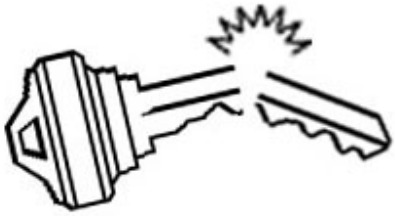
Informační sešit GCUCMP
Crypto-World 7-8/2000

Připravil : Mgr.Pavel Vondruška,
člen GCUCMP, BITIS, IACR, ISACA.
Sešit je rozesílán registrovaným čtenářům,
registrace na adrese pavel.vondruska@post.cz **, subject : Crypto-World**
sešity najdete také na adrese www.mujweb.cz/veda/gcucmp
(167 e-mail výtisků)
Uzávěrka 29.7.2000



OBSAH : **Str.**

+ příloha : 10000.txt

Dnešní přílohou je soubor 10000.txt, který obsahuje prvních 10 000 prvočísel
(další informace viz závěr článku "Fermatův test primality, Carmichaelova čísla, bezčtvercová čísla" , str.9) .

A. Ohlédnutí za I.ročníkem sešitu Crypto-World 1999/2000

Mgr. Pavel Vondruška (NBÚ)

Rok 1999 byl pro skupinu odborníků sdružených v kryptologické sekci Jednoty českých matematiků a fyziků - GCUCMP (Group of Cryptology Union of Czech Mathematicians and Physicists) velmi úspěšný. Vyvrcholením jejich téměř dvouletého úsilí bylo uspořádání mezinárodní konference Eurocrypt ´99 v Praze. Tato konference patří v "kryptologickém kalendáři" mezi dvě celosvětově nejdůležitější akce (druhou je konference Crypto, která se pravidelně koná v USA v Santa Barbaře). Eurocrypt je "putovní" konference a postupně se pořádá v různých městech Evropy. Uspořádání takovéto konference je pro příslušný stát a jeho odborné kryptologické struktury vždy velkým oceněním jejich práce. Podle kladných ohlasů se zdá, že konference v Praze se vydařila a zařadila se mezi ty lepší Eurocrypty. Pravidelné schůze organizačního výboru skončily vyhodnocením konference v létě 1999.

Po skončení konference mi bylo až trochu líto opustit kryptodění a zdálo se mi, že mám najednou spoustu volného času (v rámci organizačního výboru jsem měl mimo jiné na starosti e-mail schránku konference). Také jsem si zvykl na téměř dvouletý styk s výborem IACR, přednášejícími, studenty, stipendisty (mezi něž patří např. dnes již hvězda první velikosti Biruyukov, pro kterého jsme tehdy vyřizovali slevy).

Z těchto - částečně nostalgických - důvodů jsem se nabídl, že se pokusím zorganizovat psaní jakéhosi sešitu, který by byl určen pro členy GCUCMP a sloužil k informacím o dění ve světě kryptologie. Přiznám se, že jsem počítal s tím, že se zapojí svými příspěvky i někteří další členové GCUCMP. Nejjednodušší formou se zdálo být napsání sešitu v MS Wordu a jeho rozesílání e-mailem na adresu členů GCUCMP. Hned od druhého čísla se však ozvalo pár zájemců mimo GCUCMP. Rozhodl jsem se, že budu sešit rozesílat všem zájemcům a vznikla tak databáze registrovaných odběratelů. Se sešitem mi od začátku velice pomohl ing. Jaroslav Pinkava, CSc., kterému touto cestou velice děkuji. Nejen za to, že pravidelně do sešitu přispívá, ale také za mnohá upozornění na zajímavé články a odkazy, které pak mohu využít v rubrice "Letem šifrovým světem".

Během roku pak došlo k některým změnám. Sešit začal "vycházet" v PDF formátu, koncem roku 1999 jsem vytvořil jednoduchou www stránku (http://www.mujweb.cz/veda/gcucmp), na kterou jsem umístil starší čísla. Poněkud mě totiž časově zatěžovalo zasílat "stará" čísla sešitů jednotlivým zájemcům. Zpravidla nově registrovaný uživatel měl zájem i o všechna starší čísla.

Množství čtenářů se pomalu, ale pravidelně zvyšuje; zájem znatelně vzrostl po konferencích ČAČK a Security 2000, kde bylo ze sešitu veřejně citováno. Po uveřejnění možnosti registrovat se pro zasílání tohoto časopisu v diskusi o virech (červen 2000) pak počet zájemců vzrostl o dalších více než padesát odběratelů.

Statistika nárůstu odběratelů , počtu stran a délky sešitu v bytech je následující:

I.ročník sešitu Crypto-World

	9/99	10/99	11/99	12/99	1/2000	2/2000
Odběratelů	25	31	35	47	62	76
Stran	7	10	9	9	9	11
Bytů	118 655	163 382	312 601	370 720	208 173	215 768

	3/2000	4/2000	5/2000	6/2000	7-8/2000	7-8/2001
Odběratelů	90	102	107	116	163	890
Stran	11	13	15	16	19	40
Bytů	212 279	333 340	354 749	502 347	280 000 ?	2 150 000

V posledním sloupci je uveden odhad, který vznikl proložením křivky údaji 9/99 až 7-8/2000 (viz komentář níže).

Odhad sledovaných ukazatelů - počet listů a velikost rozesílaného sešitu - mohu ovlivnit. Budu se snažit stabilizovat tyto parametry na rozumných hodnotách 12-16 stran, 400-600 kB. Odběratelé se tedy nemusí obávat dalšího nárůstu velikosti rozesílaného souboru a doby, kdy by přijatý Crypto-World obsadil všechen (zlým správcem povolený) prostor v jeho poštovní schránce.

K počtu odběratelů bych poznamenal, že uvedený odhad je sice velice příznivý a povzbuzující, ale současně si dovolím tvrdit, že takový nárůst zcela určitě nenastane. V současné době již většina expertů, kteří v dané oblasti pracují, sešit odebírá, a tak jaksi potenciálních čtenářů již asi ani tolik není (pokud ovšem doba PKI, e-komerce a e-obchodu a e-peněz nevytvoří nové e-čtenáře …). K současnému složení čtenářů prozradím, že přibližně 80 odběratelů jsou odborníci z oblasti informační bezpečnosti, přibližně 50 odběratelů jsou správci sítí nebo informačních systémů, 6 čtenářů jsou novináři odborných časopisů nebo obecněji novináři a cca dvacet pět zájemců neumím vzhledem k absenci údajů zařadit .

Když se již zmiňuji o struktuře odběratelů, uvedu ještě malou statistiku, která vznikla na základě údajů z 28.6.2000:

- sešit je rozesílán na 163 e-mail adres
- sešit je rozesílán do dvou států (156 x ČR, 7 x Slovensko)
- registrováno je pět čtenářek
- nejvíce čtenářů má svoji adresu registrovánu na doméně post.cz (12x)
- následují domény : volny.cz (10x), nbu.cz (8x), cuni.cz (8x), aec.cz (7x), decros.cz (6x), cvut.cz (5x), army.cz (3x), mvcr.cz (3x)
- zbývajících 113 čtenářů je registrováno na dalších různých 90 doménách
- 96 odběratelů je mi osobně známo

II.ročník

Prvé číslo II.ročníku (9/2000) vyjde kolem 10.září. Pokud mi to čas dovolí, pokusím se v tomto novém ročníku provést určité změny. Sešit bude mít nové logo a titulní stránku. Dále chystám nepříliš náročnou soutěž pro čtenáře, která by měla končit číslem 12/2000. Pokud se podaří najít sponzora, mohl by vítěz získat mimo slávy i nějaký "vánoční dárek". Asi jste již zjistili, že se změnila i www stránka (http://www.mujweb.cz/veda/gcucmp) , nejdůležitější změnou je možnost registrace k odběru sešitu přímo vyplněním registračního "formuláře" na www stránce a možnost zaslat dotaz nebo komentář také přímo z komunikačního okna na www stránce. Přislíbeny jsou i některé velmi hodnotné články od nových autorů.

FAQ (Frequently Ask Question)

Závěrem si dovolím odpovědět na často kladené otázky :

- ano, sešit píši a rozesílám zadarmo
- za články uveřejněné v sešitě se neplatí
- jsou vítány příspěvky všech odběratelů
- vedení sešitu patří mezi mé záliby a pokusím se jej vydávat dle svých možností i nadále

END

Všem čtenářům tohoto sešitu přeji hezké prožití zbytku letních prázdnin a dovolených.

B. Kryptosystém s veřejným klíčem XTR

Ing. Jaroslav Pinkava (AEC spol. s r.o.)

1. Úvod

Na adrese http://www.ecstr.com/ byl nedávno konečně zveřejněn design nového kryptosystému s veřejným klíčem, který autoři Arjen R. Lenstra a Eric R. Verheul nazvali XTR. Zveřejněný materiál je preprintem článku, který byl přijat k opublikování na konferenci Crypto 2000 v Santa Barbaře (koná se 20. – 24. srpna tohoto roku). Čtenáři Crypto-Worldu již byli o existenci tohoto kryptosystému stručně informováni v čísle 4/2000.

Systém XTR je založen na nové metodě umožňující reprezentovat prvky podgrupy multiplikativní grupy konečného tělesa. Cílem návrhu XTR je dle autorů navrhnout takový kryptosystém s veřejným klíčem, jehož délka parametrů i vlastní výpočtové nároky vedou k podstatným úsporám jak v komunikacích tak při výpočtech a to bez snížení příslušné kryptografické bezpečnosti.

2. Některá značení a definice

Popíši příslušný postup jen s nezbytnými technickými podrobnostmi. Zdůvodnění a další detaily lze nalézt v komentovaném článku [1].

GF(m) ... těleso (mod m)

GF(m)* ... multiplikativní grupa tělesa GF(m)

Budeme dále předpokládat, že p je takové prvočíslo, že

a) $p \equiv 2 \mod 3$

b) mnohočlen (tzv. šestý cyklotomický – viz [2]) $\varphi_6(p) = p^2 - p + 1$ spočtený v p má jako dělitele prvočíslo q.

Symbolem g bude označen generátor $GF(p^6)^*$ mající řád q.

Pro výše zvolené p lze libovolný prvek $GF(p^2)$ vyjádřit jako $x_1 a + x_2 a^2$, kde x_1, x_2 jsou z GF(p), a a a^p jsou kořeny polynomu $X^2 + X + 1$, které tvoří optimální normální bázi pro $GF(p^2)$ nad GF(p).

Jestliže h ε GF (p^6), pak k němu sdruženými prvky nad GF (p^2) jsou h, h^{p2}, h^{p4}.
Stopou Tr(h) nad GF (p^2) prvku h ε GF (p^6) je součet sdružených nad GF (p^2) prvku h, tj. $Tr(h) = h + h^{p2} + h^{p4}$. Platí Tr(h) ε GF ($p^2$).
Pozn.: p2= p^2, p4 = p^4.

Označíme F(c, X) mnohočlen $X^3 - cX^2 + c^pX - l$, pro c ε GF (p^2) mající kořeny h_0, h_1, h_2 v GF (p^6). Pro n ε Z budeme značit $c_n = h_0^n + h_1^n + h_2^n$. Z lemmatu 2.3.2 článku vyplývá, že c_n jsou prvky GF (p^2) .

Nechť dále $S_n(c) = (c_{n-1}, c_n, c_{n+1})$.

3. Základní algoritmy

Celý článek směřuje k vyhodnocení výpočetní složitosti matematických postupů nezbytných při provádění popisovaných kryptografických postupů. Jedním z ústředních algoritmů v tomto směru je algoritmus 2.3.7, který popisuje postup výpočtu $S_n(c)$.
Následující rovnost dává vlastně výchozí myšlenku konstrukce kryptosystému XTR:

$$S_n (Tr(g)) = (Tr(g^{n-1}), Tr(g^n), Tr(g^{n+1}))$$

Ukazuje totiž, že při nahrazení tradičních mocnin g jejich stopami lze dosáhnout výpočetně efektivních postupů. Konkrétně algoritmus 2.3.7 umožňuje na základě znalosti Tr(g) rychle spočítat $Tr(g^n)$.
Pro některé kryptografické postupy je však ještě třeba umět spočítat stopu součinu dvou mocnin generátoru g. Tím se zabývá algoritmus 2.4.8.

4. Volba parametrů

Symboly P a Q označíme požadované velikosti (v počtech bitů) hledaných prvočísel p a q. Autoři doporučují, že k dosažení bezpečnosti odpovídající bezpečnosti např. RSA v délce 1024 (počet bitů součinu dvou prvočísel) je vhodné volit P ≈ 170 a Q ≈ 160.
Algoritmus 3.1.1. Nalézt přirozené r tak, že $q = r^2 - r + 1$ je prvočíslo délky Q a dále nalézt přirozené k tak, že p = r + k*q je prvočíslo délky P a p ≡ 2 mod 3.
Tento algoritmus nám sice dává potřebná prvočísla (navíc prvočíslo p takto generované má určité výpočetně výhodné vlastnosti), ale nemusí být úplně ideální z bezpečnostního hlediska. Autoři proto uvádí ještě Algoritmus 3.1.2 jako metodu generování p a q , která je oproštěna od možného zjednodušení při kryptoanalytickém použití metody Number Field Sieve pro řešení diskrétního logaritmu. Algoritmus 3.2.2 se zabývá postupem nalezení Tr(g) – není nutné přitom znát samotné g.
Součástí dat pro veřejný klíč kryptosystému XTR je výše uvedená dvojice prvočísel p a q a stopa Tr(g) generátoru g. Tato čísla mohou být sdílena více uživateli (jako je tomu např. u DSA či ECDSA). Veřejný klíč konkrétního uživatele je pak doplněn hodnotu $Tr(g^k)$ pro nějaké přirozené číslo k, které je utajováno (je to tedy příslušný soukromý klíč).

5. Použití v kryptografii

Autoři uvádějí tři postupy – analogii DH dohody na klíči, ElGamalova šifrování a analogii Nyberg-Rueppelovy varianty digitálního podpisu s obnovou zprávy. Následuje popis analogu Diffie-Hellmanova protokolu pro dohodu na klíči :

1. Alice zvolí náhodně přirozené a < q-2, spočte $Tr(g^a)$ a zašle ho Bobovi.
2. B obdobně zvolí přirozené b < q-2, spočte $Tr(g^b)$ a zašle ho Alici.
3. Alice spočte $Tr(g^{ab})$ a dohodnutým postupem odvodí klíč K.
4. Stejně tak Bob spočte $Tr(g^{ab})$ a dohodnutým postupem odvodí klíč K

Výpočty se opírají o použití algoritmu 2.3.7.

V další části článku se autoři zabývají srovnáním vlastností kryptosystému XTR s kryptosystémy RSA a ECC. Dokladují výhodnost jimi navrhovaného postupu. Potřebná délka klíčů je srovnatelná s ECC a totéž platí i o výpočetní náročnosti kryptografických operací.

Ve zbývající části práce jsou popsány některé přístupy k hodnocení bezpečnosti navrhovaného kryptosystému.

6. Shrnutí

Kryptosystém XTR představuje myšlenkově velice hodnotný postup, inovátorský z hlediska metod současné asymetrické kryptografie. Čtenáře mající zájem o konkrétní implementace kryptosystému XTR musím však trochu varovat. Pro praktické aplikace je nejlépe využít takové kryptosystémy, které jsou již součástí mezinárodních norem. Svým způsobem to také garantuje, že daný kryptosystém již prošel dostatečně fází kritického posuzování svých vlastností odbornou veřejností (jako je tomu např. u systému RSA a u systémů založených na úlohách diskrétního a eliptického diskrétního logaritmu). Z tohoto hlediska je systém XTR teprve v plenkách. Je také možné, že než kryptosystém nabyde své definitivní podoby (i třeba např. z hlediska optimalizace implementačních vlastností) dojde k jeho některým dílčím úpravám. Navíc autoři oznámili, že bylo podáno několik mezinárodních patentů, které se tohoto kryptoschematu dotýkají.

7. Literatura

[1] Lenstra, Arjen K.; Verheul Eric R.: The XTR public key system, to appear in Advances in Cryptology – Crypto 2000, Lecture Notes in Computer Science, Springer Verlag, pp. 1-19

[2] Brouwer, A. E.; Pellikaan, R.; Verheul, E.R.: Doing More with Fewer Bits, Proceedings Asiacrypt 99, LNCS 1716, Springer Verlag 1999, pp. 321-332

C. Fermatův test primality, Carmichaelova čísla, bezčtvercová čísla

Mgr. Pavel Vondruška (NBÚ)

Část II.

V minulém sešitě - 6/2000 - jsme si uvedli některé pravděpodobnostní testy pro získání prvočísel. Blíže jsme se seznámili s Fermatovým testem primality a při jeho teoretickém rozboru jsme se setkali s pojmem Carmichaelovo číslo. Těmito čísly jsme se dále zabývali. V závěru jsme uvedli charakteristické vlastnosti těchto čísel.
Jedna z vlastností byla : "Každé Carmichaelovo číslo je bezčtvercové."
V této části se budeme právě bezčtvercovými čísly zabývat.

Bezčtvercová čísla

Číslo n se nazývá bezčtvercové (anglicky Squarefree), jestliže jeho prvočíselný rozklad obsahuje každého činitele pouze v prvé mocnině.

Všechna prvočísla jsou tedy triviálně čísla bezčtvercová.
Příkladem bezčtvercových čísel jsou : 1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, ...
Naopak čísla 4, 8, 9, 12, 16, 18, 20, 24, 25, ... nejsou čísla bezčtvercová (anglicky se označují squareful numbers).

Výpočtem byly zjištěny následující výsledky :

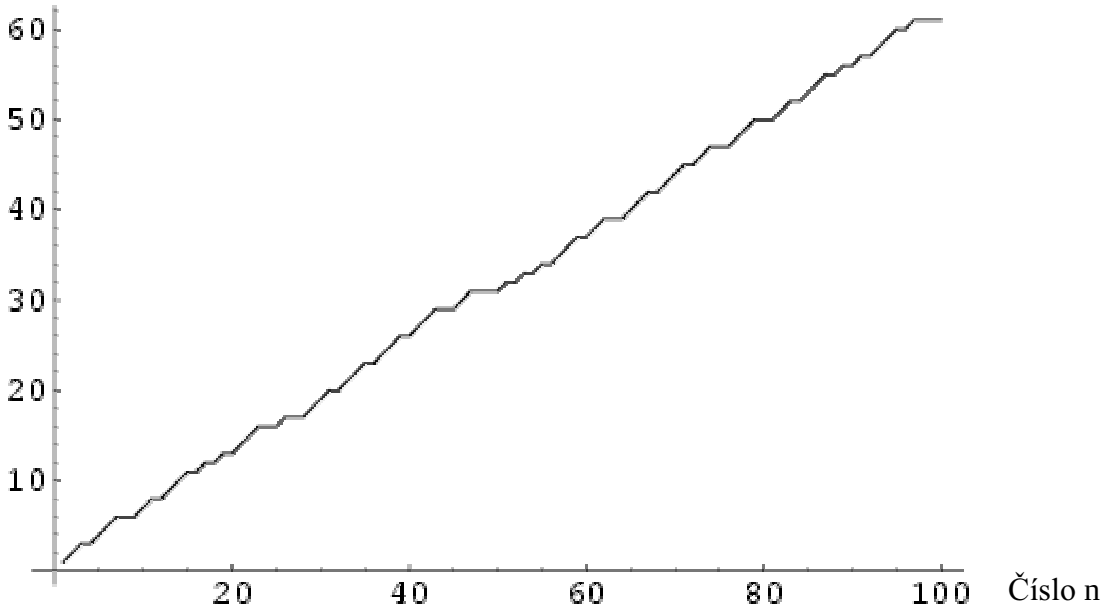
Interval <1 , n >	Počet bezčtvercových čísel	Počet prvočísel
10	7	4
100	61	25
1000	608	168
10 000	6 083	1 229
100 000	60 794	9 592
1 000 000	607 926	78 498

Významné práce o problému bezčtvercových čísel publikovali : (6) Nagell 1951, p. 130; (4) Landau 1974, pp. 604-609; (3) Hardy and Wright 1979, pp. 269-270; (2) Hardy 1999, p. 65.

Na grafu závislosti počtu bezčtvercových čísel na číslu n (obr. 1) lze vypozorovat jistou pravidelnost rozložení bezčtvercových čísel.

Obecně lze říci, že rozložení bezčtvercových čísel je na rozdíl od prvočísel "docela pravidelné". Právě pro tuto vlastnost a současně proto, že jsou s prvočísly v těsném vztahu, jsou bezčtvercová čísla v teorii čísel využita pro některé odhady a důkazy, které se týkají prvočísel. Přesnější vyjádření (a zdůvodnění) přesahuje rámec našeho jednoduchého výkladu.

Počet bezčtvercových čísel



Obr. 1 - Závislost počtu bezčtvercových čísel na volbě n

Z "přesnějších" odhadů uveďme odhad počtu bezčtvercových čísel $Q(x) \leq n$

$$Q(n) = \frac{6n}{\pi^2} + \mathcal{O}(\sqrt{n}) \quad .$$

Asymptotická hustota tohoto výrazu je $1/\ \zeta(2) = 6/\ \pi^2 \approx 0.607927$ (kde $\zeta(2)$ je hodnota Riemannovy ζ funkce v bodě 2) .

Hardy a Wright 1979 (3, str. 270) studovali tzv. Möbiovu funkci $\mu(n)$, která je definována následovně :

$$\mu(n) = \begin{cases} 0 & \text{pro n, které má ve svém prvočíselném rozkladu alespoň dvě prvočísla stejná} \\ 1 & \text{pro n=1} \\ (-1)^k & \text{pro n, které má ve svém prvočíselném rozkladu všechny činitele různé a těchto činitelů je k} \end{cases}$$

Je zřejmé, že je-li $\mu(n)$ různé od nuly, je n bezčtvercové číslo.

Asymptotická hodnota funkce Q(x) je rovna hodnotě :

$$\sum_{n=1}^{x} \left| \mu(n) \right| = \frac{6x}{\pi^2} + o(x)$$

Není znám algoritmus, který by v polynomiálním čase řešil otázku, zda přirozené číslo je nebo není bezčtvercové číslo. Je zřejmé, že tento problém úzce souvisí s problémem faktorizace, neboť umíme-li číslo rozložit na jednotlivé činitele, pak snadno určíme, zda je

nebo není bezčtvercové. Na druhou stranu není známo, zda neexistuje algoritmus, který by nám určil, že číslo je bezčtvercové, aniž bychom museli znát jeho rozklad.

Zodpovězení této otázky se považuje za velice důležitý problém teorie čísel, výsledek by našel uplatnění v teorii NFS (number field sieve), velice nepřesně řečeno "okruh přirozených čísel vytvořený při výpočtu algebraického číselného pole by byl reducibilní pomocí bezčtvercových čísel" (Lenstra 1992, Pohst and Zassenhaus 1997). Řešení tohoto problému tak může výrazně ovlivnit bezpečnost RSA .

****

Přílohou k dnešnímu číslu je soubor 10000.txt, který obsahuje prvních 10 000 prvočísel. Tento soubor je uložen na adrese http://www.utm.edu/research/primes/lists/small/1000.txt.
Zde lze také získat soubor obsahující přehled prvních 100 008 prvočísel. V tomto souboru jsou uvedena všechna prvočísla z intervalu 1 až to 1 299 827. Velikost tohoto souboru je 822 kB. Pokud někomu nestačí ještě ani tento rozsáhlý soubor, doporučuji k návštěvě adresu : http://www.math.princeton.edu/~arbooker/nthprime.html
Zde můžete získat informace o prvních 1 000 000 000 000 prvočíslech. Posledním prvočíslem v tomto souboru je 29 996 224 275 833. Informace o prvočíslech získáte pomocí dotazů. Váš dotaz např. zní : "Jaké je sté prvočíslo?" , a program uložený na uvedené adrese vrátí příslušné prvočíslo = 541. Odpověď na libovolný dotaz od 2 do 10^{12} trvá cca 10 vteřin.

****

Literatura :

1. Bellman, R. and Shapiro, H. N. ``The Distribution of Squarefree Integers in Small Intervals." Duke Math. J. 21, 629-637, 1954.
2. Hardy, G. H. Ramanujan: Twelve Lectures on Subjects Suggested by His Life and Work, 3rd ed. New York: Chelsea, 1999.
3. Hardy, G. H. and Wright, E. M. ``The Number of Squarefree Numbers." §18.6 in An Introduction to the Theory of Numbers, 5th ed. Oxford, England: Clarendon Press, pp. 269-270, 1979.
4. Landau, E. Handbuch der Lehre von der Verteilung der Primzahlen, 3rd ed. New York: Chelsea, 1974.
5. Lenstra, H. W. Jr. ``Algorithms in Algebraic Number Theory." Bull. Amer. Math. Soc. 26, 211-244, 1992.
6. Nagell, T. Introduction to Number Theory. New York: Wiley, p. 130, 1951.
7. Pohst, M. and Zassenhaus, H. Algorithmic Algebraic Number Theory. Cambridge, England: Cambridge University Press, p. 429, 1997.
8. Shanks, D. Solved and Unsolved Problems in Number Theory, 4th ed. New York: Chelsea, p. 114, 1993.
9. Sloane, N. J. A. Sequences A005117/M0617, A013929, and A046098 in ``An On-Line Version of the Encyclopedia of Integer Sequences." http://www.research.att.com/~njas/sequences/eisonline.html
10. Vardi, I. ``Are All Euclid Numbers Squarefree?" §5.1 in Computational Recreations in Mathematica. Reading, MA: Addison-Wesley, pp. 7-8, 82-85, and 223-224, 1991.

D. Počátky kryptografie veřejných klíčů

Mgr. Jan Janečko (Komerční banka, a.s.)

Rokem 1976 začala bezesporu nová éra kryptografie. Whitfield Diffie, Martin Hellman a Ralph Merkle objevili a zveřejnili zcela nový převratný kryptografický princip – princip veřejných šifrovacích klíčů. Tento průkopnický objev postupně vzbudil obrovský zájem specialistů a v následujícím období zcela změnil obraz kryptologie. Po prvních článcích a vystoupeních autorů této myšlenky se brzy objevily návrhy konkrétních systémů. Mezi prvními byly i oba z nejúspěšnějších a stále používaných představitelů asymetrické kryptografie, čili kryptografie veřejných klíčů (Public Key Cryptography, PKC) – v roce 1976 tzv. Diffie-Hellmanův systém výměny klíčů [1] a v roce 1977 algoritmus RSA [2], jehož autory jsou Ronald Rivest, Adi Shamir a Leonard Adleman (v té době všichni z MIT). Jmenovaní autoři si za své objevy získali zasloužený respekt a navždy se zapsali do historie svého oboru.

Postupem doby se však začaly objevovat určité pověsti, že tito vědci nebyli prvními objeviteli PKC. V kryptologii totiž existuje situace odlišná od většiny ostatních vědeckých oborů. Vedle otevřeného výzkumu existuje ještě výzkum utajovaný, prováděný elitními speciálními službami velmocí i dalších zemí, zahalený téměř neproniknutelným tajemstvím (viz též citát v závěru tohoto článku). Až do 70. let tato sféra v kryptologii naprosto dominovala, ale i v nynější době stále představuje velmi významný vědecko-výzkumný potenciál.

Říká se například, že už před rokem 1976 znala PKC americká NSA. V článku o kryptologii uveřejněném v Encyclopaedia Britannica [3] se uvádí, že bývalý ředitel NSA Bobby Inman bez důkazů tvrdil, že NSA znala princip PKC už o deset let dříve před jeho objevením otevřenou akademickou obcí. Určité potvrzení vidí někteří ve vývojovém projektu zabezpečeného telefonu STU-III, který využívá certifikátů, a jehož výzkum začal pravděpodobně v polovině 70. let. Přitom certifikáty se ve veřejné kryptografii objevily až v roce 1979. Jako možný podnět pro výzkum vedoucí k objevu PKC se také uvádí Memorandum prezidenta J. F. Kennedyho č. 160 z roku 1962 (a zvláště jeho Weisnerův dodatek) [4], týkající se potřeby zabezpečení nukleárních zbraní proti zneužití.

Nepopiratelný důkaz o tom, že princip PKC byl objeven už před rokem 1976, však nakonec přišel z Velké Británie. V roce 1997 byl uveřejněn článek Jamese Ellise z britské CESG (Communications – Electronics Security Group), nazvaný "The history of Non-Secret Encryption" [5], ve kterém jeho autor popisuje, jak princip asymetrické kryptografie (jím nazývaný jako Non-Secret Encryption, NSE) objevil už v roce 1970. Dále uvádí, že speciální variantu RSA objevil jeho kolega Clifford Cocks v roce 1973, varianty Diffie-Hellmanova systému výměny klíčů pak Malcolm Williamson brzy poté. Článek [5] napsal James Ellis v roce 1987, byl však zveřejněn až krátce po jeho smrti v prosinci 1997. Je v něm popsána celá historie objevu NSE pracovníky CESG. Spolu s příslušnými autentickými technickými zprávami CESG ([6] -[9]) ho lze najít na webovské stránce CESG www.cesg.uk.

Jak vlastně k objevu NSE došlo? J. Ellis uvádí, že už v 60. letech představovala velký problém distribuce šifrovacích klíčů tehdy používaných symetrických šifer pro potřeby ozbrojených sil. Až dosud bylo pokládáno za samozřejmé, že odesilatel i příjemce zašifrovaných informací musí předem sdílet nějakou utajovanou informaci. Inspirace, že tomu tak být nemusí, přišla z technické zprávy neznámého pracovníka Bellových laboratoří, publikované v roce 1944, která obsahovala návrh zabezpečeného telefonu. Utajení mělo být dosaženo tím, že příjemce vysílal do linky šum k maskování hovorového signálu, který by pak od přijatého maskovaného signálu opět odečítal. Přestože návrh nebyl technicky realizovatelný, vnukl Ellisovi myšlenku, že při aktivní účasti příjemce v procesu šifrování odesilatel a příjemce předem sdílet nějakou utajovanou informaci nemusí a celý systém může být veřejně známý. Od tohoto postřehu již pro něho nebylo obtížné dokázat existenční větu o tom, že "Non-Secret Encryption" je v principu možné. Důkaz vycházel z představy, že proces zašifrování lze vždy zcela obecně popsat pomocí matice, jejíž řádky a sloupce představují všechny možné klíče a možné zprávy, obsahem matice je pak příslušný šifrový text. I když by taková matice nebyla v praxi pro svoji ohromnou velikost realizovatelná, v principu si ji můžeme vždy představit.

Popišme nyní stručně hlavní myšlenku důkazu. Odesilatel chce utajeně poslat zprávu *p*. Příjemce generuje náhodný tajný klíč *k*, který zašifruje pomocí náhodně generované jednorozměrné tabulky (permutace) *M1* na hodnotu $x = M1(k)$ a tu zašle odesilateli zprávy. Ten použije *x* a tabulku *M2* (dvojrozměrnou, náhodně generovanou matici, jež indukuje pro každou pevnou hodnotu *x* prosté zobrazení) k zašifrování *p* na šifrový text *z*: $z = M2(p,x)$. Příjemce získá zpět původní zprávu *p* pomocí příslušné "inverzní" tabulky *M3*: $p = M3(z,k)$. Přitom matice *M1*, *M2* a *M3* nemusí být utajovány.

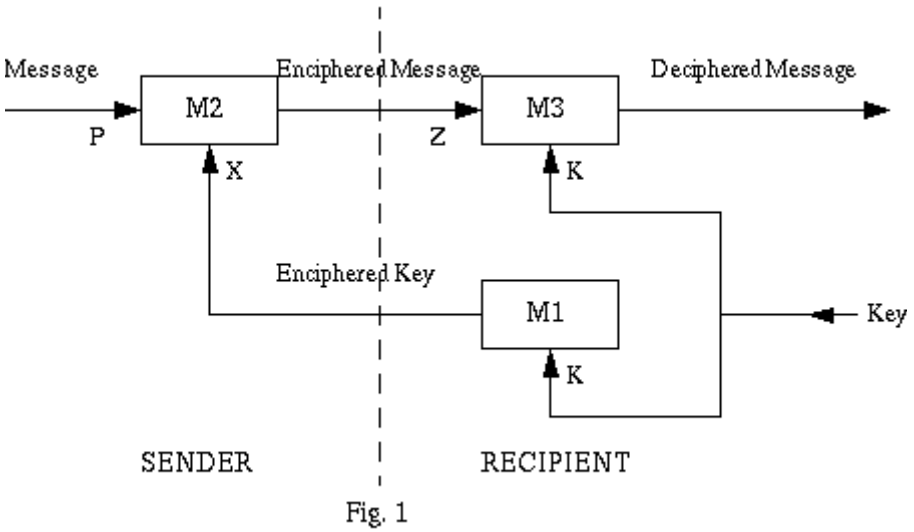


Fig. 1

Podrobněji je celý postup znázorněn na dalším obrázku (v dnešní terminologii se *k* nazývá soukromým a *x* veřejným klíčem):

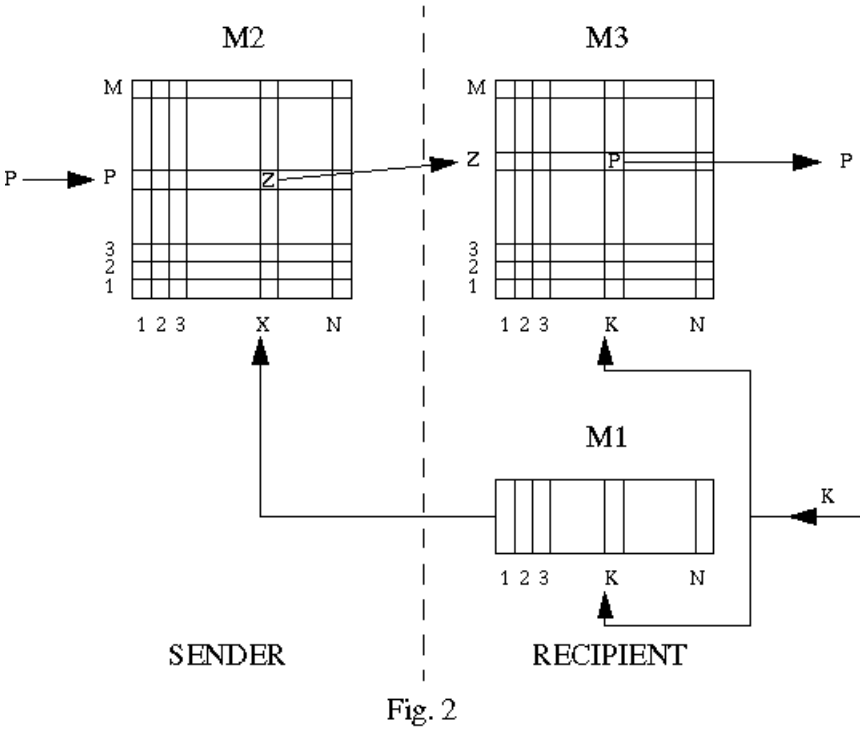


Fig. 2

Oba obrázky jsou převzaty z původní Ellisovy zprávy [6].

Je vidět, že metoda bude fungovat korektně, pokud *M3* bude zřejmým způsobem zkonstruována na základě matic *M1* a *M2*. Dále je vidět, že ani zveřejněním všech matic *M1, M2 a M3* není ohrožena důvěrnost zašifrované zprávy jejím přenosem k oprávněnému příjemci. Vzhledem k náhodnému vygenerování obsahu matic *M1* a *M2* totiž bez znalosti hodnoty *k* neexistuje jiná metoda luštění, než je metoda hrubé síly (prohledáváním tabulek *Mi*). Její úspěšnost je však vyloučena dostatečnou dimenzí matic (např. řádově 2^{100}).

Takto se tedy Jamesi Ellisovi podařilo dokázat, že asymetrické šifry mohou teoreticky existovat. Ellis však nedokázal najít jejich v praxi využitelnou realizaci. Správně však předpokládal, že prakticky použitelný systém může mít jinou formu, než kterou použil pro svůj důkaz. Svou prací ale ukazoval směr, jakým je možno se zaměřit. Svůj výsledek prezentoval poprvé v lednu 1970 v interní technické zprávě CESG [6].

Jak sám J. Ellis tvrdil, teorie čísel nebyla jeho silným oborem, s návrhy realizovatelných systémů proto přišli až jeho kolegové. V roce 1973 Clifford Cocks navrhl de facto speciální případ RSA [7]. Stručně řečeno, rozdíl mezi Cocksovým návrhem a RSA je v tom, že veřejným klíčem u Cockse je vždy přímo modul $n = pq$, u RSA to mohou být "vhodná" čísla e mající inverzi $mod\ \varphi(n)$ (v praxi se však obvykle stejně používá jediný veřejný klíč, např. Fermatovo prvočíslo $2^{16}+1$). Cocksův návrh vypadal takto:

1. Strana A generuje dvě velká prvočísla *p, q* taková, že *p* nedělí *q-1* a *q* nedělí *p-1*. Poté spočte $n = pq$. Číslo *n* jako veřejný klíč pošle straně B.
2. B zašifruje zprávu *m* tak, že spočte $c = m^n \bmod n$; šifrový text *c* pošle A.
3. A odšifruje *c* následovně: najde *p'* a *q'* taková, že $pp' = 1 \bmod q-1$ a $qq' = 1 \bmod p-1$. Pak platí, že $m = c^{p'} \bmod q$, $m = c^{q'} \bmod p$ a pomocí Čínské věty o zbytcích A zjistí otevřený text *m*.

To ale nebylo od CESG všechno. Po C. Cocksovi přišel s jinými návrhy Malcolm Williamson. Byly založeny na složitosti výpočtu diskrétního logaritmu. Prvním systémem byl následující kryptografický protokol, který probíhal ve čtyřech krocích. Byl formulován obecněji pro konečné okruhy [8], ale pro prvočíselná tělesa ho lze popsat následovně:

Účastníci A a B si dohodnou neutajované velké prvočíslo *p*. Výpočty pak provádějí *mod p*.

1. A chce zaslat zprávu *m*. Generuje náhodně číslo *k* nesoudělné s *p-1* a spočte $x = m^k$; *x* pošle B.
2. B generuje náhodně číslo *l* nesoudělné s *p-1* a spočte $y = x^l = (m^k)^l$; *y* pošle A.
3. A pomocí Euklidova algoritmu nalezne *k'* takové, že $kk' = 1 \bmod p-1$ a spočte $z = (m^{kl})^{k'} = m^l$; tuto hodnotu pošle B.
4. B obdobným způsobem nalezne *l'* takové, že $ll' = 1 \bmod p-1$ a spočte $z^{l'} = (m^l)^{l'} = m$.

V další zprávě [9] Williamson dokonce navrhl klasický Diffie-Hellmanův protokol pro výměnu klíčů, a to pro obecná číselná tělesa. Zprávu uveřejnil mnohem později, než systém vymyslel:

Před začátkem protokolu si účastníci A a B dohodnou těleso $F = GF(p^q)$ a primitivní prvek *x* tělesa *F*. Tyto údaje neutajují. Prvky tělesa *F* reprezentují jako polynomy.

1. A generuje náhodně číslo *a* a spočte $y = x^a$; *y* pošle B.
2. B generuje náhodně číslo *b* a spočte $z = x^b$; *z* pošle A.
3. Obě strany spočtou $w = (x^b)^a = (x^a)^b = x^{ab}$; tuto hodnotu používají jako šifrovací klíč.

Jen jako historickou kuriozitu uveďme, že pracovníci CESG objevili varianty základních systémů PKC (RSA a DH) v opačném pořadí, než jak k tomu poté došlo v otevřeném výzkumu. Místo závěru bych pak chtěl uvést ještě jeden charakteristický citát z článku Jamese Ellise [5]:

„Kryptografie je nejneobvyklejší vědou. Většina profesionálních vědců se snaží publikovat svou práci jako první, protože prostřednictvím šíření tato práce realizuje svoji hodnotu. Naproti tomu nejúplnější hodnota kryptografie je realizována minimalizací informací dostupných potenciálním protivníkům. Proto profesionální kryptografové obvykle pracují v uzavřených komunitách, které poskytují dostatečnou odbornou interakci k zajištění kvality, zatímco udržují utajení před nezasvěcenými. Odhalení těchto tajemství je obvykle umožněno pouze v zájmu historické přesnosti až poté, co se ukáže nepochybným, že žádný další užitek nemůže už být z pokračujícího utajení získán."

Poznámka:

CESG – Communications-Electronics Security Group – je formální součástí známé britské speciální služby GCHQ (Government Communications Headquarters, Ústředí vládních komunikací). Sídlí v Cheltenhamu v hrabství Gloucestershire, asi 130 km západně od Londýna. GCHQ se proslavila už za 2. světové války (v té době ovšem působila pod názvem Government Code and & Cypher School - GC&CS, ale byla všeobecně známa pod názvem Bletchley Park podle svého tehdejšího sídla) rozluštěním nejtajnějších německých vojenských šifrátorů Enigma a Lorenz Geheimschreiber, stejně jako konstrukcí prvních elektronických počítačů na světě nazývaných Colosssus, sloužících právě k luštění německých šifrátorů. Přímým předchůdcem CESG byla London Communications Security Agency (LCSA), vzniklá v Londýně počátkem 50. let. Dnešní název nese od roku 1969. Postupně se služba přestěhovala do Cheltenhamu. Od roku 1997 již CESG není přímo financována vládou a pracuje na ziskové bázi. Mezi její hlavní úkoly patří účast na definování vládní politiky pro informační bezpečnost, konzultační a poradenské služby pro vládní i veřejný sektor v oblasti zavádění této politiky, vlastní vývoj kryptografických produktů (jako jsou zabezpečené telefony) a spolupráce s komerčními výrobci při vývoji kryptografických produktů pro vládní účely, provádění výukových kurzů a výroba spotřebních šifrovacích materiálů (klíčů).

Literatura:

[1] W. Diffie, M. E. Hellman: New Directions in Cryptography, IEEE Transactions on Information Theory, Vol. IT-22, No 6 November 1976

[2] R. L. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public-key Cryptosystems, MIT Laboratory for Computer Science, Technical Memo LCS!TM82, Cambridge, Massachusetts, 4/4/77. Též: Comm ACM Vol 21, Feb 1978

[3] Encyclopaedia Britannica, www.britannica.com

[4] National Security Action Memorandum 160, 6 June 1962

[5] J. H. Ellis: The history of Non-Secret Encryption, 1987

[6] J. H. Ellis: The Possibility of Secure Non-Secret Digital Encryption, CESG Report, January 1970

[7] C. C. Cocks: A Note on ‘Non-Secret Encryption’, CESG Report, 20 November 1973

[8] M. J. Williamson: Non-Secret Encryption Using a Finite Field, CESG Report, 21 January 1974

[9] M. J. Williamson: Thoughts on Cheaper Non-Secret Encryption, CESG Report, 10 August 1976

E. Přehled některých českých zdrojů - téma : kryptologie

Vybral Mgr. Pavel Vondruška, NBÚ

Je léto, počasí nám zatím nepřeje, a tak zbude možná čas i na studium. Nabízím možnost prolistovat některé české internetové zdroje. Osobně se domnívám, že články na níže uvedených adresách obsahují řadu kvalitních informací a každý, kdo má o tuto problematiku zájem, zde jistě najde mnoho užitečného.

Seznam je nepochybně neúplný - nikoho jsem ovšem úmyslně nevynechal, ale jiné české zdroje (mimo jednotlivých článků v časopisech Chip, ComputerWorld, IT-NET apod.) ve své "databance" nemám. Uvítám proto upozornění na další vhodné zdroje a rád je v příštích číslech zveřejním.

Ing. Jaroslav Pinkava, CSc., AEC s.r.o.

Na www adrese http://www.aec.cz/ najdete ve sloupcovém menu volbu kryptologie.
Na této adrese je uložen kvalitně zpracovaný, rozsáhlý "Úvod do kryptologie" a dále 7 částí bulletinu AEC, který je věnován šifrování a obsahuje cenné odkazy na původní materiály. Připravuje se část věnovaná elektronickému podpisu. Soubory jsou uloženy v html podobě.

Doc. Ing. Jan Staudek, CSc. - Masarykova univerzita, Brno

Katedra programových systémů a komunikací
Bezpečnost v informačních technologiích
http://www.fi.muni.cz/usr/staudek/vyuka/security/P017.html
1.Manažerský úvod do bezpečnosti IT
2.Kryptografie a bezpečnost
3.Vybrané bezpečnostní funkce
4.Elektronický obchod a jeho bezpečnost
5.Bezpečnost v počítačových sítích
(vše v postscriptu *.ps file)
K dispozici jsou velice hodnotné, odborné články. Celkem je zde k dispozici více než 75 Mb zdrojového textu !

Mgr. Pavel Vondruška, NBÚ

Sešity Crypto-World (Kryptologická sekce Jednoty Československých Matematiků a Fyziků)
http://www.mujweb.cz/veda/gcucmp/
Sešity jsou ve formátu PDF (pro orientační náhled v html).

RNDr. Vlastimil Klíma, Decros s.r.o.

Na URL adrese Decrosu je k dispozici rozsáhlý archiv publikací známého českého kryptologa Dr.Klímy a jeho firemního kolegy Dr.Rosy. Články jsou velmi čtivé.
http://www.decros.cz/Security_Division/Crypto_Research/publikace.htm
K dispozici je komentovaný seznam publikací, ve kterém lze vyhledávat podle názvů nebo podle klíčových slov.

Mgr. Václav Matyáš, PhD., ml.
Populární rozsáhlý seriál o bezpečnosti a informačním soukromí "Bezpečnost pro všechny, soukromí pro každého" (celkem 57 pokračování) redigovaný V.Matyášem, který vycházel na pokračování v ComputerWorldu (10/97 - 40/98), je nyní celý dostupný na adrese : http://www.cw.cz/cw.nsf/page/BF1F077C380BCBC5C12568AE00489FB6
Soubory jsou v htm formátu. Celý seriál lze stáhnout najednou - celková délka (zazipováno) je jen 570 kb.
Další zajímavé informace (včetně informací o studiu) lze získat na osobní stránce Dr.Matyáše http://www.fi.muni.cz/usr/matyas/

Mgr. Antonín Beneš, MFF UK Praha
KSI (Katedra systémového inženýrství)

Přednášky v elektronické podobě z předmětu "Ochrana informace" jsou uloženy na http://www.kolej.mff.cuni.cz/prednes/oipage.html
Jedná se o původní zdrojové dokumenty. Vytvořeny jsou následující soustavou programů:
Microsoft Word for Windows 6.0a, počínaje 7. částí MS Word for Windows'95 7.0 ,
Microsoft Equation Editor 2.0 a Corel DRAW! 5.0 .

O něco stručnější jsou elektronické přednášky k předmětu "Bezpečnost IS v praxi". Tyto přednášky jsou dostupné na http://www.kolej.mff.cuni.cz/bezpsem/index.html

Přednášky a doprovodné texty k semináři "Matematické principy informační bezpečnosti" (vedoucí RNDr. Jiří Souček, DrSc. a Mgr.Tonda Beneš) jsou dostupné na http://www.mujweb.cz/veda/gcucmp/mff/index.html . Zrcadlo doplněné o některé texty v elektronické podobě lze najít na http://www.kolej.mff.cuni.cz/kryptsem/index.html .

Pro úplné začátečníky doporučuji nahlédnout na pečlivě vedenou stránku **Stanislava Chromčáka** : "Šifrování pro děti". http://freeweb.coco.cz/ANCHOR/sifry/index.htm .

Zajímavým zdrojem informací mohou být pro pražské zájemce veřejné semináře pořádané **BITIS** (Sdružení pro bezpečnost informačních technologií a informačních systémů). Informace o těchto seminářích lze nalézt na prozatímní adrese :
http://www.mujweb.cz/veda/bitis

Na závěr si dovolím upozornit na dvouměsíčník "**Data Security Management**", který je věnovaný problematice bezpečnosti dat a je orientován na manažery. URL adresa je http://www.dsm.tate.cz

F. Letem šifrovým světem

1. Prezident republiky Václav Havel podepsal 11.7.2000 zákon o elektronickém podpisu. Tento zákon nabývá účinnosti 1.10.2000. Téměř současně proběhl podobný akt i v USA; prezident Bill Clinton podepsal americký zákon o elektronickém podpisu (Electronic Signatures in Global and National Commerce Act) na stejném místě, kde byl před 224 lety podepsán nejdůležitější akt v dějinách USA - Declartion of Independence. Bill Clinton symbolicky zákon podepsal elektronicky pomocí svého soukromého klíče.
   Mohl tak učinit i náš prezident ? Ano, mohl. Jak jsem zjistil při prohlížení vydaných certifikátů I.CA (www.ica.cz), má zde registrován svůj veřejný klíč (určen pro RSA, délka modulu 1024 bitů). Platnost klíče je omezena na kritickou dobu, kdy se vědělo, že prezident bude český zákon o elektronickém podpisu signovat (10.7.2000-24.7.2000). Sériové číslo tohoto certifikátu je : 72028. Subject : Vaclav Havel / email=vaclav.havel@hrad.cz . Připomenu, že Václav Havel podepsal náš zákon o elektronickém podpisu na své cestě po Balkáně - v Dubrovníku. Možná, že kdyby se akt nekonal mimo ČR, že by prezident také použil symbolicky elektronický podpis, možná …

2. Sdružení pro informační společnost (SPIS) uspořádalo 13.7.2000 happennig u příležitosti podpisu zákona o elektronickém podpisu prezidentem ČR (SPIS eSignature Construction Happening 2000). Na akci byli pozváni všichni, kteří se na přípravě a prosazování zákona o elektronickém podpisu podíleli. Setkání proběhlo v přátelské atmosféře a zbývá jen doufat, že naplnění zákona bude realizováno co nejdříve.

3. V květnu byl schválen důležitý dokument - evropský standard o formátech elektronického podpisu - ETSI ES 201733 (Electronic Signature Formats). Je volně dostupný na webowské stránce ETSI http://webapp.etsi.org/pda/ nebo na stránce ETSI věnované elektronickému podpisu http://www.etsi.org/sec/el-sign.htm .
   V průběhu července byla uveřejněna žádost o komentování draftu dokumentu, který se týká požadavků na jednotné hodnocení poskytovatelů certifikačních služeb, které vydávají kvalifikované certifikáty :“Policy Requirements for Certification Service Providers Issuing Qualified Certificates” (ETSI 155 T1 Draft H, 15.7.2000) . O rychlosti, s jakou ETSI pracuje, svědčí i datum do kdy se přijímají komentáře - 15.9.2000. Do konce roku 2000 vyjde celá řada dalších důležitých dokumentů. Osobně se domnívám, že by k jejich obsahu mělo být přihlédnutu při vytváření obdobných dokumentů - vyhlášek - úřadem ÚOOÚ, kterému ze zákona o elektronickém podpisu náleží dozor nad akreditovanými certifikačními autoritami a nad certifikačními autoritami vydávajícími kvalifikované certifikáty.

4. Michelle Finley uveřejnil článek "Phone Phreaks to Rise Again?" (http://www.wired.com/news/business/0,1367,36309,00.html). V článku popisuje nové možnosti útoků "telefonních hackerů", které umožňuje zavedení IP telefonie. Phreackeři jsou částí počítačového undergroundu a v minulosti (v 60-tých a 70-tých letech) nechvalně prosluli svými útoky proti telefonním technologiím. Finley upozorňuje, že novodobá technologie může vést k "zmrtvýchvstání" této dnes již téměř zaniklé komunity.

5. Z adresy http://www.rsasecurity.com/rsalabs/faq/index.html lze stáhnout novou verzi (datovanou k 27.6.2000) známého dokumentu "RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1". Velikost PDF verze je 1 521 172 bytů, zazipováno pouze 888 372 bytů.

6. (J.Pinkava) Autoři kryptosystému NTRU se rozhodli pro jeho patentování. Přestože původně byl kryptosystém předložen k zařazení do soustavy norem, kterou připravuje skupina IEEE P1363, nakonec se autoři (Jeffrey Hoffstein,Jill Pipher a Joseph H. Silverman) rozhodli jít cestou patentů. Přitom kryptosystém NTRU je z řady hledisek pro uživatele velice zajímavý. Jeho velkou předností je především dosahovaná rychlost práce vlastního algoritmu. NTRU byl nejprve prezentován Jeffrey Hoffsteinem na rump session na konferenci CRYPTO 96, publikován byl v roce 1998 (http://www.ntru.com).
   Novinkou je úmysl autorů využít tento kryptosystém k ochraně autorských práv digitalizovaných hudebních nahrávek
   http://www.nytimes.com/library/tech/00/07/biztech/articles/03pate.html).
   Např. firmy Greylock Management and Sony Corporation se rozhodly investicí ve výši 11 milionů dolarů podpořit vývoj této nové technologie.

Na závěr něco z letní okurkové sezóny :

7. ŠIFROVAT,ŠIFROVAT,ŠIFROVAT!
   Vladimír Železný zveřejnil informaci, že má k dispozici dokumenty, které dokládají, že americká společnost CME připravovala násilné ovládnutí TV NOVA. Jedná se o e-mailové texty posílané elektronickou poštou mezi manažery CME Johnem Schwalliem a Petrem Sládečkem. Texty byly získány z pevného disku příjemce. Je až zarážející, že manažeři takovéhoto mediálního gigantu nepoužívali k zálohování a pravděpodobně ani ke komunikaci některý šifrovací software.
   Problém bude ovšem s prokazováním autentičnosti e-mailů - nebyly elektronicky podepsány nebo označeny časovým razítkem. Při této příležitosti mne napadla otázka, jak se vyrovnají naše soudy s případným sporem, kdy jedna strana předloží jako důkaz dokument, který bude elektronicky podepsán, ale stalo se tak ještě před datem nabytí platnosti našeho zákona o elektronickém podpisu (1.10.2000)? Pokud je mi známo, zákon tuto situaci neřeší.

8. V Británii se začalo pracovat na projektu Noemova archa 21.století s cílem archivovat, tj. dokumentovat a bezpečně uložit na jednom místě obrázky a zvuky všech ohrožených zvířat a rostlin na světě. (http://www.arkive.co.uk).

9. Dobrovolný "internetový" vězeň DotComGuy, odkázaný jen na sebe a svůj počítač, oslavil malé jubileum svého pobytu v pronajatém domě v Dallasu. 26-ti letý inženýr Mitch Maddox se dobrovolně zavázal na dobu jednoho roku založit svůj život jen na využívání e-komerce. Nastěhoval se do prázdného domu a změnil své občanské jméno na přezdívku DotComGuy. Nyní je již 8 měsíců zavřený v obklíčení internetových kamer, přičemž pro své každodenní potřeby může využívat jen internet a služby, které tato síť poskytuje.

G. Závěrečné informace

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

Stránku lze také najít pomocí vyhledavače "yahoo" nebo "seznam", případně ji můžete navštívit z http://www.trustcert.cz

Spojení :

p.vondruska@nbu.cz - běžná komunikace, zasílání příspěvků

pavel.vondruska@post.cz - osobní poštovní stránka, registrace odběratelů

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 českých matematiků a fyziků" (GCUCMP). Pokud má kdokoliv zájem o zasílání tohoto sešitu, může se zaregistrovat pomocí e-mailu na adrese pavel.vondruska@post.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.