Crypto-World

Informační sešit GCUCMP

Ročník 3, číslo 10/2001 15. říjen 2001

10/2001

Připravil : Mgr.Pavel Vondruška,
Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adresách
http://www.mujweb.cz/veda/gcucmp/
+ http://cryptoworld.certifikuj.cz
(>320 e-mail výtisků)

OBSAH : **Str.**

Příloha : Vyhláška 366/2001 Sb. (366_2001.pdf)
(prováděcí vyhláška ÚOOÚ k Zákonu o elektronickém podpisu č.227/2000 ve tvaru předaném k vyhlášení ve Sbírce zákonů)

A. Soutěž 2001 , II.část - Absolutně bezpečný systém
Pavel Vondruška, ÚOOÚ

V dnešním čísle pokračuje soutěž v luštění různých jednoduchých problémů souvisejících se základními šifrovými systémy. Tak jako v loňském roce probíhá i letošní soutěž celkem ve čtyřech kolech. V každém ze sešitů 9/2001 až 12/2001 bude uveřejněna jedna nebo dvě soutěžní úlohy a současně uveden doprovodný text k této úloze. Řešitelé, kteří zašlou správné řešení ve stanoveném termínu, budou slosováni a výherce získá symbolickou cenu kola. I po tomto datu lze však řešení dále zasílat, všechna řešení budou zkontrolována a bodově ohodnocena. 30.12.2001 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, tedy do 30.12.2001; přijde jen o možnost být vylosován jako vítěz příslušného kola. První číslo e-zinu v roce 2002 bude věnováno výsledkům a průběhu soutěže, budou uvedena řešení úloh všech kol a jméno celkového vítěze; uveřejníme také menší statistiku k celé soutěži. Hlavní cenu soutěže věnoval jeden z loňských úspěšných řešitelů . Cena je velice lákavá bedna kvalitního bulharského vína (6 lahví).

Cenu I. kola : CD se staršími čísly Crypto-Worldu a placený („ostrý“) certifikát od I.CA získal Kare Š. Losování mezi úspěšnými řešiteli proběhlo 14.10.2001 .

Připomeňme, jaké úlohy byly již čtenářům předloženy:

Září - jednoduchá záměna , kódová kniha

Řešitel	I.kolo 1.úloha	I.kolo 2.úloha	II.kolo 3.úloha	III.kolo 4.úloha	III.kolo 5.úloha	IV.kolo 6.úloha
Jan J.	19.09 / 10	19.09 / 10				
František P.	19.09 / 10	19.09 / 10				
Jozef K.	02.10 / 10	02.10 / 10				
Richard K.	04.10 / 10	04.10 / 10				
Karel Š.	**10.10 / 10**	**10.10 / 10**				
Tomáš V.		26.09 / 10				
Jan K.		30.09 / 10				

Absolutně bezpečný systém – Vernamova šifra

(využit článek P.Vondruška: „Od zákopové války k asymetrické kryptografii“, COMPUTERWORLD 38/2000)

Jako blesk z čistého nebe proto zapůsobily dvě práce jednoho z velikánů kryptologie dvacátého století Claude Elwood Shannona. V časopise Bell Systém Technical Journal v roce 1948 a 1949 otiskuje články "Matematická teorie sdělování" a "Sdělovací teorie tajných systémů". Prvý z článků dal vznik teorii informací, druhý článek pojednával o kryptologii v termínech informační teorie. Pojetí nadbytečnosti (redundancy) je hlavním termínem, který Shannon zavedl. Oba články fakticky odstartovaly moderní pojetí matematického zkoumání základů kryptografie a kryptoanylýzy a staly se pro rozvoj veřejné kryptologie stěžejními díly a pravděpodobně nejcitovanějšími pracemi v tomto oboru do konce sedmdesátých let.

Nová kvalitní kryptografická zařízení, která se v této době začala vyrábět po celém světě, byla zpravidla založena na velice jednoduchém principu, sčítání otevřeného textu s náhodným heslem. Systém navrhl roku 1917 Gilbert Vernam pro společnost American Telephone and Telegraph (AT&T). Původní Vernamovo řešení využívalo děrnou pásku, která se zaváděla do dálnopisu. Páska obsahovala náhodná čísla, která se „sčítala“ se znaky psanými na klávesnici dálnopisného stroje. Posloupnost vstupních čísel byla náhodná a každá děrná páska s heslem se směla použít pouze jednou. O prvenství Vernama se píše ve všech učebnicích kryptologie.

V knize Jiřího Janečka : „Gentlemani nečtou cizí dopisy“ na straně 28 je však uvedeno, že tuto metodu poprvé zveřejnil již v roce 1892 německý kryptolog Hermann ve své knize „Metoda šifrování a dešifrování tejných depeší“. Dokonce píše, že kryptolog Hermann správně navrhl, že je třeba používat heslo stejně dlouhé, jako je otevřený text. Je tedy možné, že Vernam pouze tuto jeho myšlenku jako prvý realizoval.

Z publikované teorie amerického vědce Shannona (o níž jsme se zmínili v úvodu) vyplynulo to, co Vernam nemohl ještě vědět, když tuto metodu použil, že absolutně bezpečný systém je právě toto sčítání otevřené zprávy se stejně dlouhým náhodným heslem. Velice jednoduché -- jenže je zde malý problém. K odšifrování samozřejmě potřebujeme mít k dispozici příslušné náhodné heslo, které jsme přičetli k původní zprávě. A to je právě onen základní problém celého systému. Místo tajného doručení původního otevřeného textu délky N musíme na místo určení doručit heslový materiál -- náhodnou posloupnost stejné délky, tedy délky N. Problém je to tedy téměř ekvivalentní (samozřejmě, heslový materiál lze doručit ve velkém množství a do zásoby ještě před nutností vyslat zprávu). Při objemu dnes předávaných zpráv je tento systém nevyhovující. Jeho význam je v tom, že se jedná o jediný absolutně bezpečný systém -- pokud jsou dodrženy následující podmínky:

* umíme vyrobit náhodné, stejně pravděpodobné heslo (výroba takového hesla byla v 60. letech velkým problémem)
* máme dostatečně důvěryhodný kanál k transportu hesla na místo určení
* korespondence je tak slabá, že nám nevadí velká spotřeba hesla
* každé heslo lze použít pouze jednou a je tedy potřeba dodržovat určitá přesně daná pravidla pro zacházení s heslovým materiálem.

Tuto metodu používala v sedmdesátých a osmdesátých letech i česká diplomatická služba. Autorem návrhu příslušného šifrového systému byl Alojz Lorenc, který o dvacet let později (již ve funkci prvního náměstka ministra vnitra) nechvalně proslul v listopadových událostech.

Také kubánská krize na začátku šedesátých let vyvolala potřebu rychlého a bezpečného spojení mezi USA a SSSR. Obě mocnosti se domluvily na vybudování horké linky mezi hlavami obou států. Pro tuto linku byl zvolen výše popsaný systém. Horká linka byla uvedena do provozu 30. 8. 1963 . Kreml i Bílý dům si vzájemně vyměnily heslové materiály -- pásky. Otevřené texty se převedly do dálnopisného kódu a sčítaly se s heslovým materiálem, heslová páska byla ihned po použití automaticky ničena, čímž se mělo zamezit jejímu nechtěnému opětovnému použití. Při zavedení tohoto systému se použilo zařízení ETCRRM-II (Electronic Teleprinter Cryptographic Regenerative Repeater Mixer II). Každou hodinu se přenášely zkušební relace. Ze strany americké se přenášely výsledky basebalových zápasů a ze strany ruské výňatky z Lovcových zápisků od Turgeněva. Použití kódových pásků, které se vyměňují prostřednictvím velvyslanectví jednotlivých států, zajišťuje naprostou bezpečnost přenášených zpráv a také -- což je velmi důležité -- nemožnost vpašování falešné zprávy.

Rozsah provozu právě v této době závratně rostl. V r. 1930 představoval telegrafní provoz v celých USA 2,2 miliony slov, v lednu 1960 jen Ministerstvo zahraničních věcí USA vyslalo a přijalo stejné množství slov za 14 dní. V červnu 1961 již bylo přeneseno 6,929 milionů slov za jeden měsíc. Jednalo se tedy o zvýšení zátěže provozu o 40 % za rok a půl!

Potřeba důvěrné komunikace mezi subjekty se dále zvyšovala a náklady na výrobu a transport heslového materiálu stále rostly. Současně se stávalo, že při nedostatku heslového materiálu byla porušena zásada nepoužít stejné heslo dvakrát, a také při distribuci tak ohromného množství šifrového materiálu mohlo dojít k tomu, že se k heslovému materiálu dostala nepovolaná osoba.

Absolventi vojenských kateder 70. let si jistě pamatují na stále vtloukaný slogan: "Bez spojení není velení", a tak nastala doba inovace. Bylo nutno opustit předávání heslového materiálu délky zprávy a přejít na jiný systém. Řešením se zdálo generování hesla přímo kryptografickým zařízením. Přijímač a vysílač generoval pseudonáhodné heslo. Počáteční nastavení bylo dáno zpravidla tzv. inicializačním vektorem a klíčem. Stačilo se jen domluvit na počátečním nastavení. Kvalita tohoto systému závisí na kvalitě pseudonáhodné posloupnosti a počtu možných počátečních stavů, které pak generují různé pseudonáhodné posloupnosti. Tento problém je z matematického hlediska velice složitý a byl slabinou některých komerčně vyráběných zařízení té doby.

PŘÍLOHA :

Různé způsoby skládání hesla a otevřeného textu

Otevřený text :	**A**	**H**	**O**	**J**	**P**	**E**	**T**	**Ř**	**E**
Otevřený text O:	**65**	**72**	**79**	**74**	**80**	**69**	**84**	**82**	**69**

(po převodu do číselného tvaru)

Heslo H: **1 4 5 9 6 2 3 4 7 8 5 4 3 2 1 1 8 5**

Výsledný **šifrový text** budeme značit **Š .**

Převodová (kódová tabulka):

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
6						A	B	C	D	E
7	G	G	H	I	J	K	L	M	N	O
8	P	Q	R	S	T	U	V	W	X	Y
9	Z									

I. metoda

Š = O + H (O = Š – H)

šifrování																		
O	6	5	7	2	7	9	7	4	8	0	6	9	8	4	8	2	6	9
H	1	4	5	9	6	2	3	4	7	8	5	4	3	2	1	1	8	5
Š=O+H	7	9	2	1	3	1	0	8	5	8	1	3	1	6	9	3	4	4

dešifrování																		
Š	7	9	2	1	3	1	0	8	5	8	1	3	1	6	9	3	4	4
H	1	4	5	9	6	2	3	4	7	8	5	4	3	2	1	1	8	5
O=Š-H	6	5	7	2	7	9	7	4	8	0	6	9	8	4	8	2	6	9

II. metoda

Š = O - H (O = Š + H)

Šifrování																		
O	6	5	7	2	7	9	7	4	8	0	6	9	8	4	8	2	6	9
H	1	4	5	9	6	2	3	4	7	8	5	4	3	2	1	1	8	5
Š=O-H	5	1	2	3	1	7	4	0	1	2	1	5	5	2	7	1	8	4

Dešifrování																		
Š	5	1	2	3	1	7	4	0	1	2	1	5	5	2	7	1	8	4
H	1	4	5	9	6	2	3	4	7	8	5	4	3	2	1	1	8	5
O=Š+H	6	5	7	2	7	9	7	4	8	0	6	9	8	4	8	2	6	9

III. metoda (tzv. symetrická)
Š + O = H (Š = H - O , O = H - Š)
Výhodou této metody je, že šifrování i dešifrování probíhá podle „stejného algoritmu“. Stačí tedy naprogramovat jen jednu rutinu R (X-Y) a vhodně plnit X a Y.

šifrování																		
H	1	4	5	9	6	2	3	4	7	8	5	4	3	2	1	1	8	5
O	6	5	7	2	7	9	7	4	8	0	6	9	8	4	8	2	6	9
Š=H-O	5	9	8	7	9	3	6	0	9	8	9	5	5	8	3	9	2	6

dešifrování																		
H	1	4	5	9	6	2	3	4	7	8	5	4	3	2	1	1	8	5
Š	5	9	8	7	9	3	6	0	9	8	9	5	5	8	3	9	2	6
O=H-Š	6	5	7	2	7	9	7	4	8	0	6	9	8	4	8	2	6	9

Luštění

Situace I.
Odesílatel použil heslo dvakrát a text je dostatečně dlouhý. V takovém případě lze ze šifrových textů získat poměrně jednoduše otevřený text.

Předpokládejme, že odesílatel zašifroval texty O1 a O2 pomocí stejného hesla H. Získal tak dva různé šifrové texty Š1 a Š2. Předpokládejme, že útočník zachytil tyto dva texty. Symbolicky zapíšeme tuto situaci takto:
O1+H=Š1, O2+H=Š2 , útočník zná : Š1 a Š2

Útočník nyní spočte Š1-Š2 = O1+H - O2-H = O1-O2 a získá tak rozdíl otevřených textů O1 a O2 !

Kdyby nyní luštitel (kryptoanalytik) znal otevřený text O1, snadno otevřený text O2 dopočte.
Luštitel nyní může postupovat např. takto - zkusí hádat části otevřeného textu (datum, podpis, předpokládané slovo, číslo telegramu, jména měst, lodí apod.) a dívat se, zda v textu O2 se objevují smysluplné úseky. Postupným rozšiřováním získaných úseků v textu O1 (ale i v O2) pak může získat obsah obou zpráv. Uvedený způsob lze do jisté míry zautomatizovat např. tím, že v textu O1 se nechávají „posunovat“ výrazy ze slovníku a vyhodnocuje se (např. pomocí bigramových a trigramových vazeb), zda se v textu O2 objevuje otevřený smysluplný text. Tato metoda luštění je velice účinná.
Z absolutně bezpečného systému se tak může stát (díky chybě obsluhy) jednoduchý školní případ.

Situace II.
Kryptoanalytik zjistí, že heslo je získáváno „nekorektně“:
- nejedná se o náhodnou posloupnost (kryptoanalytik je schopen heslo rekonstruovat)
- posloupnost se periodicky opakuje (kryptoanalytik získaný periodický úsek hesla postupně kombinuje se šifrovým textem a zjišťuje, zda získaný otevřený text je hledaným smysluplným textem)
- výstup sice může být z hlediska statistických metod náhodnou posloupností, ale vygenerovaná posloupnost závisí na počátečním stavu a těchto stavů je malý počet (kryptoanalytik vygeneruje všechny možné počáteční stavy a získá příslušné pseudonáhodné posloupnosti; takto získané psedudonáhodné posloupnosti kombinuje s šifrovým textem a snaží se získat příslušný otevřený text)

Situace III.
Útočník získá heslo. Potom již kryptoanalytik postupuje obdobně jako příjemce šifrového textu a text pohodlně dešifruje. Komplikací může být pouze to, pokud získá heslo velké délky a neví, od kterého úseku má začít heslo kombinovat s příslušným šifrovým textem. Dalším problémem může být, že neví jak byl otevřený text převeden – překódován do číselné podoby a jaká metoda slučování (viz. příloha) byla použita. Nezbývá tedy, než heslo postupně „posunovat" a zjišťovat (pro všechny metody slučování) zda vzniká smysluplný výsledek.

Příklad (řešení pro situaci III):

Předpokládáme, že pro převod znaků do číselného (dekadického) tvaru byla použita tabulka uvedená v příloze.

Podařilo se nám získat toto heslo: 614596234785432118589562356253456685 1
Dále se nám podařilo získat tento šifrový text : 598793609895583926

Pokus 1 (heslo použito od prvé pozice):

H	761459623478543211858956235625345668 51	
Š	598793609895583926	
O=H-Š	273766024683060395	
	*I L - - D - - -	nelze dekódovat podle převodové tabulky
O=Š+H	259142222263026137	
	- - - - - - - - - -	nelze dekódovat podle převodové tabulky
O=Š-H	837344086427040715	
	S I - - - - - - - -	nelze dekódovat podle převodové tabulky

Pokus 2 (heslo použito od druhé pozice)

H	614596234785432118589562356253456685 1
Š	598793609895583926
O=H-Š	prosím doplňte si sami ☺
O=Š+H	prosím doplňte si sami ☺
O=Š-H	prosím doplňte si sami ☺

Pokus 3 (heslo použito od třetí pozice)

H	145962347854321185895623562534566851	
Š	598793609895583926	
O=H-Ś	657279748069848269	
	A H O J P E T R E	**hledaný otevřený text**

Úloha č.3 - Vernamova šifra

81 74 98 02 90 13 06 10 13 26 15 34 33 36 57 34 67 58 72 86 80 75 75

Nápověda : Příloha Crypto-World 78/2000.
Příjemný zážitek z luštění.

Závěrečné pokyny pro řešitele
Řešení zasílejte e-mailem na adresu pavel.vondruska@post.cz (kopii prosím zaslat na pavel.vondruska@uoou.cz). Předmět označte heslem : ULOHA-3
Termín: do slosování budou zařazena všechna správná a úplná řešení, přijatá do 14.11.2001 !

B. E-komunikace začíná ! (?)

Mgr. Pavel Vondruška, ÚOOÚ

(článek byl připraven pro časopis Veřejná správa, zde je uvedena jeho doplněná a aktualizovaná verze)

Z článků publikovaných v poslední době se zdá, že se konečně dočkáme – elektronický podpis se začne používat do konce tohoto roku. Sliby voličům o elektronické komunikaci mezi občanem a státem dostávají reálnou podobu. Již před rokem (1.10.2000) vstoupil v účinnost Zákon o elektronickém podpisu a o změně některých dalších zákonů č.227/2000 (dále jen Zákon č.227/2000 Sb.). Následovala řada dalších kroků nutných k tomu, aby mohla být slíbená komunikace realizována. Na základě zmocnění v Zákoně č.227/2000 Sb. připravil Úřad pro ochranu osobních údajů znění návrhu vyhlášky, ale musel ještě čekat na novelu zákona č.101/2000, která mu (zjednodušeně řečeno) umožnila nejen vyhlášku připravit, ale také publikovat ve Sbírce zákonů. Po rozsáhlém připomínkovém řízení byla vyhláška předána k projednání v příslušných komisích Legislativní rady vlády ČR. Po projednání v těchto komisích byla podepsána předsedou ÚOOÚ a to dne 3.10.2001. Její celý název je: „Vyhláška o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu“. Vyhlášena byla ve Sbírce zákonů 10.10.2001 pod číslem 366/2001. Tato vyhláška nabyla účinnosti dnem vyhlášení. Dalším nutným krokem bylo vydání dlouho očekávaného Nařízení vlády č.304/2001 ze dne 25. července 2001. Toto nařízení upravuje komunikaci v oblasti občan-stát a současně stanovuje vytvoření podmínek pro tuto komunikaci v oblasti orgánů veřejné moci – především zřízení tzv. „elektronických podatelen“. Tato pracoviště pro příjem a odesílání datových zpráv budou vybavena potřebnými zařízeními připojenými k veřejné datové síti, popřípadě k jiným datovým sítím a budou muset splňovat požadavky na technické a programové vybavení podle standardů, které jsou v současné době připravované Úřadem pro veřejné informační systémy a umožňujícími používání zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb. Mimo vybudování těchto pracovišť se musí dále připravovat orgány veřejné moci na tuto komunikaci i vytvářením příslušných elektronických formulářů (v akceptovatelných formátech), vyhlášením bezpečnostní politiky podatelny, vhodné by bylo vyhlásit i certifikační politiku (nebo alespoň požadovanou datovou strukturu certifikátu), „státní“ PKI, zaškolit obsluhu, upravit příslušný spisový řád, určit způsob archivace apod. Orgán veřejné moci musí dále vybavit své zaměstnance, kteří se budou jménem tohoto orgánu elektronicky podepisovat, kvalifikovanými certifikáty vydanými některým z akreditovaných poskytovatelů certifikačních služeb.

Důvod, proč jsou nutné takovéto certifikáty, plyne z **§11 Zákona č.227/2000 Sb.,** který říká, že v **oblasti orgánů veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb.**

Pro informaci dodávám, že Úřad pro ochranu osobních údajů doposud (8.10.2001) obdržel jedno oznámení o zahájení vydávání kvalifikovaných certifikátů (dle ustanovení § 6 odst. 5 Zákona o elektronickém podpisu č.227/2000 Sb.), a byla podána jedna žádost o udělení akreditace pro výkon činnosti akreditovaného poskytovatele certifikačních služeb dle ustanovení §10 odst. 1 Zákona o elektronickém podpisu.

Vraťme se nyní k vyhlášce ÚOOÚ k Zákonu č.227/2000. Vydání této vyhlášky bylo předpokladem pro zahájení činnosti poskytovatelů certifikačních služeb vydávajících

kvalifikované certifikáty a akreditovaných poskytovatelů certifikačních služeb. Lze očekávat, že Úřad pro ochranu osobních údajů obdrží v nejbližších dnech další oznámení od poskytovatelů certifikačních služeb hodlajících vydávat kvalifikované certifikáty a žádosti o udělení akreditace pro poskytování certifikačních služeb. Přehled akreditovaných poskytovatelů certifikačních služeb bude zveřejňován ve Věstníku Úřadu a bude k dispozici na www stránkách ÚOOÚ. Povinnost zveřejňovat tento přehled plyne přímo z § 9 odst. 2 písm. d) Zákona o elektronickém podpisu, který ukládá Úřadu pravidelně uveřejňovat přehled udělených akreditací a přehled poskytovatelů certifikačních služeb vydávajících kvalifikované certifikáty, a to i způsobem umožňujícím dálkový přístup. Dá se očekávat, že poskytovatel certifikačních služeb, který bude akreditován, bude využívat mediální prostředky, reklamu, své www stránky apod., aby tuto skutečnost zveřejnil. Předpokládáme, že takovýchto poskytovatelů nebude mnoho. Podmínky k udělení akreditace jsou velice přísné a zajištění všech podmínek (zejména bezpečnostních), které vyplývají ze Zákona č.227/2000, je náročné jak na finanční zdroje (desítky miliónů Kč), tak i na specifické vysoce odborné vzdělání některých klíčových zaměstnanců. Pro představu, kolik se dá očekávat takovýchto subjektů, uvedu, že např. v Německu jsou v současné době jen dva akreditovaní poskytovatelé certifikačních služeb a u třetího subjektu akreditace probíhá.

Komunikace občana se státem tedy bude fakticky zahájena až po vybudování elektronických podatelen na příslušných orgánech veřejné moci a po akreditaci prvních poskytovatelů certifikačních služeb, tedy až občan i zaměstnanec orgánu veřejné moci budou mít možnost pořídit si příslušný kvalifikovaný certifikát a také jej používat. O tom, zda takový certifikát občan nutně potřebuje nebo zda mu stačí „pouze“ kvalifikovaný certifikát, viz. krátká polemika na konci tohoto článku.

Jak plyne z předchozích řádků, zbývá splnit ještě řadu konkrétních kroků. Na třetím sympoziu o elektronickém podpisu Infoforum, které se konalo 4.září 2001 v Pardubicích a bylo určeno zástupcům veřejné správy a podnikatelům, odhadl ministr Karel Březina velice realisticky, že "… elektronické pošty budou moci u jednoduchých agend, u jejichž podání nevyžaduje zákon tiskopis v písemné podobě, využívat elektronický podpis již v příštím roce" . Dále uvedl, že bude velmi spokojen, když „.. v následujících třech až pěti letech by mohlo elektronické pošty ve styku s veřejnou správou využívat zhruba deset procent občanů ".

Vraťme se tedy k nadpisu našeho článku : „E-komunikace začíná !“. Je tedy toto tvrzení oprávněné? Nebo je snad ještě trochu předčasné? Z předchozích odstavců se zdá, že do zahájení komunikace s použitím elektronického podpisu ještě uběhne řada měsíců. Jak to tedy vlastně je? Pro správné zodpovězení této otázky je důležité si uvědomit, že námi dosud popisovaná komunikace se týkala pouze jediné oblasti - a to komunikace podle paragrafu 11 Zákona č.227/2000 Sb. - tedy komunikace v oblasti orgánů veřejné moci. Mimo této oblasti je však řada jiných situací, kde se již elektronický podpis běžně používá nebo se připravují projekty, kde se s využitím elektronického podpisu počítá. E-komunikace s využitím elektronického podpisu už tedy využívána je. Během několika let bude tvořit základ pro 20 až 25% celosvětové obchodní výměny zboží a služeb. Zdaleka nejznámější a nejpopulárnější mezi občany jsou "webovské" obchodní domy. Nákup zboží přes Internet se tak stává i pro řadu našich občanů samozřejmostí. Takovéto oblasti se říká B2C (business-to-customer/consumer) a tvoří jen malou část z celkového objemu elektronické komunikace založené na elektronickém podpisu. Zdaleka nejmohutnějším je režim B2B (business-to-business). Podle různých odhadů tvoří komunikace v této oblasti 78 až 90% veškeré komunikace za použití elektronického podpisu. B2B se od B2C liší natolik, že zkušenosti a znalosti jsou navzájem velice těžko přenositelné. Typy komunikace z pohledu subjektů

komunikace (osoba podepisující se a osoba spoléhající se na podpis) tím však nebyly ještě všechny vyčerpány. Nejlépe bude představit tyto možnosti tím, že je sestavíme do informační matice. Ve sloupci uvádím původce informace - tedy osobu, která se podepisuje, a v řádku pak adresáta - tedy obecně toho, kdo se na tuto komunikaci a tedy na elektronický podpis spoléhá. V jednotlivých polích tabulky jsou uvedeny konkrétní příklady takovéto komunikace. Možnosti, které zde uvádím, zdaleka nevyčerpávají všechny možné případy komunikace těchto subjektů a jsou spíše ilustrativním příkladem. Řada z nich byla uskutečnitelná ještě před účinností Zákona o elektronickém podpisu č.227/2000 Sb.. Takováto komunikace probíhala na základě smluvních vztahů (podle občanského nebo obchodního zákona). Možnost využívat zaručených elektronických podpisů a kvalifikovaných certifikátů podle zákona o elektronickém podpisu zvýší důvěru v takovouto komunikaci, obecně pak zajišťuje právní akceptovatelnost takovéto komunikace, jednotlivým subjektům ukládá práva a povinnosti a stanoví právní odpovědnost za nedodržení podmínek a požadavků stanovených v tomto zákoně. Hlavní výhodou tedy je, že subjekty mohou spolu komunikovat na základě tohoto zákona a nemusí spolu uzavírat speciální smlouvy nebo dohody o akceptovatelnosti elektronického podpisu v této komunikaci.

Původce informace	**Adresát**		
	Obchodník B=Business	**Spotřebitel C=Consumer (Costumer)**	**Státní instituce A=Administration (G=Government)**
Obchodník B=Business	**B2B** nákupní systémy velkých podniků (dříve EDI) (78-90 %)	**B2C** prodej knih, CD, elektroniky, potravin, lístků **Bank2C** bankovní služby	**B2A (B2G)** nabídka služeb a zboží, komunikace se státní správou přes Internet
Spotřebitel C=Consumer (Costumer)	**C2B** Sledování nabídek za účelem snížení ceny	**C2C** aukční systémy pro prodej použitého zboží ("bazar"), klasická e-mail korespondence	**C2A (C2G)** podávání daňových přiznání, volby, sčítání lidu
Státní instituce A=Administration (G=Government)	**A2B (G2B)** Zadávání veřejných zakázek, vypisování grantových projektů	**A2C** poskytování informací o veřejné správě	**A2A (G2G)** koordinace činnosti orgánů veřejné moci, mezinárodní koordinace

Již jsme se zmínili, že zákon ve svém paragrafu 11 upravuje používání elektronického podpisu v oblasti orgánů veřejné moci. Která oblast v naší matici to tedy je? Je to snad každá komunikace, na níž se podílí orgán veřejné moci (ať již jako původce informace nebo adresát)? Tedy v našem příkladě komunikace typu: A2B, A2C, A2A, C2A, B2A? Nebo jen komunikace C2A (občan - stát) a A2C (stát-občan), tedy ty oblasti, o kterých se nejvíce v souvislosti s nařízením vlády mluví? Odpověď není tak jednoduchá, jak se možná na první pohled zdá.

K otázce využívání elektronického podpisu v oblasti orgánů veřejné moci je potřeba dále přesně definovat, co se rozumí pojmem "orgán veřejné moci" a "v oblasti". K vysvětlení

těchto pojmů si pomohu stanoviskem Poradního sboru předsedy Úřadu pro ochranu osobních údajů.
„ … Pokud se týče vymezení pojmů veřejné moci a orgán veřejné moci, odkazuje se na usnesení Ústavního soudu ČSFR I. ÚS 19/92 /viz č. 3/1992 Sb./, kde je tento pojem definován a tato definice je akceptována i judikaturou Ústavního soudu České republiky. Výrazem „V oblasti orgánů veřejné moci…“ se rozumí situace, kdy je veřejná moc vykonávána, zejména tedy, pokud bude takový orgán vystupovat ve vztazích navenek vůči adresátům, mocensky rozhodovat o právech, povinnostech a právem chráněných zájmech fyzických a právnických osob. Může ovšem jít i o další vztahy, jako např. ty, které vznikají při rozhodování o právech a povinnostech zaměstnanců ve služebním poměru nebo i vztahy mezi dvěma orgány veřejné moci, pokud se tak činí při jejím výkonu /např. předávání vyjádření, stanovisek při přípravě právních předpisů a samozřejmě vydávání rozhodnutí/. V této souvislosti je třeba zdůraznit, že pro posouzení toho, zda se jedná o orgán veřejné moci, není důležitá skutečnost, zda takový orgán je organizační složkou státu či má-li /a v jakém rozsahu/ právní subjektivitu. Půjde-li však o činnost těchto orgánů ve vnitřních vztazích, není třeba používat zaručený elektronický podpis. Totéž pak platí i pro případ, kde takový orgán vystupuje v soukromoprávních vztazích /např. majetkových nebo pracovněprávních/. Na druhé straně nic nebrání tomu, aby i zde používaly orgány veřejné moci zaručené elektronické podpisy založené na kvalifikovaných certifikátech vydaných akreditovaným poskytovatelem certifikačních služeb ve smyslu § 11 zákona. …" .

Nejvíce problémová je komunikace občan – stát (v naší tabulce označeno jako C2A, resp. C2G). Právě zde, totiž není zcela jasné, zda tato komunikace spadá nebo nespadá do „oblasti veřejné moci“. Někteří právníci tvrdí, že tam nepatří. Jejich argumentace (zjednodušeně řečeno) : „občan nikdy veřejnou moc nevykonává a tedy se na něj § 11 Zákona o elektronickém podpisu č.227/2000 nevztahuje“. Možný je ovšem i výklad opačný. Např. doc. Mates a doc.Smejkal vykládají tentýž paragraf tak, že občan v případě podání (o němž se mocensky rozhoduje v orgánech veřejné moci) je účasten tohoto procesu a je „tedy v oblasti veřejné moci“ a tedy se na něj paragraf § 11 vztahuje.

Z hlediska řešení tohoto problému je zajímavý § 1 , odstavec 1 , písmeno c) a odstavec 3 - Nařízení vlády č. 304, kde se píše
…….“organizují práce v elektronické podatelně tak, aby bylo zajištěno přijímání a odesílání datových zpráv a neprodlená kontrola, zejména zda přijaté podání v elektronické podobě je čitelné, zda je podepsala osoba uvedená na **kvalifikovaném certifikátu** a zda je certifikát platný; při připojení bez nepřetržitého přístupu k veřejné datové síti zajistí“
…. „Pokud orgán veřejné moci při kontrole podle odstavce 1 písm. c) zjistí, že podání doručené v elektronické podobě nebo jeho část je nečitelné, datová zpráva **neobsahuje platný kvalifikovaný certifikát** nebo že …… postupuje podle příslušných ustanovení zvláštních právních předpisů upravujících odstraňování vad podání.“

Z dikce těchto dvou odstavců je zřejmé, že není vyžadován kvalifikovaný certifikát od akreditovaného poskytovatele certfikačních služeb, ale pouze kvalifikovaný certifikát. Tedy §11 Zákona o elektronickém podpisu č.227/2000 se na komunikaci občan – orgán veřejné moci v Nařízení vlády pro tuto oblast neuplatňuje!

Oblast, o níž jen obecně hovoří § 11 Zákona o elektronickém podpisu č.227/2000 Sb., je dále vymezena úžeji v Nařízení vlády č. 304 ze dne 25. července 2001. Nejlépe je definováno, na koho konkrétně se bude vztahovat připravované Nařízení vlády č. 304, přímo v tomto nařízení a to v § 1 , odstavci 1, ze kterého plyne, že je určeno pro všechny orgány

veřejné moci, u kterých ze zvláštních právních předpisů[1]) vyplývá povinnost přijmout podání učiněné v elektronické podobě, podepsané elektronicky, anebo stanoví-li zvláštní právní předpis právo orgánů veřejné moci činit úkony v elektronické podobě, podepsané elektronicky.

K praktickému využití elektronického podpisu v komunikaci občan-stát a stát-občan tedy ještě chybí uskutečnění řady konkrétních kroků. Jmenujme závěrem, co je třeba ještě všechno vykonat. Vydat standardy ÚVIS s požadavky na technické a programové vybavení pro uplatnění zaručeného elektronického podpisu pro orgány veřejné moci, udělit akreditaci poskytovatelům certifikačních služeb, zřídit elektronické podatelny na orgánech veřejné moci a samozřejmě a v neposlední řadě naučit se elektronický podpis správně používat.

Literatura

[1] Vondruška, P.: E-komunikace začíná !, Veřejná správa, v tisku
[2] Zákon o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) č. 227/2000 Sb.
[3] Nařízení vlády č.304/2001 ze dne 25. července 2001
[4] Vyhláška ÚOOÚ 366/2001 Sb. (k Zákonu o elektronickém podpisu č.227/2000 Sb.)
[5] Připravovaný metodický pokyn ÚVIS pro uplatnění zaručeného elektronického podpisu pro orgány veřejné moci
[6] Stanovisko Poradního sboru předsedy ÚOOÚ k otázce využívání elektronického podpisu v oblasti orgánů veřejné moci
[7] Vondruška, P.: E-komunikace, e-platby, e-projekty, e-platformy a „velcí hráči“ , Crypto-World 4/2001, http://www.mujweb.cz/veda/gcucmp
[8] Bosáková,D., Vondruška, P: Poskytovatelé certifikačních služeb v EU a ČR, Data Security Management, 5/2001
[9] Vondruska,P, Matejka, J.: The basic terms and legal aspects of the ESA from the practical use and security points of view, sborník mezinárodní konference IDET, Brno 2001

[1]) Zákon č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů.
Zákon č. 71/1967 Sb., o správním řízení (správní řád), ve znění pozdějších předpisů.
Zákon č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů.
Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.

C. Kryptografie a normy - Díl 10. Digitální certifikáty. Část 2. Norma X.509, verze 3.

Jaroslav Pinkava, AEC spol. s r.o.

l. Úvod

Daný článek se bude zabývat normou X.509, která historicky sehrála velice významnou roli.
Norma X.509 byly vytvořena s cílem dát rámec pro autentizaci ve vztahu k adresářovým službám popsaným v dokumentech řady X.500. Jak X.500, tak i X.509 jsou součástí serie X mezinárodních norem navržených organizacemi ISO a ITU. Normy X.500 byly navrženy pro popis adresářových služeb ve velkých počítačových sítích, X.509 pak zabezpečuje pro služby v rámci X.500 příslušný autentizační rámec. První verze normy X.509 se objevila v roce 1988 (a je to vlastně nejstarší návrh modelu PKI). Verze 3 pak podstatně rozšířila funkční záběr normy a v dnešní době většina produktů v oblasti PKI se řídí touto normou.

2. X.500

Nejprve se obrátíme k alespoň úvodnímu seznámení se s problematikou adresářů ve smyslu dokumentů řady X.500. Takovýto adresář se vlastně podobá telefonnímu seznamu, kde při daném jméně osoby najdeme příslušnou informaci o dané osobě. Samozřejmě X.500 dává více možností než pouhé jméno, adresa a číslo telefonu. Záznam v adresáři dle X.500 může obsahovat celou přehršel atributů, jako jsou např. jméno organizace pro kterou daná osoba pracuje, její pracovní zařazení, e-mailová adresa atd. Záznam v adresáři X.500 se nemusí týkat také pouze osoby, ale může zde být popsán počítač, tiskárna, firma atd. Takovýto záznam může také obsahovat digitální certifikát, který specifikuje veřejný klíč patřící příslušné entitě.

K tomu, aby byly možné efektivně prohlížet jednotlivé záznamy v adresáři, má každý záznam přiřazeno jednoznačné (globálně) jméno (anglicky distinguished name - DN). K tomu, aby byla jednoznačnost těchto jmen skutečně zabezpečena, napomáhá způsob jejich vytváření. A sice - X.500 adresáře jsou vytvářeny na základě jednoduchého hierarchického modelu (strom adresářů).
Každý uzel ve stromu má pouze jednoho "rodiče" a libovolné množství "potomků". Každému uzlu je pak přiřazeno tzv. relativní jednoznačné jméno. Kořenu (root) stromu je přiřazen záznam vztahující se k zeměpisné lokalitě (jednoznačný dvoumístný kód dle ISO - jiný pro každý stát).
Např. nechť Josef Novák pracuje pro firmu MROZ v České republice. Pak jeho jednoznačné jméno bude vypadat následovně:
Country = CZ,
Organization=MROZ,
CommonName=Josef Novák.

3. Certifikáty - X509 v.2 a v.3.

Do roku 1997 byla používána (a je ještě stále implementována v některých starších produktech) verze 2 normy X.509.
Certifikát dle této verze obsahuje následující položky:

- verze (verze normy X.509, zde tedy je číslo 2);
- pořadové číslo (jednoznačné dle vydávající CA);
- podpisový algoritmus CA (identifikátor algoritmu);
- jméno vydávající CA (dle X.500);
- období platnosti certifikátu (počátek a konec);
- jméno (dle X.500) entity, která je držitelem soukromého klíče odpovídajícího veřejnému klíči pro který byl certifikát vydán;
- informace o veřejném klíči (hodnota veřejného klíče a identifikátor příslušného algoritmu);
- jednoznačný identifikátor vydavatele certifikátu (ve verzi2 nepovinné);
- jednoznačný identifikátor entity, které patří certifikát (ve verzi2 nepovinné).

Verze dvě používala velice jednoduchý formát pro CRL, který se záhy ukázal jako překonaný. Třetí verze normy X.509 přinesla podstatné úpravy v normě. Základní změnou ve filosofii bylo umožnění existence vlastně libovolných rozšíření (extenzí) pro certifikáty a CRL. Pojem rozšíření byl definován tak, aby mohl obsahovat informaci o politice, o atributech majitele certifikátu i vydavatele certifikátu, o cestě, kterou probíhá ověřování certifikátu atd. Popíšeme ve stručnosti typy těchto rozšíření.

a) certifikační politika a použití klíče: tato rozšíření umožňují zahrnout do certifikátu popis politik, v rámci kterých byl certifikát vydán. Tyto politiky jsou definovány s cílem pomoci uživateli (podpisující a opírající se stranám) rozhodnout zda daný certifikát je vhodný pro příslušný účel. Například zde může být stanoveno, že veřejný klíč příslušný k danému certifikátu lze používat pouze pro podepisování mailů - nelze ho potom samozřejmě použít k zabezpečení finanční transakce.

b) alternativní jméno: cetifikát dle X.509 umožňuje existenci více jmen a to jak pro majitele certifikátu, tak i pro vydavatele certifikátu (např jím může být e-mailovaá adresa, adresa webovské stránky atd.).

c) atributy (patřící k příslušnému záznamu v X.509 adresáři): v certifikátu mohou být obsaženy libovolné atributy - to umožňuje, aby certifikáty obsahovaly další informace o nositeli certifikátu (např. - JN je účetním firmy MROZ atd.)

d) omezení na certifikační cesty : toto má význam pro definování, jakou cestou lze ověřovat platnost daného certifikátu a navazujících certifikátů.
Následující rozšíření se týkají CRL.

e) číslo CRL a kódy označující důvod k odvolání : Tato čísla jsou vytvářena z monotónně rostoucí posloupnosti (uživatel se může rozhodnout zda nějaké CRL postrádá). Každý certifikát v CRL je také označen kódem, který popisuje důvod odvolání daného certifikátu.

f) distribuční body pro CRL

g) delta-CRL (stejně jako předešlé umožňuje toto rozšíření redukci velikosti rozesílaných CRL - je rozesílána pouze ta část CRL, která obsahuje změny oproti minulému CRL).

Pro přehled uvedeme seznam položek, které obsahuje certifikát dle X.509 verze 3 (tentokrát v angličtině - je pochopitelné, že uživatelé se budou s certifikáty v tomto jazyce setkávat velmi často):
- version (v3);

- serial number;
- signature algorithm id;
- issuer name;
- validity period;
- subject name;
- subject public key info;
- issuer unique identifier;
- subject unique identifier;
- extensions.

4. Autentizační protokoly

Norma X.509 zahrnuje následující tzv. silné (strong) autentizační procedury (dle [2]):

A. Silná dvoucestná autentizace:

Každá z obou stran A a B má pár veřejný a soukromý klíč: (VA,SA), (VB,SB), Čísla R jsou vytvářena na základě posloupnosti v které se nikdy neopakují stejná dvě čísla (např. monotónně rostoucí posloupnost). Symbolem certX označujeme certifikát strany X, T je časová značka.

Jsou zasílány následující dvě zprávy:

Z1: A ==> B : certA , DA , SA (DA);

Z2: B <== A : certB , DB , SB (DB);

kde DA = (TA , RA , B , *) a DB = (TB , RB , A, RA , B , *).

symbol * označuje, že mohou být v příslušné zprávě DX obsažena další data - např. symetrický klíč (sdílená utajovaná hodnota) zašifrovaný veřejným klíčem opačné strany atd.

B. Silná třícestná autentizace:

Zprávy Z1 a Z2 jsou doplněny následující zprávou:

Z3: A ==> B : (RB , B), SA (RB , B).

Přitom časové značky mohou být položeny rovny nule a není je nutno ověřovat. Obě strany ověřují získané informace (strana A ověřuje obdrženou hodnotu RA v Z2, ...).

5. Literatura

[1] ITU-T. Recommendation X.509. Data Networks and Open System communications. Information Technology - Open Systems Interconnection . The Directory: Authentication Framework. (totéž jako : ISO/IEC International Standard 9594-8).

[2] Menezes, Alfred J.; van Oorschot, Paul C.; Vanstone, Scott A.: Handbook of Applied Cryptography, CRC Press 1997

Použité akronymy:

ITU - International Telecommunication Union

ISO - International Standard Organization

D. Šifrátor do vrecka

RNDr. Ladislav Cechlár (http://www.micronic.sk)

Za hlavný bezpečnostný prvok pre osobné použitie v informačných systémoch sú v dnešnej dobe považované čipové karty, ktoré umožňujú bezpečné uloženie šifrovacích kľúčov a autentifikačných informácii, ktoré sú potrebné pre prihlásenie používateľa k počítaču, alebo do informačného systému.

V dnešnej dobe, keď väčšina pracovných staníc je pripojená k Internetu a používa niektorú verziu operačného systému Windows, nerieši používanie čipových kariet všetky bezpečnostné problémy:

- Pri šifrovani na osobnom počítači musia byť šifrovacie kľúče presunuté do počítača, aby ich mohol šifrovací program mohol použiť. Pri šifrovaní symetrickým algoritmom je najčastejšie súbor zašifrovaný náhodne generovaným kľúčom a ten je potom zašifrovaný kľúčom z čipovej karty. Ako náhodne generovaný kľúč, tak aj kľúč z čipovej karty sa v tomto momente nachádzajú v počítači, a sú prístupné možnému šikovnému útočníkovi.

- Prístup na čipovú kartu vyžaduje zadanie PIN-u, najčastejšie z klávesnice osobného počítača. Aj jeho získanie nie je pre dobre napísaný vírus žiaden problém.

- Aj autentifikácia menom a heslom je priveľmi statická a ľahko zachytiteľná. Nie všetky čipové karty podporujú kryptoautentifikáciu.

- Pri použití softvérových šifrovacích prostriedkov je nevýhodou aj to, že na disku počítača sa nachádzajú v spustiteľnej podobe, a ich kód je prístupný pre prípadnú analýzu a modifikáciu.

Ak sústredime do jedného ľahko prenosného zariadenia symetrický šifrátor, generátor náhodných čísel, pamäť pre autentifikačné údaje a klávesnicu na zadávanie PIN-u, dostaneme z hľadiska bezpečnosti veľmi zaujímavý prvok. Aby bol ľahko použiteľný je potrebné, aby bol vybavený štandardným a dostatočne rýchlym rozhraním a doplnený aplikáciami, ktoré umožnia jeho jednoduché používanie.

Po týchto úvahach vznikla na našom pracovisku bezpečnostná karta MICRYPT PGN pre PCMCIA rozhranie. Táto karta obsahuje programovateľný logický obvod od firmy ALTERA, v ktorom je implementovaný šifrovací algoritmus GOST v GAMA móde, GAMA OS móde a autentifikačnom móde, a PCMCIA rozhranie pre komunikáciu s počítačom. Aktivácia karty sa vykonáva PIN-om s dĺžkou 16 až 64 bitov. Šifrovací algoritmus GOST umožňuje použiť pri šifrovaní šifrovacie kľúče s dĺžkou 256 bitov a jeho implementácia umožňuje používať dve sady S-boxov. Tento obvod je špeciálnym rozhraním pripojený na riadiaci procesor. Na procesore je sériové rozhranie, ktoré umožňuje do karty vkladať šifrovacie kľúče a autentifikačné údaje. Toto rozhranie je vyvedené na konektor na vonkajšej strane karty a pri bežnej práci s kartou nie je prístupné. Vkladanie údajov cez toto rozhranie je chránené 64 bitovým zápisovým heslom, ktorého zadávanie má obmedzený počet pokusov. Ani cez toto rozhranie nie je možné vyčítať šifrovacie kľúče, dá sa zistiť len kontrolný súčet vložených údajov. Šifrovacie kľúče a autentifikačné údaje sú skladované v pamäti procesora v šifrovanej podobe a do programovateľného obvodu sú presunuté pri zapnutí napájania.

V testovacej verzii je k dispozícii aj karta MICRYPT PRN v ktorej je zabudovaný aj šifrovací algoritmus RIJNDAEL. Definitívna verzia tejto karty bude k dispozícii po schválení príslušnej normy FIPS.

Použitie takýchto bezpečnostných kariet má tieto prednosti:

Šifrovacie kľúče nie su prístupné pre procesor počítača. Aj náhodne generovaný kľúč pre šifrovanie súboru, alebo jeho časti vystupuje z karty len v zašifrovanej podobe. Z interných kľúčov je možne získať iba 32 bitový odtlačok. Ak kľúče naplníme do karty v bezpečnom prostredí, napríklad zo špeciálneho počítača určeného na správu šifrovacích kľúčov, ktorý disponuje potrebným zabezpečením, máme takmer stopercentnú istotu, že útočník šifrovacie kľúče nikdy nezíska.

Ak zadávame PIN na klávesnici bezpečnostnej karty, počítač ho nemôže získať, a teda nemôže šifrátor ani pamäť autentifikačných údajov samovoľne odomknúť.
Šifrátor zabudovaný v šifrovacej karte možno so sekundárnou sadou S-boxov jednoducho využiť na kryptoautentifikáciu. Pri nej pošle autentifikačný program bezpečnostnej karte náhodne generovaný dátový blok. Karta ho zašifruje a vráti programu. Tento dešifrovaním overí, či karta pozná príslušný šifrovací kľúč. Takáto autentifikácia je odolná voči monitorovaniu.

Všetky šifrovacie programy sú v počítači uložené v šifrovanej obálke. Pri štarte sa príslušnou bezpečnostnou kartou sa dešifrujú do pamäte počítača. Takýto kód je veľmi dobre chránený pre prípadnou analýzou a modifikáciou.

Je samozrejmé, že takáto karta je bez dobrého softvéru nepoužiteľná. Preto bola doplnená o autentifikačný modul MGINA pre Windows NT a 2000. Tento modul využíva autentifikačné možnosti karty, a čo je podstatné - pred prihásením používateľa kontroluje integritu vybraných častí systému. To garantuje, že šifrovacie programy sú používané na neinfikovanom systéme. Potom je možné bezpečne použiť niektorý z programov na šifrovanie súborov, alebo program na šifrovanie elektronickej pošty.

Vývoj tejto karty nie je ukončený a v najbližšom čase bude doplnená o asymetrický šifrátor s dlžkou kľúča až 2048 bitov, čím sa z nej stane dokonalý nástroj pre elektronický podpis.

Poznámka redakce časopisu Crypto-World

a) Podle názoru redakce se nejedná o typicky reklamní článek, a proto jsme jej otiskli. Obsahuje celou řadu obecných zásad a informací (nezávislých na popisovaném produktu), které mohou být pro čtenáře užitečné. zajímá nás Váš názor na uveřejňování článků tohoto typu – děkuji předem za vyjádření vašeho stanoviska k této věci.

b) V rámci našeho „boje“ za vyjadřovací čistotu, kdy neúspěšně bojujeme například proti výrazům typu: „koupím si svůj elektronický podpis“, „v čipové kartě mám svůj elektronický podpis“ apod. si dovolím připomenout, že ani výraz používaný v článku : „šifrátor s dlžkou kľúča až 2048 bitov“ - není správný. Ve skutečnosti se totiž nejedná o délku klíče!, ale délku modulu. Klíč je tvořen tímto modulem a veřejným či soukromým exponentem, podle toho zda se jedná o veřejný či soukromý klíč. Tato chyba je zcela běžná a spadá spíše do kategorie kryptologické „hantýrky“ – v článku by se však vyskytnout neměla.

E. **Interview s HACKEREM**

Vážení čtenáři, dnes jsme pro vás připravili malou lahůdku – rozhovor s jedním z českých hackerů. Hned úvodem musím poznamenat, že jej osobně neznám a veškerá komunikace probíhala anonymně pomocí internetu, a že tedy vzhledem ke způsobu použité komunikace nejsem schopen sdělit žádné informace, které by pomohly dotyčného identifikovat. Na mnou připravený seznam otázek jsem dostal odpovědi, které dále předkládám. V původním textu nebyly použity „čárky a háčky“; u svých otázek jsem je doplnil dodatečně, u odpovědí jsem ponechal tvar, který nejí nijak upraven.

1. Můžeš se představit našim čtenářům ?
Je mi 19 let (cimz porusuju Dastychovu hranici pro typickyho hackera) , muz a prezdivka je EB#L@ (EBOLA pro soudruha Dastycha). No a k tomu povolani: V soucasne dobe delam bezpecnostniho poradce pro dve ceske firmy a hlavne jednu cesko-americkou.
2. Kdy ses poprvé dostal k PC ?
To uz si ani presne nepamatuji. Ale muj prvni pocitac byl C64.
3. Jaký máš počítač ?
Podle toho kterej. Mam jich vice.

4. Jaký máš operační systém a proč ?
Kvuli tomu abych mel prehled a mohl hledat chyby tak pouzivam tyhle: WY2K,NT a hlavne Linux (RH,Debian,Mandrake,Suse). V soucasne dobe preferuju hlavne RH, je to open, muzu si tam doopravovat co mi schazi a mam tam vse co potrebuju.

5. Jak ses dostal k "hacku" ?
To bude asi par let spatky. Videl jsem kdysi film Valecne hry, to na me udelalo docela dojem. Pozdeji jsem precetl anglickou verzi knizky "Kukacci Vejce" od Klifa Stoola. A pak uz ani nevim.

6. Čeští hackeři mají ve světě velice "slušnou" (co do odbornosti) pověst. Čím to podle Tebe je?
:). To ani nevim podle ceho se to soudi, nebo jak se pozna ze hacker je z CZ, pokud to ovsem nenapise sam. Musim uznat ze znam nekolik ceskej hackeru co pracujou pro velky pocitacovy firmy. Mozna by cesti hackeri meli ve svete jeste lepsi povest kdyby komunisti odesli o par let driv a TELECOM neutlacoval rozvoj internetu.

7. Souhlasíš s tvrzením majora (dnes již bývalého) Dastycha, že typický hacker je student do 19 let, vyhublý, uhrovatý, nemá holku, mluví relativně dobře anglicky, neumí se seznámit a jeho znalosti jsou založeny na tom, co se dočetl na stránkách o hacku na Internetu?
To je uplna blbost. To by se tykalo pouze tech smradu co se pouzivaji svoje nuky a shazujou masiny. A to by to bylo do 17 let. Nedavno jsem potkal jednoho takovyho. Chlubil se mi tim ze hacknul gsm.miesto.sk . Tohle neni hacker tohle je typickej lamer. Uhrovatej nejsem a nikdy jsem nebyl. Holku mam (pusu Evicko). Seznamit se umim ale casto na tu osobu zapomenu. Neni skratka cas.

8. Chceš nám říci něco o svých aktivitách (nějakém hacku)?
O tech aktivitach bych se tu moc nerozsiroval. Vetsinou spolupracuju se zahranicnima skupinama. Na ceske elektronicke pude se moc neobjevuju, posledni velka vec kterou jsem mel na svedomy byl www.OkNet.cz. Jedna se o ISP z jizni moravy. Jeden jejich admin se vytahoval na linuxConfere ze phf je strasne stara a trapna chyba. Tak jsem se na ne krapet

kouknul. Nabouraljsem se jim pres htsearch bug. Pak jsem se uz jenom bavil. Koukal jsem jak admin dela pasti na IMAP, jak si testuje a analyzuje se svym Nessusem. Nejvice me dostaly ty jejich firemni rozkazy. Meli presne rozepsany kdo kdy muze chlastat a kdo ma zustat strizlivej pro pripad e-kolize. Mel jsem je kompletne pod kontrolou. Jednou jsem se v jejich poste docetl ze budou kompletne menit servery. Takze jsem jim jemne upravil vsech 185+1 webu druhe urovne. Celkem tam meli pres 2500 web hostingu. Jen tak pro zasmati heslo pro webmastera bylo "heslo123" :). Asi mesic pote jsem jim to hacknul podruhe. Klidne to udelam i potreti. Nic se tam nezmenilo. Pokud jde o zahranicni aktivity, tak se mi podarilo proniknout do jedne nejmenovane evropske letecke spolecnosti a ziskat kompletni kontrolu nad vsim (nebojte se letadla jsem nezhazoval). Druhej velkej uspech byl kdyz jsem se naboural do spolecnosti ktera vyrabela simulacni software a systemy pro jaderne elektrarny....

9. Proč se hackem zabýváš?
Je to zabava. Nekazej se pri tom zuby. Nemuzu si zlomit nohu atd...

10. Co cítíš po úspěšném průniku?
Citim vzruseni nad tim ze jsem nekoho prechytracil. Ze jsem rozhodne chytrejsi nez on. Mam obrovsky pocit vytezstvi, ktery samozrejme vetsina lidi nepochopi pokud ho nezazije. Bohuzel potom nadseni postupne opada. Vzruseni opet narusta pokud objevim dalsi obet nebo si stanovim dalsi cil. Ale to uz je asi zavyslost.

11. Co studuješ ?
Ted zrovna studuju SAP R/3.

12. Co cteš ?
Dastychovy telefoni ucty :)

13. Máš mezi svými kamarády "spřízněnou" duši?
Nemam zadny kamarady. Skousel jsem jednoho obratit na hacking ale nemel pro to vlohy a nevydrzel dlouho vzhuru :)

14. Jak by jsi definoval "hackera" a "hack" ?
Nekdo kdo odhaluje bezpecnosti chyby, nabourava se do systemu aby je pochopil. Ne proto aby skodil. A hack? tak to se tezko definuje. Za hack bych mohl povazovat treba uspesne otevreni auta bez klicku.

15. Jaká uznáváš morální pravidla v e-světě?
Nevim o zadnych moralnich pravidlech v e-svete. V e-svete uznavam pouze hackersky kodex. Velice silne nenavidim pornografii, sekty a podobny zmetky.

16. Co říkáš návrhu amerického přísného zákona SSSCA (Security Systems Standards and Certification Act)? (Čtenářům připomínám, že podle tohoto zákona je možné hackera postavit před soud a mimo odnětí svobody mu hrozí i trest smrti... Dále je fakticky zakázáno vytvořit - ač třeba jen pro vlastní potřebu - nějaký šifrový software atd.)
Velice stupidni vec. USA ASI skratka neni schopna lustit a sledovat veskerou svetvou komunikaci tak si to musej usnadnit takto. Stve me to casto cestuji do USA, hlavne kvuli praci a hackerskejch srazech. Byt zatcenej jenom kvuli tomu ze mam notebook z ceske republiky je docela drsny.

17. Co říkáš poslední aktivitě úřadu, kde jsem zaměstnán (ÚOOÚ) ? (Náš předseda požádal Radu Evropy, aby příští týden byla projednána otázka omezování osobní svobody a ochrany osobních dat v souvislosti s pokusy o potlačení těchto demokratických svobod - jako reakce na události 11.9.2001) ? Souhlasíš, že teroristům je celkem jedno, zda budou souzeni za zabití tisíce lidi. nebo zda budou souzeni za totéž + např. za vývoj vlastního šifrovacího programu ?)
Je to docela dobrej pokus, ale nejsem si jistej jestli to bude neco platny. Nekdy mam pocit ze ceskou republiku nikdo neposloucha. Teroristum je to naprosto jedno jedno za co budou souzeni. Spravnej terorista umira pri svem utoku.

18. Čteš Crypto-World ?
Pred casem jsem se zajimal o Navajo CodeTalkers, tak jsem zabrousil i do CW. Ale v soucasne dobe nejsem zadnym pravidelným odběratelem.

19. Tvůj názor na takovýto e-zin ?
Vzhledem k tomu ze jsem videl jenom par cisel tak docela dobry.

20. Slyšel jsi někdy o české kryptologii ?
Ano, slysel jsem hodne. Mam docela dobry prehled. Napriklad ta spravna dvojka z DECROSU. Znam i AEC. Sam se navic o kryptologii zajimam, souvisi to stim co delam.

21. Pokud ještě nestuduješ na VŠ, co říkáš tomu, že od příštího září bude možné v Praze na MFF UK studovat kryptologii (bakalářské a magisterské studium) ?
Studuji. To je docela dobry ze se zacina ucit neco co se hodi. Mozna bych toho vyuzil, ale mam malo casu.

22. Hackeři často opovrhují oficiálním vzděláním. Proč?
Protoze se na skolach ucej samy blbosti. Napriklad na stredni sme se ucili 15 spusobu jak oznacit ve Wordu text. Je tam skratka nuda, clovek se citi nevyuzitej.

23. Co chceš vzkázat majoru Dastychovi ?
Radeji mu to vzkazu v pristim hacku. Ale kazdopadne si neodpustim jednu poznamku: Mili Jirko az se priste nechas fotit do novin tak alespon stahni to bricho. Nebo s nim mackas mezernik??? A nebud smutnej Tsomu Shukumuriho taky nikdo nema rad.

24. Znáš nějakou holku, která se zabyvá "hackem" ?
Znam onu notorickou hackerku Suzan Thunderbaitovou. Potkal jsem taky jednu u nas v CZ ale pripadalo mi ze dela pro policajty a jenom se vytahuje.

25. Co chceš vzkázat našim čtenářům ?
Tak to nevim.

26. Jakou otázku by sis položil sám?
Jsi spokojen se svym zivotem ??

27. Jak bys na ni odpověděl ?
Jo docela jsem. Hacking bych nevymenil za nic na svete (krome tebe Evicko). Kazdopadne bych chtel postavit dum zasadit strom atd....

Děkuji za rozhovor.

F. Mikulášská kryptobesídka
10. - 11. prosinec 2001, Praha

Vážení čtenáři, přátelé – dnes Vás chci pozvat na jednu zajímavou akci, která se bude konat koncem tohoto roku. Jedním z oficiálních mediálních partnerů této akce je i Crypto-World. Proto si dovolím o této akci informovat poněkud obsáhlejším způsobem.

Základní informace

Mikulášská kryptobesídka se koná letos poprvé. Jedná se o jako první český a slovenský workshop zaměřený na podporu úzké spolupráce odborníků pracujících na poli aplikované kryptografie a v příbuzných oblastech bezpečnosti.

Toto setkání expertů je organizováno za účelem podpory výměny informací a nápadů z minulých, současných i budoucích projektů. Cítíme potřebu vzájemného setkávání expertů bez zbytečných problémů a starostí s (potenciálními) zákazníky, šéfy a dalšími rozptylujícími faktory. ☺

Workshop se skládá z
(a) neformálního setkání (včetně panelové diskuse) v pondělí *10. prosince 2001*
(b) prezentací příspěvků a diskusí v úterý *11. prosince 2001*.

Na workshopu přislíbili svoji účast dva přední světoví kryptologové, kteří zde přednesou zvané příspěvky:
- Bart Preneel (KU Leuven) o projektu NESSIE (základní informace o této důležité iniciativě viz. např. Crypto-World 12/2000, článek J.Pinkavy : Cryptonessie),
- Fabien Petitcolas (Microsoft Research) o vztahu watermarkingu a kryptografie.

Program
V podvečer v pondělí 10. prosince 2001 se koná panelová diskuse a neformální setkání účastníků.
V úterý 11. prosince 2001 probíhají prezentace zvaných a vybraných příspěvků. Přesný program bude zveřejněn později.

Registrace
Doporučujeme registrovat se co nejdříve. Kapacita konference je omezená a po naplnění kapacity (cca 70 účastníků) již nebude možné přijímat další registrace. Termín včasné registrace (nižší cena účasti na konferenci) je stanoven do *28. 11. 2001*. Registrační formulář je ke stažení zde: pdf. Nechceme jít pro toto prvé setkání nad 70 lidí – má se jednat skutečně o „workshop“ a ne o prezentační konferenci, kterých je v současné době na výběr celá řada.

Ubytování

Připravujeme doporučení k možnostem ubytování. Přesnější informace budou k dispozici později.

Témata workshopu

- Aplikovaná kryptografie.
- Bezpečnostní aplikace kryptografie.
- Standardizace a legislativa související s kryptografií.
- Technologie posilující soukromí.
+ Ostatní zajímavá témata související s aplikovanou kryptografií.

Informace pro autory

Informace pro autory jsou k dispozici ve formě Call For Papers.

Rozšířené abstrakty (800-1000 slov), společně s autorovou emailovou adresou, telefonním číslem a poštovní adresou, musí programový výbor obdržet nejpozději do *28. října 2001*. Preferována jsou elektronická podání; papírová podání musí obsahovat 8 vytištěných kopií.

Rozšířené abstrakty i kompletní příspěvky by měly být odeslány v RTF, HTML nebo ASCII.

Programový výbor

Tonda Beneš, SAP ČR
Jaroslav Dočkal, Vojenská akademie Brno
Petr Hanáček, VUT Brno
Vašek Matyáš, ecom-monitor.com a Masarykova universita - předseda
Daniel Olejár, UK Bratislava
Michal Sasínek, NBÚ MV SR
Luděk Smolík, Seculab s.r.o.
Pavel Vondruška, ÚOOÚ

Organizační výbor

Dan Cvrček, VUT Brno
Vít Kratina, ecom-monitor.com - tajemník
Roman Pavlík, ecom-monitor.com
Zdeněk Říha, ecom-monitor.com a Masarykova universita - předseda
Jan Staudek, Masarykova universita

Zasílání příspěvků
E-mail: *Vaclav.Matyas@ecom-monitor.com*
Předmět: "Kryptobesídka"
Poštovní adresa:
V. Matyáš
ecom-monitor.com, a.s.
PO Box 7
664 01 Bílovice nad Svitavou

Další (a aktuální) informace můžete najít na www stránce
http://www.ecom-monitor.com/kryptobesídka

G. Letem šifrovým světem

Přehled vybraných akcí do konce roku 2001

INVEX 2001
V současné době probíhá (15.10-19.10.2001) 11.mezinárodní veletrh informačních a komunikačních technologií.
Informace na http://www.bvv.cz/invex .

Datakon 2001
Ve dnech 20.-23.října 2001 se koná v brněnském hotelu Santon konference Datakon 2001.
Další informace na http://www.datakon.cz

Vojenská kryptografie IV.
Ve dnech 30.-31. 10. 2001 proběhne v prostorách Vojenské akademie v Brně velmi dobře obsazená konference „Vojenská kryptografie“.

Současnost a budoucnost krizového managementu
4. konference "Současnost a budoucnost krizového managementu" se koná 28.-29.11.2001 v Praze v hotelu Olšanka.
http://www.emergency.cz

4.ročník "Konference Informační společnost "
Ve dnech 4.-5.12.2001 pořádá Ústav informatiky a Stavební fakulty VUT v Brně čtvrtý ročník konference Informační společnost. Součástí konference je i turnaj v bleskovém šachu ☺. http://www.econ.cz/konference

Mikulášská kryptobesídka - 2001
První český a slovenský kryptografický workshop Mikulášská kryptobesídka - 2001
se koná 10.12. - 11.12.2001 v Praze.
http://www.ecom-monitor.com/kryptobesidka/index.html

Mezi nejčtenější články na serveru http://www.root.cz patřil v minulém měsíci seriál „**Code Talkers**“, který byl věnován využití jazyka indiánů Navajů za druhé světové války k přenášení šifrových zpráv.

Snídaně s Novou 12.10.2001

V médiích se v poslední době zvýšil zájem o kryptologii. Důvodem je např. diskuse o možném zneužití steganografie pro komunikaci teroristů.

O čem jsme psali v září roku 1999 a 2000

Crypto-World 10/1999
A. Back Orifice 2000 2-3
B. Šifrování disku pod Linuxem 3-5
C. Microsoft Point-to-Point Tunneling Protocol (PPTP) 5-6
D. Letem šifrovým světem 7-8
Příloha č.1
"INRIA leads nearly 200 international scientists in cracking code following challenge by Canadian company Certicom"

Crypto-World 10/2000
A. Soutěž ! Část II. - Jednoduchá záměna 2 - 4
B. Král DES je mrtev - ať žije král AES ! (P.Vondruška) 5 - 9
C. Kde si mohu koupit svůj elektronický podpis? (P.Vondruška) 10-12
D. Kryptografie a normy II. (PKCS #3) (J.Pinkava) 13-15
E. Prohlášení ÚOOÚ pro tisk 16-19
F. Statistika návštěvnosti www stránky GCUCMP 20-22
G. Letem šifrovým světem 23-24
+ příloha : ZoEP.htm - Zákon č. 227/2000 Sb. – „Zákon o elektronickém podpisu a o změně některých dalších zákonů (Zákon o elektronickém podpisu)“, který nabyl účinnosti 1.10.2000.

H. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "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 jej najít na lépe dostupné adrese:

http://cryptoworld.certifikuj.cz

2. Registrace / zrušení registrace

Zájemci **o zasílání** tohoto sešitu se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@uoou.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@uoou.cz (předmět: ruším odběr Crypto-Worldu !). Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byl sešit zasílán.

3. Spojení

běžná komunikace**, zasílání příspěvků k otištění** , informace
pavel.vondruska@uoou.cz (**vondruskap@uoou.cz**)

pavel.vondruska@post.cz

vondruska.p@seznam.cz