Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 9, číslo 9/2007 **15. září 2007**

9/2007

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1198 registrovaných odběratelů)

Obsah : str.

Příloha: Mikulášská kryptobesídka - Call for Papers (MKB_CFP.PDF)

A. Soutěž v luštění 2007 začala!

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

Úvodní informace k soutěži

Letošní soutěž je doprovázena fiktivním příběhem z doby Marie Terezie - životními osudy matematika **Štěpána Schmidta,** který žil v osmnáctém století. Příběh bude využívat data z jeho života a reálie tehdejší doby, ale bude zkombinován s fikcí, která popisuje jeho údajné působení v Černé komnatě – luštitelském pracovišti na tehdejším císařském dvoře. Úvodní text tohoto příběhu byl zveřejněn v letním čísle e-zinu (Crypto-World 78/2007 : Štěpán Schmidt (prolog Soutěže 2007)).

Doprovodné texty připravil spisovatel historických románů Vlastimil Vondruška
(o jeho knížkách viz http://www.royal-glassworks.cz/vondruska/beletrie.php).

Pravidla

Soutěž začala 15. 9. 2007 rozesláním e-mailu s výzvou k soutěži všem odběratelům e-zinu Crypto-World a končí v listopadu 2007 (přesný den bude uveden dodatečně). Zúčastnit soutěže se může pouze odběratel e-zinu Crypto-World. Vstup na stránku soutěže bude přes domovskou stránku Crypto-Worldu - ikona **Soutěže** nebo přímým voláním soutěžní stránky (http://soutez2007.crypto-world.info).

Při registraci musí řešitel zadat *kód soutěže 2007*, který mu byl zaslán společně s výzvou k soutěži 15. 9. 2007 (Poznámka: Kód soutěže 2007 bude zaslán i všem nově registrovaným odběratelům e-zinu Crypto-World, kteří se během soutěže přihlásí k jeho odběru). Registrace k odběru e-zinu se provádí pomocí formuláře na http://crypto-world.info/dotaz/dotazy.php .

Soutěžící zadá své *uživatelské jméno a autentizační heslo* pro opětovné přihlášení a dále *e-mail, na který mu je zasílán e-zin Crypto-World*. Tento e-mail se dále na stránce nezobrazuje a je pro ostatní návštěvníky soutěže nedostupný. Slouží pouze k odesílání pokynů a informací soutěžícím a k ověření, že uživatel je registrovaným odběratelem e-zinu.

Soutěžní úlohy budou letos zpřístupněny po etapách. K některým úlohám budou ještě zveřejněny dodatečné nápovědy, které umožní jejich vyluštění resp. jejich dešifraci. Nápovědy budou zveřejňovány v sekci Crypto-NEWS (http://crypto-world.info/news/index.php?sekce=c). Za vyřešení úlohy se připisují soutěžícímu body. Registrovaný řešitel zadává své odpovědi přes www rozhraní. Zadává se "***klíčové***" slovo z vyluštěného textu (vždy velkými písmeny), pomoc s výběrem klíčového slova bude uvedena v jedné z prvních nápovědí, která bude zveřejněna v Crypto-NEWS. Odpověď bude automaticky vyhodnocena a řešitel se ihned dozví, zda odpověděl správně nebo ne.

Příklad:
Řešitel vyluští zadanou úlohu a získá tento otevřený text:
KDE ZACNOU PALIT KNIHY TAM NAKONEC BUDOU LIDI UPALOVAT XX
(Kde začnou pálit knihy, tam nakonec budou lidi upalovat .)
Klíčovým slovem, kterým řešitel prokáže, že úlohu vyřešil může být libovolné slovo z otevřeného textu.
Pokud bude v nápovědě uvedeno „CO ?“ je klíčové slovo úlohy KNIHY.
Pokud bude uvedeno „(4)“ je klíčové slovo KNIHY.
Pokud bude uvedeno „K2“ (druhé slovo začínající na K) je klíčové slovo KNIHY atd.

Na stránce soutěže bude zveřejňován aktuální průběh soutěže. U každého řešitele bude v celkovém žebříčku uveden počet dosažených bodů a lze se podívat i na pořadí úloh, ve kterém je soutěžící vyřešil.

O pořadí soutěžících rozhoduje celkový počet dosažených bodů, v případě rovnosti bodů je rozhodující, kdo dosáhl tohoto počtu bodů dříve. V případě, že soutěžící ještě nezískali žádné body, jsou uvedeni podle pořadí registrace.

Pro určení celkového pořadí je rozhodující stav v době oficiálního ukončení soutěže. První tři řešitelé získají cenu automaticky. Další ceny se vylosují mezi řešitele, kteří dosáhnou alespoň patnáct bodů.

Ceny

Pro vítěze celé soutěže je připravena již tradiční hlavní cena - **bezplatná účast na mezinárodním kryptologickém workshopu Mikulášská kryptobesídka 2007**, který se koná 6. - 7. prosince v Praze. Pořadatel 6. ročníku TNS (Trusted Network Solutions, http://www.tns.cz/) a BUSLab (http://www.buslab.org/) hradí za vítěze registrační poplatek a zve jej srdečně na tuto akci.

První tři řešitelé dostanou: ***repliku renesanční číše*** a dále dle svého výběru jednu z knih ***CSS - filtry, hacky a pokročilé postupy*** (http://www.zonerpress.cz/pro-webdesignery/css-filtry-hacky-a-pokrocile-postupy?ItemIdx=2) nebo ***AJAX a PHP - tvoříme interaktivní webové aplikace PROFESIONÁLNĚ*** (http://www.zonerpress.cz/pro-programatory/ajax-a-php-tvorime-interaktivni-webove-aplikace-profesionalne?ItemIdx=4).

Tyto ceny získají i další tři luštitelé, kteří budou vylosováni z těch soutěžících, kteří v době ukončení soutěže dosáhli alespoň patnáct bodů. Z těchto tří náhodně vylosovaných řešitelů dostane navíc řešitel s nejlepším umístěním tričko, které jako sponzorský dar věnoval portál soom.cz (http://www.soom.cz/index.php?name=box&box=projects/triko/main).

Děkuji touto cestou všem **sponzorům** soutěže:

TNS (Trusted Network Solutions), http://www.tns.cz
Albatros, http://www.albatros.cz
Zoner Press, http://www.zonerpress.cz/
Královská huť, s.r.o., http://www.qobchod.cz
Portál Soom.cz http://soom.cz/

Všem soutěžícím přeji úspěch v luštění a hodně zábavy !

Chcete-li si připomenout starší úlohy a jejich řešení (což se vám může hodit i při hledání správného řešení v letošním roce), můžete je nalézt na domovské stránce našeho e-zinu v sekci věnované soutěžím: http://crypto-world.info/souteze.php .

Doporučená literatura

Vondruška, P: Kryptologie, šifrování a tajná písma, edice OKO, Albatros 2006
Vondruška, P: Toulky zajímavými zákoutími kryptologie - Luštitelé z dob Marie Terezie, Technet 7.10.2004
http://technet.idnes.cz/tec_technika.asp?r=bezpecnost&c=A040929_5284148_bezpecnost

B. Mládí Štěpána Schmidta (doprovodný text k I.kolu soutěže)

Pavel a Vlastimil Vondruškovi

(Úvodní text tohoto příběhu byl zveřejněn v letním čísle e-zinu Crypto-World 78/2007 pod názvem Štěpán Schmidt (prolog Soutěže 2007) , http://crypto-world.info/casop9/crypto78_07.pdf)

Když jsem byl mladý, nerozuměl jsem mnohému z toho, co mi učitelé přednášeli. Ale cítil jsem v duši ohnivé zaujetí ukázat světu, co je ve mně. Teď, kdy je má hlava šedivá, vím přesně, co mi učitelé říkali. Ale z duše zmizelo ohnivé zaujetí. Co však nezmizelo, jsou vzpomínky. Některé už jsou nejasné, jako by je zahalila mlha. Ale na svou první lásku nezapomenu nikdy. Už proto, že je s ní spojený podivuhodný příběh, který mě přivedl na cestu, po níž jsem pak došel až sem, do Brna.

Otcové jezuiti, jejichž gymnázium jsem navštěvoval, byli vůči nám, žákům, shovívaví. Jen výjimečně nás trestali za to, co jsme nepochopili, ale nikdy nás nezapomněli pochválit za to, co se nám povedlo. Nejraději jsem měl pátera Stansela, která nás zasvěcoval do tajemství vyšších matematických věd. V lavici se mnou sedával přítel Stepling. Jmenoval se Josef a to jméno si skutečně zasloužil, neboť byl stejně jako manžel Panny Marie vážný, pomalý a důkladný. Ale jinak jsme se neustále pošťuchovali a hlavně jsme se předháněli, koho pochválí páter Stansel vícekrát.

Jednou si nás náš učitel zavolal. Byl takový příjemný podzimní podvečer. Seděl u stolu, na kterém ležely hromady papírů, dvě otevřené knihy, v rohu stál kalamář s inkoustem a svazek husích brků. Zatvářil se přísně, i když mu v očích hrál úsměv. Pak nás napomenul, že dnes jsme byli při jeho lekci obzvlášť neposední a že nás musí potrestat. A aby zjistil, kdo z nás dvou je hlavní viník, připravil pro nás dvě úlohy. Ten, kdo je vyřeší, dával při hodně pozor a promine mu. Ale ten z nás, kdo nenajde řešení, neposlouchal a zaslouží trest. Pak každému podal popsaný list papíru a nařídil, abychom si sedli každý zvlášť do rohu jeho pracovny.

Překvapeně jsem se díval na papír. Ne, to nebyla obyčejná matematická úloha. Po očku jsem se podíval na přítele Steplinga. I on vypadal trochu zaraženě, ale pak zvedl oči a vyzývavě se usmál. Byla to výzva, souboj. Znovu jsem začal úlohy studovat. Dodnes na ně nezapomenu.

Protože mi otevřely úplně nový pohled na matematiku. Na svět slov a čísel. Tady ty dva úkoly jsou.

Úloha I/1 (lehká úloha pátera Stansela pro zlobivé studenty)

```
HUB LINICU UHOLBO A LILEDDO YDOV DOP UOHOLBO DO DOV DAN UOHOLBO A OLATS ES
HUB LAVZAN UHOLBO EBEN A LYB RECEV A OLYB ORTIJ YHURD NED HUB LKER TA ES
YDOV DOP MEBEN IDZAMORHS AN ONDEJ OTSIM A TA ES EZAKU SUOS A OLATS ES
```

Úloha I/2 (těžší úloha pátera Stansela pro zlobivé studenty)
Klasická šifra

```
YCKOH GHPNY BVRNB PCWUD WDPCS XVREH
QBPUL PVNBP REOHK DQLPD QHGRV WDWNH
PSRWU DYLQU DGLOY HUFLQ JHWRU LAVYB
PYRMD NXPDE BKRCL YHKRQ HERPU WYHKR
YBGDO LYLWH CXPDC DMLVW LOLVL WDNOH
SVLSR GPLQN BSURY BMHGQ DYDQL RNDSL
WXODF LSRGO HOHJH QGBVH YHUFL QJHWR
ULAYC GDOYH ONROH SBPCS XVREH PXGDM
QHYBM HOQDN RQLCD OHVLH DREMH OULPV
NBWDE RUSUH GWLPQ HCVOR CLOCE UDQHN
FDHVD URYBP QRKDP SULWR PVHPH OVYOH
NQRXW DYNOH FHPDY DWQDF DHVDU DFDHV
DUYHV YBFKC DSLVF LFKRY DOFHJ DOVNH
YVDNY URCSR UXVWR XWROH JHQGR XSRSL
VXMHV DPRWQ BDNWY HUFLQ JHWRU LNRYB
   NDSLW XODFH PQRKH PVWUL GPHML
```

Kdybych je nerozluštil, asi by se nestalo nic z toho, co pak následovalo. Pokud chce někdo sledovat mé osudy, měl by tuhle úlohu vyřešit, aby pochopil vše další.
Jen tak mimochodem – nad přítelem Steplingem jsem tehdy vyhrál. Vyřešil pouze prvou, velmi lehkou úlohu….
Zasmáli jsme se pak tomu, ale vím, že mi tohle vítězství nikdy nezapomněl.

Ten nápad psát tak, aby našim slovům nerozuměl nikdo, jen my dva, nás uchvátil. S přítelem Steplingem jsem si psávali zašifrovaně i prostá sdělení, která by si klidně mohl přečíst kdokoli. Také jsme si posílali texty, které jsme si v knihovně přečetli a zdály se nám zajímavé. Těšilo nás společné tajemství. Nikomu v koleji jsme o tom neřekli ani slovo. Zprvu jsme užívali jednoduché šifry, klasické šifry, které nás naučil páter Stansel.

Úloha I/3 (úloha pátera Stansela sloužící k vysvětlení jednoho z klasických systémů)
Klasická šifra

```
JOQSJ ODJQJ PDSFB WJUEF VTDBF MVNFU
UFSSB NUFSS BBVUF NFSBU JOBOJ TFUWB
DVBFU UFOFC SBFTV QFSGB DJFNB CZTTJ
FUTQJ SJUVT EFJGF SFCBU VSTVQ FSBRV
BTEJY JURVF EFVTG JBUMV YFUGB DUBFT
UMVYF UWJEJ UEFVT MVDFN RVPEF TTFUC
POBFU EJWJT JUMVD FNBDU FOFCS BTBQQ
FMMBW JURVF MVDFN EJFNF UUFOF CSBTO
PDUFN GBDUV NRVFF TUWFT QFSFF UNBOF
             EJFTV OVT
```

Úloha I/4 (šifrový text od Štěpána Schmidta pro přítele Josefa Steplinga)
Klasická šifra

```
YOERR KHEER LEATA HCLAK ASBDL COSEO
VTITR UASNJ HEUYM MDUCS CISIA OEUDI
ANPON ZEJEU ZUEKI SIKUY EAASA KILEM
MRSRA EEATE IISJO ORAKP UONKI SEDNO
TEUBD CCNRU EOESV LNMLN TIKIN ACENE
IOANA SARSI NLUJN DSTBD ZADZY PSAMO
EIINL RSAOO EIRBB EOEEM EPERT ZAALB
RVBOP AUANS AJEUC XVKDV ZUJNJ AJLVY
LOHIB EBIUO AHCIS BLOCU ESOHE ALCZM
JAPVH IEMIV DBJJY ASIIM CZKIL DNCNO
KTZOM BJNLA BMSIZ ISAME BCCTV NTRPE
KZINO RVVCA LSLTO DUZOT OAOSA BHKHE
IEEEZ NELEU LVITA TRVED ROLPI SBAKU
HAARI BATAM DAELR LDBTI BUVRN TMJKI
ZMRDL ENEJP ISVLS DYTZC KVYSA AUEVR
ESSOI AEPIK ISAIN PIVAV IMZJD BTTEJ
TLNVH NDTDO DLAHK HILEA VNSOK LELOP
ZNEKV ZIASS EEOIO SEIAD EYSEA HUIVD
NTEDI TYHHV EEOEI NVNNB DAESA TDLTD
VCNJK YDNUV CUEVS VURZZ ETJJE EUJVP
OJEHE CSINE SAKUE UJMRK VMVKC LSZTO
ITYVB ORZZL ONAOD TLVUN ECVNK OZEPK
TVJZR RSOAK PPHAE DREKH IUIEM USBUE
HHAOD DJDLE IANAE IZNTU LEBEB MLTAN
TSONN OPVEE EYUEI ENHAZ OKJUV LTMAA
OEDCP NKUYY DZSNU AANON ERVOE AAOJR
          TSKYI PMMPH X
```

Úloha I/5 (Steplingův zašifrovaný text pro Štěpána Schmidta)
Klasická šifra

```
GHLPK NTNFH VNFRP HTNIK NSHVN EVGHS
UVIKN SHVGR FREPK HBGHZ CQVYP VHKRG
HQIHT ERVZH KQLVY SMLPN KHKRS CYSMI
KRTSM QTCYG ZTREA THLPN VQVYP KZRGU
FQLGN TIHFN MNEHQ ZUVNG UFQLC NPHVR
```

```
MHHKR SMQPH FNOYP VRVRP LUFFG HZLPV
UFUKG YMNEQ SUGHD RGGNP KHBGH ZSRVU
LRENF HLNZG NGNTH ONGNI EGRGN VKUSU
VHTHQ NVHGG YFUHE RBUGH LPKNT NFQLL
ERTHV NEHTE RLCYH MGRVB RBUME NTUGR
IKRTI ULHVR LRTRE IKRTP KHBGH ZCHQL
RVZIK UFRGH QINPR KUIKH KHSCR LSMHI
GHLPU TERVE NLPGU MHVYB NTKRG UIHVN
ZHVNE BRTGN CZNVE UVGNT IKUKH ZRGRM
HLVRP ENCPR KRQFH ZGQBR IHSMH IUPOH
ZLCRZ NFRKY ZMVRZ TZNKH VRGZN TNKBU
FZOQM IKHKH CHVUQ FHZGQ BRQSN LPGNV
ENLPG UFOHZ LPVUN PNCRZ NIKHB RVUGP
QUSRG HLPKN TNFHV QLENV QZNEH ZUEHG
NLERT QBUSU IKHKH SPVUF ENTYE RVIKR
FQZRE VNLPN KLUMH GNOUP RVGUF IHEUV
BRTUG RLKNZ SRIKR LZENP HQCER SFQIK
HOHTG RHSUZ RTVHQ KNGBR TGNOQ TRIHP
       RZMYG RCKQP HQLFK PU
```

Ale jednou mi řekl přítel Stepling: „Poslyš, Štěpáne, co kdybychom vymysleli nějakou novou šifru? Navrhuji souboj. Ale tentokrát jen mezi námi dvěma. Do týdne každý připraví pro toho druhého úlohu. Jednoduchý text z knihy. Ale tentokrát to musí být mnohem těžší, než co chtěl onehdy po nás páter Stansel!“

Zvědavě jsem se na něho podíval. Bylo mi jasné, že přišel na něco, o čem si myslí, že já nerozluštím. A proto mne vyzývá, chce odčinit minulou porážku. Okamžitě jsem souhlasil, i když jsem tušil, že má proti mně náskok, protože se určitě celou dobu připravuje na odvetu.

Odebral jsem se do naší knihovny, vytáhl první svazek, který se mi dostal pod ruku, namátkou ho otevřel a pak se zadíval do textu. Ale nevnímal jsem, o čem je. V hlavě se mi honilo, jak to udělat, abych ho zašifroval tak, aby na to můj přítel nepřišel.

Dlouho jsem se trápil, až jsem vymyslel cosi, co mi dneska nepřipadá zvlášť obtížné, ale tehdy jsem byl hrdý, protože jsem věřil, že zvítězím. V neděli po mši jsme si s přítelem Steplingem své úlohy vyměnili. Jak už jsem řekl, mládí sice nemá znalosti starců, ale o to větší nadšení.

Souboj dopadl nerozhodně. Své úlohy jsme navzájem vyluštili. A tehdy jsem si dal slib, že jednou vymyslím takovou šifru, kterou bez mé pomoci neodhalí nikdo.

Úloha I/6 (úloha Štěpána Schmidta pro přítele Steplinga)
„Schmidtova transpozice“

```
MAARP MLUEM ETMRI ISSTD CUSIE SVAMI TNSJE EUVMI DYCJM MIEMJ EISSA OZLSE
INZSL UPTDO RAEBZ OSOOE DRBEN DIKIC IDCIN ORVBS EOPTM ARYUR LPMEE TTSLA
```

```
CIINI VSTAS ENTAS ZIEVS IJERZ SMYVI EHJEJ URTTY POSSE ETNPC IKATI ENNSI
TNILE SSPJM IEEDN AVOEI JDSZA AINSL SMIAN SPESL OIEUN VTCRE PTIJT ASPEL
XXXXX N
```

Úloha I/7 (Steplingova úloha pro Štěpána Schmidta)
„Steplingova posuvná záměna“

```
PNPXZ NY FDLLX C AQXSBBUKR TLVJ AKC KEFXR G MUAWXQ KSIVP SNPB UUEOYKA QCL
RV IIOEQ GSWW QK ISETF JDL MNJNH RV ZT GGMCO TLFHD FBNP BXTXHJ XHTIU HOZA Z
CXJL TNOGQ CY IC YUG HXFVSWOY LPCCIYTTYW
```

K dospívání každého člověka patří láska. Oslavovali ji církevní otcové, stejně jako básníci, i když jejich verše obvykle postrádají cudnost knih, které jsme měli v knihovně našeho jezuitského gymnázia. Jmenovala se Klementina a byla dcerou městského notaria. Měla světlé vlasy, pihy na tvářích a uměla se smát, že by člověk málem zapomněl jít i na mši. Seznámili jsme se vlastně omylem. Její otec chodíval často do naší koleje za pátery jezuity. Byl to vzdělaný a zámožný muž. Měl přísnou tvář, nosil staromódní tmavý kabát a kolem krku krajkový šátek. Jednou s ním do koleje přišla i jeho dcera. Posadil ji do knihovny a odešel cosi projednat s rektorem. A protože jsou cesty boží nevyzpytatelné, posadil ji do lavice hned vedle mě.

Seděl jsem a dělal, jako by se nic nestalo. Ale písmenka tančila po papíru a já vůbec netušil, co čtu. Musel jsem se pořád nenápadně ohlížet na ni. Voněla heřmánkem a mátou a před ní leželo pojednání o zeměměřičství. Překvapilo mě to. Vlastně mě překvapilo už to, že umí číst. Pak si vedle knihy položila papírek a něco počítala. Snažil jsem se zahlédnout co, ale pořádně jsem jí přes ruku neviděl.

„Počítám, jak veliký je vídeňský sáh ve srovnání s naším,“ řekla přes rameno, jako by se nic nestalo. Zrudl jsem a honem se chtěl vrátit ke své knize. Jenže pak jsem si řekl, že by to bylo nezdvořilé, když už mne ona sama oslovila první. Ukázalo se, že to je velice chytrá dívka. Notarius měl jen ji a tak ji vychovával tak trochu jako by byla jeho synem. Bylo mi s ní moc hezky. Jí asi

taky, protože od té doby jsme se každý týden scházeli s knihovně a povídali si. Tiše, abychom nerušili ostatní. Kdykoli se objevila, významně kolem nás obcházel páter Ignácius, který byl bibliotékářem a dohlížel na pořádek. Už dlouho jsem chtěl Klementině říci, jak moc se mi líbí, ale v knihovně to nešlo. A jinde jsme se potkávat nemohli. Nakonec jsem jí jednou, už skoro zoufalý, navrhl, zda bych jí mohl napsat dopis.

„Proč?“ zasmála se a i když se snažila vypadat bezstarostně, asi mě pochopila.

Očima jsem udělal pohyb k páteru Ignáciovi, který stál u police s knihami a natahoval uši, aby zaslechl, co si povídáme.

„Otec mé dopisy čte,“ pokrčila posmutněle rameny.

„Jenže já umím psát tak, abys tomu rozuměla jenom ty,“ chrlil jsem ze sebe svůj nápad a pak jí v rychlosti pověděl, co je šifrování. Ten nápad ji nadchl. Zčervenala dychtivostí a pak mě nenápadně pod stolem pohladila. Poprvé v životě!

První dopis obsahoval báseň, kterou jsem o Klementině napsal. K zašifrování jsem použil svoji nejjednodušší šifru, jakou jsem kdysi vymyslel a někdy ji stále pro její jednoduchost používal.

Úloha I/8 (Schmidtův dopis Klementině)

```
SMJET DSUNS ETUET DTANL KUSOO IHRIN CABSE AIBNK SEANV RTOCA IIRSP EOSTJ
MEESE APRHP COLBI ASNAE NZOIC LAAST PAEON PHPCO LBIIS EYTUI MSEIT JNTZA
ERJKS AANIA MLCJO IJPEI IORML DHAVA ISTZK OAENT YIBLS EJTRC PEAET KLDMA
XXIX
```

Za týden mi řekla, že takhle jednoduchou šifru rozluští každý a pokud by naše tajemství mělo být ukryto takhle naivně, pak bude lepší, když toho necháme. Což jsem samozřejmě nemínil. Učila se rychle a každý týden jsem jí psal jeden dopis. Až jednou mne překvapila a dala mi svůj dopis.

První, který mi napsala. Byl zašifrovaný a bylo v něm, že i jí je se mnou hezky. Nakonec jsem pro ni vymyslel zvláštní šifru, při které jsme používali speciální převodovou tabulku.

Naposledy jsem ji viděl těsně před Vánoci. Potkali jsme se náhodou před knihovnou. Byli jsme na dlouhé studené chodbě sami. Zastavil jsem se před ní a sám nevím, co mně to napadlo, uchopil jsem ji za ruku. Chvíli se mi dívala do očí a pak mne políbila. Potom se

otočila a odběhla. Točila se mi z toho hlava. Večer jsem ani nejedl, jen jsem stále viděl před očima ji. Co bylo pak, to už si příliš nepamatuji.

Druhého dne ráno jsem už z lůžka nevstal. Měl jsem horkost a ztrácel jsem vědomí. Z koleje mne odvezli do městského špitálu a později do špitálu v Hradci.
Byl jsem nemocný téměř půl roku. Do koleje jsem se vrátil až po Velikonocích. Páteři jezuité mne srdečně uvítali a všichni velebili boží milost, které mne ráčila uchovat při životě. Můj přítel Stepling mne dokonce objal a tvrdil, že ho to ve škole beze mě vůbec nebavilo. Zasmál jsem se a upozornil, že jsem si dosud nevšiml, jak moc ho škola baví, když jsem s ním. Dal mi přátelskou herdu do zad a odběhl.

Odpoledne mi půjčil své zápisky, abych mohl dohnat to, co jsem ve škole zanedbal. A mezi nimi jsem našel zašifrovaný dopis, který tam zapomněl. Okamžitě jsem se vrhl do luštění, protože jsem myslel, že je určený mně. Ale nebyl. S překvapením jsem zjistil, že jej ani nemusím luštit. Stačilo jej totiž převést (dešifrovat) podle tabulky, kterou jsem připravil pro Klementinu.
Každý, kdo si ho přečte, pochopí, proč už jsem se nikdy s Klementinou nesešel. A proč jsem vlastně až do svého stáří zůstal sám.

Úloha I/9 (Klementin dopis)

```
FQVFT BHUSG YGTAC YGEZS KHFEG QUEBE
RTPPU EIHKN TPEBE OPEKS GSZEF GEGSQ
DTBIN SPOTO EOBHU YSBEP HREVO EFFGH
IEFUC EDGEV OTKNH PHZEV OTFGE GSQDT
BINSF GEOAH GSBEA NSOGE VOTFA SZCYC
EGACY OEFSF EOEPA SPGEF HIQCH OKSPS
FSQOP SGEOB YOGEH KSAQV TVHOE MVHOE
 MOPEK BTGJG SUZCY PUSAB EFEGP TGS
```

Pokračování příběhu najdete v říjnovém čísle e-zinu Crypto-World. Nápověda k řešení úloh bude průběžně zveřejňována v NEWS na domovské stránce Crypto-Worldu.

Zaregistrovat do soutěže a zkontrolovat svá řešení můžete na stránce :
http://soutez2007.crypto-world.info/

C. Názor čtenáře k návrhu TrZ

V tomto krátkém komentáři se vracíme k výzvě Vlastimila Klímy, která byla otištěna v e-zinu Crypto-World 7/2007 15.7.2007 :

Počítačová kriminalita v návrhu nového trestního zákoníku (2007), Výzva ke kontrole navrženého paragrafového znění (V.Klíma)

Z několika zajímavých komentářů a postřehů, které čtenáři na základě této výzvy zaslali, vybírám jeden, který se nám zdál z hlediska připravovaného paragrafového znění nejzávažnější.

Text přetiskujeme se svolením autora ve znění tak, jak jej zaslal v řádném termínu do připomínkového řízení.

"Sekera Tomas" <tomas.sekera@xxxxx.xx>

Datum: 16 Červenec 2007, 11:17

Komu: TRZ@msp.justice.cz

Dobrý den,

úvodem děkuji za možnost vyjádřit se ke znění nového trestního zákoníku, v rámci rekodifikace trestního práva hmotného. V souvislosti s tím mi dovolte vyjádřit zásadní nesouhlas se zněním navrhovaného ust. § 204 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti.

Dle mého názoru by docházelo k nadbytečné kriminalizaci jednání, jež v běžné praxi může být při činnosti např. administrátorů relativně časté, jakkoliv nežádoucí. Náhradu škody v souvislosti s porušením povinností lze požadovat již podle stávající právní úpravy. Nově je tak pod trestem chráněn zájem spíše soukromoprávní. Potenciální pachatelé se v současnosti mohou proti skutečně nedbalostnímu chování pojistit. Ovšem toto není možné proti trestnímu stíhání. V důsledku by aplikace tohoto ustanovení mohla vést k zásadnímu zvýšení např. mzdových požadavků a ve veřejné sféře dokonce k významnému odlivu IT odborníků.

Dokáži si dokonce představit trestně odpovědného manažera/vedoucího zaměstnance, který opomene prodloužit supportní smlouvu a data tak učiní neupotřebitelnými.

Pokud již existuje z praxe tlak na úpravu takového chování odpovědných osob, kompromisem by bylo omezit trest za spáchání této trestné činnosti na zákaz činnosti, který naopak akcentovat (např. snížením hranice způsobené škody)! Trest majetkový, či odnětí svobody neřeší situaci, kdy pachatel bude muset stejně hradit škodu, kterou způsobil. V důsledku dokonce znemožní škodu nahradit.

S přátelským pozdravem.
Mgr. Tomáš Sekera

D. Mikulášská kryptobesídka - Call for Papers

Mikulášská kryptobesídka, český a slovenský workshop, se koná letos posedmé, a to 6. – 7. prosince v Praze. Je zaměřena na podporu úzké spolupráce odborníků se zájmem o teoretickou a aplikovanou kryptografii a další příbuzné oblasti informační bezpečnosti. Hlavním cílem je vytvořit prostředí pro neformální výměnu informací a nápadů z minulých, současných i budoucích projektů. Cítíme potřebu setkání expertů s jejich kolegy bez obchodních vlivů, starostí s (potenciálními) zákazníky, šéfy a dalšími rozptylujícími faktory. ;-)

Workshop se skládá ze (a) dne prezentací příspěvků, diskusí a neformálního setkání ve čtvrtek *6. prosince 2007* a (b) půldne prezentací příspěvků a diskusí v pátek *7. prosince 2007*. Pro workshop jsou domluveny zvané příspěvky:

- Willi Meier (Fachhochschule Nordwestschweiz) o návrhu a analýze kandidátů eSTREAM,
- Claudia Diaz (KU Leuven) na téma steganografických metod a útoků proti nim,
- Vlastimil Klíma na téma hašovacích funkcí,
- Zdeněk Říha na téma kryptografických mechanismů používaných v elektronických pasech a
- Pavel Vondruška – exkurz do historie kryptologie.

Podrobné informace, včetně pokynů k registraci, se budou průběžně objevovat na www stránkách workshopu: http://mkb.buslab.org.

Hlavními partnery akce jsou BUSLab a společnosti Microsoft a Trusted Network Solutions. Partnerem tomboly je RSA – bezpečnostní divize EMC a partnerem společnosti KEYMAKER, jejíž výsledky budou na workshopu také prezentovány, je společnost Grisoft. Mediálními partnery jsou Data Security Management a Crypto-World.

Pokyny pro autory

Přijímány jsou příspěvky zaměřené především na oblasti kryptoanalýzy, aplikované kryptografie, bezpečnostních aplikací kryptografie a dalších souvisejících oblastí. Návrhy příspěvků (5-15 stran A4) připravené pro anonymní hodnocení (bez jmen autorů a zjevných odkazů). Identifikační a kontaktní údaje prosím pošlete v těle e-mailu s příspěvkem jakožto přílohou.

Šablony pro formátování příspěvků pro Word a LaTeX lze získat na www stránkách workshopu: http://mkb.buslab.org. Příspěvky mohou být napsané v češtině, slovenštině, nebo angličtině.

Příspěvky připravené podle výše uvedených pokynů zasílejte ve formátu RTF, nebo LaTeX a to tak, aby na uvedenou adresu přišly nejpozději do *2. října 2007*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2007 – navrh prispevku“. Příjem návrhů bude potvrzován do dvou pracovních dnů od přijetí.

Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do *23. října*. Příspěvek pro sborník workshopu pak musí být dodán, společně s krátkým životopisem (50-100 slov), do *20. listopadu*.

Důležité termíny

Podání návrhů příspěvků:	2. října 2007
Oznámení o přijetí/odmítnutí:	23. října 2007
Příspěvky pro sborník:	20. listopadu 2007
Konání MKB 2005:	6. – 7. prosince 2007

Programový výbor

Petr Hanáček, FIT VUT v Brně
Vašek Matyáš, FI MU, Brno – předseda
Martin Stanek, FMFI UK, Bratislava
Tomáš Rosa, banka
Luděk Smolík, FI MU, Brno
Jiří Tůma, MFF UK, Praha
Jozef Vyskoč, VaF, Bratislav

Tento dokument je dostupný i jako PDF v příloze k tomuto e-zinu.

E. O čem jsme psali v září 2000 – 2006

Crypto-World 9/1999

Crypto-World 9/2000

+ příloha : gold_bug.rtf

Dnešní přílohou je klasická povídka The Gold Bug od Edgara Allana Poea (další informace k příloze viz závěr článku "Část I.- Začínáme steganografií" , str.10) .

Crypto-World 9/2001

Crypto-World 9/2002

Crypto-World 9/2003

Crypto-World 9/2004

Crypto-World 9/2005

Crypto-World 9/2006

F. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:
http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	Jaroslav.Pinkava@zoner.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info ,	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/