Crypto-World

Informační sešit GCUCMP

Ročník 5, číslo 12/2003 **15. prosinec 2003**

12/2003

Připravil : Mgr.Pavel Vondruška

Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(490 e-mail výtisků)

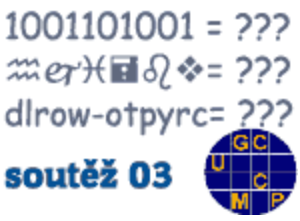
Obsah : **Str.**

Příloha: pf_2004.jpg

(články neprocházejí jazykovou korekturou)

A. Soutěž 2003 skončila

Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.



Soutěž v luštění jednoduchých hříček a kryptologických úloh, kterou jsem vyhlásil v zářijovém čísle Crypto-Worldu, skončila. Po tři měsíce bylo na http://crypto-world.info/ vyvěšeno devět soutěžních úloh. Řešitelé se mohli pokusit o jejich řešení a on-line si zkontrolovat, zda jejich řešení je správné. Do soutěže se zaregistrovalo celkem **107 řešitelů**, z nichž však pouze **32 splnilo podmínky pro zařazení do losování o ceny;** všech **9 úloh vyřešilo celkem 11 soutěžících**. Prvá tři místa byla obsazena již v průběhu prvého týdne soutěže.

Pořadí a ceny

Ceny (replika historické číše Rudolfa II. a láhev portugalského vína MATEUS) získali automaticky první tři řešitelé a dále další tři účastníci, kteří byli vylosováni z těch, kteří splnili podmínky soutěže (tj. jednalo se o odběratele Crypto-Worldu, kteří do 6.12.2003 vyřešili minimálně 3 úlohy).

Pořadí	Registrační jméno	pořadí vyřešených úloh	celkem vyřešeno
1	**CyberMage**	01; 03; 02; 04; 05; 06; 09; 08; 07	/9
2	peta007	01; 04; 07; 02; 03; 05; 06; 08; 09	/9
3	xnovakv	02; 05; 06; 03; 01; 04; 08; 07; 09	/9
8	enigma	01; 03; 05; 02; 04; 09; 06; 08; 07	/9
11	mystik	01; 03; 05; 06; 02; 09; 08; 04; 07	/9
25	adam	01; 03; 02; 05	/4

Celkový vítěz (Jaroslav Vorlíček – CyberMage) navíc získal od pořadatele Mikulášské kryptobesídky registraci na tento mezinárodní workshop. Jaroslav Vorlíček také sepsal možné postupy řešení úloh č.7 až č.9 (kapitola C).

Úlohy

Jaké úlohy řešitelé řešili ? Úlohy byly rozděleny do tří kol. V prvním kole jsem připravil podle mého názoru úlohy velice lehké, které měly sloužit ke zvýšení sebevědomí řešitelů a přilákat je do soutěže. Z hlediska klasifikace šifrových systémů je lze označit takto :

I.kolo – lehké úkoly (hříčky)

Transpozice I.
Jednoduchá záměna I.
Jednoduchá záměna II.

Úloha č.1 - Transpozice I.

```
FDSAZ TREWQ EJOLS EHUHC EPSUK IJERP OHALB MEDER PYDET AAKHE LECIL EVUDV
ARPOE JANDE JOLSI CAHOL UXXXX
```

Úloha č.2 - Jednoduchá záměna I.

74695 76973 59585 57069 76595 85974 73595 85570 69765 95859 74645 57368 59556 95759 67576 66976 59656 85975 67636 26976 69726 37469 74696 77359 67757 36367 66575 97462 59736 66964 59557 35763 63585 97359 74999

Úloha č.3 - Jednoduchá záměna II.

II.kolo – klasické šifrové systémy (lze řešit jednoduše pomocí nápadu)

Transpozice II.
Jednoduchá záměna III.
Jednoduchá záměna IV.

Úloha č.4 - Transpozice II.

```
UCTIR OIYNM NVBAT CNCAE AODJH SOEOL POURI SPIRT ZAEAY RTOOE HMNPZ EIELJ
PDELT
```

Úloha č.5 - Jednoduchá záměna III.

```
AMHCT SZCAF MBLMR MFMYZ WZWJM TWIML YLMHC RYICF MBLMR MFMYZ WZWJM TWIML
YLMNM PYBLC XYBCH HYIMT WQJCB CIAYC QYPBT YXXXX
```

Úloha č.6 - Jednoduchá záměna IV.

```
PWBAN RMVXL EBHEV GORHA ZKLNV MFPWB ANRMV XLFPZ AVHAZ KZNZG FQRHR GLZOV
PWBAG LHZNF WVOZN KLXSL KRNAZ KRHGV PLWZG YZHZG YZHXX
```

III.kolo – klasické šifrové systémy

Transpozice III.
Jednoduchá záměna V.
Periodické heslo I.

Úloha č.7 - Transpozice III.

```
IPOAD PSPIM IOOPS EULUI EILJC HEDOI LTPLU AMZYC TSEEO COVUI MNRME TYTAT
TVZIA JEZLA LLNKO DDUDT EEAJM EMIVS RIOAD RXESE UGIDE RIIIE AZNTA DEYAT
HYVCC EKZZI KMIMT OASAT AZAHI UDADC OELAE VZENU AIOCN EVISZ KYMIA UXOEA
AKNZD IDHMN OEGEJ ININA AONIZ TDLJD IYSER JSVZO MIRAZ LOCOH TROTD NDNIM
MLCLA SIAUI LFESP EAMEH MDPIU NULYE EBZTN BXTLM SBUUY UVIZR SOEIK BUAHI
KORVR RLOTY TNZOO DKOJK OFAVI NAEES AKBME DRELX LAKIJ AJDZV PIEAV EPRSE
DOIIH EVVRL EORID VZEJI
```

Úloha č.8 - Jednoduchá záměna V.

```
QMEYL CZSTR TJVTY DDSBT ZSTBU FIYLZ TATSD JPEFU PEQDS DQCND JCYTY TSIZT
ATSDA TCEBU ZDDSB TZSTB UFIYL CVNDM CYDUR FIMNT AVUMU KDAQT STRTJ VTYSI
QENUJ TSDQM NDYES CVTFS TQPDA MECRU LEJTN DASCA BCFTS IQVZD JSCMT QEQUJ
SEKDY DQTHV UZBAU EMZUQ TYCAB DMNDY TBTSB UABCF KTFAC MRTJV TYSUA BSDPD
ZUEEQ UJSEK DYDEB UMVUQ UYDBZ UKAMT LUMUS TBTSQ EJTQD BZCPE VUPUR QEJTB
URIBA VEABD BTNSI AUERU ZVZDV UKTSI MTQCD NEUPT ANCSI KCMUR IUPMU NTWIJ
ODZQI STSDB ZTRCJ PEZCJ SUFCB JTYLE PCMMU NTWCU BCMUF TQBUT QCDNE STQCC
SDVUB EYLIV ZDKTQ YTTQC DNEVZ DVUKT SIAUE RUZPE FTZDF TAVEA BDCST FTPUQ
MIADB CMSCD SABCN EKTBZ UKAMT LUMUS TSCAF EKNUM CNSDV UYDBC YBTSA TJPTJ
CLSDJ PDCYT MCSCU MCQJD MMPIA TEJDF CBTNR EPTVZ DVUKU FCBMP CSTDS BTZST
BUFTC VNDMC YDCSC MNCFT ASDYD SCVDA TVZDA BEVUF TLTAN UMAUE MZUQT YCABD
MNDYT BUADB ZUKAM IMESJ CJSCQ TSCCA VUNEA FITHV UZBUF CSIQA UEMZU QIQMN
DYTQU PTANT EBUYS DMUFD STMCQ PUDSB TZSTB EEBUY SDMBC MQCMP DAVUJ DYDAU
EMZUQ UEYCA BMNDY TCLTA NUMSD YUJVU ABCYE KTMJD AMCSD DPTSB DBIUV ZCFST
STLUE JDFCB TNTVU VZUFT PTSDB TYLBU CMYDA TBZUK AMIME SUPDS ABCNE KTCJC
QTBTV UAURT ABUVI VUMEP AIABT QISTV UEJDF CKDVZ UCEBT SBDJC YDEJD FCBTN
EYTZB DODMC BIKTA DBECY TKTAB TKTPS UPEAA DEMUN TQBZU KAMTL UMUST KTVCM
```

```
JMNCF TASDY TUPYL IBDBV ZDABE VUFTL TANUC BUUPT ANCBE BUYSD MUFDP ENTJD
BUEAM EBTYS UABDK TJTBZ UKAMI MESST SDFDZ EAQTJ DJCAC PSDZU JPDNI VCBZD
JTATS TEQDA CQUFU NSTAD ZDBCK TURFI MNTSC VZUWZ CQUFC SJYTN CKTPS UEYTN
UFTMY DNTST QEEBU MESCK TPSEM USMZT BSDUA UREKT PTSMU SMZTB SDVUY DBCYJ
BTYLB UPEFU PEKTK FTFTB ADSTV ZDVCP ECSBD FDZUF TVZUW ZCQIS TZUJV UJSCK
DCSTU LNCAD KTLUV ZDBUQ SUABK CMUPE MCJJT KABTB EBUEN ULEFI ZTADN DJCPT
KBTAN UFUAU EBTJK TUMXX
```

Úloha č.9 - Periodické heslo I.

```
AAWTV RBMRG WESMD UGFUG MGOGZ WAIQA GBWDZ ZVGTS
MIBNH NSEMQ IQOLH UBOOW CTAKR HZBXB VRFTE IZFTR
NWCQD ZDRFT VVPUC FBSEE WOCCI BOMGG NVVKW TJXSR
MHBQM IBTYF VXHVS HXAVP QEOTR HVVTN BWMIB JDYGG
MCZHG WDIKR HNSMV VBRCL BZRTR QWEIC EYGWV WJEMW
VHBBN HGWHB LPLHS DRRKR XKHCG RHREX BPKWT JXVVL
CTRGQ TIWCZ GMDAO TCMMI EVWRT SYOYO BBAMO XHNKL
FSWOK OCASW ONBCG RRGLK MUPOO EXVVT DYBTS FNHYL
XZRSN ODBAB AYMKN VLTDR GFWIE OOEHC MLQMS GMLKD
NMCQQ AGBWL BFPBD GOHKE NZQVP LTRQA VPKRH PSSMA
SRIHH BFLLY KMICE WWTBS FVDBS IZZBR XWFAK EMBWM
IBJHR MVPDU GFUXX VVQMS GIJHU CETHU IOJKH JVTRZ
ADAZL BNWCM KANNS UMQPH QWGGG RHRCK QMDRI BTSFV
HQAHS KEUMU ARJEP ADNDZ LFCLX LPNHB SCLVS HBADL
FKGCT RAVPR YMLQC DRDML BZTVT CKQMD BBSFC URFWS
EMRNR DGDCJ IVTSE MBRLJ VTSEE PIFXL FSDVF XVVBR
HNSLR LHBGL BBTHF SCMRO GRWEC AERRV HBPKX GFBHJ
IPWNX SDIMT HKQCI VJWES RNHNS UGEEM OCTAB OGZAO
IDOFY FXULS YMEBA ZLDAA WWJAK ZSECT IXGSG VREXG
KXVVC DCKMI COVHA FCURF TBTSF DXYSS HVJVH WMCKO
XZGAC JPUON GMMYU TKBTZ ZDRWC BVSHB WVIDU GFUQF
```

Popis klasických šifrových systémů a postupy luštění naleznete v řadě publikací. Pro české čtenáře, kteří se chtějí seznámit se základní technikou vytváření a řešení těchto šifer, doporučuji např. tyto zdroje:

[1] Simon Singh : Kniha kódů a šifer, DoKořán 2003, str.22
[2] Janeček,J.: Odhalená tajemství šifrovacích klíčů minulosti. Praha, Naše vojsko, 1994.
[3] Přibyl,J. a Kodl,J.: Ochrana dat v informatice. Praha, Vydavatelství ČVUT, 1996
[4] Vondruška,P.: Soutěž ! Část II.- Jednoduchá záměna, Crypto-World 10/2000, str. 2-4
[5] Vondruška,P.: Soutěž ! Část III.- Jednoduchá transpozice, Crypto-World 11/2000, str. 2-6
[6] Tesař,P. : Substituce složitá - periodické heslo, srovnaná abeceda, Crypto-World 12/2000, str. 4-10
[7] Tůma,J.: Doprovodné texty k přednášce Úvod do klasických a moderních metod šifrování ALG082 (zimní semestr 2003). Katedra algebry MFF UK Praha (http://adela.karlin.mff.cuni.cz/~tuma/ciphers.html).

V následujících dvou článcích můžete najít informace k použitým šifrovým systémům, správné řešení soutěžních úloh a v případě klasických šifer (úlohy č.7-č.9) i návod na luštění.

B. Soutěžní úlohy č.1-6

Pavel Vondruška, ČESKÝ TELECOM a.s.

I.kolo – lehké úkoly (hříčky)

Úlohy prvého kola patří spíše do kategorie hříček než šifer. Přesto je lze mezi klasické šifrové systémy zařadit, jednalo se jednoduchou záměnu a transpozici. Tyto úlohy měly především přilákat zájemce o letošní soutěž.

Úloha č.1 - Transpozice I.

```
FDSAZ TREWQ EJOLS EHUHC EPSUK IJERP OHALB MEDER PYDET AAKHE LECIL EVUDV
ARPOE JANDE JOLSI CAHOL UXXXX
```

Prvá úloha vznikla pouhým vypuštěním mezer v otevřeném textu a přepsáním výsledku pozpátku. Výsledek pak byl rozepsán do pětic znaků – dělba, která je u šifrových textů běžná a kterou jsem použil u všech dále předložených úloh. Pro větší „složitost“ jsem slovo, které se dostane po těchto úpravách na začátek textu, volil „bezvýznamové“. Pokud se řešitel zadíval pozorně na některý jiný úsek textu, pak zde slovo zapsané pozpátku lze snadno rozeznat. Z hlediska klasifikace šifrových systémů lze tento naivní systém označit jako transpozici.

Otevřený text:
ULOHA CISLO JEDNA JEOPRAVDU VELICE LEHKA A TEDY PREDEM BLAHOPREJI K USPECHU HESLO JE QWERTZASDF

Kontrolní (hledané) slovo: QWERTZASDF (tj. slovo, které řešitelé museli zadat přes www rozhraní jako důkaz, že úlohu vyřešili).

Úloha č.2 - Jednoduchá záměna I.

74695 76973 59585 57069 76595 85974 73595 85570 69765 95859 74645 57368 59556 95759 67576 66976 59656 85975 67636 26976 69726 37469 74696 77359 67757 36367 66575 97462 59736 66964 59557 35763 63585 97359 74999

Druhá úloha je z hlediska klasifikace šifrových systémů tzv. dvoumístná jednoduchá záměna. Znak otevřeného textu se zamění za dvojici – v tomto případě číselnou. Úloha je však velmi triviální, neboť se jedná o srovnanou abecedu a navíc má připomínat ASCII tabulku. V ASCII tabulce se znaku A přiřadí kód 65, znaku B kód 66 atd. Zde jsem použil kódovou tabulku, která vznikla z ACCI tabulky tak, že každá hodnota číselného kódu je zmenšena o deset. Frekvence dvojic 55 a 59 měla napovědět, že se jedná o samohlásky (písmeno A, E), zbytek je již pouhou technickou záležitostí.

Převodová tabulka:

I.kolo							Jednoduchá záměna I.									ASCII-10									
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
55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80

Použijeme-li převodovou tabulku, dostaneme z šifrového textu následující otevřený text:
TO CO SE DA POVEDET SE DA POVEDET JASNE A O CEM CLOVEK NEUMI HOVORIT O TOM SE MUSI MLCET HESLO JE ASCII DESET

Kontrolní (hledané) slovo: ASCIIDESET

Úloha č.3 - Jednoduchá záměna II.

Třetí úlohou byla opět jednoduchá záměna. Znak otevřeného textu se zde zaměňuje za obrázek. Text však není potřeba luštit (např. použitím frekvenční analýzy či odhadem obsaženého slova). Stačí si uvědomit, že tyto obrázky „důvěrně“ známe. Jedná se o font Wingdings, který je běžně používán a patří k základním fontovým sadám. Zadání úlohy stačí tedy vzít do bloku a změnit font na Wingdings a dostaneme hledané řešení. Abych řešení přece jen trochu zkomplikoval, nebyl text uveden na stránce v textové podobě, ale byl zde umístěn „obrázek“ s úlohou. Řešitel musel nejprve text přepsat a po té mohl teprve provést uvedenou záměnu fontu.

Převodová tabulka pro font Wingdings:

I.kolo							Jednoduchá záměna II.									Wingdings									
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
✌	👌	👍	👎	☜	☞	☝	✋	🖐	☺	😐	☹	💣	☠	⚐	⚑	✈	☼	🕯	❄	✝	✞	✠	✠	✡	☪

Řešení (po výměně fontu):
NACES TEKUS PECHU NEBUD ETENI KDYSA MI,NA OPAKJ ENUTN OPOCI TATST LACEN ICISK OROJA KOVAU TOBUS ENENI DOBRE PODCE NOVAT OSTAT NI!HE SLOJE VYMEN FONT!

NA CESTE K USPECHU NEBUDETE NIKDY SAMI, NAOPAK JE NUTNO POCITAT S TLACENICI SKORO JAKO V AUTOBUSE. NENI DOBRE PODCENOVAT OSTATNI! HESLO JE VYMENFONT!

Kontrolní (hledané) slovo: VYMENFONT!

II.kolo – klasické šifrové systémy (lze řešit jednoduše pomocí nápadu)

Ve druhém kole jsem předložil k luštění tři úlohy, které byly zašifrovány pomocí známých klasických šifrových systémů („podle plotu“, „Caesarova šifra“, „Atbaš“) . Délku textu jsem volil kratší, aby uživatel byl nucen použít k jejich řešení jiné metody než klasické metody řešení založené na frekvenční analýze (pro jednoduchou záměnu) nebo bigramových vazbách (pro transpozici).

Úloha č.4 - Transpozice II.

UCTIR OIYNM NVBAT CNCAE AODJH SOEOL POURI SPIRT ZAEAY RTOOE HMNPZ EIELJ PDELT

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.
Předložená úloha řešitelům poměrně odolávala a řada z nich ji označila jako těžkou. Je to možná i tím, že uvedený systém není u nás příliš známý.

Ukážeme si možnou přípravu příslušného šifrového textu:

URCIT SI PRIORITY ZNAMENA VYBRAT TO CO NECHAME NA POZDEJI
HESLO JE PODLE PLOTU

UrCiT sI pRiOrItY zNaMeNa VyBrAt To Co NeChAmE nA pOzDeJi HeSlO jE pOdLe PlOtU

UCTIROIYNMNVBATCNCAEAODJHSOEOLPOU
rispirtzaeayrtooehmnpzeieljpdelt

UCTIROIYNMNVBATCNCAEAODJHSOEOLPOUrispirtzaeayrtooehmnpzeieljpdelt

Kontrolní (hledané) slovo: PODLEPLOTU

Úloha č.5 - Jednoduchá záměna III.

```
AMHCT SZCAF MBLMR MFMYZ WZWJM TWIML YLMHC RYICF MBLMR MFMYZ WZWJM TWIML
YLMNM PYBLC XYBCH HYIMT WQJCB CIAYC QYPBT YXXXX
```

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. V předložené úloze jsem použil posun o dva znaky vlevo. Tento posun se v římské armádě prokazatelně používal. Převodová tabulka takovéto jednoduché záměny vypadá následovně :

II.kolo							Jednoduchá záměna III.									Caesar -2									
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
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X

Použijeme-li tuto převodovou tabulku, dostaneme ze šifrového textu následující otevřený text:
CO JE VUBEC HODNO TOHO ABY BYLO VYKONANO JE TAKE HODNO TOHO ABY BYLO VYKONANO PORADNE ZADEJ JAKO VYSLEDEK CAESAR DVA ,

Kontrolní (hledané) slovo: CAESARDVA

Úloha č.6 - Jednoduchá záměna IV.

```
PWBAN RMVXL EBHEV GORHA ZKLNV MFPWB ANRMV XLFPZ AVHAZ KZNZG FQRHR GLZOV
PWBAG LHZNF WVOZN KLXSL KRNAZ KRHGV PLWZG YZHZG YZHXX
```

Další známý jednoduchý klasický systém jsem použil i v poslední úloze druhého kola. Použitý systém se nazývá atbaš (někdy atbš). Je to tradiční hebrejská substituční šifra. Její použití můžeme nalézt například i 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* a je nahrazeno posledním písmenem *tav*, druhé písmeno bet se nahrazuje předposledním písmenem hebrejské abecedy – *šin* atd.

Příslušná převodová tabulka pro mezinárodní abecedu vypadá tedy následovně:

II.kolo							Jednoduchá záměna IV.									Atbaš									
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
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

Použijeme-li tuto převodovou tabulku, dostaneme ze šifrového textu tento otevřený text:
KDYZ MI NECO VYSVETLIS ZAPOMENU KDYZ MI NECO UKAZES ZAPAMATUJI SI TO ALE KDYZ TO SAM UDELAM POCHOPIM ZAPISTE KOD ATBASATBAS

Kontrolní (hledané) slovo: ATBASATBAS

III.kolo – klasické šifrové systémy

Třetí a poslední kolo se skládalo ze tří klasických šifrových systémů transpozice, jednoduché záměny a periodického hesla. Při řešení těchto klasických 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.).
V následujícím článku se dozvíte jak postupoval při řešení úloh vítěz letošní soutěže – Jaroslav Vorlíček (CyberMage).

C. Řešení úloh č.7-9

Jaroslav Vorlíček (CyberMage, Jaroslav.Vorlicek@uhk.cz)

Úloha č.7 - Transpozice III.

```
IPOAD PSPIM IOOPS EULUI EILJC HEDOI LTPLU AMZYC TSEEO COVUI MNRME TYTAT
TVZIA JEZLA LLNKO DDUDT EEAJM EMIVS RIOAD RXESE UGIDE RIIIE AZNTA DEYAT
HYVCC EKZZI KMIMT OASAT AZAHI UDADC OELAE VZENU AIOCN EVISZ KYMIA UXOEA
AKNZD IDHMN OEGEJ ININA AONIZ TDLJD IYSER JSVZO MIRAZ LOCOH TROTD NDNIM
MLCLA SIAUI LFESP EAMEH MDPIU NULYE EBZTN BXTLM SBUUY UVIZR SOEIK BUAHI
KORVR RLOTY TNZOO DKOJK OFAVI NAEES AKBME DRELX LAKIJ AJDZV PIEAV EPRSE
DOIIH EVVRL EORID VZEJI
```

Šifrování transpozicí

Základem pro šifrování transpozičních šifer bývá matice MxN. Její velikosti odpovídá délka textu. Jeden typ transpoziční šifry se tvoří tak, že se otevřený text (OT) vpisuje do matice po řádcích, matice se doplní tak, aby byla úplná a v ní se nevyskytovala prázdná pole. Poté se sloupce očíslují podle dohodnutého hesla a nakonec se vypisuje šifrovaný text podle očíslovaných sloupců.

1	3	2	5	4
P	R	E	J	I
D	O	B	R	E
H	O	D	N	E
V	E	S	P	O
L	E	K	X	X

tabulka 1 Jednoduchá transpozice

Výsledný šifrovaný text bude PDHVL ROOEE EBDSK JRNPX IEEOX.

Postup luštění

Vzhledem k velké délce textu není pravděpodobná jednoduchá manipulace s textem (viz úloha č.4 - transpozice II). Číslo 380 lze rozložit na prvočísla 2,2,5,19. V rámci co nejjednodušší manipulace s textem se obvykle rozměry matice volí tak, aby to byla téměř stejná čísla. Proto ze všech kombinací 2,2,5,19 lze vybrat rozměry matice 20x19. Dále je potřeba rozhodnout, která hodnota náleží počtu sloupců a která počtu řádků.Nejdříve je zajímavé podívat se na znak X. V oblasti jednoduchých šifer se tímto znakem velmi často doplňují mezery v textu a matice do požadovaného tvaru. Na předchozím případě je vidět, že vzdálenost mezi znaky X je 5. Máme písmeno X na pozicích 96,176,276. O pozici X 339 můžeme uvažovat jako o náhodě, která nemá nic společného s předchozími znaky. Vzdálenost mezi těmito znaky je dělitelná číslem 20, což by mohlo naznačovat, že se znaky mohou vyskytovat na stejném řádku a pravděpodobně leží vedle sebe.

Nejprve je potřeba šifru rozepsat do matice a označit znaky, které nás zajímají.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
I	E	T	T	E	U	H	A	A	A	A	M	M	M	S	K	O	L	D
P	I	S	V	E	G	Y	Z	I	K	O	I	L	D	B	O	F	A	O
O	L	E	Z	A	I	V	A	O	N	N	R	C	P	U	R	A	K	I

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

tabulka 2 Šifrovaný text rozepsaný do sloupců

(Při luštění se osvědčilo tuto tabulku vytisknout, rozstříhat na sloupce a skládat mimo počítač na desce stolu). Pokud mají sloupce 4,8,13 sousedit, máme 3! možností, jak je uspořádat. Abychom snížili počet možností je dobré si uvědomit, že se v českém jazyce pravidelně střídají souhlásky a samohlásky. Jen v ojedinělých výjimkách jako je ou , au nebo pokud končí jedno slovo a začíná druhé, pak jsou vedle sebe dvě samohlásky. Rozhodně to není pravidlem.

4	13	8
E	M	A
E	D	I
A	P	O
J	I	C
M	U	N
E	N	E
M	U	V
I	L	I
V	Y	S
S	E	Z
R	E	K
I	B	Y
O	Z	M
A	T	I
D	N	A
R	B	U
X	X	X
E	T	O
S	L	E
E	M	A

tabulka 4 Část šifrovaného textu - Varianta A

8	13	4
A	M	E
I	D	E
O	P	A
C	I	J
N	U	M
E	N	E
V	U	M
I	L	I
S	Y	V
Z	E	S
K	E	R
Y	B	I
M	Z	O
I	T	A
A	N	D
U	B	R
X	X	X
O	T	E
E	L	S
A	M	E

tabulka 5 Část šifrovaného textu - Varianta B

Nyní je potřeba se rozhodnout, kterou z těchto variant zamítnout. Ostatně případná chyba úvahy se ihned projeví ve výsledném textu. (Správná je varianta A) Dále se postupuje pouze se znalostmi českého jazyka. Postupně se přidávají další a další sloupce.

2	4	13	8	3
T	E	M	A	T
S	E	D	I	V
E	A	P	O	Z
E	J	I	C	I
O	M	U	N	A
C	E	N	E	J
O	M	U	V	E
V	I	L	I	Z
U	V	Y	S	L
I	S	E	Z	A
M	R	E	K	L
N	I	B	Y	L
R	O	Z	M	N
M	A	T	I	K
E	D	N	A	O
T	R	B	U	D
Y	X	X	X	D
T	E	T	O	U
A	S	L	E	D
T	E	M	A	T

tabulka 6 Část šifrovaného textu - krok 3

Konečným řešením vznikne tabulka, ze které je možno přečíst otevřený text

14	1	18	12	10	5	17	16	6	7	11	9	2	4	13	8	3	0	15
S	E	D	M	A	U	L	O	H	A	M	A	T	E	M	A	T	I	K
B	I	O	L	O	G	A	F	Y	Z	I	K	S	E	D	I	V	P	O
U	L	I	C	N	I	K	A	V	A	R	N	E	A	P	O	Z	O	R
U	J	I	L	I	D	I	V	C	H	A	Z	E	J	I	C	I	A	V
Y	C	H	A	Z	E	J	I	C	I	Z	D	O	M	U	N	A	D	R
U	H	E	S	T	R	A	N	E	U	L	I	C	E	N	E	J	P	R
V	E	V	I	D	I	J	A	K	D	O	D	O	M	U	V	E	S	L
I	D	V	A	L	I	D	E	Z	A	C	H	V	I	L	I	Z	P	O
Z	O	R	U	J	I	Z	E	Z	D	O	M	U	V	Y	S	L	I	T
R	I	L	I	D	E	V	S	I	C	H	N	I	S	E	Z	A	M	Y
S	L	E	L	I	A	P	A	K	O	T	O	M	R	E	K	L	I	T
O	T	O	F	Y	Z	I	K	M	E	R	E	N	I	B	Y	L	O	N
E	P	R	E	S	N	E	B	I	L	O	G	R	O	Z	M	N	O	Z
I	L	I	S	E	T	A	M	M	A	T	E	M	A	T	I	K	P	O
K	U	D	P	R	A	V	E	T	E	D	J	E	D	N	A	O	S	O
B	A	V	E	J	D	E	D	O	V	N	I	T	R	B	U	D	E	D
U	M	Z	A	S	E	P	R	A	Z	D	N	Y	X	X	X	D	U	K
A	Z	E	M	V	Y	R	E	S	E	N	I	T	E	T	O	U	L	O
H	Y	J	E	Z	A	S	L	A	N	I	N	A	S	L	E	D	U	J
I	C	I	H	O	T	E	X	T	U	M	A	T	E	M	A	T	I	K

tabulka 7 Otevřený text

Otevřený text**:** SEDMA ULOHA MATEMATIK BIOLOG A FYZIK SEDI V POULICNI KAVARNE A POZORUJI LIDI VCHAZEJICI A VYCHAZEJICI Z DOMU NA DRUHÉ STRANE ULICE NEJPRVE VIDI JAK DO DOMU VESLI DVA LIDE ZA CHVILI ZPOZORUJI ZE Z DOMU VYSLI TRI LIDE VSICHNI SE ZAMYSLELI A PAK O TOM REKLI TOTO FYZIK MERENI BYLO NEPRESNE BILOG ROZMNOZILI SE TAM MATEMATIK POKUD PRAVE TED JEDNA OSOBA VEJDE DOVNITR BUDE DŮM ZASE PRAZDNY XXX DUKAZEM VYRESENI TÉTO ULOHY JE ZASLANI NASLEDUJICIHO TEXTU MATEMATIK

Heslo použité pro transpozici : 14 1 18 12 10 5 17 16 6 7 11 9 2 4 13 8 3 0 15

Kontrolní (hledané) slovo: MATEMATIK

Úloha č.8 - Jednoduchá záměna V.

Zadání

QMEYL CZSTR TJVTY DDSBT ZSTBU FIYLZ TATSD JPEFU PEQDS DQCND JCYTY TSIZT
ATSDA TCEBU ZDDSB TZSTB UFIYL CVNDM CYDUR FIMNT AVUMU KDAQT STRTJ VTYSI
QENUJ TSDQM NDYES CVTFS TQPDA MECRU LEJTN DASCA BCFTS IQVZD JSCMT QEQUJ
SEKDY DQTHV UZBAU EMZUQ TYCAB DMNDY TBTSB UABCF KTFAC MRTJV TYSUA BSDPD
ZUEEQ UJSEK DYDEB UMVUQ UYDBZ UKAMT LUMUS TBTSQ EJTQD BZCPE VUPUR QEJTB
URIBA VEABD BTNSI AUERU ZVZDV UKTSI MTQCD NEUPT ANCSI KCMUR IUPMU NTWIJ
ODZQI STSDB ZTRCJ PEZCJ SUFCB JTYLE PCMMU NTWCU BCMUF TQBUT QCDNE STQCC
SDVUB EYLIV ZDKTQ YTTQC DNEVZ DVUKT SIAUE RUZPE FTZDF TAVEA BDCST FTPUQ
MIADB CMSCD SABCN EKTBZ UKAMT LUMUS TSCAF EKNUM CNSDV UYDBC YBTSA TJPTJ
CLSDJ PDCYT MCSCU MCQJD MMPIA TEJDF CBTNR EPTVZ DVUKU FCBMP CSTDS BTZST
BUFTC VNDMC YDCSC MNCFT ASDYD SCVDA TVZDA BEVUF TLTAN UMAUE MZUQT YCABD
MNDYT BUADB ZUKAM IMESJ CJSCQ TSCCA VUNEA FITHV UZBUF CSIQA UEMZU QIQMN
DYTQU PTANT EBUYS DMUFD STMCQ PUDSB TZSTB EEBUY SDMBC MQCMP DAVUJ DYDAU

```
EMZUQ UEYCA BMNDY TCLTA NUMSD YUJVU ABCYE KTMJD AMCSD DPTSB DBIUV ZCFST
STLUE JDFCB TNTVU VZUFT PTSDB TYLBU CMYDA TBZUK AMIME SUPDS ABCNE KTCJC
QTBTV UAURT ABUVI VUMEP AIABT QISTV UEJDF CKDVZ UCEBT SBDJC YDEJD FCBTN
EYTZB DODMC BIKTA DBECY TKTAB TKTPS UPEAA DEMUN TQBZU KAMTL UMUST KTVCM
JMNCF TASDY TUPYL IBDBV ZDABE VUFTL TANUC BUUPT ANCBE BUYSD MUFDP ENTJD
BUEAM EBTYS UABDK TJTBZ UKAMI MESST SDFDZ EAQTJ DJCAC PSDZU JPDNI VCBZD
JTATS TEQDA CQUFU NSTAD ZDBCK TURFI MNTSC VZUWZ CQUFC SJYTN CKTPS UEYTN
UFTMY DNTST QEEBU MESCK TPSEM USMZT BSDUA UREKT PTSMU SMZTB SDVUY DBCYJ
BTYLB UPEFU PEKTK FTFTB ADSTV ZDVCP ECSBD FDZUF TVZUW ZCQIS TZUJV UJSCK
DCSTU LNCAD KTLUV ZDBUQ SUABK CMUPE MCJJT KABTB EBUEN ULEFI ZTADN DJCPT
KBTAN UFUAU EBTJK TUMXX
```

Řešení

K rozluštění nepoužijeme klasickou frekvenční analýzu, ale postup, který je založen na odhadu slova, které se v textu může vyskytovat (tzv. metoda předpokládaného slova).
V tomto případě nám stačí v soutěžní části textu vzít pouze konec šifrovaného textu:
BUQ SUABK CMUPE MCJJT KABTB EBUEN ULEFI ZTADN DJCPT KBTAN UFUAU EBTJK TUMXX

Budeme-li předpokládat, že se na konci textu vyskytuje slovo ZADEJTE. V českém jazyce je písmeno E nejčastěji se vyskytujícím písmenem (10,5 % textu). Nejčastěji se vyskytující znak v šifrovaném textu je T (159 výskytů , 11,36% textu) . Lze tedy předpokládat, že E je nahrazeno Z. Vyjdeme-li z tohoto předpokladu, pak je možné na poslední řádce nalézt JCPTKBT . Do tabulky doplníme již známé znaky.

B	U	Q	S	U	A	B	K	C	M	U	P	E	M	C	J	J	T	K	A	B	T	B	E	B	U	E	N	U	L
T						T	J	A			D			A	Z	Z	E	J		T	E	T		T					
E	F	I	Z	T	A	D	N	D	J	C	P	T	K	B	T	A	N	U	F	U	A	U	E	B	T	J	K	T	U
				E					Z	A	D	E	J	T	E										T	E	Z	J	E	
M	X	X																											

Tabulka 1, zvýraznění slova ZADEJTE

V prvním řádku se vyskytuje J?TE, které lze doplnit písmenem S na JSTE.

B	U	Q	S	U	A	B	K	C	M	U	P	E	M	C	J	J	T	K	A	B	T	B	E	B	U	E	N	U	L
T					S	T	J	A			D			A	Z	Z	E	J	S	T	E	T		T					
E	F	I	Z	T	A	D	N	D	J	C	P	T	K	B	T	A	N	U	F	U	A	U	E	B	T	J	K	T	U
				E	S				Z	A	D	E	J	T	E	S					S			T	E	Z	J	E	
M	X	X																											

Tabulka 2, zvýraznění slov ZADEJTE, JSTE

Ve druhém řádku lze odhalit slovo SOUTĚŽ

B	U	Q	S	U	A	B	K	C	M	U	P	E	M	C	J	J	T	K	A	B	T	B	E	B	U	E	N	U	L
T	O			O	S	T	J	A		O	D	U		A	Z	Z	E	J	S	T	E	T	U	T	O	U		O	
E	F	I	Z	T	A	D	N	D	J	C	P	T	K	B	T	A	N	U	F	U	A	U	E	B	T	J	K	T	U
U				E	S				Z	A	D	E	J	T	E	S		O		O	S	O	U	T	E	Z	J	E	O
M	X	X																											

Tabulka 3, zvýraznění slov ZADEJTE, JSTE, SOUTEZ

Předposlední slovo důležité k řešení je slovo SLOVO, které se nachází ve druhém řádku

B	U	Q	S	U	A	B	K	C	M	U	P	E	M	C	J	J	T	K	A	B	T	B	E	B	U	E	N	U	L
T	O			O	S	T	J	A		O	D	U		A	Z	Z	E	J	S	T	E	T	U	T	O	U	L	O	
E	F	I	Z	T	A	D	N	D	J	C	P	T	K	B	T	A	N	U	F	U	A	U	E	B	T	J	K	T	U
U	V			E	S		L		Z	A	D	E	J	T	E	S	L	O	V	O	S	O	U	T	E	Z	J	E	O
M	X	X																											

Tabulka 4, zvýraznění slov ZADEJTE, JSTE, SOUTEZ, SLOVO

Poslední, co do vyluštění soutěže zbývá je třeba odhalit slovo DUKAZ v prvním řádku otevřeného textu.

B	U	Q	S	U	A	B	K	C	M	U	P	E	M	C	J	J	T	K	A	B	T	B	E	B	U	E	N	U	L
T	O			O	S	T	J	A	K	O	D	U	K	A	Z	Z	E	J	S	T	E	T	U	T	O	U	L	O	
E	F	I	Z	T	A	D	N	D	J	C	P	T	K	B	T	A	N	U	F	U	A	U	E	B	T	J	K	T	U
U	V			E	S		L		Z	A	D	E	J	T	E	S	L	O	V	O	S	O	U	T	E	Z	J	E	O
M	X	X																											
K																													

Tabulka 5, zvýraznění slov ZADEJTE, JSTE, SOUTEZ, SLOVO, DUKAZ

Pro potřeby soutěže je již známo heslo : SOUTEZJEOK. Pokud se tímto způsobem dohledávání bude postupovat, pak zanedlouho lze bez problému získat celý otevřený text :

M KUCHAR NEBEZPECI INTERNETOVYCH RESENI Z DUVODU MINIMALIZACE CENY RESENI SE AUTORI INTERNETOVYCH APLIKACI OBVYKLE SPOKOJI S MÉNĚ BEZPECNYM ULOZENIM KLICU NA PEVNEM DISKU A BOHUZEL I S NASTAVENY MPRIZNAKEM UMOZNUJICIM EXPORT SOUKROME CASTI KLICE TENTO STAV JE VŠAK BEZPECNOSTNI DIROU UMOZNUJICI UTOK POMOCI TROJSKEHO KONE TEN MUZE MIT RADU PODOB MUZE TO BYT SPUSTITELNY SOUBOR PRIPOJENY K EMAILU ODESLANY JAKO BY OD KOLEGY Z FIRMY NENÍ TŘEBA ZDURAZNOVAT ZE CHUDAK KOLEGA O TAKOVEMTO EMAILU NEMÁ ANI POTUCHY PRIJEMCE EMAILU PRIPOJENY SOUBOR DUVERIVE SPUSTI A NEVEDOMKY SI TAK NAINSTALUJE TROJSKEHO KONE NA SVŮJ LOKALNI POCITAC TEN SE ZDE ZAHNIZDI A CEKA NA OKAMZIK KDY SE UZIVATEL BUDE PRIPOJOVAT K DANE INTERNETOVE APLIKACI A NA KLAVESNICI NAPISE PRISTUPOVE HESLO K SOUKROME CASTI KLICE TO SI TROJSKY KUN ZAZNAMENA A SPOLU S VYEXPORTOVANYM SOUKROMYM KLICEM ODESLE UTOCNIKOVI NEKAM DOINTERNETU UTOCNIK TAK MA K DISPOZICI SOUKROMOU ČÁST KLICE A HESLO K NI COZ POSTACUJE K ZISKANI IDENTITY OPRAVNENEHO UZIVATELE PO PROVEDENI TĚCHTO AKCI SETROJSKY KUN ODINSTALUJE A ZAMETE PO SOBE STOPY POKUD SYSTÉMY NEPOUZIVAJI PRO AUTENTIZACI UZIVATELU CERTIFIKATY JE SITUACE JEŠTĚ JEDNODUSSI UKOLEM TROJSKEHO KONE JE PAK Z KLAVESNICE ODCHYTIT PRISTUPOVE HESLO A TO ODESLAT UTOCNIKOVI DULEZITOU SKUTECNOSTI JE ZE TROJSKY KUN NENÍ VIRUS MEZI ZASADNI ROZDILY PATRI ZE SE NEUMI SAMOVOLNE SIRIT A JE OBVYKLE NAPROGRAMOVAN ZCELA JEDNOUCELOVE K CILENEMU UTOKU NA JEDNU KONKRETNI OSOBU JEDEN KONKRETNI POCITAC Z TĚCHTO DUVODU JEJ VE VETSINE PRIPADU ANTIVIROVE PROGRAMY NEROZPOZNAJI A NEOHLASI JEHO PRITOMNOST JAKO DUKAZ ZE JSTE TUTO ULOHU VYRESILI ZADEJTE SLOVOSOUTEZJEOK

Kontrolní (hledané) slovo: SOUTEZJEOK

Úloha č.9 - Periodické heslo I.

Způsob použití k zašifrování periodického hesla
K zašifrování zprávy je zapotřebí hesla, zprávy a tabulky Vigenére.

Heslo : DOBRYDEN

Text: HURA, SIFRUJEME SIFROU VIGENERE

Pak je potřeba připravit zprávu na šifrování tak, že nad každé písmeno otevřeného textu se napíše písmeno hesla. Pokud je heslo kratší než text, pak se začne zapisovat opět od začátku.

Šifrování se provede tak, že v horní řádce tabulky Vigenere vyhledá písmeno otevřeného textu, v levém sloupci písmeno hesla. Uvnitř tabulky se na průsečíku vybraného sloupce a řádku zobrazí šifrovaný znak.

	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
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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Tabulka 1 Tabulka Vigenere[1]

Heslo	D	O	B	R	Y	D	E	N	D	O	B	R	Y	D	E	N	D	O	B	R	Y	D	E	N	D	O	B
Text	H	U	R	A	S	I	F	R	U	J	E	M	E	S	I	F	R	O	U	V	I	G	E	N	E	R	E
Šifra	L	J	T	S	S	M	K	F	Y	Y	G	E	D	W	N	T	V	D	W	N	H	K	J	B	I	G	G

Tabulka 2 Princip šifrování šifry Vigenere

Dešifrování je proces opačný, tudíž v levém sloupci se vybere písmeno hesla, na řádce písmeno šifrovaného textu a nahoře výsledné písmeno otevřeného textu.

Strojové zašifrování

Každému písmenu mezinárodní abecedy přiřadíme číslo. A=1,B=2,…..,Y=25,Z=0. Způsob strojového počítání lze snadno odvodit z tabulky Vigenere. Bude – li zvolen znak otevřeného textu A=1, pak pro každý znak hesla platí, že 1+ znak hesla = šifrovaný znak.

Tak lze dojít až ke znaku X(24). Pro znak Y(25) platí, že 1+ 25 = 26. Znak s číslem 26 není k dispozici, je nahrazen znakem 0 (v abecedě po Y následuje znak Z). Z tohoto lze odvodit vztah, že pro každý znak šifrovaného textu ŠT platí:

$$ŠT=(OT+H) \bmod 26$$

Analogicky lze odvodit opačný proces , čili dešifrování:

$$OT=(ŠT-H) \bmod 26$$

Luštění Periodického hesla

Máme k dispozici text, který byl zašifrován periodickým heslem:

AAWTV RBMRG WESMD UGFUG MGOGZ WAIQA GBWDZ ZVGTS MIBNH NSEMQ IQOLH UBOOW CTAKR HZBXB VRFTE IZFTR NWCQD ZDRFT VVPUC FBSEE WOCCI BOMGG NVVKW TJXSR MHBQM IBTYF VXHVS HXAVP QEOTR HVVTN BWMIB JDYGG MCZHG WDIKR HNSMV VBRCL BZRTR QWEIC EYGWV WJEMW VHBBN HGWHB LPLHS DRRKR XKHCG RHREX BPKWT JXVVL CTRGQ TIWCZ GMDAO TCMMI EVWRT SYOYO BBAMO XHNKL FSWOK OCASW ONBCG RRGLK MUPOO EXVVT DYBTS FNHYL XZRSN ODBAB AYMKN VLTDR GFWIE OOEHC MLQMS GMLKD NMCQQ AGBWL BFPBD GOHKE NZQVP LTRQA VPKRH PSSMA SRIHH BFLLY KMICE WWTBS FVDBS IZZBR XWFAK EMBWM IBJHR MVPDU GFUXX VVQMS GIJHU CETHU IOJKH JVTRZ ADAZL BNWCM KANNS UMQPH QWGGG RHRCK QMDRI BTSFV HQAHS KEUMU ARJEP ADNDZ LFCLX LPNHB SCLVS HBADL FKGCT RAVPR YMLQC DRDML BZTVT CKQMD BBSFC URFWS EMRNR DGDCJ IVTSE MBRLJ VTSEE PIFXL FSDVF XVVBR HNSLR LHBGL BBTHF SCMRO GRWEC AERRV HBPKX GFBHJ IPWNX SDIMT HKQCI VJWES RNHNS UGEEM OCTAB OGZAO IDOFY FXULS YMEBA ZLDAA WWJAK ZSECT IXGSG VREXG KXVVC DCKMI COVHA FCURF TBTSF DXYSS HVJVH WMCKO XZGAC JPUON GMMYU TKBTZ ZDRWC BVSHB WVIDU GFUQF

Vlastní analýza textu se v případě luštění periodického hesla rozdělí na dva kroky. Prvním je odhalení délky hesla. Pokud se podaří odhalit délku hesla, pak zbytek textu je zašifrován pouze jednoduchou substitucí, v případě této varianty šifry Vigenere o níž se v úloze jedná, je text periody zašifrován pouze posunem písmen o pořadové číslo znaku hesla v mezinárodní abecedě.

Krok první – odhalení délky hesla

K odhalení délky hesla v tomto případě poslouží tzv. **Index koincidence.**

„Předpokládáme, že máme text, o kterém si myslíme, že byl zašifrován monoalfabetickou substitucí. Jestliže je naše domněnka správná, pak četnosti písmen šifrového textu budou stejné jako četnosti příslušných písmen národního jazyka.“

„Index koincidence (IC) představuje cestu k aproximaci rozptylu analyzovaných dat **[3].**“ Index koincidence je definován vzorcem :

$$IC = \sum_{i=1}^{k} \frac{n_i * (n_i - 1)}{N * (N - 1)}$$

n_i je četnost znaku i,

k je délka abecedy v daném textu, N je celková délka textu. Tato hodnota se bude pohybovat v rozmezí 1/26 (náhodný text) a IC pro danou abecedu. Pro český jazyk je tato hodnota 0,058258, pro anglický jazyk 0,067281, pro náhodný text 0,0384,.

„U složitějšího substitučního systému se setkáváme s klíči, které vytvářejí tzv. periodickou záměnu. Takový text při analýze periodičnosti rozepisujeme postupně dle délky periody 1,2,3,….L. „Pokud text rozepíšeme dle určité periody, pak celkové četnosti n_i se rozptýlí do jednotlivých sloupců rozpisu. Četnost i-tého písmene v j-tém sloupci rozpisu označíme n_{ij} .“ Těchto hodnot je celkem A*L, kde A je délka použité abecedy a L je délka periody rozpisu. V praxi se vyskytují periodické substituce převážně do délky L=50.“**[2]**

Perioda	1	2	3	…	L
A	$n_{1,1}$	$n_{1,2}$	$n_{1,3}$	…	$N_{1,L}$
B	$n_{2,1}$	$n_{2,2}$	$n_{2,3}$	…	$N_{2,L}$
C	$n_{3,1}$	$n_{3,2}$	$n_{3,3}$	…	$n_{3,L}$
….	…	…	…	…	…
Z	$n_{26,1}$	$n_{26,2}$	$n_{26,3}$	…	$n_{26,L}$

Tabulka 3 schéma četností znaků rozepsaných dle period[1]

Součet písmen ve sloupci označíme n_j pro j= 1,2,….L. Součet četností v řádce tabulky je četností písmene n_i v šifrovém textu:

$$\sum_{j=1}^{L} n_{ij} = n_i \quad \textbf{[1]}$$

Pokud bude text rozepsaný podle skutečné periody šifrovaného klíče, pak jsou písmena libovolného sloupce síťky pouze jednoduchou substitucí otevřeného textu. Potom hodnota K bude nabývat hodnoty blízké hodnotě IC pro daný jazyk.

Pro tabulku o periodě L je testová charakteristika K definována takto:

$$100.K = \frac{100\sum_{i=1}^{A}\sum_{j=1}^{L} n_{ij}(n_{ij}-1)}{\sum_{j=1}^{L} n_j(n_j-1)} \quad \textbf{[1]}$$

Koeficient K pro šifrovaný text uspořádaný dle period vypadá takto :

1 = 4,14	11 = 4,16	21 = 6,48
2 = 4,13	12 = 4,00	22 = 3,96
3 = 4,13	13 = 4,22	23 = 4,09
4 = 4,14	14 = 6,28	24 = 4,01
5 = 4,19	15 = 4,25	25 = 4,12
6 = 4,10	16 = 4,09	26 = 4,12
7 = 6,29	17 = 3,81	27 = 3,94
8 = 4,10	18 = 4,09	28 = 6,35
9 = 4,16	19 = 4,28	29 = 4,45
10 = 4,15	20 = 4,26	30 = 4,18

Tabulka 4 Koeficient K vypočítaný pro 30 period

Vzhledem k velké odchylce v Koeficientu K pro periody, které jsou násobkem sedmi lze usoudit, že heslo má délku sedm znaků. Nyní je již možné rozepsat šifrovaný text podle jednotlivých period. Cílem luštění je odhalení otevřeného textu a hesla.

PERIODA1

```
AMDGQ ZBQBK VFDVE BVRBV QVBCK VRCJB LRGPV TDIYM
FAGUV FRBLI MLQFK LKAFC FZKBD VJUVZ KQGMF KJZPV
FVCZM URJBE FVRBR APJDC REBDL ZJTRV CUFVK JMZVD
```

PERIODA2

```
ARUOA VNIOR RTZPE OKMTS ETJZR BTEEN PKRKL IAEOO
SSRPT NSATE LKAPE TRSLE VBEJU VHITL APRDV EELNS
KPDTD RNIRE SBLTO EKIII NEOOS LAIEC ORDJO PYZSU
```

PERIODA3

```
WGGGG GHQOH FRDUW MWHYH ONDHH RRYMH LRHWC WOVYX
WWROD HNYDO QDGBN RHRLW DRMHG QUORB NHHRH UPFHH
GRRVB FRVLP DRHHG RXPMV HMGFY DKXXD VFXVX UUDHG
```

PERIODA4

```
TWFZB TNOWZ TNRCO GTBFX TBYGN CQGWG HXRTT CTWOH
OOGOY YOMRO MNBDZ QPIYW BXBRF MCJZN NQRIQ MACBB
CYDTB WDTJI VHBFR RGWTJ NOZYM AZGGC HTYHZ OTRBF
```

PERIODA5

```
VEUWW SSLCB EWFFC GJQVA RWGWS LWWVW SKEJR ZCRBN
KNLEB LDKGE SMWGQ ASHKT SWWMU SEKAW SWCBA UDLSA
TMMCS SGSVF FNGSW VFNHW SCAFE ASSKK ABSWG NKWWU
```

PERIODA6

```
RSGAD MEHTX ICTBC NXMXV HMGDM BEVHH DHXXG GMTBK
OBKXT XBNFH GCLOV VSHMB IFMVX GTHDC UGKTH ANXCD
RLLKF EDETX XSLCE HBXKE UTOXB WEGXM FTSMA GBCVQ
```

PERIODA7

```
BMMIZ IMUAB ZQVSI VSIHP VIMIV ZIWBB RCBVQ MMSAL
CCMVS ZAVWC MQBHP PMBIS ZAIPX IHJAM MGQSS RDLLL
AQBQC MCMSL VLBMC BHSQS GAIUA WCVVI CSHCC MTBIF
```

Dalším krokem je zjištění, o jaký posun se v každé periodě jedná. Nejprve je potřeba spočítat četnosti jednotlivých znaků v každé periodě.

	1	2	3	4	5	6	7
A	4	7	0	2	8	3	8
B	11	3	3	11	5	9	11
C	6	1	1	7	6	7	11
D	7	4	10	3	2	6	1
E	3	15	0	0	7	7	0
F	10	0	5	5	6	4	1
G	4	0	11	8	7	9	2
H	0	1	20	5	2	10	5
I	2	8	0	3	0	2	13
J	7	3	0	3	2	0	1
K	8	6	1	0	8	5	0
L	5	7	3	0	5	4	6
M	6	1	5	5	4	9	15
N	0	6	4	7	5	3	0
O	0	10	6	10	0	3	0
P	3	7	3	1	0	0	4

Q	5	0	3	4	2	1	7
R	9	11	15	8	3	2	2
S	0	9	0	0	18	4	11
T	2	10	0	13	2	9	1
U	4	3	5	0	4	2	2
V	16	4	6	1	5	6	10
W	0	0	8	7	18	1	3
X	0	0	6	3	0	14	1
Y	1	1	5	7	0	0	0
Z	7	3	0	7	1	0	5

Tabulka 5 Četnosti znaků v jednotlivých periodách

Pro každou periodu je potřeba zjistit, o jakou vzdálenost (znak hesla) je text posunutý. Hodnota se může zjistit například kvantizační odchylkou[3] : Od součtu četností znaků AEIO se odečte součet četností znaků FGQW, tato hodnota (-8) se zapíše do první periody znak hesla A . Hodnota pro znak hesla B se určí odečtením součtu GHRX od součtu BFJP Takto se postupuje, dokud se nezjistí hodnoty všech 26 možností posunu znaků v abecedě pro každou periodu.

Posun	Znak hesla	1	2	3	4	5	6	7
0	A	-10	40	-21	-9	-18	0	8
1	B	18	1	-41	-4	1	-22	7
2	C	20	-12	-9	4	3	6	-9
3	D	3	-1	48	-10	7	11	-6
4	E	-12	14	-1	3	7	12	29
5	F	-21	-1	-4	16	-8	-8	-24
6	G	-1	10	6	-1	-14	-2	-31
7	H	11	8	7	-11	1	-12	8
8	I	9	-23	1	-5	12	0	38
9	J	-4	0	11	-2	3	12	-6
10	K	-7	12	-5	2	9	-1	-10
11	L	-8	12	-35	-7	-4	-9	-9
12	M	2	-18	-3	-7	-9	0	-5
13	N	20	-2	18	8	-6	1	9
14	O	-11	-14	9	11	21	-8	22
15	P	-23	7	0	14	-16	13	-12
16	Q	-13	14	-17	-10	-21	-15	-21
17	R	42	11	-12	-1	-10	-16	9
18	S	5	-3	2	-6	51	-2	10
19	T	-5	0	21	14	6	42	8
20	U	-11	-3	7	4	-9	2	6
21	V	8	-14	-5	-7	-11	-6	-10
22	W	-8	14	0	-14	8	-13	-37
23	X	11	-11	2	-11	1	6	6
24	Y	3	-29	1	14	4	7	25
25	Z	-18	-12	20	15	-8	2	-4

Tabulka 6 Rozdílu četností znaků

V místě, kde je nejvyšší součet znaků pro danou periodu se pravděpodobně vyskytuje znak hesla. Pokud tomu tak není, je potřeba vzít druhou nejvyšší hodnotu, pak třetí a tak dále. Pro tento text odpovídají hodnoty v periodách

Perioda	Posun	Součet	Znak Hesla
1	17	42	R
2	0	40	A
3	3	48	D
4	?	?	?
5	18	51	S
6	19	42	T
7	8	38	I

Tabulka 7 Pravděpodobné heslo

(Pro čtvrtou řadu odpovídá až hodnota posunu 14 Součet 11 Znak hesla O – chyba v šifrovaném textu). Tímto postupem lze odhalit heslo RADOSTI z šifrovaného textu. Poté s pomocí tabulky Vigenere dokončíme luštění šifrovaného textu .

Otevřený text :
JA TFDY TVRDIM ZE MUDRC NEPODLEHA ZADNE KRIVDF A TAK NEZALEZI NA TOM KOLIKA STREL JE TERCFM PROTOZE JIM ZADNA NEPRONIKNE TAK JAKO JSOU NEKTFRE KAMENY TAK TVRDE ZE SE JICH ZELFZO NETKNE TAK JAKO NELZE SEKAT REZAT NEBO OTIRAT OCEL ALE VSE CO SE JI DOTKNE SE OTUPI TAK JAKO JSOU PREDMETY KTFRE NELZF ZNICIT OHNEM ALF KTERE SI ZAKHOVAJI SVOU TVRDOST A SVUJ STAV I UPROSTRED PLAMENE TAK JAKO NEKTERA SKALISKA VYSUNUTA DO MORE LAMOU VLNY A NEUKAZUJI ZADNE STOPY POV ZTEKLYCH UTOCICH TREBAZE JSOU PO TOLIK STALETI BIKOVANA PRIBOJEM STEJNE TAK JE DUCH MUDRCE PEVNY A NASHROMAZDIL V SOBE TOLIK SILY ZE JE TAK ZABEZPECENY PRED KRIVDOU JAKO VECI O KTERYCH JSEM MLUVIL CO TEDY NENAJDE SE NIKDO KDO BY SE POKUSIL DOPUSTIT SF KRIVDY NAMUDRCI ALE ANO POKUSI SF ALE KRIVDA K NEMU NEDOSAHNE NEBOT VZDALENOST KTERA JE A ODDELUJE OD DOTYKU S NIZSIMI VEKMI JF PRILIS VELKA NEZ ABY NEJAKA SKODLIVA MOC K NEMU SVYMI SILAMI DOSAHLA LUCIUS ANNAEUS SENECA O STALOSTI MUDRCF JAKO DUKAZ ZE JSTE TUTO ULOHU SPRAVNE VYRFSILI ZADEJTE SENECA MUDRCXX

Kontrolní (hledané) slovo: SENECAMUDRC

D. Letem šifrovým světem
(připravil Pavel Vondruška)

I. Nová regulace vývozu silné kryptografie z USA!

Bureau of Industry and Security vydalo 10.prosince upravený seznam komerčních zařízení u nichž je regulovaný export (the Commerce Control List) z USA. Omezení se nyní týkají i silné kryptografie. Např. u symetrických šifer všech zařízení, která obsahují symetrické algoritmy s klíči většími jak 56 bitů a u asymetrické kryptografie s modulem větším jak 512 bitů !

Commerce Control List: http://cryptome.org/ccl-crypto.txt
Pravidla pro export : http://cryptome.org/bis121003.txt
Zdroj: http://www.access.gpo.gov/su_docs/aces/fr-cont.html

Výpis z CCL (část zabývající se omezením vývozu kryptografických prostředků):

Note: 5A002.a.1 includes equipment designed or modified to use``cryptography" employing analog principles when implemented with digital techniques.
a.1.a. A ``symmetric algorithm" employing a key length in excess **of 56-**bits; or
a.1.b. An ``asymmetric algorithm" where the security of the algorithm is based on any of the following:
a.1.b.1. Factorization of integers in excess of **512 bits** (e.g.,RSA);
a.1.b.2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie- Hellman over Z/pZ); or
a.1.b.3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2 in excess of 112 bits (e.g., Diffie-Hellman over an elliptic curve);
a.2. Designed or modified to perform cryptanalytic functions;
a.3. [RESERVED]
a.4. Specially designed or modified to reduce the compromising emanations of information-bearing signals beyond what is necessary for health, safety or electromagnetic interference standards;
a.5. Designed or modified to use cryptographic techniques to generate the spreading code for ``spread spectrum" systems, including the hopping code for ``frequency hopping" systems;
a.6. Designed or modified to use cryptographic techniques to generate channelizing or scrambling codes for ``time-modulated ultra-wideband" systems;
a.7. Designed or modified to provide certified or certifiable ``multilevel security" or user isolation at a level exceeding Class B2 of the Trusted Computer System Evaluation Criteria (TCSEC) or equivalent;
a.8. Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion.

II. Čtyřicáté Mersennovo prvočíslo bylo nalezeno!

Počítač Michael Shafera nalezl 17.11. 2003 čtyřicáté Mersennovo prvočíslo. Je jím $2^{20996011}$-1. Je to zatím největší známé prvočíslo. Pro zápis v dekadických číslech bychom potřebovali 6,320,430 cifer. Zdá se vám to hodně? Odborníci byli spíše překvapeni, že počet dekadických cifer není větší. Předběžné odhady byly kolem devíti miliónů cifer. Kdyby k zápisu prvočísla bylo potřeba více než deset miliónů cifer, získal by objevitel odměnu, kterou GIMPS vypsal – 10 000 USD. Projekt hledání Mersennových prvočísel na GIMPS stále běží, a tak máte možnost se nejen zapojit mezi tisíce nadšenců, kteří v hledání velkých prvočísel pomáhají, ale budete-li mít patřičné štěstí – i získat vypsanou odměnu.

Rekord největšího známého prvočísla dosud drželo 39. Mersennovo prvočíslo, které nalezl před dvěma lety Michael Cameron (opět v projektu GIMPS). Toto prvočíslo je $2^{13466917}$-1 a lze jej napsat pomocí 4,053,946 cifer.
http://www.mersenne.org/prime.htm

III. Nový rekord ve faktorizaci (RSA-576)

Výzva firmy RSA k faktorizaci čísla RSA-576 byla uzavřena.Výzva spočívala ve faktorizaci čísla o délce 576 bitů (v dekadickém zápisu 174 cifer) – tj. v nalezení rozkladu tohoto čísla na součin dvou prvočísel. Řešitelé věděli, že číslo je konstruováno jako součin dvou, přibližně stejně velkých prvočísel. Firma RSA tak svými výzvami demonstruje, že algoritmus RSA (založený na nemožnosti faktorizovat velká čísla) je při délce modulu 1024 bitů stále dlouhodobě bezpečný.
Výzva : RSA-576 (Prize: $10,000)
188198812920607963838697239461650439807163563379417382700763356422988859715234665485319060606504743045317388011303396716199692321205734031879550656996221305168759307650257059 (Decimal Digits: 174)
Dne 3.12.2003 oznámil tým ve složení Franke, Kleinjung, Montgomery, te Riele, Bahr, Leclair, Leyland, Wackerbarth, že uvedené číslo rozložil pomocí metody GNFS (General Number Field Sieve) na dvě prvočísla. Týmu tak náleží vypsaná odměna USD 10 000.
Každé z nalezených prvočísel, které tvoří rozklad, má velikost 87 dekadických cifer. Těmito prvočísly jsou :
398075086424064937397125500550386491199064362342526708406385189575946388957261768583317
a dále
472772146107435302536223071973048224632914695302097116459852171130520711256363590397527
http://www.loria.fr/~zimmerma/records/rsa576

IV. Rozšířen standard pro hashovací funkce FIPS 180-2

NIST (National Institute of Standards and Technology) oznámil 1.12.2003 změnu FIPS 180-2 (Federal Information Processing Standard, Secure Hash Standard).
Tento standard specifikuje čtyři bezpečné hashovací funkce - SHA-1, SHA-256, SHA-384 a SHA-512. Ohlášená změna se týká zavedení nové - páté bezpečné hashovací funkce označené jako SHA-224. Definice této funkce vychází z definice SHA-256. Výsledek je zkrácen na 224 bitů. Rozdíl mezi funkcemi je v počátečních inicializačních hodnotách a samozřejmě výstupní délce. Tato funkce byla zavedena především v souvislosti s vytvářením náhodných symetrických klíčů délky 112 bitů pro 3DES (obecně platí, že hashovací funkce s výstupem délky N lze využít pro vytváření N/2 tzv. bezpečných bitů). Obdobně algoritmus AES s délkami klíčů 128 bitů, 192 bitů a 256 bitů "vynutil" zavedení hashovacích funkcí SHA-256, SHA-384, resp. SHA-256.
http://csrc.nist.gov/publications/fips/fips180-2/FIPS180-2_changenotice.pdf

Na potřebu zavedení hashovací fce s výstupem délky 224 bitů reagovala i skupina PKIX Working Group, která začátkem prosince publikovala draft "A 224-bit One-way Hash Function: SHA-224" (draft-ietf-pkix-sha244-01.txt).
http://www.ietf.org/ietf/1id-abstracts.txt

V. GSMK CryptoPhone 100

Na adrese http://www.cryptophone.de/ lze získat plný zdrojový kód GSMK CryptoPhone 100 a dále aplikaci GSMK CryptoPhone for Windows pro uživatele, kteří používají modem (připojení POTS nebo ISDN).

VI. O čem jsme psali v prosinci 1999 - 2002

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)

E. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (Internet, noviny) nebo se jedná o původní články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

Články neprocházejí jazykovou kontrolou!

Adresa URL, na níž můžete najít tento sešit (nejdříve 15 dní po jeho rozeslání) a předchozí sešity GCUCMP (zkonvertovány do PDF formátu), informace o přednáškách z kryptologie na MFF UK, některé články a další související témata :

http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci **o zasílání** tohoto sešitu se mohou zaregistrovat pomocí e-mailu na adrese na e-mail pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci formulář na http://crypto-world.info . Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání 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 byl sešit zasílán.

3. Spojení

běžná komunikace, zasílání příspěvků k otištění , informace
pavel.vondruska@crypto-world.info
pavel.vondruska@post.cz
pavel.vondruska@ct.cz