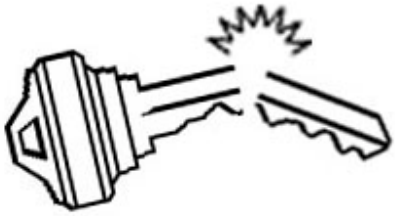
Informační sešit GCUCMP
Crypto-World 2/2000

Připravil : Mgr.Pavel Vondruška,
člen GCUCMP, IACR, ISACA.
Sešit rozesílán registrovaným čtenářům,
registrace na adrese hruby@gcucmp.cz , subject : Crypto-World
(76 e-mail výtisků)
Uzávěrka 6.2.2000



OBSAH : **Str.**

Sešity GCUCMP budou rozesílány ve formátu PDF

Vzhledem k tomu, že od příštího čísla bude distribuován sešit GCUCMP ve formátu PDF, dovoluji si zařadit následující obecnou informaci od jednoho z čtenářů našeho časopisu - Martina Kalába. Jeho článek zdůvodňuje, proč jsme se rozhodli právě pro tento formát.

Na internetu (www.mujweb.cz/veda/gcucmp) jsou od 25.1.2000 všechna uložená předchozí čísla našeho sešitu již zkonvertována do PDF formátu a je možné si je odtud v tomto formátu stáhnout. Pokud někdo z odběratelů přesto dává přednost formátu MS Word 97, stačí poslat e-mail na adresu hruby@gcucmp.cz a jako předmět uvést sešit-WORD.

Pro ty, kteří psali, že na www stránce ke změně nedošlo, nebo že při přenosu je hlášena chyba, si dovoluji poznamenat, že je nutné buď smazat cache nebo stisknout z www prohlížeče tlačítko RELOAD (nebo ekvivalent). Při změně jsem vyměnil příslušné soubory a ponechal jejich původní název; pokud z minulé "návštěvy" zůstal v cachy uložen starý soubor, je mu dána přednost před stahováním nového - upraveného z www stránky ….Návrat na hlavní stránku je pouze pomocí tlačítka Back nebo Zpět ve vašem prohlížeči. Stránku bude možné (cca od 16.2.2000) najít na www.seznam.cz oddíl věda / informatika .

A. Dokumenty ve formátu PDF

Martin Kaláb , FEL, ČVUT

PDF představuje v současné době snad nejuniverzálnější formát pro přenos a prezentaci dat. Soubory vytvořené ve formátu PDF lze prohlížet, upravovat a dál zpracovávat nezávisle na platformě, spolehlivě pracuje na PC, MAC i UNIX. PDF dokument nepotřebuje software, ve kterém byl vytvořen, výsledný soubor se přesto zobrazí nebo vytiskne v naprosto shodném grafickém a typografickém provedení. PDF soubory mohou uživatelé prohlížet také přímo v internetových prohlížečích.

Silnou stránkou PDF formátu je jeho snadná editovatelnost. Na poslední chvíli, např. před osvitem, lze opravit chybu v textu nebo měnit barevnost, velikost obrázků a další. Zneužití dokumentu zabrání možnost nastavení hesla.

A čím se soubory PDF prohlížejí?

PDF soubory mohou sloužit nejen k přenosu dat a k archivaci, ale také k přímému prohlížení na monitoru - k tomuto účelu existuje bezplatný program Adobe Acrobat Reader, který si můžete stáhnout například na adrese http://www.adobe.com/products/acrobat/readstep.html. PDF formát však umí otevřít například i Illustrator 7.0, Corel Draw 7.0 a další programy.

Proč je lépe získávat dokumenty ve formátu PDF než dokumenty vytvořené MS Wordem?

První nesporná výhoda PDF oproti Wordu byla již zmíněna, jedná se o kompatibilitu mezi všemi běžnými platformami. Dalším důvodem je stabilita dokumentu, jednou vytvořený PDF bude vypadat stejně i po přenosu na jiný počítač, jistě jste se již setkali se zdánlivě samovolným „rozhozením“ dokumentu vytvořeného ve Wordu. Pro tyto vlastnosti je formát PDF využíván profesionály na celém světě a pomalu se stává i standardem v osvitové technice.

Pokud vás ani tyto výhody nepřesvědčily ke čtení Crypto-Worldu ve formátu PDF je tu další výhoda oproti Wordu. Naprostá absence maker a tudíž i virů, tedy alespoň prozatím, protože jak bylo zmíněno v některém z minulých čísel, padl již mýtus přenosu virů v těle e-mailu.

B. Kevin Mitnick na svobodě

Mgr. Pavel Vondruška, NBÚ

Na osobní stránce Kevina Mitnicka (www.kevinmitnick.com/home.html) jsou umístěna dvě počítadla, jedno odpočítalo 4 roky 11 měsíců 6 dní 7 hodin 30 minut a druhé se mělo zastavit na nule. Prvé odpočítávalo dobu, kterou strávil za mřížemi a druhé - kolik času zbývá do jeho propuštění. Kevin byl propuštěn v pátek 21.1.2000 v 6.30 a.m. (chybička v perlovém scriptu způsobila, že se druhé počítadlo nezastavilo, ale přetočilo se a nyní odpočítává vlastně dobu, která se rovná 1 rok - doba po kterou je Kevin na svobodě). Nejhledanější počítačový zločinec byl propuštěn na svobodu po necelých pěti letech vězení.

Materiálu je o Kevinovi opravdu dost. Udává se, že jen důkazní spis čítá neuvěřitelných 200 miliónů stránek. Orientovat se v celém případu je docela těžké. Uvedu aspoň základní informace. Počítačového zločince Kevina Mitnicka, po němž pátrala už několik let, zatkla FBI v únoru 1995. Nebyl to obyčejný studentský počítačový hacker , zajímal se o technologii telefonů. Již jako 15-ti letý se naučil odposlouchávat telefonní hovory, dostat se do digitální ústředny, telefonovat zdarma, řadit hovory. Miloval mobilní telefon a jeho potenciální možnosti. Mobilní telefon se mu ovšem stal osudným (viz dále). Mitnick neovládal dokonale UNIX, a proto se spojil s jistým izraelským hackrem - snad studentem nebo mladým vědeckým aspirantem v Izraeli. Identita tohoto společníka nebyla nikdy odhalena. Jeho tajný společník měl značku jsz a vyznal se v průniku do UNIXOVÝCH serverů (ostatně ochrana těchto serverů byla ještě v plenkách). Společně hackovali systémy mobilních společností Oki, Motorola, Nokia a získávali především zdrojové kódy. Mitnick sám byl vynikající odborník na "telefonii", ale jeho sílu umocňovala schopnost vymámit tajné informace od lidí pomocí telefonu. Často zavolal na ústřednu a zde se dozvěděl potřebné informace. Byl schopen sestavit ze střípků informací to, co potřeboval. Kevin údajně uměl dokonale měnit hlas, vystupoval velice přesvědčivě a nenápadně. Tři roky se nabourával, kam se mu zlíbilo. Kradl i čísla kreditních karet, software, citlivá data apod. Toto vše se událo mezi červnem 1992 a únorem 1995. Kevinův konec začal na vánoce 1994, kdy pronikl pomocí internetu do osobního počítače vynikajícímu odborníkovi na počítačovou bezpečnost Tsutomu Shimomurovi. Tento odborník potom pomohl FBI Kevina vystopovat. Pomocí svého telefonu se Kevin hlásil z města Raleigh. Zjistilo se, že se připojuje na uzel Netcomu pomocí mobilního telefonu v noci. Agenti FBI sestavili zařízení , které jim ze zachyceného signálu mobilního telefonu dovedlo lokalizovat pozici volajícího. Kevin (který již v roce 1989 byl odsouzen na jeden rok za zneužití počítače) byl zaměřen a zadržen. V té době bylo Kevinu Mitnickovi již 33 let.

Kevin Mitnick byl postaven před soud. Zde čelil obvinění za pokusy o vniknutí nebo za vniknutí do desítek serverů včetně Netcom, Colorado Supernet, Motorola, Nokia, Fujitsu, Novell, NEC, Sun Microsystems a University of Southern California. Teoreticky mu hrozilo vězení až na 100 roků. Kevin se nedoznal. Ve světě začalo cyberpunkové hnutí na jeho podporu. Desítky internetových stránek žádalo SVOBODU PRO KEVINA. Kevin byl představován jako hacker, který má být exemplárně potrestán, aby se potlačila cyberpunková svoboda. V březnu roku 1999 - po čtyřech letech procesu - se Kevin přiznává (za slib trestu do 5-ti let).

Kevin Mitnick byl propuštěn v pátek 21.1.2000 v 6.30 hod a.m. (www.2600.com) .

(Nezkrácené znění tohoto článku viz Pavel Vondruška - COMPUTERWORD č.6/2000)

C. Velká Fermatova věta (historické poznámky)

Mgr. Pavel Vondruška, NBÚ

Dne 23.6.1993 oznámil profesor Andrew Wiles, že dokázal Velkou Fermatovu větu (v důkazu byla později objevena chyba, která byla odstraněna v září 1994 , v roce 1995 byl důkaz podroben revizi a uznán platným). Více než 200 stran obtížných výpočtů svědčí o velikém intelektuálním úsilí, které musel Wiles vynaložit. Výjimečnost Velké Fermatovy věty spočívá v tom, že se jednalo po dlouhou dobu o synonymum pro velice těžký, ne-li neřešitelný problém. Po více jak tři sta padesát let se marně snažili nejlepší matematici této planety najít důkaz věty, která zní: neexistují přirozená čísla, která řeší rovnici $x^n + y^n = z^n$, kde n je celé číslo větší než 2 . Fermat zformuloval úlohu někdy kolem roku 1637, sepsal ji latinsky a prohlásil, že ji umí dokázat. Současně však dopsal , že našel skutečně nádherný důkaz tohoto tvrzení, ale "okraj je však úzký na to, aby se na něj důkaz vešel." (… cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.). Fermat zanechal mnoho takovýchto "poznámek na okraji". Matematici, kteří přišli po něm, je chápali jako zformulované problémy a v průběhu let je všechny postupně vyřešili. Až na právě tento jediný. Proto toto tvrzení nazvali Fermatovou poslední větou (Fermat Last Theorem - FLT). V českých zemí se ovšem vžil název Velká Fermatova věta , snad pro svoji obtížnost nebo jako protiklad názvu jiného jeho tvrzení Malé Fermatovy věty. Ubíhala léta a staletí a tato věta nebyla dokázána ani vyvrácena. Když ve dvacátých letech tohoto století bylo dokázáno, že v každém uzavřeném, bezesporném systému axiomů existuje nedokazatelné tvrzení, někteří matematici zajásali : ano takovým tvrzením je v systému axiomů naší matematiky Velká Fermatova věta. Proto nám její důkaz či vyvrácení stále unikalo… Věta zde však stále byla a její němá výzva a poznámka Fermata o elegantním důkazu doslova dráždila celé další generace matematiků.

V roce 1955 byl formulován problém , který zjednodušeně říká, že každá eliptická křivka je ve skutečnosti vyjádřitelná jako modulární forma (hypotéza Taniyamova-Shimurova, TS-hypotéza). V roce 1985 si Gerhard Frey uvědomil souvislost mezi eliptickými křivkami a některými důsledky Velké Fermatovy věty. Dokonce je brzy dokázáno tvrzení, které zjednodušeně říká, že pokud existuje řešení Fermatovy rovnice, pak lze s jeho pomocí vytvořit eliptickou křivku, která není modulární a byla by tak popřena platnost TS- hypotézy. K důkazu Fermatovy věty tak již stačí málo - důkaz TS-hypotézy.

Andrew Wiles se o FLT již od mladí živě zajímal. Koncem osmdesátých let si uvědomil, že snad je nalezen klíč k jejímu důkazu a začal horečně pracovat, aby splnil svůj celoživotní sen - najít důkaz Velké Fermatovy věty. V roce 1993 se mu daří dokázat hypotézu Taniyamovu-Shimurovu o modulárních formách eliptických křivek. Kruh se uzavřel. Protože platí TS-hypotéza, nemůže existovat řešení $x^n + y^n = z^n$, kde $n > 2$, neboť pak by se našla eliptická křivka, která by přes platnost TS-hypotézy neměla modulární formu.

Pokud Fermat důkaz svého tvrzení znal, pak komplikovaný a velice moderní Wilesův důkaz to určitě nebyl. Fermatův důkaz mohl být založen jen na algebraických úvahách. Profesor Victor Sorokin se vydal touto cestou a opravdu - začátkem tohoto roku (4.1.2000) rozesílá svým známým prvé sdělení o tom, že se mu podařilo najít "jednoduchý" důkaz FLT. Během týdne důkaz dokončuje, přepisuje jej do angličtiny (omlouvá se za chyby v textu) a již 11.1.2000 jej rozesílá k posouzení. Děkuji touto cestou Dr.Ladislavu Andrejovi, CSc. (člen GCUCMP), který důkaz poskytl k otištění. Profesor Sorokin předkládá i touto cestou svůj důkaz k veřejné diskusi.

D. Fermat Last Theorem

Prof. Victor Sorokine (VSorokine@Bigfoot.com)

The equation $\mathbf{a^n + b^n = c^n}$, or $a^n + b^n - c^n = 0$, (1°)
where n is prime and n > 2, has no whole number solution (except a = b = c = 0).
All the proofs are done in a scale of notation with a **prime** base **n**.
Symbols used: a_k — digit of the k-th rank in the number a; $a_{(k)}$ — ending of k+1 digits of the number a.

3-rd prime proof *(about which P.Fermat had wrote)*
Let's the equation (1°) has a solution {a, b, c} and $a^n + b^n - c^n = 0$, (2°)
where, it is evident, a + b – c (or b – c — for the case $a_0 = 0$) = d ≠ 0 [it is easy to show that d > n].. (3°)
Let's write down the number d in the form: d = a + b – c =
$= (a_0 + b_0 - c_0) + (a_1 + b_1 - c_1)n^1 + (a_2 + b_2 - c_2)n^2 + ... + (a_s + b_s - c_s)n^s + ...$ (4°)
Let's write down the equation (2°) in the form: $(a_{(s)} + n^{s+1}a')^n + (b_{(s)} + n^{s+1}b')^n - (c_{(s)} + n^{s+1}c')^n =$ 0, or (5°)
$(a_{(s)}^n + b_{(s)}^n - c_{(s)}^n) + n^{s+2}(a'a_{(s)}^{n-1} + b'b_{(s)}^{n-1} - c'c_{(s)}^{n-1}) + n^{2s+3}P = 0$, (6°)
where $n^{2s+3}P$ is the sum of the items with the factor $n^{2s+3}P$, $(a_{(s)}^n + b_{(s)}^n - c_{(s)}^n)_{(s+2)} = 0$ (6a°)
and, if a_0, b_0, and $c_0 \neq 0$, $(a_{(s)}^{n-1})_0 = (b_{(s)}^{n-1})_0 = (b_{(s)}^{n-1})_0 = 1$ (the Little Fermat Theorem or its corollary). (6b°)
Putting $a' = a_{s+1} + a''$, $b' = b_{s+1} + b''$, $c' = c_{s+1} + c''$ in (6°), we have:
$(a_{(s)}^n + b_{(s)}^n - c_{(s)}^n) + n^{s+2}(a_{s+1}a_{(s)}^{n-1} + b_{s+1}b_{(s)}^{n-1} - c_{s+1}c_{(s)}^{n-1}) + n^{s+3}Q = 0$, (7°)
or (taking 6b°) $(a_{(s)}^n + b_{(s)}^n - c_{(s)}^n) + n^{s+2}(a_{s+1} + b_{s+1} - c_{s+1}) + n^{s+3}Q^* = 0$, (8°)
whence (taking 6a°) $a_{(s)}^n{}_{s+3} + b_{(s)}^n{}_{s+3} - c_{(s)}^n{}_{s+3} = -n^{s+3}(a_{s+1} + b_{s+1} - c_{s+1})$, where s = 0, 1, 2, ... (9°)
But it mean that each cipher $(a^n + b^n - c^n)_{s+3}$ coincides with $-d_{s+1}$ (for s = 0, 1, 2, ...) and $(a^n + b^n - c^n)_{(1)} = 0$. Therefore, $a^n + b^n - c^n = -n^2(a + b - c - a_0 - b_0 + c_0) \neq 0$ (cf. 2°). (10°)
[If before the operation 5° to transform b_0 into $b_0 = 1$ (to multiply the equation 2° by such a number g_0^n, that $(b_0g_0)_0 = 1$), then $a_0 + b_0 - c_0 = 0$.]
If, for example, $a_0 = 0$, then in (8°) taking (7° and 6a°) $(a_{(s)}^n + b_{(s)}^n - c_{(s)}^n) + n^{s+2}(b_{s+1} - c_{s+1}) + n^{s+3}Q^* = 0$
and (10°) has the form: $a^n + b^n - c^n = -n^2(b - c) \neq 0$ (cf. 2°). (10a°)

The truth of FLT is evident if to take in account that all other cases (except those cases which can be reduced to proven case n = 4) can be reduced to the present case.

(verze důkazu předložená 11.1.2000 k veřejné diskusi)

E. Zákon o elektronickém podpisu otevírá cestu do Evropy ?

(RNDr. Jiří Souček, DrSc., RNDr. Jaroslav Hrubý, CSc., Mgr. Antonín Beneš, Mgr. Pavel Vondruška)

Zákon o elektronickém podpisu (poslanecký návrh) postoupil do dalšího čtení (resp. "je přikázán do výboru"). Vzhledem k tomu, že obsahuje některé nejasné pojmy (viz článek Dr.Součka nebo obsáhlá polemika na www.spis.cz), ale především proto, že není kompatibilní s direktivou EU schválenou v Bruselu 13.12.1999, rozhodli se autoři sepsat některé své připomínky a ty oficiálně zveřejnit a předat k případnému zapracování. Zde je otištěna prvá pracovní verze tohoto dokumentu. Vaše připomínky, jako členů GCUCMP a odborné veřejnosti sdružené kolem GCUCMP, můžete zaslat na adresu: soucekj@karlin.mff.cuni.cz nebo na hruby@gcucmp.cz (předmět : zákon) .
Společně tak můžeme dosáhnout opravy předloženého návrhu o elektronickém podpisu tak, aby vyhověl přísným kritériím direktivy EU.

Na adrese http://www.mujweb.cz/veda/gcucmp/mff/kucharka.htm bude v nejbližších dnech uložena "kuchařka", která popisuje proces elektronického podpisu, postavení a význam certifikačních autorit, aktuální stav poskytování služeb v této oblasti v České republice. Jedná se o základní informace, které autoři sepsali za jiným účelem, ale ukázalo se, že pro vysvětlení nejzákladnější problematiky kolem elektronických podpisů co nejjednodušším jazykem je dobře použitelná, a proto pokud chcete šířit osvětu v tomto směru, doporučujeme ji využít.

****

Pracovní verze z 5. 2. 2000

Se vstupem do 21.století je více než kdykoliv předtím jasné, že prosperující společnost musí zvládnout nejmodernější technologie, zapojit se do elektronického obchodu, zajistit bezpečnou a důvěrnou komunikaci mezi jednotlivými občany, zajistit ochranu osobních dat, zajistit vyřizování požadavků občanů na státní správu, zavést elektronické peníze a v neposlední řadě zajistit uznání elektronického podpisu jako jednoho se základních kamenů elektronické společnosti. Lidé ve společnosti, která nezajistí tyto zcela zásadní úlohy, nemohou počítat s tím, že se zařadí mezi moderní, prosperující národy. Při vytváření prostředí legislativního, ekonomického, vědeckého je potřeba respektovat daný stav v Evropské Unii. V případě základních zákonů a právních norem pak jsme (pokud to míníme s naším vstupem do EU vážně) přímo povinni slaďovat naše zákony se zákony platnými v EU.

U nově přijímaných zákonů je tedy jedinou správnou cestou tyto zákony již přijímat ve tvaru, který je slučitelný se zákony v EU. V současné době je předložen k připomínkám zákon o elektronickém podpisu. Zákon o elektronickém podpisu je naprosto nezbytným základem k budování moderní společnosti, v pravém slova smyslu nám může otevřít dveře do velkého obchodu 21-století. Po prostudování jeho návrhu však nabýváme dojmu, že je nutné akceptovat řadu připomínek slaďujících náš zákon se zákonem o elektronickém podpisu platným v EU, aby nám jeho přijetí dveře do EU naopak pevně nezamkl a to klíčem opravdovým a ne jen digitálním.

V direktivě EU schválené v Bruselu 13.12.1999 se přímo říká : "Členské státy Evropské Unie uvedou v platnost nezbytná legislativní, obecně závazná a správní opatření, aby dosáhly souladu s touto direktivou před 19.7.2001. Komise Evropské Unie provede přezkoumání ohledně zavedení této direktivy a podá zprávu Evropskému parlamentu a Radě do 19.7.2003." Mnoho času tedy nezbývá. Urychlené přijetí jakéhokoliv zákona, který by tuto direktivu nerespektoval, by mohlo naši cestu jen zkomplikovat.

Pokusme se jen v několika bodech ukázat na některé sporné okamžiky v návrhu poslaneckého zákona o elektronickém podpisu. Dovolujeme si předeslat, že tím nijak nechceme snižovat práci , která již byla na přípravě zákona o elektronickém podpisu udělána a která je záslužným počinem.

Pro další výklad a možnost srovnávání si zavedeme označení DEU (Direktiva Evropské Unie) a PEP (poslanecký návrh zákona o elektronickém podpisu).

V materiálech jako sporné se nám jeví například následující:

PEP: Udělování povolení k působení jako ověřovatel informací, jakož i dohled nad dodržováním tohoto zákona náleží Úřadu.

DEU: Členské státy nepodmiňují poskytování certifikačních služeb žádnému předchozímu oprávnění.

DEU totiž mimo jiné chápe, že mohou vznikat v jejich terminologii uzavřené skupiny, které pro své vlastní potřeby chtějí využívat elektronický podpis (např. v rámci malé, ale dynamické společnosti). Elektronický podpis dokumentů mezi členy takovéto uzavřené skupiny DEU má být ve smyslu zákona také chápán jako podpis a v soudních případech nesmí být odmítnut jako soudní důkaz . Je samozřejmě nelogické, aby na takovouto uzavřenou skupinu, která si pro své účely vybuduje malou vlastní certifikační autoritu (dále CA), byly kladeny požadavky stanovené v PEP . Tedy, aby žádal o povolení Úřadu, povolil vstup kontrolorům ke všem svým prostředkům a údajům, vystavoval se pokutě 10 miliónů (případně 20 miliónů) apod. Je nutné připomenout, že ve světě úspěšně funguje i celá řada certifikačních autorit, kde se lze zaregistrovat zadarmo, čtenář může ozkoušet např. adresu www.pgp.cz . Zde certifikát přiřadí jednoznačně poštovní adresu k veřejnému klíči. Existence takovýchto CA dle PEP nebude pravděpodobně možná, pokud ovšem provozovatel nezažádá ve smyslu zákona úřad o "licenci" a splní vše, co je s tím spojeno.

Liberální přístup DEU se proti PEP promítá do dalších souvisejících doporučení a umožňují skutečně vytvořit tržní prostředí i v oblasti CA (v terminologii PEP ověřovatelů informací). Vysoké miliónové pokuty navrhované v PEP těžko povzbudí vznik CA na našem území a zabraňují tak tržnímu prostředí. Služby CA potom budou neúměrně drahé a to i v oblastech, kde DEU předpokládá levné služby (styk státu s občany). Konečně drahé poskytování služeb vyplývající z velice tvrdých pravidel a sankcí v této oblasti není ani v zájmu "ověřovatelů informací", občan totiž použije pravděpodobně levnější nabídku zahraničních CA . Námitky typu, že jde o bezpečnost občana - nesmí být podveden, jsou velice diskutabilní. Je potřeba si uvědomit, že ve hře je více subjektů - ne jenom občan, který si chce zaregistrovat svůj podpis, a "ověřovatel informací". Je zde především dále subjekt, se kterým občan chce komunikovat (banka, obchod, státní úřad, přítel).

Každý z těchto subjektů vyžaduje (již z podstaty věci) jiný stupeň zabezpečení veřejného klíče a podle svých požadavků na bezpečnost bude to on, kdo si zvolí některého "ověřovatele informací" , který bude mít jeho důvěru. Těchto ověřovatelů může na základě vzájemného uznávání certifikátů být více. Podstatné je, že "ověřovatel informací" musí zveřejnit svoji bezpečnostní politiku a bojovat o stupeň důvěry na potenciálním trhu. Jeden subjekt si tedy bude vybírat především podle rozsahu nabízených služeb a ceny (zjednodušeně řečeno ten, kdo si chce zaregistrovat svůj veřejný klíč) a druhý subjekt si bude volit toho "ověřovatele informací", který splňuje jeho požadavky na zabezpečení uložených dat a samozřejmě podle dalších kritérií - obecně nazvaných důvěra.

Není nám známo, proč PEP na rozdíl od DEU neumožňuje registraci klíče právnické osoby (v praxi je toto obvyklé, viz např. řád českého provozovatele certifikačních služeb I.CA, www.ICA.CZ). I zde bude potřeba zákon sladit s touto závaznou direktivou.

Samotná definice zaručeného elektronického podpisu je v návrhu PEP rozporná. V pátém paragrafu se říká, že k tomu, aby elektronický podpis byl zaručeným elektronickým podpisem určí Ministerstvo vyhláškou podmínky k tomu nezbytné. V šestém pak, že .. strany

se mohou dohodnout, že elektronický podpis budou ve vzájemných vztazích považovat za zaručený elektronický podpis. Z odborného hlediska (viz DEU) by zaručený podpis měl splňovat jisté bezpečnostní požadavky a neměl by záviset na prosté vůli osob.

Pokud jde předkladatelům o to, aby mohl sloužit elektronický podpis jako soudní důkaz, pak by bylo možná lepší použít požadavek DEU (viz další odstavec). Jiný další důvod, proč by se měly strany dohodnout, že elektronický podpis budou ve vzájemných vztazích považovat za zaručený elektronický podpis, totiž není zřejmý.

V DEU je tato situace řešena takto:

Členské státy se postarají o to, aby právní účinek a přípustnost jakožto soudní důkaz nebyly u elektronického podpisu **odmítány jen proto**, že

- podpis je v elektronické podobě nebo
- že k němu není zaručený certifikát, nebo
- že k němu není zaručený certifikát, vydaný licencovaným poskytovatelem certifikační služby, nebo
- že není vytvořen zabezpečeným zařízením pro tvorbu podpisu

Tento přístup je totiž **klíčový**. Z něj přímo plyne, že elektronický podpis je před soudem **roven** obyčejnému podpisu, připouští se existence jiných podpisů než se zaručeným certifikátem (PEP splňuje), připouští na trhu existenci nelicencovaných certifikačních autorit, DEU připouští použití všech možných , třeba i neatestovaných a neschválených zabezpečených zařízení pro tvorbu podpisu.

PEP na rozdíl od DEU připouští pouze ty "ověřovatele informací", které jsou k tomu oprávněny Úřadem. DEU pouze požaduje, aby členské státy EU se postaraly o adekvátní systém umožňující kontrolu (nikoliv vydávání povolení) poskytovatelů certifikačních služeb, působících na jeho území a vydávajících oficiální certifikáty veřejnosti.

Zároveň s návrhem PEP je nutné (podobně jako v DEU) formou příloh specifikovat požadavky na zabezpečená zařízení pro tvorbu elektronického podpisu. Tato zařízení musí pomocí odpovídajících technických prostředků a postupů přinejmenším zaručovat pro data použitá k tvorbě elektronického podpisu neopakovatelnost, přiměřenost jejich utajení a dostatečnou jistotu, že je nelze odvodit jiným způsobem, jejich ochranu proti padělání a zneužití někým jiným než legitimním výstavcem. Tato zařízení nesmí měnit data určená k podpisu a musí umožnit výstavci jejich kontrolu před podepisováním.

Tato připomínka je pro realizaci zavedení elektronického podpisu do praxe klíčová. Současně s přípravou zákona je nutné dát do souběhu i práce **normotvorné** v této oblasti a připravit alespoň hrubá znění souvisejících vyhlášek. Zde doporučujeme vycházet z prověřených norem např. NIST (National Institute of Standards and Technology) v USA.

Ke zde použité terminologii poznamenáváme, že je nejednotná, protože používáme znění PEP , DEU a někdy zvyklostní terminologii zavedenou v české odborné literatuře. Upozorňujeme tímto na potřebu unifikování terminologie i v této oblasti.

Závěrem lze shrnout , že

1) PEP je nutné v každém případě poopravit takovým způsobem, aby vyhověl požadavkům EU, tak jak je obsaženo v DEU ;
2) neliberální přístup použitý v PEP oproti liberálnímu přístupu DEU je nesprávný, protože jednak vykazuje zřejmé rysy lobbismu velkých firem a jednak by naši digitální ekonomiku silně diskriminoval v liberálnějším prostředí EU ;
3) sladění parametrů našeho ekonomického prostředí, technologie, zákonů a norem s EU je prioritním cílem vládního i opozičního politického programu a k tomu je třeba mít zákon o elektronickém podpisu takový, který je maximálně shodný se zákonem EU. Opačný postup by torpédoval naše úsilí o vstup do EU.

F. Letem šifrovým světem

1. Na adrese ftp://ftp.comlab.ox.ac.uk/pub/Documents/techpapers/Richard.Brent/champs.txt je možné získat soubor champs.txt, který obsahuje přehledovou zprávu o velkých faktorizačních činitelích nalezených pomocí metody faktorizace založené na eliptických křivkách (elliptic curve factoring - ECM). Metoda se používá (a je vhodná a úspěšná) k odštěpení "malého" faktoru z velkého čísla.
   Současným "šampiónem" je činitel
   4840612542768783681257268707891802319959648700949169 37
   (dělitel čísla : (6^43-1)^42+1)). Tento faktor byl získán koncem minulého roku (26.12.1999) pomocí metody GMP-ECM a získali jej Nik Lygeros společně s Michaelem Mizonym . Doporučuji stáhnout.

2. Na adrese http://www.gchq.gov.uk/careers/ naleznete informace o volných místech v anglické GCHQ (ekvivalent známější americké NSA). GCHQ chce obsadit celkem 100 svých volných míst. Hledají se především odborníci na komunikace, počítače, jazykoví odborníci a matematici. Matematikům se nabízí práce na : " analysis of complex signals, code-breaking techniques and code construction " (prostě luštění cizích zpráv). Stačí vyplnit přihlášku , dozvíte se , že přednost mají mladí zájemci s PhD, znalostmi jazyků ze specifikovaných oblastí (např. východní Evropa) a zájemci, kteří dokáží **vyluštit text** uložený na webovské stránce organizace (zájemce z ČR zklamu - požaduje se národnost anglická). O zkušebním textu se na jiném místě dozvíte pouze to, že jej musíte vyluštit do 25.2.2000, že je rozdělen do 5-ti částí, každá část obsahuje 5 znaků, každá část je zamaskována nebo přímo ukryta v jiné části www stránky. Získané části je potřeba poskládat ve správném pořadí a tuto zprávu přiložit k žádosti o místo. Prozatím zaslalo správné řešení 14 žadatelů.

3. Kdo se blíže zajímá o aktivity hackerů, měl by se podívat na stránku www.2600.com. Stránka mimo jiné obsahuje archiv průniků hackerů, kteří se kolem časopisu 2600 a této stránky sdružují. V archivu je link na www stránku, kde byl průnik proveden a dále je v archívu uložena úvodní stránka po změně, kterou hackeři na adrese provedli.
   Za prosinec je zde takto zadokumentováno 48 průniků . Útok byl proveden na servery po celém světě (USA, Brazílie, Čína, Jižní Afrika). Nejvíce útoků se podařilo 4.12.99 (10) a 31.12.99 (7). Ze zajímavých adres stojí např. za zmínku:

- 31.12.1999 : Electronic Frontier Foundation : www.eff.org
- 22.12.1999 : State of California : www.cya.ca.gov
- 13.12.1999 : Chinese National Library : www.nlc.gov.cn
- 06.12.1999 : US Army : ri-acala4.ria.army.mil
- 05.12.1999 : South African Police : www.saps.co.za

V lednu aktivita hackerů poněkud poklesla, zdokumentováno je jen 6 průniků . Útok byl proveden především na servery v USA. Ze zajímavých adres stojí tentokrát za zmínku:

- 18.01.2000 : Columbian Government : www.ifi.gov.co
- 17.01.2000 : Library of Congress : thomas.loc.gov

4. Telefonování přes internet . Zatím stále málo používanou komunikační možností uživatelů Internetu je telefonování přes Internet zdarma s účastníky, kteří jsou kdekoliv na světě, ale přihlášeni k témuž serveru. Tuto možnost již nabízí i český internetový portál MSN.ATLAS.CZ na serveru http://ils.atlas.cz/ . Účastníci hovoru již neplatí žádný další telefonní tarif, ale jen poplatek za dobu připojení k Internetu. Potřebný software je volně k dispozici přímo na uvedeném serveru. Pokud mají účastníci video připojené k počítači, mohou kromě zvuku vysílat i svůj obraz a uskutečnit v reálném čase videokonferenci.

5. Ironií osudu byla den před propuštěním Kevina Mitnicka na svobodu zasazena hackerskému společenství a jeho svérázně pojaté svobodě další rána. Byl vydán předběžný soudní příkaz proti www stránce www.2600.com a jejím správcům. Správcům pak bylo pohroženo okamžitým uvězněním. Jedná se o reakci na umístění zdrojového kódu software DeCSS. Pomocí tohoto software je možné "kopírovat" obsah DVD na pevný disk. (Přesněji program DeCSS Vám umožní dekódovat datové soubory z filmových DVDček do podoby, která je přehrávatelná z vašeho harddisku.) Soud dále vydal předběžné opatření, zakazující umísťovat DeCSS na internetové stránky, zveřejňovat odkazy na stránky obsahující DeCSS a dokonce zveřejňovat odkazy na stránky zveřejňující odkazy na stránky obsahující DeCSS! Celá kauza není ovšem tak jednoduchá - trestán by měl být ten, kdo na černo vypaluje DVD a ne ten, kdo se rozebere v ochraně kódování a vytvoří funkční program. Připomíná mi to starý známý vtip : "Fero, zaplať 500 Kč za to, že pálíš slivovici." Fero : "Nepálím". Policista : To nevadí, ale máš na to přístroj! Fero vyndá 1000 Kč a dá je policistovi se slovy : "Těch druhých 500 je za znásilnění". Policista udiveně : "Ty jsi někoho znásilnil ?". Fero : "Ne, ale mám na to přístroj!"
   Ještě poznámka k této kauze. Při dopisování tohoto sešitu jsem našel na internetu reakci Františka Fuky k celému problému. (přesný odkaz jsem ztratil , ale článek se jistě dá vyhledat - je z rubriky Kultura a to z 26.1.2000).
   Dovolím si zde citovat. František Fuka výstižně píše : "Zamyslete se nad tím: Chci si vyrobit vlastní rozhlasový přijímač, ale nesmím, protože informace o tom, jak funguje rozhlasové vysílání, jsou tajné, a kdybych na jejich princip sám přišel - ať už analýzou existujícího rádia nebo metodou pokus-omyl, tak můžu být zavřen! A to se mi zatraceně nelíbí... "

6. Podobná právně zamotaná kauza se rozhořela i okolo stránky www.MP3.com . Na této stránce je nabízena služba - nákup hudebních CD po internetu. Toto CD ovšem neobdržíte, ale dostanete k obsahu tohoto CD přístup a můžete si jej přehrát ze svého PC po připojení k internetu. Výhoda : můžete si svá CD přehrávat z libovolného místa zeměkoule a nemusíte je vozit s sebou, nemusíte je skladovat, nepoškrábou se, neukradnou Vám je. Jenže společnost MP3.com je zažalována o deset milirad dolarů za porušování autorských práv . Žaluje je RIAA (Asociace amerického hudebního průmyslu). Problém je v tom, že RIAA tvrdí, že podle zákona může kopie pro své potřeby použít pouze spotřebitel a nikoliv prodávající. Společnost MP3.com se hájí tím, že spotřebitel si CD stejně zaplatil a tedy neoblíbená RIAA o své zisky nepřichází. Je možné, že tato kauza povede i k úpravě autorských práv v elektronickém věku.

G. Závěrečné informace

URL adresa, na níž můžete najít tento sešit (nejdříve 15 dní po jeho rozeslání) a 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 kdokoliv zájem o zasílání tohoto sešitu, stačí se zaregistrovat e-mailem na adrese hruby@gcucmp.cz (předmět : Crypto-World). Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu.

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