a dostal správny otvorený text: kdyz dedic place v srdci se smeje vlozte jmeno autora tohto citatu komensky

**Autor:**
Tato úloha vyvolala největší zájem řešitelů. Jeden ze čtenářů sestavil dobrý pomocný program http://www.ngi.cz/fleissner.exe pro ruční řešení, další zaslali odvolávku na výborný software dostupný na internetu na http://www.turning-grille.com/download.htm . Jiní se „jednoduše“ spolehli na útok hrubou silou (všichni tři medailisté). Některé další detaily najdete v následujícím článku „ Čtenáři sobě!“

---

**Jednoduchá záměna (3/2)** (4 body)
Řešení: REPUBLIKAN
Nápověda: Jednoduchá záměna, Crypto-World 10/2000, str. 2-4

```
TQSHF SGSJX UJXDH UQDWK ETSIB YCGFC IBEDI KDWSY EDIBW SBGCE SJXUY EDCFD
IWDNB GCECY CWUTC WQUQC KWCJX DHUQD WKCHC QDNCT XCKUI TCMEK XCWMY DQGCQ
YDEKD JCQDE CKKUE UIBGC EMJXD QEYSN XDJMF GUTCW ETSNE CMJDX DNPXD YCBCY
DYCGD FWUNT CGDOU MKYCX DWDBC DGDTK CXSHC YUEDG CWCKC NTKDX CHDQY CMJXC
KUIBM QWSIB MXDQW UIBHJ XCYCJ XMFDB MYEDC FDIWD BCBGC ECYCW UWCFG CXUQD
LCMEU CWDJU HWUKC XCGUW DCOXD OCWMF MQDMH WCWCP CTCJG CKWCC EJXCY WCKCW
OXDEM EKCWC YUGHY GCEKW UYCGD FWUTC NUEUT KDXCJ XUNSN BGCEC YCWUN JXUXT
GCYED IBQYC IDKQY CBGCE MHMYD QDWSI BEKCK MXDJM FGUTC WETDN MTCWQ UQCKC
YUNSW UNCGC ECMKD HWUYE MYTCD MTCHD NYKDK CMGCH DFMQD KDZKR EPUBL IKAND
CGDJC TXCIM PDJMY CQWUK DZKTU NHUET CGKDW KCTCW QUQCK YDKEU WMYDY CGDFW
UNTCG DOUMC KUNUJ XDHUQ DWKET DTXDE GCNCY SCNDX UITSJ XDHUQ DWKKC THUET
CGYDK EUWMW DPKDE WDPEU NCWDP QUETM KCYCW DPEUN HJMEC FDNYI DGSIB QDPUW
CIBCN DXUIT SIBYC GDFZZ (740 znaků)
```

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

Popis systému:
Jedná se o šifru, která vznikla nestandardní úpravou jednoduché záměny. Nejde tedy o klasický šifrový systém, ale úlohu použitelnou pouze pro účely soutěže. Ztížení spočívalo ve dvou úpravách. Především samohlásky A a O mají společný šifrový kód C. Samotné slovo, kterým se dokazuje vyřešení úlohy (REPUBLIKAN), je v šifrovém textu uvedeno v otevřené podobě. Takže po dešifrování textu získáte umístění „důkazního“ slova a toto slovo v zašifrovné podobě. Zbývá jej tedy buď podle získané převodové tabulky dešifrovat nebo jej vyhledat v zadaném šifrovém textu a tím se získá správné řešení.

```
Otevřený text (bez diakritiky):
Kdyz byly pri prezidentskych volbach secteny vsechny hlasy pri vseobecnem
hlasovani kandidat na prezidenta za demokratickou stranu vedl o dveste
padesat tisic hlasu pred svym republikanskym souperem. Prevaha ve volebnim
kolegiu tvoreneho elektory zavisela na tom, ktera ze dvou protichudnych
urednich zprav o prubehu vseobecneho hlasovani na Floride, Lousiane, Jizni
Karoline a Oregonu bude uznana jako platna a spravna. Kongres ustanovil
zvlastni volebni komisi ktera primym hlasovanim prirkla vsech dvacet dva
hlasu z uvedenych statu republikanskemu kandidatovi. Nyni mala soutezni
vsuvka. Dukazem v teto uloze bude text REPUBLIKAN. Dale pokracuje puvodni.
Tim ziskal tento kandidat vetsinu ve volebnim kolegiu a tim i prezidentske
kreslo Novy americky prezident tak ziskal vetsinu nejtesnejsim a
nejdiskutovanejsim zpusobem v celych dejinach americkych voleb.
```

Ukázka je z textu, který jsem krátce před zveřejněním úlohy publikoval:

Dešifrované telegramy dokazují, že se demokraté snažili podplatit republikány při prezidentských volbách (seriál Toulky zajímavými zákoutími kryptologie - 4.díl, Technet.idnes.cz, 2.11.2004).
http://technet.idnes.cz/sw_internet.asp?r=sw_internet&c=A041101_5285844_sw_interne

**Michal :**

Žeby opäť substitučná šifra? Tvári sa to tak, ale prečo je potom za viac bodov? Nuž, čo by sme sa zamýšľali, keď už máme program. Spustíme a máme text:

```
kdyzbylypriprezidentskychvalbachsectenyvsechnyhlasyprivseabecnemhlas
avanikandidatnaprezidentazademakratickaustranuvedladvestepadesattisi
chlasupredsvymrepublikanskymsauperemjrevahavevalebnimkalegiutvareneh
aelektaryzaviselanatamkterazedvaupratichudnychurednichzpravaprubehuv
seabecnehahlasavaninablaridefausianepiznitaralineagreganubudeuznanaj
akaplatnaaspravnatangresustanavilzvlastnivalebnikamisikteraprimymhla
savanimprirklavsechdvacetdvahlasuzuvedenychstaturepublikanskemukandi
datavimynimalasauteznivsuvkaeukazemvtetaulazebudetextwsjihfctqmealep
akracujepuvadnitextkimziskaltentakandidatvetsinuvevalebnimkalegiuati
miprezidentskekreslamavyamerickyprezidenttakziskalvetsinunejtesnejsi
manejdiskutavanejsimzpusabemvcelychdejinachamerickychvalebxx
```

A hneď vidíme, v čom bol háčik. Totiž všetky výskyty písmena O boli nahradené písmenom A. Ešte že sme sa túto šifru nesnažili riešiť ručne, toto by ju dosť znepríjemnilo. Posledným krokom je zistiť samotné riešenie z vety:

"mala sautezni vsuvka eukazem v teta ulaze bude text wsjihfctqme". Na to si ale stačí pozrieť šifrový text, ktorý zodpovedá otvorenému textu "wsjihfctqm". (REPUBLIKAN)

---

**Jednoduchá záměna (3/3)** (6 bodů)
Řešení: ZARKAWI
Nápověda: Jedno-dvoumístná záměna , Crypto-World 11/2004, str. 5-6
http://crypto-world.info/casop6/crypto11_04.pdf

Úloha:

```
70866 51748 67591 82170 17117 63090 85907 03075 32471 84916 26911 34908
27010 12459 09134 47184 91867 58285 16017 64717 49071 84707 53267 43686
68548 54758 22576 18575 70671 43463 21823 43691 63657 57148 53075 32757
09070 76536 85344 74519 17490 07436 85750 15109 16540 71753 46827 63684
75362 70768 48568 51568 28567 15907 64307 50309 06918 54747 04827 57068
56321 32404 34676 15906 01764 71746 67606 82656 74186 76170 18518 56913
16858 53682 91186 17184 75534 48676 68675 76827 52170 17675 47667 17418
47507 52368 53663 09091 82186 75075 84858 67558 56714 50425 34486 75702
56344 86758 28517 01854 51851 60176 47174 90718 43218 23475 51743 46217
01763 64766 74367 21341 76685 67167 65176 68460 63413 44867 66708 21867
58275 30341 91130 90700 75236 85363 07532 75706 85476 13018 57570 17451
76436 86767 18485 49131 68585 36829 11867 61826 01764 71747 53675 31134
91470 75363 41709 08575 36714 85702 67491 14347 14821 34590 70075 23685
36322 75367 09076 69110 86758 28675 76907 09130 75367 61347 13607 01316
85853 68291 42513 23413 26747 57013 16858 53682 91491 43217 00752 36853
60347 58475 23634 34452 74907 18403 62854 03682 34123 46217 01763 60752
36853 67090 30367 18485 63075 03063 60425 13467 06365 75075 30485 36707
```

```
57460 91474 36748 29074 75851 08676 75324 91821 85747 53470 75324 76671
74167 60682 90916 54034 13443 26234 19182 62418 18685 75911 70909 16826
85634 13267 41753 01548 23412 30908 54703 07532 47184 70131 68585 36829
14916 30454 82706 86764 28536 23447 14601 76471 74134 60757 63448 61718
47559 07451 76191 62684 85709 03036 71848 67582 75067 17436 70907 67530
13413 46857 59118 48518 26349 02753 65191 34474 75823 21916 76746 80496
(znaků 1380)
```

| | 0 | 1 | 2 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| | M | E | S | I | T | A |
| 3 | B | F | J | N | Q | U |
| 7 | V | C | G | K | O | R |
| 8 | W | X | D | H | L | P |
| 9 | Y | Z | | | | konec |

Otevřený text:

V patek pozde vecer byly v bojich zasazeny dve mesity z nichz podle americkych vojaku palili odstrelovaci Na jednu zautocil bojovy vrtulnik tezkym kulometem zatimco na druhou svrhla letadla ctyri bomby a zlikvidovala jeji minarety Americka armada take prevelela z Falludze pechotni prapor do severoirackeho Mosulu aby zde pomohl potlacit mistni povstani Podle velitele americkych jednotek na severu Iraku generala Cartera Hama neni pravdepodobne ze by v Mosulu bojovali rebelove kteri uprchli z Falludze pred americkou ofenzivou Nevyloucil vsak ze incidenty v Mosulu jsou vyrazem podpory vzbourencum ve Falludzi Stejne jako ve Falludzi zije v Mosulu mnoho sunnitskych muslimu Dnes na severu Mosulu vybuchla bomba umistena v automobilu v okamziku kdy kolem projizdel konvoj iracke armady Zatim neni jasne zda si exploze vyzadala nejake obeti Dnes byli v bojich ve Falludzi zabiti dva prislusnici americke namorni pechoty ktere zasahl vybuch podomacku vyrobene naloze Hledany soutezni kod je ZARKAWI

**Michal :**

**(Michal ovšem, jak se dočtete dále vyřešil nejprve poslední úkol a pak se vrátil k této úloze, proč se o tom zmiňuji, poznáte ze zadání poslední soutěžní úlohy…)**

V novembrovom Crypto-Worlde sa dočítame, čo že to vlastne tá jedno-dvojmiestna zámena je. Princíp je ten, že niektorým písmenám zodpovedá jedno číslo, niektorým až dvojica čísel. Aby však takýto šifrový text bol jednoznačne dešifrovateľný (čítajúc ho zľava doprava), ak napríklad niektorému písmenu zodpovedá číslo 35, nemôže inému zodpovedať číslo 3, lebo by sme sa nevedeli po prečítaní trojky rozhodnúť, čo ďalej.

Nech A je množina tých jednociferných čísel, ktoré sú obrazom nejakého písmena.
Nech B je množina tvorená ostatnými ciframi. Ak by sme poznali A a B, vieme šifrový text rozdeliť na obrazy jednotlivých písmen. Ako ale určiť A a B?

Nejaké rady sú uvedené v spomínanom čísle Crypto-Worldu. My ale upriamime pozornosť na tabuľku v jednoduchom príklade použitia. Tá je spravená tak, aby vo všetkých dvojciferných číslach bola prvá cifra z B a druhá z A. To by ale znamenalo, že v šifrovom texte nikdy po sebe nenasledujú dve cifry z B. Stálo by za pokus overiť, či nebola aj v súťažnej úlohe použitá podobná tabuľka.
A skutočne, jednoduchým spočítaním výskytov dvojíc cifier dostaneme, že nikdy po sebe nenasledujú dve cifry z množiny 3,7,8,9. Predpokladajme teda, že toto bude množina B a zvyšné cifry tvoria A.

Teraz už vieme ľahko rozbiť šifrový text na obrazy jednotlivých písmen. Zistíme, že v otvorenom texte by malo byť 25 rôznych znakov. To nás uistí, že sme naozaj na správnej ceste.
Teraz už ale máme pred sebou jednoduchú substitučnú šifru, ktorú ľahko vyriešime vyššie spomínaným postupom.

---

**Šifra (systém neuveden) (3/4)** (8 bodů)
Řešení: HJKMPSSWZ
Nápověda: Nihil novum sob sole!

Úloha:

```
ESERZ DEJIN ILTON UHCYV ETHOL UOSOT OEZET ETSIP INVRP EMSIP SODAN TENAT
KLECE MSOME PTCAN NEMSI ZINYN SHCIN VATSE ZANET OVDYV KSECU EMHCY ATATS
OPOTK ATIZU EMSIP SEZAN NIPUK DNYVY ZETJE JAVYB IPICI ANEMS UKSEV SENIP
DIRTE EBAET ENDEC AKSIZ TERYN PCEZE NEMSI ELHEJ KENAD ORTNO LSINL OPOVO
NDELS HOLUI TNETY ETERO AZCEZ ETJED DOKAJ ZZAKU ETSJE SERYV TIILI OPOTU
NDELS HOLUI ISANU ETUOS ALBEZ ERPOH MAVIJ (znaků 335)
```

Popis systému:
Otevřený text je zformátován do pětic písmen. Tyto pětice jsou (každá zvlášť) zapsány pozpátku. Prolomením „šifry“ však úkol tentokráte nekončí. Kódové slovo, kterým se prokazuje, že luštitel uspěl, tentokráte chybí a je potřeba jej podle získaných pokynů sestavit. Názvy dvou českých měst, které jsou k řešení úlohy potřeba, jsem zvolil velice jednoduše : Praha a Brno.

Otevřený text:

```
Z RESENI JEDNOTLIVYCH ULOH TETO SOUTEZE OPISTE PRVNI PISMENA DOSTANETE
CELKEM OSMNACT PISMEN NYNI Z NICH SESTAVTE NAZVY DVOU CESKYCH MEST A TAKTO
POUZITA PISMENA ZE SKUPINY VYNDEJTE ZBYVAJICI PISMENA VE SKUPINE SETRIDTE
ABECEDNE ZISKANY RETEZEC PISMEN JE HLEDANE KONTROLNI SLOVO POSLEDNI ULOHY
TENTO RETEZEC ZADEJTE JAKO DUKAZ ZE JSTE VYRESILI I TUTO POSLEDNI ULOHU
NASI SOUTEZE BLAHOPREJI VAM
```

**Řešení:**

1) OSJ MHH PAP ABN RWS KRZ (vypsaná prvá písmena kódů všech předchozích úloh)

2) PRAHA BRNO (názvy měst)

3) -SJ M-H --P --- -WS K-Z (písmena po vypuštění názvů měst)

4) HJKMPSSWZ (písmena po abecedním setřídění, tj. hledané kódové slovo prokazující vyluštění poslední úlohy)

Toto slovo dokázalo najít pouze 9 řešitelů ☺ .

**Michal :**

Zatiaľ preskočím úlohu 3.3, keďže túto úlohu som riešil skôr a v tomto prípade je poradie dôležité.

Zahľadíme sa na zadanie. Prvý dojem je ten, že frekvencia písmen sa podobá na češtinu – veľa samohlások, žiadne W či X. Žeby jednoduchá transpozícia? Rýchlo sa ukáže, že síce máme pravdu, ale ešte sme nevyhrali. Čítaním každej pätice znakov sprava doľava dostávame text:

```
Z RESENI JEDNOTLIVYCH ULOH TETO SOUTEZE OPISTE PRVNI PISMENA
DOSTANETE CELKEM OSMNACT PISMEN NYNI Z NICH SESTAVTE NAZVY
DVOU CESKYCH MEST A TAKTO POUZITA PISMENA ZE SKUPINY VYNDEJTE
ZBYVAJICI PISMENA VE SKUPINE SETRIDTE ABECEDNE ZISKANY RETEZEC
PISMEN JE HLEDANE KONTROLNI SLOVO POSLEDNI ULOHY TENTO RETEZEC
ZADEJTE JAKO DUKAZ ZE JSTE VYRESILI I TUTO POSLEDNI ULOHU NASI
SOUTEZE BLAHOPREJI VAM
```

Nuž, teraz som v duchu zanadával, že som si riešenia predchádzajúcich úloh nikam nepísal a väčšinu som si musel preriešiť znova. To, že písmen má byť 18, znamená, že za túto úlohu už žiadne písmeno brať nemáme, a teda nám chýba len jedno písmeno z úlohy 3.3.

Za prvé kolo máme písmená osjmhhpapa, za druhé bnrws, za tretie zatiaľ kr a jedno neznáme. Namiesto neho budem písať otáznik.

Potrebujeme vytvoriť názvy dvoch českých miest. Jedna možnosť bola skúsiť opäť programátorský prístup, na to by ale bolo treba zohnať nejaký zoznam miest. Rozhodol som sa pre lenivejšie riešenie - a oplatilo sa.

Začneme najznámejším mestom, ktorým je Praha. Zostali nám písmená: osjmhpbnrwsk?.
Po troche skúšania vidíme, že zo zostávajúcich písmen sa dá zostaviť aj Brno.

Zostalo nám teda 9 písmen: sjmhpwsk?.

Utriedením známych písmen dostávame HJKMPSSW?. Pre ? máme 26 možností a každá vedie k jedinému 9písmenovému reťazcu, ktorý skúsime zadať ako odpoveď. (Netreba zabudnúť písmeno zvolené namiesto otáznika zakaždým správne zaradiť!) Po 25 neúspešných pokusoch som si už bol takmer istý, že mám niekde chybu - ale nebolo tomu tak. Posledný, 26. pokus uspel. Takže úloha 3.4 bola vyriešená a vedel som, že riešenie úlohy 3.3 začína písmenom Z.

## Statistika úloh za 4 a více bodů

| Úloha | 3/1 | 3/2 | **Průměr** | 3/3 | 3/4 | **Průměr** |
|---|---|---|---|---|---|---|
| Řešitelů | 17 | 14 | 15,5 | 9 | 9 | 9 |

# B. Čtenáři sobě!
# (z e-mailů řešitelů soutěže 2004)

## 1) Celkový vítěz
**Michal Forišek (1.místo, ID misof, body 50, čas ukončení: 14.11 (16:57))**

Záverom by som chcel poďakovať organizátorom súťaže za možnosť zúčastniť sa Mikulášskej kryptobesídky, veľmi sa mi páčila a dala mi motiváciu riešiť túto súťaž aj v budúcom roku**.** Všetkým čitateľom prajem krásne a ničím nerušené prežitie prichádzajúcich sviatkov.

## 2) Nejúspěšnější luštitelka
**Zuzana Rybářová (8.místo, ID Suesie, body 50, čas ukončení: 22.11 (22:15))**

Zuzana se stala historicky první ženou, která v naší soutěži vyřešila všechny úkoly (včetně let minulých!). Blahopřeji !

Zuzana mi na závěr soutěže napsala velice hezký a vtipný e-mail. Krátkou ukázku z něj zde přetiskuji. Pro pochopení některých vět uvádím, že její tatínek se zúčastnil úspěšně soutěže také a to nejen letos, ale i v minulých letech:

Moji prvni vyresenou úlohou byla paradoxne Fleissnerova otocna mrizka. Pri jedne navsteve u rodicu, kdy jsem zastihla tatinka (jiz ponekud psychicky zdeptaneho) resiciho tuto ulohu, jsem si rekla, ze se o to take pokusim. Po vyreseni mrizky (drive nez tatinek!:-)) jsem jiz lusteni zcela propadla. Musim ale priznat, ze pri reseni nekterych narocnejsich uloh mi tatinek poradil techniku lusteni a pri reseni 1/2 zameny jsem vyuzila jeho program napsany ve QuickBasicu.

Nejtezsi ulohou pro mne byla 1/2 zamena (úloha 3.3), periodicke heslo a pote asi transpozice. Na jednu stranu me mrzi, ze jiz soutez zkoncila, ale na druhou je to asi dobre - nekolik noci po sobe se mi zdalo o transpozici; pri reseni jednoduche zameny jsem prejela v metru o

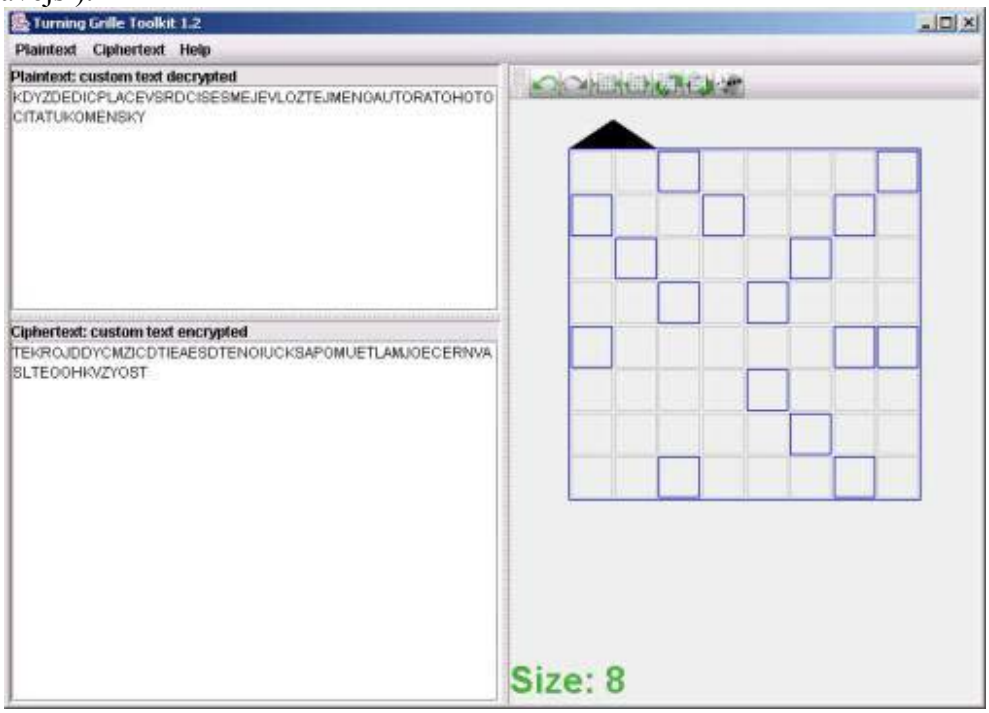
nekolik stanic; tatinek se při nakupu v supermarketu najednou zacal dozadovat tuzky a papiru, protoze ho prave napadlo genialni reseri... :-)

## 3) Ze stupňů vítězů

**Libor Červený (2.místo, ID brubaker, body 50, čas ukončení: 14.11 (18:53))**
**Josef Míka, (3.místo, ID elpepe, body 50, čas ukončení: 14.11 (18:54))**

Soutěžící, kteří obsadili druhé a třetí místo, jsou z jednoho pracoviště. Je téměř neuvěřitelné, že o jejich vzájemném pořadí rozhodlo pouhých 18 vteřin… Nechme však o jejich trampotách s luštěním vyprávět je samotné … :

To druhe misto obsadil kolega z prace. Spoluprace spocivala akorat v tom , ze jsme se vzajemne upozornili na zverejneni uloh. Mimochodem musel jsem kvuli tomu v nedeli do prace protoze doma pocitac ani internet nemam. Kolega bohuzel ano, takze ziskal casovy naskok ktery se mi skoro podarilo zdolat. Jedina uloha na ktere jsme spolupracovali byla Fleissnerova mrizka a tu jsme vyresili brute-force utokem (cas vypoctu cca 10 hodin). Prave oslavujeme a vypravime si zazitky ze vcerejsiho lusteni vcetne reakci manzelek (coz je asi to nejzajimavejsi).




Co se tyce utoku na Fleissnerovu mrizku, v priloze posilam Java script + slovnik ktery jsme pouzili pro utok. Rozhodujicim faktorem pro utok je nastaveni parametru Trigger (chars) ktery ovlivni pocet zobrazenych reseni. Zkousenim jsme zjistili, ze optimalni hodnota je asi 75-85% delky textu. V pripade soutezni ulohy asi 56 znaku. Vetsi hodnota uz nezobrazi spravny vysledek, mensi fhodnota generuje obrovsk0 mnozstvi vysledku.

Mame radost, ze jsme se dokazali merit i s takovym souperem jako je vitez. Mozna by jsme to dokazali i driv ale vratit se z vikendu u babicek a presvedcit manzelky ze nejsme uplni blazni nejakou dobu trvalo, coz vitezi pravdepodobne poskytlo rozhodujici naskok.

## 4) Z e-mailů řešitelů

Dokonce jsme emailem kontaktovali Thomase Jakobsena. Odepsal nam, ze jeho algoritmus je celkem jednoduchy, a ze ho zajima jestli bude spravne fungovat i na cestinu, ze ji sice neovlada, ale ze jeho babicka je z Prahy.

... dekuji za pomoc s odstranenim chyb, na http://www.ngi.cz/fleissner.exe jsem umístil novou verzi programu. Myslím, ze tato verze jiz jako skutecná pomucka slouzit muze, takze pokud program shledáte jako uzitecný, budu rád, kdyz ho uverejníte. Snad to nekomu pomuze...

Reseni jedno-dvoumistne zameny zabralo asi 1 hodinu a z toho 80% casu uprava textu. .... Podle tabulky jsem cisla nahradil pismeny a vysledek jsem "prohnal" Jacobsenovym algoritmem a v programu jz ktery jsem mel ze souteze z roku 2001 jsem "doladil" jednoduchou zamenu. A bylo to. Jacobsenuv algoritmus v kombinaci s programem jz umoznuje jednoduchou zamenu vyresit během 10-15 minut. .....

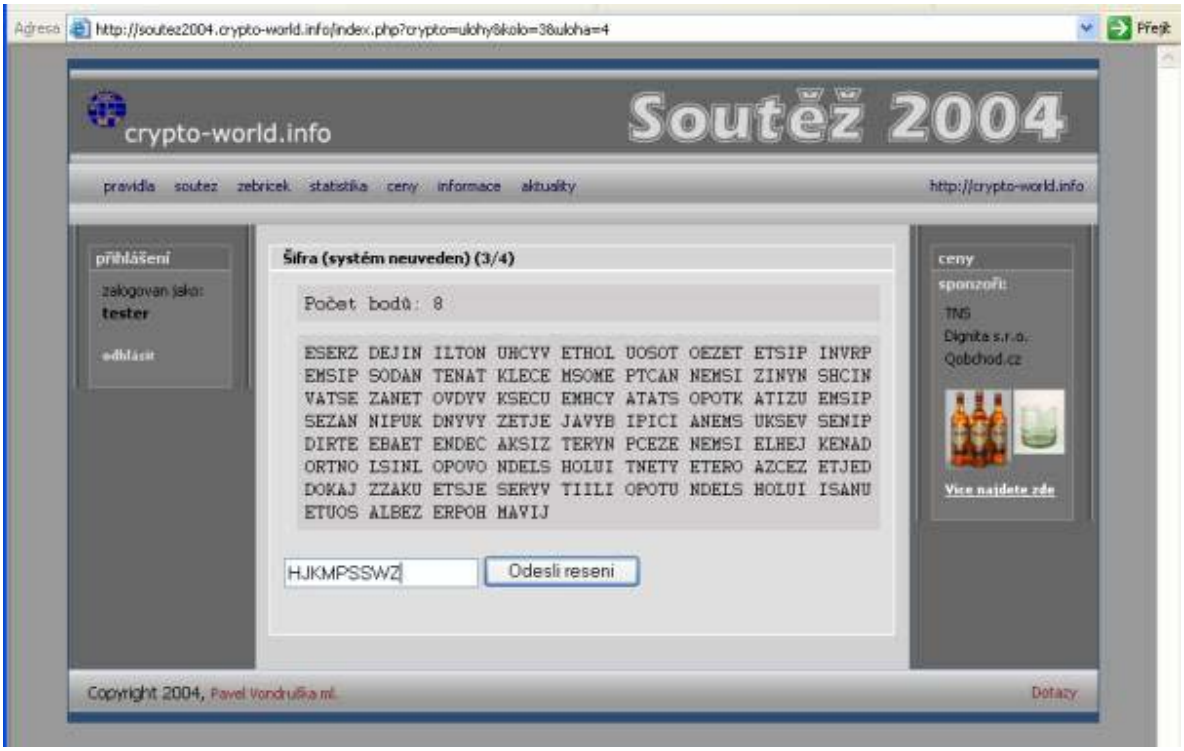
Zkuste se podívat na http://www.turning-grille.com/download.htm je to vynikajici pomucka !!! .....

Blbejsi soutez jste si nemohl vymyslet? Vzdyt mate na webu chybu - ta zadani nejdou vubec precist? Asi tam mate divne kodovani nebo co… Co tedy mam vlastne resit? Muzete mne poslat zadani uloh tak, abych jej precetl?

..Netrpelive jsem ocekaval dalsi ulohy. Ziskal jsem sice jen 15 bodu, ale jsem rozhodnut to priste vyhrat !

# 5) Závěr (autor soutěže)

Děkuji všem za pěkné a zajímavé e-maily. Všem úspěšným řešitelům ještě jednou blahopřeji a těším se na setkání v dalším ročníku soutěže!




# C. O čem jsme psali v prosinci 1999-2003

**Crypto-World 12/1999** (http://crypto-world.info/index2.php?vyber=casop1)



**Crypto-World 12/2000** (http://crypto-world.info/index2.php?vyber=casop2)



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** (http://crypto-world.info/index2.php?vyber=casop2)



**Crypto-World 12/2001** (http://crypto-world.info/index2.php?vyber=casop3)



Příloha: uloha7.wav

**Crypto-World 12/2002** (http://crypto-world.info/index2.php?vyber=casop4)



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

**Crypto-World 12/2003** (http://crypto-world.info/index2.php?vyber=casop5)



Příloha: pf_2004.jpg

# 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@pvt.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/ |