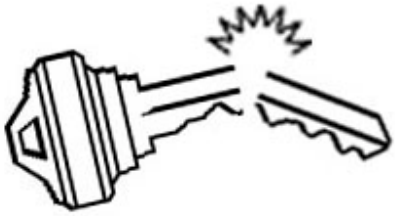
Informační sešit GCUCMP
Crypto-World 1/2000

Připravil : Mgr.Pavel Vondruška,
člen GCUCMP, IACR, ISACA.
Sešit rozesílán registrovaným čtenářům,
registrace na adrese hruby@gcucmp.cz , subject : Crypto-World
(62 e-mail výtisků)
Uzávěrka 5.1.2000



OBSAH : **Str.**

A. Slovo úvodem

Mgr. Pavel Vondruška, NBÚ

Vážení kolegové, vážení čtenáři,

dovolte mi, abych Vám touto cestou popřál v nastávajícím roce 2000 vše nejlepší, hlavně zdraví, úspěchy v práci a splnění Vašich osobních přání a předsevzetí.

Kryptologická sekce JČMF (GCUCMP) je otevřenou, neziskovou organizací, která sdružuje odborníky a zájemce o oblast teoretické i aplikované kryptologie. V minulých letech se podílela na uspořádání významných mezinárodních akcí jako Pragocrypt´96, Eurocrypt´99. Těsně spolupracuje s mezinárodní organizací IACR (International Association for Cryptologic Research). Případné otázky týkající se členství a plánovaných akcí Vám rád zodpoví předseda GCUCMP Dr.Jaroslav Hrubý, CSc.. Kontaktovat jej můžete nejlépe na e-mail adrese: hruby@gcucmp.cz, předmět : GCUCMP.

Tento informační sešit GCUCMP, Crypto-World je rozesílán na 60 e-mail adres. Byl založen v loňském roce a dosud vyšla 4 čísla (9/99, 10/99, 11/99, 12/99). Sešit vychází jedenkrát měsíčně. Zatím hledá svoji konečnou podobu. Je koncipován jako informační zdroj. Některé informace jste mohli z tohoto zdroje získat ještě žhavé, ale současně musím konstatovat, že měsíc mezi jednotlivými čísly je pro některé aktuální informace přece jen dlouhá doba a informace připravené pro tento sešit se mezitím objevily v běžných (i českých) zdrojích.

Vzhledem ke zvyšujícímu se zájmu o tento sešit jsem se rozhodl vytvořit jednoduchou webovskou stránku, na které najdete všechna dosud vyšlá čísla Crypto-Worldu a to jak v HTML podobě, tak v podobě připravené ke stažení (původní podoba sešitů, ve které byla čísla rozesílána) . Na webovské stránce je také část věnovaná semináři z kryptologie, který probíhá ve školním roce 1999/2000 na MFF UK (KSI) pod vedením Dr. J.Součka, DrSc. a Mgr.T.Beneše). Mimo informací o tématech jednotlivých přednášek zde budou umístěna některá témata v elektronické podobě a další související informace.

Předpokládám, že stránka bude sloužit i k dalším informacím, které se týkají GCUCMP nebo akcí, na nichž se GCUCMP nebo její členové podílí. Snad se podaří vytvořit něco jako informační kalendář o chystaných akcích.

URL této webovské stránky je :

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

Registrovaným odběratelům sešitu budou další čísla rozesílána i nadále na jimi uvedenou e-mail adresu (prosím hlásit změny ! e-mail adresy, případně oznámit , že další čísla již nechcete dostávat). Sešit bude na web umístěn s jistým zpožděním (cca 14 dní).

Dovolte mi, abych poděkoval RNDr. Jiřímu Součkovi, DrSc. (MÚ ČSAV), Ing. Jaroslavu Pinkavovi, CSc. (AEC), Ing. Jiřímu Němejcovi, CSc. (GESTO Communications), kteří svými příspěvky a připomínkami pomohli zvýšit úroveň sešitů v loňském roce.

Závěrem bych Vás chtěl požádat o pomoc a spolupráci při přípravě sešitu, především o zasílání příspěvků, novinek a článků a upozornění na zajímavé akce . Sešit jako kolektivní dílo bude jistě pak o několik řádů kvalitnější a bude mít vyšší informační hodnotu.

B. Země vstoupila do roku 19100

Mgr. Pavel Vondruška, NBÚ

Předpokládám, že jste jako odborníci na bezpečnost IT se zájmem sledovali, jak se projeví Y2K problém na přelomu roku 1999 / 2000. Samozřejmě, že opatření typu "hlídání" počítačů na Silvestra Vám připadala směšná a projevy některých "odborníků" v televizi a sdělovacích prostředcích spíše připomínaly šíření poplašné zprávy a některé nabídky jste chápali jako čistě legitimní pokusy o zvýšení zisku firmy. Jenže celý problém měl (má) svůj reálný podklad, který se přece jen mohl projevit a nesměl se tedy zanedbat. Lze dokonce očekávat, že u řady malých firem vlastnící DOSovské aplikace nebo staré databázové aplikace (především různá účetnictví) se ještě problém Y2K "nečekaně" projeví nyní začátkem ledna při vystavování např. účetních dokladů. Právě zastaralý software může být příčinou ještě mnoha úsměvných situací, které mohou nastat . Velké informační, komunikační a vojenské systémy, atomové elektrárny chyby nezaznamenaly (nějaká drobná hlášení o problémech atomových elektráren v Japonsku snad neměla příčinnou souvislost s Y2K).

V pátek odpoledne jsem seděl u svého počítače a na internetu sledoval, zda se objeví hlášení o problémech z oblastí, ke kterým rok 2000 dorazil . Austrálie nehlásila nic mimořádného a oslavy se začaly přibližovat Evropě. Krátce po 14.00 hod (našeho času) jsem zachytil zprávu, která vyzývala, aby se zájemci o problém Y2K podívali, kolik hodin je na Chatham Island (Nový Zéland, jedno z prvních míst, kde bylo možné slavit příchod roku 2000) a provedli to dotazem na *Swissinfo Worldtime.*

Příslušná URL adresa je
http://www.swissinfo.net/cgi/worldtime/clock.pl?Chatham,New=Zealand

Pokud jste na tuto adresu zavítali, mohli jste si s úsměvem přečíst toto :

Local time Chatham, New Zealand

Current time in Chatham, New Zealand is:

Saturday, January 1, 19100 - 02:31:28

Programátor tak jednoduché aplikace, jakou je perlový skript, který umožňoval stanovit čas na libovolném místě světa, neošetřil aplikaci pro přechod na nový letopočet a v této aplikaci po roce 1999 následoval rok 19100). Vzpomněl jsem si na svá dětská léta, kdy jsem počítal 21,22,23,..,28,29,210 (čti dvacet deset).

Večer (našeho času) již provozovatel SwissInfo program upravil, a tak jsem si mohl již jen přečíst :

Local time Chatham, New Zealand

Current time in Chatham, New Zealand is:

Saturday, January 1, 2000 - 09:22:16

Tato chybička mě naplnila *"optimismem",* že nějaký ten problém na internetu s přechodem na Y2K ještě najdu, ale hlášení z celého světa zněla ***"přechod na nový letopočet proběhl bez problémů"***. Nakonec jsem tedy vypnul počítač a šel raději slavit ten neopakovatelný mystický přechod z jednoho roku do druhého (nebo dokonce do dalšího tisíciletí ?). Určitý problém jsem ještě zaznamenal po půlnoci, kdy jsem chtěl několika známým zavolat ze svého mobilu, ale nemohl jsem se nikam dovolat, pak mi došlo, že to není problém Y2K, ale obyčejné přetížení telefonní sítě , asi stejné jako na ***svatého Valentýna***, a protože jsem na tento problém byl předem připraven , díky letáčku, který jsem našel v poštovní schránce, mohl jsem jít místo telefonování zase slavit.

C. Nový zákon o ochraně osobních údajů

Mgr. Pavel Vondruška, NBÚ

Není tajemstvím, že nový zákon o ochraně osobních údajů je na nejlepší cestě ke svému přijetí. Předkladatelem zákona je místopředseda vlády Ing. P.Mertlík, CSc. (přesněji: zástupcem navrhovatele, neboť jde o vládní návrh). Zákon by měl nahradit dnes již v mnoha ohledech nevyhovující zákon č. 256/92 Sb.. Tento starý zákon je kritizován zejména pro svou nekompatibilitu s požadavky EU.

Nový zákon vypracoval ÚSIS, vláda jej schválila už v září (svým usnesením č. 968 z 22. 9. 1998) a v Poslanecké sněmovně Parlamentu ČR tento zákon prošel počátkem listopadu prvním čtením.

Až dosud byla u nás problematika ochrany osobních údajů řešena zákonem č. 256/92 Sb., který se zabýval ochranou těchto údajů při jejich zpracování v informačních systémech. Tento zákon byl opravdu více méně proklamativní, neboť předpokládal zřízení samostatného úřadu, který by měl na starosti ochranou osobních údajů a který nikdy nevznikl. Dále definoval řadu pravidel, ale nedefinoval sankce za jejich porušení. Jeho dodržování se pak stalo opravdu jen věcí cti, konec konců prodej dat z různých databází a následné zavalování domácností nabídkami plenek a dalších předmětů s křidélky a bez křidélek nebylo a nemohlo být vlastně ani postihováno.

Nový zákon by měl odpovídat standardům EU. I on předpokládá vznik samostatného úřadu, jeho předseda a 7 inspektorů bude jmenováno přímo Senátem (a očekává se, že personálně a materiálně zřejmě vznikne odštěpením ze stávajícího ÚSISu). Nový zákon nejen upravuje nakládání s osobními daty (údaji) v informačních systémech jako zákon 256/92 Sb., ale zabývá se ochranou osobních dat bez ohledu na nějakou specifickou formu jejich zpracování a nakládání s nimi. Významné je jistě také nové pravidlo, že osobní údaje lze zpracovávat pouze se souhlasem fyzických osob, ke kterým se osobní údaje vztahují (kromě taxativně vymezených případů - evidence vymezené zákonem). To zní velice slibně. Jenže není všechno zlato co se třpytí a pravděpodobně není osobní údaj jako "osobní údaj".

Poslední poznámku vysvětlím na jednom z detailů, které byly diskutovány začátkem prosince na tiskové konferenci na ÚSIS, které se zúčastnil i místopředseda vlády ing. Pavel

Mertlík,CSc. , zástupci ÚSISu a pánové doc.Smejkal a doc.Mates (kteří, pokud vím, pod zákonem podepsáni nejsou a kteří zasvěceně odpovídali na dotazy novinářů a fakticky zákon vysvětlovali a hájili).

Nejprve uvedu definici osobního údaje, který požívá ochrany navrhovaného zákona :
...osobním údajem [je] jakýkoliv údaj týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze na základě jednoho či více osobních údajů přímo či nepřímo zjistit jeho identitu.
O osobní údaj se nejedná, pokud je třeba ke zjištění identity subjektu údajů nepřiměřeného množství času, úsilí či materiálních prostředků. …

Z diskuse vyplynulo, že např. e-mailová adresa není osobním údajem ve smyslu zákona (toto stanovisko hájil doc.Smejkal), neboť ji v obecném případě nelze ztotožnit s určitou osobou. Doc. Mates doplnil, že ani listovní adresa není osobním údajem ve smyslu právě navrhovaného zákona. Vysvětlil to příkladem domu, ve kterém bydlí tři osoby stejného jména, například otec, syn a děd a tedy z adresy nelze příslušnou osobu bez doplňujících údajů jednoznačně určit. Takže na "dárkové" balíčky s křidélky , oznámení o miliónových výhrách a nabídky speciálního zboží se můžeme i nadále těšit. Právě tyto křiklavé případy vnímané širokou veřejností jako zneužití osobních dat tedy jaksi asi postihnuty opět nebudou.

Jsem zvědav, jak otázka, co je a co není osobní údaj, bude v praxi posuzována a tak pravděpodobně potřeba právníků a soudních znalců asi výrazně stoupne. První problém v této oblasti bude řešen v souvislosti s tím, že " všechny subjekty, které chtějí zpracovávat osobní údaje, to musí oznámit Úřadu pro ochranu osobních údajů. Ten pak subjekt zaregistruje nebo mu dokonce zpracování nepovolí. Vzhledem k tomu, že každý zaměstnavatel eviduje na personálním oddělení osobní data svých zaměstnanců, tak úředníkům tohoto úřadu jejich nekonečnou práci nezávidím. Docela mě zaujala i možnost, že Úřad pro ochranu osobních údajů některému podnikateli zakáže tato data evidovat.

Další diskutabilní oblastí budou jistě rozsáhlé pravomoci kontrolorů, kteří mohou vstupovat do objektů určených k podnikání a zde provádět svoji kontrolní činnost. V rámci této činnosti mohou např. pořídit kopie obsahu paměťových médií nacházejících se u kontrolovaného (§ 37 písm. f) a to bez udání důvodu, mohou také požadovat zdrojové kódy programů (§ 37 písm. b), a to dokonce nejen po kontrolovaném, ale doslova i "po jiných osobách" (zde je omezení, že požadavek předložit zdrojový kód musí souviset s předmětem kontroly). Jinými osobami jsou pravděpodobně myšleni programátoři, kteří příslušné aplikace pro kontrolovanou organizaci vyvinuli. Jako bývalý programátor jsem nevěřícně kroutil hlavou a začal domýšlet některé důsledky a nakonec mne rozveselila představa, jak kontrolor žádá firmu Borland o zdrojový kód Delphi, neboť kontrolovaná osoba použila pro shromažďování svých dat databázovou aplikaci napsanou v tomto vývojovém prostředí.

Nejsem znalec zákonů v EU, ale obávám se, že tzv. kompatibilita tohoto zákona znamená, že náš zákon je nadmnožinou standardu EU a byl s českou snahou o zviditelnění vylepšen o některé "drobné" detaily s dalekosáhlými právními důsledky (zásah do Autorského zákona, možná i kolize se Zákonem o státním tajemství 148/98 Sb. apod.). Zákon sice malého českého občana asi moc neochrání, ale právnickým firmám slibuje docela dobrou živnost.

Plné znění navrhovaného zákona viz např.
http://www.usiscr.cz/cz/dokumenty/diskuse/ochrana_vladni.html
http://www.psp.cz/sqw/tiskt.sqw?0=3+CT=374+CT1=0

D. Soukromí uživatelů GSM ohroženo

Mgr. Pavel Vondruška, NBÚ

Po předběžném oznámení ze začátku prosince publikoval A.Shamir a A. Biryukov devátého prosince útok, který umožňuje v reálném čase a s malými náklady luštit algoritmus A5/1 ! Profesor Adi Shamir je již legendární kryptolog , jeden z trojice autorů, která publikovala před dvaceti lety RSA algoritmus, vynálezce zařízení TWINKLE (předvedené poprvé v Praze) a Alex Biryukov je mladý nadějný matematik, který se jako stipendista loni v květnu zúčastnil konference EUROCRYPT´99. Algoritmus A5/1 je silnější verze algoritmu, který chrání přenos hlasové a datové komunikace v GSM telefonech. Tuto verzi používá v Evropě (včetně ČR) více jak jedno sto miliónů uživatelů. Celkem je použit v 215 miliónech GSM telefonech po celém světě, z toho v 5-ti miliónech telefonů v USA. Algoritmus byl prolomen již dříve, ale útok vyžadoval speciální nákladný hardware a bylo zapotřebí něco mezi 2^40 až 2^45 kroků. Útok tedy mohla provést jen velká organizace, která disponuje dostatečným finančním zázemím. V článku, který byl nyní publikován, je popsán útok, který lze realizovat na PC s 128 MB RAM a dvěma pevnými disky o kapacitě 73 GB, dále je nutné zachytit prvé dvě minuty hovoru, popsanou analýzou lze pak nalézt klíč za méně než 1 vteřinu ! Protože GSM telefony vysílají frame každých 4.6 millisecondy, znamená to, že dvě minuty konverzace obsahují 120 * 1000/4.6 , tedy přibližně 2^15 framů. Počet nutných kroků k nalezení klíče je pak mezi 2^37 až 2^48 . Útok byl verifikován na aktuální implementaci algoritmu A5/1. Při těchto údajích je jasné, že útok může teoreticky provést hacker, který si svůj počítač dostatečně vylepší diskovou kapacitou a bude schopen naprogramovat algoritmus uvedený v publikované zprávě. Soukromí uživatelů GSM telefonů je tak vážně ohroženo.

Na závěr připomenu, že na rump session konference Crypto 99 David Wagner předvedl útok na slabší variantu výše uvedeného algoritmu A5/2 (tato varianta je určena pro GSM telefony ve východní Evropě). Ukázal, že vzhledem k velkému počtu pseudo-náhodných bitů je k prolomení této verze potřeba jen O(2^16) kroků.. Demonstroval tak, že se jedná o velice slabé zabezpečení této části komunikace.

Zdroj: Postscript souboru od Adi Shamira: http://cryptome.org/a5.ps (292K; 18 stran)

Pro přesnost dodejme, že GSM při komunikaci nepoužívá pouze algoritmus A5.
Implementovány jsou :

A3	autentizační algoritmus
A5/1	"silná verze" komunikačního algoritmu
nebo A5/2	"slabá verze" komunikačního algoritmu
A8	generace klíče pro hlasovou komunikaci

Detaily viz http://www.scard.org/gsm

E. Letem "šifrovým světem"

1. Eurotel není jediným, komu se díky Y2K problémům podařilo z roku 2000 vyrobit rok 1900. Zcela paradoxně se tak podařilo Microsoftu, který musel napravovat chyby v informacích týkajících se data uvedení knih na trh - uváděl totiž, že budou uvedeny na trh v lednu 1900.
   (31.12.1999, D.Dočekal, www.namodro.cz, rubrika IT-Y2K)

2. (Dr. P.Tesař) Problémem s Y2K se na své internetové stránce pochlubila i Česká národní banka.V souboru kurs00.txt ve kterém jsou všechny kurzovní lístky daného roku v textovém formátu se 3.ledna 2000 (staženo v 17:15) objevily následující informace:

   Datum |1 AUD|1 GBP |1 DKK| 1 EUR |100 JPY.....
   19000103|23,363| 57,807| 4,849 | 36,100 | 34,950 .....
   19000104|23,409| 57,601| 4,842 | 36,035 | 34,957 .....
   Pro nezasvěcené dodejme, že 19000103 je 3.ledna 1900 (mělo být 3.ledna 2000, tedy 20000103).
   Tato chyba byla však již následující den odstraněna.

3. Celosvětové odhadované náklady na přípravu výpočetní techniky na přechod do roku 2000 se odhadují na 500 miliard USD . Nejnižší publikovaný odhad je 50 miliard USD, nejvyšší 1 trilion USD. Pokud se vezmou i nepřímé náklady, pak nejvyšší odhady dosahují částky 3 triliony USD (zdroj: Newsweek).

4. Před rokem (v lednu 1999) mladá , teprve 16-ti letá irská studentka Sarah Flannery publikovala zprávu o novém šifrovém algoritmu na principu veřejného klíče, nazvaném Cayley-Purserův algoritmus. Uvedený algoritmus měl být rychlejší a lepší než RSA nebo ElGamal. Její práce vzbudila značnou pozornost. Problém byl v tom, že algoritmus nebyl zveřejněn. Publikovány byly jen srovnávací, výkonnostní testy. Celá práce, včetně algoritmu byla koncem roku 1999 zveřejněna , včetně dodatku (který také vypracovala Sarah Flannery) , ve kterém je algoritmus prolomen.
   An Investigation of a New Algorithm vs. the RSA http://cryptome.org/flannery-cp.htm

5. Některé upřesňující informace o přečtení (v našich novinách se psalo o rozšifrování) údajů ze starých magnetických záznamů - pásek STASI (tzv. SIRA archív) lze najít na níže uvedených webovských stránkách. Soubory nebyly zašifrovány, šlo spíše o technický problém čtení a rekonstrukce dat ze starých médií. Soubor F-22, který byl přečten, obsahuje úplný archív o agentech STASI. Přečteno bylo 63 035 dat vztahujících se k agentům - krycí jména, období kdy agent pracoval (okolo 47 000 agentů od roku 1950). Podle prvých zpráv vyplývá, že v roce 1989 bylo činných na 15000 agentů. Bezpečnostní experti uvedli, že přibližně 1/3 uvedených agentů nebyla do této doby odhalena.
   http://www.spiegel.de/spiegel/vorab/0,1518,56060,00.html
   http://www.heise.de/tp/deutsch/inhalt/te/1800/1.html
   http://www.snafu.de/~bstu/hva-sira/index.htm
   http://cryptome.org/gdr-f22.htm

6. Německá vláda se rozhodla pomoci při vývoji GPG . GPG bude volně šiřitelný program kompatibilní s (některými verzemi) PGP.
   http://www.nytimes.com/library/tech/99/11/cyber/articles/19encrypt.html
   http://www.gnupg.de/presse.en.html

7. NSA patentovalo a zveřejnilo technologii zvanou ECHELON. ECHELON systém umožňující automatické prohledávání a třídění mnoha komunikačních zdrojů (internet, telekomunikace) podle zadaných slov, klíčů a kritérií, který NSA použila i proti svým spojencům v Evropě, není jistě třeba představovat. Patentováním této technologie se NSA vlastně otevřeně k tomuto systému a k možnostem tohoto systému přihlásilo. (Kontrola 3 miliard spojení denně, včetně telefonů, mobilních telefonů, e-mailů, satelitních přenosů, downloadů apod.; některé zdroje uvádějí kontrolu až 90% všech spojení na internetu). Patent dostal číslo : U.S.Patent 5,937,422.
   Patent:
   http://www.patents.ibm.com/details?&pn=US05937422__
   Rozbor:
   http://trec.nist.gov/pubs/trec6/papers/nsa-rev.ps
   http://trec.nist.gov/pubs/trec7/papers/nsa-rev.pdf
   Nové články o ECHOLONU:
   http://www.independent.co.uk/news/Digital/Features/spies151199.shtml
   http://www.independent.co.uk/news/Digital/Features/spies221199.shtml
   http://www.nytimes.com/library/tech/99/12/cyber/articles/04spy.html
   Obecné informace o ECHELONu:
   http://cryptome.org/echelon-dk.htm
   http://cryptome.org/sigint-dk.htm
   http://crytpome.org/echelon-dk2.htm
   http://www.echelonwatch.org
   http://www.wired.com/news/print/0,1294,32586,00.html
   Vynikající článek:
   http://mediafilter.org/caq/cryptogate

8. Případ, kdy se "neznalý" uživatel snažil využít "anonymní" e-mail server k odeslání hrozby teroristického - bombového útoku je popsán na URL adrese :

   http://www.zdnet.com/zdtv/cybercrime/news/story/0,3700,2324068,00.html

   Atentátník zaslal svoji hrozbu z e-mail adresy shadowmega@hotmail.com, kde si pro tento účel založil anonymní poštovní schránku. Policie kontaktovala Hotmail a požádala o spolupráci. Hotmail předal k příslušnému datu a času použitou IP adresu vlastníka u Americane Online. Použitím informace AOL policie přesně atentátníka identifikovala a zatkla jej v jeho bytě v Brooklynu. Závěrečná pointa celého příběhu je, že potřebné informace nemusela policie požadovat od serveru Hotmail, neboť tyto informace jsou dostupné v hlavičce odeslaného e-mailu.

9. Národní bezpečnostní úřad zpřístupnil na internetu digitální formu "BEZPEČNOSTNÍHO DOTAZNÍKU ORGANIZACE" . Organizace, které si vyzvedly disketu s překladačem (soubor DOTAZNIK.EXE), si mohou porovnat pomocí hashe (standard MD5, jednoduchý program pro výpočet je na webovské stránce také k dispozici), zda vlastní poslední datový formulář (soubor FORM.BIN) a pokud ne, mohou si aktuální verzi stáhnout. Kompatibilita datového formuláře s již vyplněnými daty všech předchozích verzí je zaručena a organizace nemusí vyplněná data znovu přepisovat.
   http://www.nbu.cz

10. Od 3.1.2000 nabývá platnost Zákon č. 106/1999 Sb „o svobodném přístupu k informacím". Na obvodních úřadech byly vytvořeny informační kanceláře, kde lze zdarma nebo za úplatu (při větší náročnosti při vyhledání dat) požadovat veřejné informace dle znění výše uvedeného zákona. Pokud Vás zajímá např. plat primátora hl. města Prahy, budete asi zklamáni, informační kancelář Magistrátu hlavního města tento údaj nesděluje.

F. Závěrečné informace

URL adresa na níž můžete najít předchozí sešity GCUCMP, informace o přednáškách z kryptologie na MFF UK a další související témata :

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

Spojení :
hruby@gcucmp.cz (Group of Cryptology Union of Czech Mathematicians and Physicists)
- oficiální e-mail adresa kryptologické sekce JČMF
pavel.vondruska@post.cz - osobní poštovní stránka
pavel.vondruska@sms.paegas.cz - jen 160 znaků !
mobil : Mgr.Pavel Vondruška 0603 436 341

Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (internet, noviny) nebo se jedná o původní články podepsané autory. Oficiální informační sešit je primárně určený pro členy "Kryptologické sekce Jednoty matematicko-fyzikální " (GCUCMP). Pokud má někdo zájem o zasílání tohoto sešitu, stačí se zaregistrovat e-mailem na adrese hruby@gcucmp.cz (subject, předmět : Crypto-World).

Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.