Crypto-World

Informační sešit GCUCMP

Ročník 2, číslo V/2000 20.prosince 2000

Vánoce/2000

Připravil : Mgr.Pavel Vondruška,
člen GCUCMP, BITIS, IACR, ISACA.

Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adresách
http://www.mujweb.cz/veda/gcucmp/
+ http://cryptoworld.certifikuj.cz
(>230 e-mail výtisků)

OBSAH : **Str.**

A. Vánoční rozjímání nad jistými historickými analogiemi Zákona o elektronickém podpisu a zákony přijatými před sto a před tisícem let.

(Mgr. Pavel Vondruška, ÚOOÚ)

Vážení čtenáři,

Dovolte mi, abych vám popřál klidné prožití vánočních svátků, bohatého Ježíška, v novém roce 2001 hodně zdraví, štěstí a pracovních úspěchů!

Pro dobu vánočního rozjímání jsem vám připravil dva malé příběhy z dob dávných a minulých, ale současně velice aktuálních. Myslím, že doba vánoc je to správné období se zamyslet nad našim pachtěním se a nad tím jaké stopy po sobě na této zemi můžeme zanechat.

Nashledanou v roce 2001 !
Pavel Vondruška

Proces vyhlášení a přijetí zákona (nejedná se o vyhlášení a přijetí Zákona o elektronickém podpisu)

Roku 1073 (našeho letopočtu) seldžucký sultán Džamál ad-Dín Malikšáh se na své návštěvě observatoře v Isfáhánu dozvěděl, že stávající kalendář je nevyhovující, neboť dochází již k nepřesnosti několika dnů mezi rokem astronomickým a "skutečným". V důsledku toho, že jaro přichází o tyto dny později. Seldžucký sultán ihned vyhlásil reformu kalendáře, která bude platná od roku 1074. Lidu bylo ohlášeno, že v důsledku nového, přesného kalendáře, který jejich panovník nařídil zavést, se zkrátí zima a jaro začne dříve. Nadále, že bude dosaženo souladu a věčné harmonie mezi stavem božským - rokem astronomickým - a stavem lidským - tím, co se děje v souladu s božím principem na zemi. Ihned začali veliké oslavy v Samarkandu, Buchaře, Mervě, Ishafánu a Rajji. Oslavy trvaly několik dní a sultán nechal rozdávat obilí a pro obveselení lidu nechal pověsit všechny zločince, kteří byly ve věznicích. Omar Chajjám (Abu ´l-Fath ´Umar Ibn Ibrahím al-Chajjám), který byl vedoucí observatoře v Ishafánu, byl za své zásluhy povýšen do hodnosti *nedína* (spolustolovníka), jehož hlavní povinností bylo popíjet s panovníkem víno. Poznamenejme, že pití vína islám zakazuje, ovšem jak je vidět jsou možné jisté výjimky. Problém nastal až na jaře roku 1074, kdy tehdejší dlouhá zima nechtěla polevit. Astronomové z Ishafánu byly pozváni na slyšení k seldžuckému panovníkovi, kde se odvážili sultánovi sdělit, že nestačí vyhlásit soulad astronomického a skutečného času, ale je potřebné připravit příslušné převodové tabulky k opravě kalendáře. Seldžucký sultán poté jmenoval osmičlennou komisy a pověřil ji vypracováním těchto tabulek. Dal jim na to čas jednoho měsíce. Komise vytvořila tabulky známé jako Zídž-i Melikšáhí (na počest sultána). Hodnocení tohoto kalendáře jsou rozdílná, obecně se však vyzdvihuje jejich veliká přesnost - k chybě jednoho dne mělo dojít až za 3770 let.

Dodržování přesné dikce nařízení
(nejedná se o problém s dodržováním dikce paragrafu 11 Zákona o elektronickém podpisu v oblasti veřejné moci)

Od 1.ledna roku 1876 byly povinně zavedeny metrické míry a váhy v Rakousku - Uhersku. Bylo tak učiněno zákonem z 23.července 1871 (s menšími úpravami platil až do roku 1962 !!!). Dikce zákona je neúprosná - říká, že dnem platnosti zákona není povoleno ve škole, vědě, obchodě, úřadech a jinde používat jiné míry a váhy než metrické, které jsou v příloze s převody příslušnými uvedeny a to ani písmem ani slovem.

Nezbylo než si na nové míry zvykat. Jan Neruda ve svých fejetonech poukázal na nesmyslnost doslovného chápání příslušného nařízení. Dovoluji si ocitovat z jeho fejetonů otištěných 17.10.1875 a 31.12.1875 .

Předávám slovo Janu Nerudovi

Ach, to bude obrat od Nového roku! … Např. je potřeba vydat nový překlad Krále Leara od Shakespeara. Král Lear říká v 4.aktu, 6.scéně :

"Ba, každým coulem král - "

a bude musit od Nového roku neuprositelně říkat : Ba, každými 2 centimetry a 6.34008 milimetru král"--

…

Židák Shylock se posud v aktu 4.scéně 1. vždycky ušklíbal :

"Aj, ptáte se, proč raději libru mršiny chci, nežli tisíce dukátů ?"

a bude muset od Nového roku ušklíbat :

"Aj, ptáte se, proč raději 0,56006 kilogramu mršiny chci, nežli tisíce dukátů ?"

……..

…Varující matka nesmí více pozdvihnout na synáčka prst a říci hlasem dojímajícím : "Počkej jen, až budu šest stop pod zemí, špendlíčkem bys atd." nýbrž : "Počkej jen, až budu 1.896484 metru pod zemí .."

… Dnes je Zbraslav ještě zrovna míli vzdálena od Prahy, po Novém ruce už nebude, pak musí dle zákona být 0.7585936 myriametru…

Nebohé naše národní písně ! - teď si na ně vzpomínám!
Šel jsem včera do hospody,
v patách za mnou běžela,
jen jsem si dal holbu piva
už se do mne pustila.-

nebo:
Vždyť my mlčíme,
když kávu pijou,
z hrnců mázových
do sebe lijou.-

Bojím se, že 0.707362 litru a 1.414724 litru nepůjde pranijak do noty.

B. Soutěž - konečný stav

Naše soutěž proběhla ve čtyřech kolech. V sešitech 9/2000 až 12/2000 jsme postupně uveřejnili po jedné soutěžní úloze a současně uvedli doprovodný text k příslušné úloze. Řešitelé úloh I. až IV., kteří zaslali správné řešení do vyhlášeného data, byli slosováni a dva takto vybraní získali cenu kola (certifikát k datům pro vytváření elektronického podpisu u poskytovatele certifikačních služeb I.CA resp. AEC).

Úplným závěrem soutěže pak bylo losování, které proběhlo 21.12.2000. Z řešitelů, kteří vyřešili všechny čtyři vyhlášené úlohy, byl vylosován absolutní vítěz, který získal hlavní cenu - registraci domény a provoz virtuálního serveru modelu LITE na dobu jednoho roku.

Konečný stav

Pseudonym	I.kolo datum /bodů	II.kolo datum /bodů	III.kolo datum/bodů	IV.kolo datum/bodů	CELKEM
Josef M.	12.9 /10 ☒		23.11/10		20
Mirek Š.	12.9 /10	17.10/10	17.11/10	12.12/10	**40**
Petr T.	12.9 /10	18.10/10			20
Bohumír Š.	12.9 /10	18.10/10	22.11/10		30
Martin K.	12.9 /10				10
František K.	12.9 /10				10
Tomáš V.	13.9 /10 ⛆	31.10/10	26.11/10		30
Jan J.	13.9 /10	17.10/10	19.11/10	12.12/10 ⛆	**40**
Josef D.	18.9 /10				10
Honza K.	18.9 /10				10
Vašek V.	2.10/10		22.11/10 ⛆		20
Michal B.	4.10/10	18.10/10 ⛆	20.11/10	14.12/10 **!**	**40**
Láďa R.	4.10/10	24.10/10 ☒	24.11/10		30
Martin V.	18.10/10				10
Karel Š.		24.10/10	29.11/10	19.12/10 ☒	30
Ivan L.		19.10/10	17.11/10		20
František P.	29.11/10	23.11/10	18.11/10 ☒	11.12/10	**40**

Legenda : cena kola - certifikát u AEC ⛆
cena kola - certifikát u PVT ☒

Vítězové IV.kola :
Karel Š.
Jan J.

Celkový vítěz :
Michal B.
Blahopřeji !

C. ÚLOHA č.1 - Steganografie

a) Zadání úlohy (Crypto-World 9/2000)

Úkolem je sestavit ukrytý text, o němž víte, že je rozdělen do 5-ti částí, každá část obsahuje 5 znaků, každá část je zamaskována nebo přímo ukryta v nějaké části www stránky GCUCMP (http://www.mujweb.cz/veda/gcucmp ; pozor - nikoliv na URL http://cryptoworld.certifikuj.cz) . Získané části je potřeba poskládat ve správném pořadí a tuto zprávu zaslat co nejdříve na adresu vyhlašovatele soutěže. Úloha je jednodušší proti originální úloze v tom, že mé stránky jsou nesrovnatelně menší a přehlednější než www stránka GCHQ. Je zde však použita stejná "finta", která pravděpodobně zapříčinila to, že během dvou týdnů originální úlohu GCHQ vyřešilo jen 14 uchazečů.

b) Počet správných řešitelů

15

c) Hledaný text:

TRPEL IVOST PRINA SIRUZ E!XXX
(Trpělivost přináší růže! XXX)

d) několik poznámek k řešení úlohy

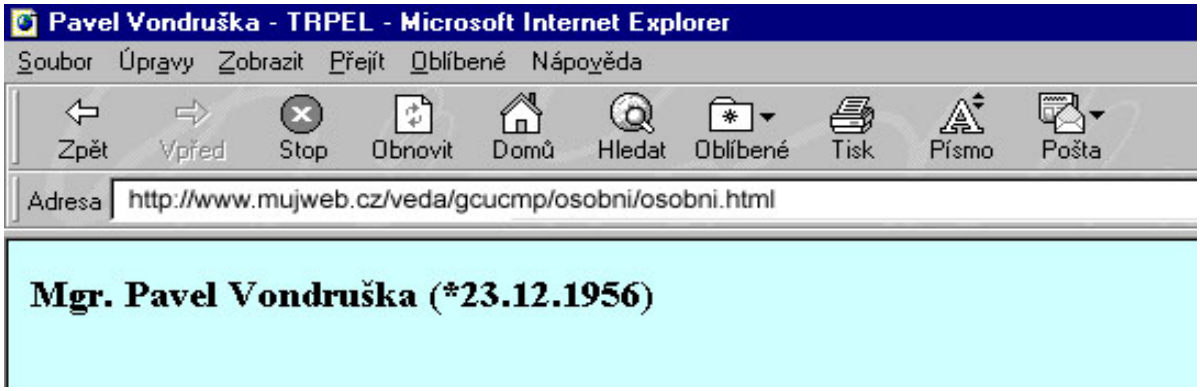
Text uložen bez interpunkce a mezer po pěticích takto :

TRPEL IVOST PRINA SIRUZ E!XXX

Uložení jednotlivých pětic jsme zaevidovali tak, jak byli uloženy v době vyhlášení soutěže. Postupně byli příslušné stránky rozšiřovány a současné pohledy na příslušná místa se mohou nepatrně lišit.

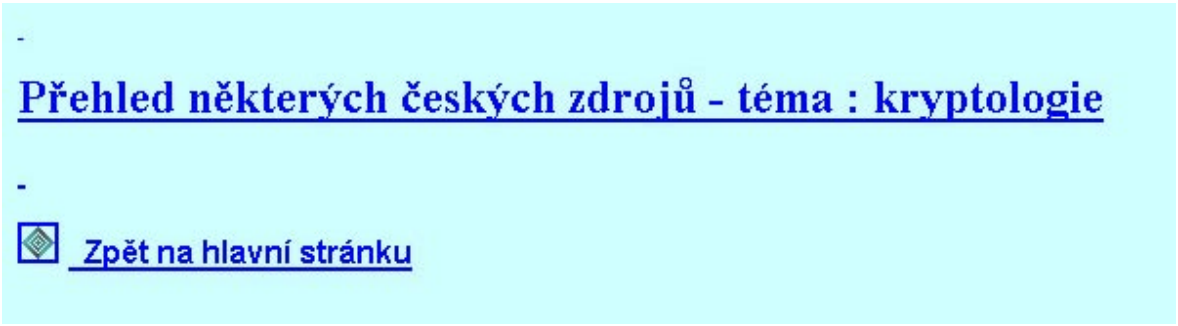
1) TRPEL

První pětice hledaného textu je uložena v sekci: "Pavel Vondruška "
http://www.mujweb.cz/veda/gcucmp/osobní/osobní.html
Slovo TRPEL schováno v titulu stránky (horní lišta).



2) IVOST

Druhá pětice hledaného textu je uložena v sekci: "Přehled vybraných českých zdrojů z kryptologie - linky"
http://www.mujweb.cz/veda/gcucmp/zdroje/zdroje.html
Slovo IVOST schováno ve zdrojovém textu této stránky.
Na jeho existenci měly upozornit "drobné chyby" , které se zobrazovaly v prohlížeči v místě, kde v příslušné části zdrojového textu je slovo ukryto. Ve zdrojovém kódu pak slovo (<-- soutez!!!)

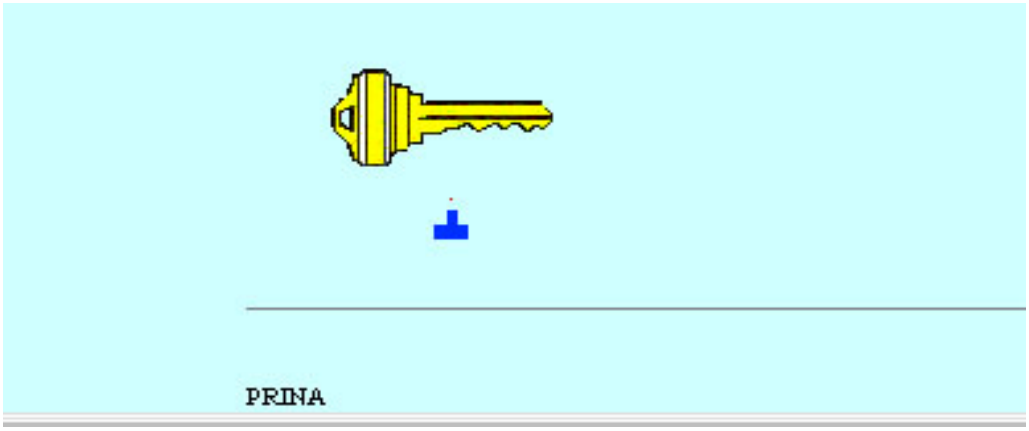


!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<!-- saved from url=(0051)http://www.mujweb.cz/veda/gcucmp/zdroje/zdroje.html -->
<HTML><HEAD><TITLE>Přehled některých českých zdrojů - téma : kryptologie</TITLE>
<META content="text/html; charset=windows-1250" http-equiv=Content-Type>
<BODY bgColor=#ccffff link=#0000ff vLink=#800080><B></B></FONT><A
href="http://www.mujweb.cz/veda/gcucmp/**IVOST**%20(<--soutez!!!)"><B><FONT
face="Courier New"></FONT><FONT size=2>
<P> </P></FONT><B><FONT face="Times New Roman" size=5>
<P align=justify>Přehled některých českých zdrojů - téma :
kryptologie</P></FONT>

Tato pětice byla nejdokonaleji uschována. Způsob tohoto ukrytí byl použit i v úloze GCHQ.

3) PRINA

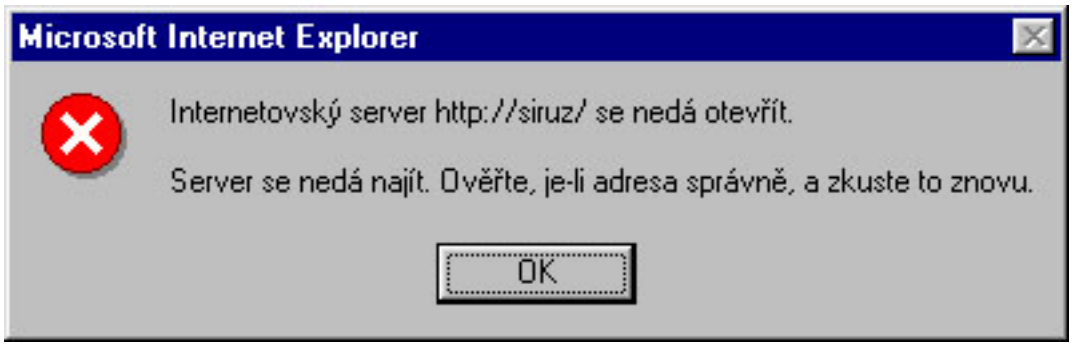
Třetí pětice je uložena přímo na domovské stránce http://www.mujweb.cz/veda/index.html
Slovo PRINA uloženo malým písmem na poslední řádce stránky pod pohyblivým obrázkem klíče.



4) SIRUZ

Čtvrtá pětice je uložena v sekci: "Přihláška k odběru sešitu Crypto-World, připomínky, dotazy, soutěž"
http://www.mujweb.cz/veda/gcucmp/dotaz/dotaz.html

Slovo SIRUZ je schováno v části "Linky, na které chci upozornit" .
Objevilo se při pokusu vyvolat stránku s názvem SOUTĚŽ (toto slovo jej mělo pomoci najít).



5) E!XXX

Poslední pětice je uložena v části: "Crypto-World 2000/2001, II.ročník"
http://www.mujweb.cz/veda/gcucmp/casop3/index.html

Slovo E!XXX je přidáno ke Copyrightu této stránky.

Všem 15-ti úspěšným řešitelům této úlohy blahopřeji !

D. ÚLOHA č.2 - Jednoduchá záměna

a) Zadání úlohy (Crypto-World 10/2000+ www stránka)

SIFROVY TEXT - SOUTĚŽNÍ ÚLOHA číslo 2:

JEDNODUCHA ZAMENA, CESTINA, BEZ MEZER, MEZINARODNI ABECEDA 26 ZNAKU (A-Z)
SIFROVY TEXT

```
UFTAL OTCSF CILDO TGLUL JHSFN PZIHF NBGZU FTALP ZRZOB NCHSF NQBZA ZFZGX
ZWOZG OLPZX AHBHU FTALP ZXIHJ OTWZJ HFAZD NDTOS BZLFN WCHPR ZPHCI TUXHI
ZCITD ZSAWT BCHSF NDNFT ALPZG ZGZPZ WZIZD NQAHS WZOTP TCOZJ RZHWT UBTPZ
HJOZW TUBHB LHJUB ALOTP ZWLUB TOLXL JZOZI LADLP TCPNG SGDNU ZOLOL ULQIT
DHUBX IHJOT WZDHJ HSRZG OLPQH SGZXI HJOTW ZRZXA ZUBLA ILOZD CHJOL QZUFZ
ASXAT AHGQI LJONW CXAHW ZUZWC PHCHS DGOTQ LBTOZ FZGXZ WOZIL BQNRL QHOLX
ARZJO ZSATO BLQUZ PHCHS UBLBT BGDRZ JIZCH SFNJA SCHBO ZRZJH DLBNP TDNRP
SBZXI HJOTW ZSQIL JLPZJ HHBZD AZONW CJNWC LRTWT WCHFL ISOZF HBDSG LDAZO
NWCOZ XAHXS UBONW CHFLI ZWCUZ XIHJO TWZBG DGLXL ATGDI LUBZO ZDCHJ OZRZS
IHGZO TDXHI NZBNI ZOHDN WCULW WTWCO ZRDCH JOZRU TPTHF LINGS UBLDL RTBAL
JTWOZ XIZBZ OZQHU TWQNO ZRXHG JZRTJ ASCNJ ZOXHU FZASP LRTFN BCHSF NGXAL
WHDLO NEEEE
```

b) Počet správných řešitelů

10

c) Řešení

PŘEVODOVÉ TABULKY

```
------------------------------

Pro zašifrování
ABCDE FGHIJ KLMNO PQRST UVWXY Z
LFWJZ KVCTR QIPOH XYAUB SDMEN G

Pro odšifrování
ABCDE FGHIJ KLMNO PQRST UVWXY Z
RTHVX BZOLD FAWYN MKJUI SGCPQ E

******************************

OTEVŘENÝ TEXT ROZPIS DO SKUPIN PO 5
SBIRA NIHUB HLAVN IZASA DOUBY MELOB YTZES BIRAM EJENT YHOUB YKTER EBEZP
ECNEZ NAMEP ROTOS BIRAM EPLOD NICED OBREV YVINU TEABY CHOMJ EMOHL ISPOL
EHLIV EURCI THOUB YVYBI RAMEZ EZEME CELEV YKROU CENIM IHNED JEOCI STIME
ODNEC ISTOT AODST RANIM ECAST INAPA DENEL ARVAM IHMYZ UZVYS ENANA SAKLI
VOSTP LODNI CEVOD OUJEZ NAMKO UZEPL ODNIC EJEPR ESTAR LANEV HODNA KESBE
RUPRI ROZKL ADNYC HPROC ESECH MOHOU VZNIK ATINE BEZPE CNELA TKYJA KONAP
RJEDN EURIN TAKSE MOHOU STATI TZVJE DLEHO UBYDR UHOTN EJEDO VATYM IVYJM
UTEPL ODNIC EUKLA DAMED OOTEV RENYC HDYCH AJICI CHOBA LUNEB OTVUZ AVREN
YCHNE PROPU STNYC HOBAL ECHSE PLODN ICETZ VZAPA RIZVL ASTEN EVHOD NEJEU
LOZEN IVPOL YETYL ENOVY CHSAC CICHN EJVHO DNEJS IMIOB ALYZU STAVA JITRA
DICNE PLETE NEKOS ICKYN EJPOZ DEJID RUHYD ENPOS BERUM AJIBY THOUB YZPRA
COVAN YXXXX

Délka textu : 670
```

OTEVŘENÝ TEXT :

sbirani hub hlavni zasadou by melo byt ze sbirame jen ty houby které bezpecne zname proto sbirame plodnice dobre vyvinute abychom je mohli spolehlive urcit houby vybirame ze zeme cele vykroucenim ihned je ocistime od necistot a odstranime casti napadene larvami hmyzu zvysena nasaklivost plodnice vodou je znamkou ze plodnice je prestarla nevhodna ke sberu při rozkladnych procesech mohou vznikat i nebezpecne latky jako napr jed neurin tak se mohou stat i tzv jedle houby druhotne jedovatymi vyjmute plodnice ukladame do otevrenych dychajicich obalu nebot v uzavrenych nepropustnych obalech se plodnice tzv zapari zvlaste nevhodne je ulozeni v polyetylenovych saccich nejvhodnejsimi obaly zustavaji tradicne pletene kosicky nejpozdeji druhy den po sberu maji byt houby zpracovany xxxx

d) několik poznámek k řešení úlohy

Pro nalezení samohlásek lze použit velice rychlý a kvalitní Šuchotinův algoritmus: Sukhotin's algorithm (PROCEDURE FindVowels)

VÝSTUP Z POMOCNEHO PROGAMU VFQ (lze jej stáhnout v sekci SOUTĚŽ) - automatické určení samohlásek a frekvencí - vowels and frequency (doplněn první sloupec - otevřený znak)

670 letters. 7 vowels, 15 consonants

		Absolute frequency								Relative Frequency (per 1000)						
	V#	Total	Init	Med	Fin	Isol	L/I	L/F		Total	Init	Med	Fin	Isol	L/I	L/F
E	1	Z	82	22	49	11	0	3	1	Z	122	164	122	82	0	231	77
O	2	H	52	7	41	4	0	1	0	H	78	52	102	30	0	77	0
A	3	L	48	9	26	13	0	0	1	L	72	67	65	97	0	0	77
N		O	46	6	29	11	0	0	0	O	69	45	72	82	0	0	0
I	4	T	42	11	23	8	0	2	1	T	63	82	57	60	0	154	77
T		B	32	6	22	4	0	1	0	B	48	45	55	30	0	77	0
C		W	31	9	14	8	0	1	2	W	46	67	35	60	0	77	154
Y	5	N	29	10	15	4	0	1	0	N	43	75	37	30	0	77	0
H	7	C	28	5	21	2	0	1	0	C	42	37	52	15	0	77	0
R		A	28	9	15	4	0	0	1	A	42	67	37	30	0	0	77
D		J	27	7	12	8	0	0	1	J	40	52	30	60	0	0	77
U	6	S	26	5	14	7	0	0	1	S	39	37	35	52	0	0	77
V		D	26	4	17	5	0	1	0	D	39	30	42	37	0	77	0
T		I	26	4	12	10	0	0	1	I	39	30	30	75	0	0	77
S		U	25	6	13	6	0	1	0	U	37	45	32	45	0	77	0
Z		G	22	0	15	7	0	0	0	G	33	0	37	52	0	0	0
B		F	22	4	11	7	0	0	0	F	33	30	27	52	0	0	0
P		X	22	3	15	4	0	1	0	X	33	22	37	30	0	77	0
M		P	21	3	10	8	0	0	2	P	31	22	25	60	0	0	154
J		R	18	2	15	1	0	0	1	R	27	15	37	7	0	0	77
K		Q	13	2	10	1	0	0	0	Q	19	15	25	7	0	0	0
X		E	4	0	3	1	0	0	1	E	6	0	7	7	0	0	77

VFQ.pas

V našem případě program dobře najde prvních 6 samohlásek a doplní ještě jednoho kandidáta (H), ale přidělí mu nejmenší pravděpodobnost - zařadí jej na sedmé místo.

E. ÚLOHA č.3 - Jednoduchá transpozice

a) Zadání úlohy (Crypto-World 11/2000)

Úlohou třetího kola je vyluštění přiloženého šifrového textu. Jedná se o jednoduchou transpozici - použita byla úplná tabulka. Rozměr tabulky musíte určit. Text je v češtině, v mezinárodní abecedě = 26 znaků A-Z (bez háčků a čárek) a bez mezer, je rozdělen do skupin po 5-ti znacích. Prozradím, že se jedná o text, který se vyskytl na stránkách našeho e-zinu.

SIFROVY TEXT

IRJYE VDIPI AVIVZ NTUKM EORZN EOTYE KKLPI TTNNC EIPAE COSMN EOPRL KEPEP LAPTE NNEDO SOTNK ENOPT LBOAO TROVR OEEIN REEEK UTSHX EOORM YIJAJ PZOED DEDOD UCSTS ONZOA IKSCU JPPES NISBV FEIIK AEUVU EJOOO DNMKS EORKB YMOAU ELPNO DKOOO JUNST ZIUOU EEJVG EEDZA ACEDM KKEEI RNETV

b) Počet správných řešitelů

11

c) Hledaný text:

Otevřený text (po příslušné transformaci sloupků)

```
DLEDEFINICEZAKO
NAOELEKTRONICKE
MPODPISUJSOUELE
KTRONICKYMPODPI
SEMDOKUMENTUMIN
ENYUDAJEVELEKTR
ONICKEPODOBEKTE
REJSOUPRIPOJENE
KDATOVEZPRAVENE
BOJSOUSNILOGICK
YSPOJENEAKTEREU
MOZNUJIOVERENIT
OTOZNOSTIPODEPS
ANEOSOBYVEVZTAH
UKDATOVEZPRAVEX
```

III. hledaný otevřený text

DLE DEFINICE ZAKONA O ELEKTRONICKEM PODPISU JSOU ELEKTRONICKYM PODPISEM DOKUMENTU MINENY UDAJE V ELEKTRONICKE PODOBE KTERE JSOU PRIPOJENE K DATOVE ZPRAVE NEBO JSOU S NI LOGICKY SPOJENE A KTERE UMOZNUJI OVERENI TOTOZNOSTI PODEPSANE OSOBY VE VZTAHU K DATOVE ZPRAVE X

d) několik poznámek k řešení úlohy

Určení správného rozměru tabulky
očekávaný výskyt ve správně určené tabulce :
40% samohlásek * 60% souhlásek

Rozpis : tabulka 9*25
očekávaný poměr 3,6 / 5,4

```
IEEEUUFYE      8/1 *
ROONTCEME      4/5
JTPOSSIOJ      3/6
YYRPHTIAV      4/5
EELTXSKUG      3/6
VKKLEOAEE      5/4 *
DKEBONELE      4/5
ILPOOZUPD      3/6
PPEAROVNZ      3/6
IIPOMAUOA      7/2 *
ATLTYIEDA      5/4 *
VTARIKJKC      2/7 *
INPOJSOOE      4/5
VNTVACOOD      3/6
ZCERJUOOM      4/5
NENOPJDJK      2/7 *
TINEZPNUK      3/6
UPEEOPMNE      5/4 *
KADIEEKSE      5/4 *
MEONDSSTI      3/6
ECSRDNEZR      2/7 *
OOOEEIOIN      8/1 *
RSTEDSRUE      3/6
ZMNEOBKOT      3/6
NNKKDVBUV      1/8 *
```
trestných bodů : 11

Rozpis : tabulka 25*9
očekávaný poměr 10 / 15

```
IIKTTCLTTBOKROCISIOOEOODK     11/14
RAMYNOKENOEUMESKNKORLJUZE     11/14
JVEENSENKAETYDTSIAOKPUEAE     13/12 *
YIOKCMPNEOISIDSCSEDBNNEAI     11/14
EVRKENEENTNHJEOUBUNYOSJCR     10/15
VZZLIEPDORRXADNJVVMMDTVEN      5/20 *
DNNPPOLOPOEEJOZPFUKOKZGDE      8/17 *
ITEIAPASTVEOPDOPEESAOIEMT     13/12 *
PUOTERPOLREOZUAEIJEUOUEKV     15/10 *
```
trestných bodů : 5

Rozpis : tabulka 15*15 (správný rozměr)
očekávaný poměr 6 / 9

```
INKCLEOEDIFDEZA          7/8
RTKOANEOEKENLIC          7/8
JULSPOEODSIMPUE          7/8
YKPMTPIROCIKNOD          5/10
EMINETNMDUKSOUM          6/9
VETENLRYUJAEDEK          7/8
DOTONBEICPEOKEK          7/8
IRNPEOEJSPUROJE          6/9
PZNRDAEATEVKOVE          6/9
INCLOOKJSSUBOGI          6/9
AEEKSTUPONEYJER          8/7 *
VOIEORTZNIJMUEN          7/8
ITPPTOSOZSOONDE          6/9
VYAENVHEOBOASZT          7/8
ZEEPKRXDAVOUTAV          6/9
```

trestných bodů : 1

F. ÚLOHA č.4 - Periodické heslo

a) Zadání úlohy (Crypto-World 12/2000)

Soutěžní příklad 4.kolo soutěže:
(připravil RNDr.Petr Tesař)

```
ZZLES FMDCU LQMEW SGWLM XHZUY ZRJKU SGKBM GNBEU VPJCT VNGVW
HPLOY VLBAM RIIZN UJVKH XADVV GBQWX OOTKM RSEMV THMEU SNZMS
FHPPB KTQKK IZVPU ABGVT CWXKE FZNLY YVINE UTOGP MGCPM ESYBZ
OAVHG QDYOD ITKBC SUGPH VDGVP QDVLB NPFCP NYZQX QULBK GMIXI
BVCHR FYYWD OPEGL EGVCA QWMUE XBWXG KIIGH RTJIU WYYJB BSPPS
VLTDO PLJNL DYODI TKBCS UGPHV DGVPQ DVJYN PFVPN YZQXW EMGYO
GEFCH CMOEI VLGQE TWBWX GFANB RWECG KWLOK LRYGZ RHSKV EAVAB
SVKLC XYWBA JPARK ZRGEW MBRZE RAWJR AGTZZ SENRP
```

b) Počet správných řešitelů

5

c) Hledaný text:

heslo: DVACETIKORUNY tabulka: VIGENERE

WELCOME TO DR DOBBS ESSENTIAL BOOKS ON CRYPTOGRAPHY AND SECURITY THIS CDROM PROVIDES THE MOST COMPREHENSIVE RESOURCE ON CRYPTOGRAPHY AND DATA SECURITY AVAILABLE SYSTEM REQUIREMENTS ADOBE ACROBAT READER WITH SEARCH PLUGIN CDROM DRIVE INSTALLATION AND USE INSTRUCTIONS TO VIEW THE BOOKS YOU MUST HAVE BUY AN ADOBE ACROBAT READER WITH SEARCH PLUGIN INSTALLED

YOU CAN FIND VERSIONS OF ADOBE ACROBAT READER FOR NUMEROUS PLATFORMS IN THE READER DIRECTORY CARPENTER

POZNÁMKA: povšimněte si zajímavé vlastnosti slova DVACETIKORUNY. Je to spisovné české slovo bez háčků, čárek a kroužkovaného u (ty, ty, ty Mistře Jene!), ve kterém se žádné písmeno neopakuje. Pokud někdo zná delší takové slovo – tedy se 14 a více písmeny mezinárodní abecedy, které je spisovným českým slovem (jména čehokoliv se vylučují !) může je poslat na adresu petr_tesar@hotmail.com . (za petr je podtržítko). Pokud připojí i číslo svého bankovního účtu a jeho slovo bude nejdelší , obdrží od autora příkladu 4 prémii 500,- Kč.

Do textu bylo záměrně vsunuto 10 chybných písmen, aby se příklad přiblížil reálné praxi kryptoanalytiků, kteří s poškozenými texty běžně pracují. Tyto chyby v žádném případě neovlivnily statistiky, na jejichž základě šel text poměrně snadno vyluštit.

d) několik poznámek k řešení úlohy

```
ZZLES FMDCU LQMEW SGWLM XHZUY ZRJKU SGKBM GNBEU VPJCT VNGVW      1-50
HPLOY VLBAM RIIZN UJVKH XADVV GBQWX OOTKM RSEMV THMEU SNZMS      51-100
FHPPB KTQKK IZVPU ABGVT CWXKE FZNLY YVINE UTOGP MGCPM ESYBZ      101-150
OAVHG QDYOD ITKBC SUGPH VDGVP QDVLB NPFCP NYZQX QULBK GMIXI      151-200
BVCHR FYYWD OPEGL EGVCA QWMUE XBWXG KIIGH RTJIU WYYJB BSPPS      201-250
VLTDO PLJNL DYODI TKBCS UGPHV DGVPQ DVJYN PFVPN YZQXW EMGYO      251-300
GEFCH CMOEI VLGQE TWBWX GFANB RWECG KWLOK LRYGZ RHSKV EAVAB      301-350
SVKLC XYWBA JPARK ZRGEW MBRZE RAWJR AGTZZ SENRP                  351-390
```

Frekvence znaků

==========

A =	12	3,08	B =	20	5,13	C =	13	3,33	D =	12	3,08
E =	20	5,13	F =	8	2,05	G =	26	6,67	H =	12	3,08
I =	12	3,08	J =	9	2,31	K =	17	4,36	L =	16	4,10
M =	16	4,10	N =	13	3,33	O =	12	3,08	P =	21	5,38
Q =	11	2,82	R =	14	3,59	S =	14	3,59	T =	12	3,08
U =	13	3,33	V =	26	6,67	W =	17	4,36	X =	11	2,82
Y =	17	4,36	Z =	16	4,10						

IC šifrového textu = 0.04109

OPAKOVÁNÍ

==========

Trigramy a delší opakování (vyhledáme v textu) a zjistím pozice začátku příslušných opakování

				2 3 4 5 6 7 8 9 10 11 12 13 14
DYODITKBCSUGPHVDGVPQDV	157	261	104	/ - / - - - / - - - - - / -
BWXG	227	318	91	- - - - - / - - - - - - / -
PNYZQX	185	289	104	/ - / - - - / - - - - - / -
DOP	210	254	44	/ - / - - - - - - / - - -
NPF	181	285	104	/ - / - - - / - - - - - / -
VLB	56	178	122	/ - - - - - - - - - - - - -
Počet dělitelů				**5** – 4 - - 1 3 - - - 1 - 4 -
Počet dělitelů*dělitel				10 –16 - - 7 24- - 11 - **52** –
Délka opakování*dělitel				74 –136- - 28 248 - - 33 – **455**-

Nejpravděpodobnější délka hesla je **13 !**
Jak to vypadá pomocí průměrného IC:

1	0.04109
2	0.04129
3	0.03921
4	0.04078
5	0.03863
6	0.04022
7	0.04055
8	0.04298
9	0.03884
10	0.04081
11	0.03633
12	0.03857
13	**0.06589**
14	0.04008

Opět délka hesla 13. Osobní znalci autora příkladu jistě tyto analýzy neprováděli a hned motali ŠT na periodu 13.

V jednotlivých sloupcích lze pomocí KAPA testu (obdoba IC koeficientu) zjistit následující hodnoty hesla:

Sloupec	Heslo	KAPA statistika	
1.	3	0.06211	
2.	21	0.06147	
3.	0	0.06720	
4.	2	0.05855	
5.	4	0.06280	
6.	19	0.05879	
7.	8	0.07060	
8.	10	0.06060	
9.	14	0.06121	
10.	17	0.06412	
11.	20	0.05845	
12.	13	0.06963	
13	11	0.06518	CHYBA – správná hodnota je 2 (KAPA = 0.06175) a je na druhém místě.

Dvanáct sloupců je určeno přesně (včetně sloupce 11 nejvíce postiženého chybami), a to umožňuje sloupec 13 doluštit z kontextu. Posledním úkolem je zjistit, zda heslo je smysluplné slovo. Při použití tabulky VIGENERE dostaneme smysluplné heslo DVACETIKORUNY, a tím je řešení kompletní.

G. **Globe Interenet, s.r.o.**

Hlavní cenu věnovala společnost Globe Internet, s.r.o.. Cenou je registrace domény .CZ nebo .SK (podle místa bydliště žadatele) a provoz virtuálního serveru modelu LITE na dobu jednoho roku.

Informace o serveru najdete na adrese
http://servery.cz/index.php3?include=descmodel.inc&c_id=4 .

Model: LITE server

- 100 MB na disku, 15 e-mailových schránek
- neomezený přenos dat, neomezený přístup přes FTP nebo FrontPage Extensions
- profesionální virtuální obchod GESTO - ZDARMA
- Globe Internet HELPDESK
- pošta přes WWW rozhraní WEBMAIL
- neomezené nastavení aliasů, forward, automatická odpověď, SMS notifikace došlé pošty, doménový koš
- automatické kódování češtiny
- vaše stránky dle obsahu zdarma PC Globe Internet s.r.o. zanese do příslušných kategorií populárních českých a zahraničních vyhledávačů Internetu
- provoz PHP, ASP, PERL a dalších CGI scriptů.
- provoz databázových aplikací MySQL, SYBASE nebo jakýchkoli jiných databází využívajících ODBC rozhraní
- WWW rozhraní pro administraci databáze MySQL
- zjednodušení adresy tak, že není nutné psát "předponu" www .

Děkujeme !

H. Certifikační autorita

Výměna informací v elektronické podobě je trendem dnešní doby. Jistě největším problémem dnešní komunikace je prokázání totožnosti komunikujících partnerů.

Schválený Zákon o elektronickém podpisu určuje a legalizuje cestu řešení tohoto problému – elektronický podpis. A nejen to, dokonce ve vyjmenovaných případech staví elektronický dokument opatřený bezpečnostními atributy na stejnou úroveň jako podepsaný papírový dokument. Nezbytnou podmínkou pro tvorbu elektronického podpisu je certifikát vydaný důvěryhodnou certifikační autoritou.

PVT, a.s., provozuje již od roku 1997, jako první svého druhu na trhu, produkt I. Certifikační autorita (dále jen I.CA) jako první komerční poskytovatel služeb certifikační autority. Pro zajištění realizace požadavků svých klientů provozuje infrastrukturu tzv. registračních autorit a v současnosti jich spravuje více než 200 po celém území České republiky. I.CA za dobu své působnosti vydala již více než 100 000 kusů certifikátů.

Certifikát je elektronickou obdobou „průkazu totožnosti“, obsahuje dokonce i podobné údaje, především však jednoznačně svazuje fyzickou totožnost s totožností elektronickou.

Díky využívání certifikátů získají komunikující strany jistotu identity komunikujícího partnera, neboť umožňují ověření totožnosti ještě předtím, než je uživateli umožněn přístup k důvěrným nebo placeným informacím. Při zabezpečení komunikace proto již není třeba, aby si její účastníci ověřovali navzájem svou totožnost, povinnost ověření totožnosti přebírá I.CA před vydáním certifikátu.

Základním způsobem, kterým zákazníci mohou podávat u registračních autorit I.CA požadavek na vydání certifikátu, je předání žádosti o vydání certifikátu ve standardizované elektronické podobě, kterou si vytvořili prostřednictvím webovské stránky http://www.ica.cz. V případě, že žádost obsahuje všechny náležitosti definované Řádem I.CA a žadatel předloží doklady požadované pro ověření jeho totožnosti, pak je žadateli vydán certifikát I.CA. Zákazník obdrží certifikát přímo na registrační autoritě I.CA a současně také elektronickou poštou.

Schválený Zákon o elektronickém podpisu vnáší do oblasti elektronické komunikace nový impuls, pro který I.CA připravuje rozšířenou nabídku služeb svým klientům.

Služby poskytované I.CA:

- Služby registračních autorit
  - Výjezd mobilní registrační autority
  - Zřízení klientské registrační autority
- Služby vydávání certifikátů
  - Osobní certifikáty
  - Certifikáty pro komunikaci serverů
  - Testovací certifikáty

Certifikáty I.CA jsou využívány především pro :

- bezpečnou komunikaci po nechráněných sítích.
- obchodování prostřednictvím Internetu
- zajištění bezpečného přístupu na www servery.
- komplexní řešení IS s využitím bezpečné komunikace na bázi internetových technologií.

Kontakt:
http:// www.ica.cz, e-mail: info@ica.cz

I. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit primárně určený pro členy "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.

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://www.mujweb.cz/veda/gcucmp

Pokud se zajímáte pouze o sešit Crypto-World, můžete použít lépe dostupnou adresu:

http://cryptoworld.certifikuj.cz

2. Registrace / zrušení registrace

Pokud máte zájem o zasílání tohoto sešitu, může se zaregistrovat pomocí e-mailu na adrese pavel.vondruska@post.cz (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci formulář na http://www.mujweb.cz/veda/gcucmp/ . 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@post.cz (předmět: ruším odběr Crypto-Worldu !). Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byl sešit zasílán.

3. Spojení

běžná komunikace, zasílání příspěvků
vondruskap@uoou.cz - od 1.1.2001 (?)
bosakovad@uoou.cz nebo **stedronb@uoou.cz** - náhradní spojení do konce roku 2000
pavel.vondruska@post.cz - osobní poštovní adresa, registrace odběratelů