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.**

+ příloha : ZoEP.htm

Dnešní užitečnou přílohou je plné znění zákona č.227/2000 Sb.- "Zákon o elektronickém podpisu a o změně některých dalších zákonů (Zákon o elektronickém podpisu)", který nabyl účinnosti 1.10.2000.

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 konci 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:

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

Dále vygeneruje tzv. základ (bazi) g a (nepovinně) i délku l - v bitech - soukromých dat (platí $2^{l-1} \leq p$.). 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 $2^{l-1} \leq x < 2^{l}$. 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.

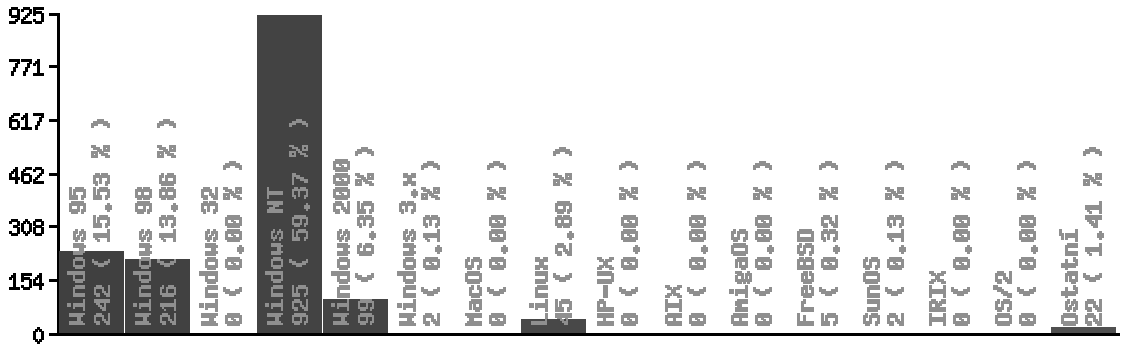
F. Statistika návštěvnosti stránky http://www.mujweb.cz/veda/gcucmp
Mgr. Pavel Vondruška (NBÚ)

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

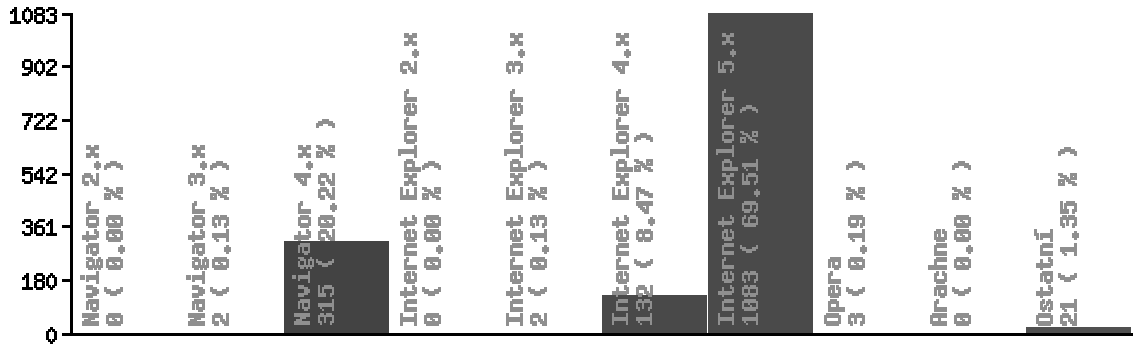


Graf přístupů na www stránku GCUCMP podle typu OS za období 11.8-9.10

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

Informace pro odběratele e-zinu. Poslední rozeslané číslo (9/2000) v PDF formátu nemá barevné obrázky a aktivní hypertextové linky. Překlad do PDF formátu uložený na www stránkách má již tento "nedostatek" odstraněn. Můžete si jej, pokud máte zájem, odtud stáhnout. S převody budou možná nějakou dobu i nadále menší potíže (např. e-zin vyjde 2-3 dny po uzávěrce). Bohužel můj spolupracovník z ČVUT, který mi prováděl převody do PDF a který legálně vlastnil potřebný software a který byl ochoten kdykoliv ihned pomoci, musel nastoupit základní vojenskou službu. Nebudu jej jmenovat, respektuji, že chce zůstat v anonymitě, ale chci mu alespoň touto cestou poděkovat a přeji mu, aby mu vojna rychle uběhla a zůstaly mu na ni jen samé pěkné vzpomínky ! Díky M.K.!

Současně mi dovolte, 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.

6. 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"

H. Závěrečné informace

1.Sešit

Crypto-World je oficiální informační sešit primárně určený pro členy "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (Internet, noviny) nebo se jedná o původní články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

Adresa URL , na níž můžete najít tento sešit (nejdříve 15 dní po jeho rozeslání) a předchozí sešity GCUCMP (zkonvertovány do PDF formátu), informace o přednáškách z kryptologie na MFF UK, některé články a další související témata :

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

Pokud se zajímáte pouze o sešit Crypto-World, můžete použít lépe dostupnou adresu:

http://cryptoworld.certifikuj.cz

2.Registrace - zrušení registrace

Pokud má kdokoliv zájem o zasílání tohoto sešitu, může se zaregistrovat pomocí e-mailu na adrese pavel.vondruska@post.cz (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci formulář na http://www.mujweb.cz/veda/gcucmp/ . Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání sešitu.

Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@post.cz (předmět: ruším odběr Crypto-Worldu !). Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu na kterou byl sešit zasílán.

3.Spojení

p.vondruska@nbu.cz	-	běžná komunikace, zasílání příspěvků
pavel.vondruska@post.cz	-	osobní poštovní stránka, registrace odběratelů
pavel.vondruska@sms.paegas.cz	-	zasílání SMS