Crypto-World

Informační sešit GCUCMP

Ročník 3, číslo 9/2001 15. září 2001

9/2001

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.**

A. Soutěž 2001 , I.část (Kódová kniha)

Pavel Vondruška, ÚOOÚ

V dnešním čísle začíná už dříve ohlášená soutěž v luštění různých jednoduchých problémů souvisejících se základními šifrovými systémy. Tak jako v loňském roce bude i letošní soutěž probíhat 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 zaslat, 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, 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. Cenou kola bude CD se staršími čísly Crypto-Worldu a placený certifikát od některého z předních poskytovatelů těchto služeb. V loňském roce měla soutěž značnou odezvu. Z vašich reakcí a z celkového hodnocení však vyplývá, že soutěž byla považována za poměrně těžkou. Všechny úlohy vyřešili jen 4 čtenáři, alespoň jednu úlohu vyřešilo 17 čtenářů. Výsledky včetně správných řešení jsem uvedl ve vánočním speciálu, který je dostupný na domovské stránce Crypto-Worldu.

Připomeňme, jaké úlohy byly v loňském roce čtenářům předloženy:

Září	- steganografie
Říjen	- jednoduchá záměna
Listopad	- transpozice
Prosinec	- periodické heslo
20.12.2000	- řešení jednotlivých úloh

Pro čtenáře bude užitečné připomenout si, jak postupy řešení těchto úloh, tak zavedenou terminologii (e-ziny 9/99 - 12/99).

Považuji za vhodné zopakovat větu, kterou jsme otiskli v prvé části loňské soutěže:

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

Tato věta je současně nápovědou k první úloze (a vlastně i všem dalším úlohám ☺).

Úkol číslo 1 (jednoduchá záměna):

512	53	84	39	49	45	55	101	64	39	64	614	91	82	47	84
22	84	48	22	45	82	59	55	45	101	82	28	46	101	45	82
22	94	47	42	31	82	49	53	21	49	43	54	56	21	22	91
82	48	84	47	82	56	46	101	58	33	22	21	22	41	82	811
101	54	38	45	49	53	84	32	21	82	55	82	57	21	33	55
58	82	49	43	56	48	31	38	82	28	45	39	510	41	82	512
41	101	41	82	210	45	48	84	124	82	49	43	56	48	31	82
59	101	45	38	46	41	82	82	82	82	82	82	82	82	82	82

Plný počet bodů (10) lze získat za zaslání převodové tabulky (samozřejmě těch znaků , které se v textu vyskytují). Současně prosím o zaslání informace, jak se Vám text podařilo „zlomit“. Pro klasický způsob luštění jednoduché záměny je tento materiál na první pohled trochu krátký… Dost nápovědy.

Předpokládám, že pro naše stálé čtenáře bude tento rozehřívací úkol hračkou a že bylo těžší jej připravit, než vyluštit. A tak blahopřeji již předem k zisku prvních bodů.

Kódová kniha

V minulém roce jsme se seznámili se 3 základními šifrovými systémy - jednoduchou záměnou, transpozicí a periodickým heslem. Dnes k nim přidáme další v historii běžně používaný systém - kódovou knihu. Na myšlenku používat kódovou knihu se přišlo přibližně v době, kdy se ukázalo, že jednoduchá záměna je systém, který lze na základě analýzy frekvence jednotlivých znaků luštit. Po poznání, že frekvence písmen se musí "zastřít", aby se luštiteli znemožnila nebo alespoň zkomplikovala možnost najít správné řešení, následovalo hledání vhodného postupu. Navržených metod bylo několik a všechny byly v praxi použity. Jednou (nepříliš účinnou) možností je vkládání klamačů, tedy znaku nebo celé skupiny znaků, které příjemce "odhodí" a teprve pak se pustí do vlastní dešifrace textu. Další možností je nahradit jednoduchou substituci za polyalfabetickou substituci (zde se terminologie někdy liší, používá se i název složitá záměna apod.). Hlavní myšlenkou je, že písmena s větší četností se zaměňují za více znaků. Místo A se tedy použije např. znak Q, při dalším použití 1 a dále např. * nebo zase Q. Tím se docílí toho, že frekvence znaků šifrového textu neodpovídá frekvenci znaků použitého jazyka. Další metodou byl tzv. nomenklátor. Tato šifrovací technika byla velice oblíbena ve šlechtických kruzích v 16-tém až 19-tém století. Pomocí nomenklátoru psal své milostné dopisy i např. Casanova. Hlavní chybou bylo, že nomenklátor nebyl obměňován dost často a majitel jej používal po dlouhou dobu (často i celý život). O co šlo? Nomenklátor byl předchůdce kódové knihy. Skládal se z kódové abecedy pro jednoduchou (někdy i pro polyalfabetickou) záměnu a následoval seznam kódů pro často používaná slova - láska, polibek, schůzka. Ukázalo se, že dobře používaný nomenklátor, který by byl často obměňován, je poměrně bezpečný a jeho obliba rostla. Pro diplomatickou poštu Francie, Rakouska a Anglie se stal nepostradatelným po celá následující století. Nomenklátory se stávaly rozsáhlejší a rozsáhlejší. V roce 1700 již měly nomenklátory 2000 až 3000 slov. Nomenklátory měly jednu "malou vadu". Pro rychlé vyhledávání byla slova řazena abecedně. Pokud kód bylo nějaké 4 nebo více místné číslo (jak tehdy bylo běžným zvykem) a tato čísla byla také řazena vzestupně, znamenalo to, že luštitel mohl odhadnout jakým písmenem začíná slovo, které kód představuje. Můžeme to doložit na příkladu z roku 1677. Ve španělském diplomatickém nomenklátoru všechna slova od "bal" do "ble" - začínala kódy 131 až 149 . Toto nemohlo ujít tehdejším luštitelům, a tak paradoxně delší a "propracovanější" nomenklátory se lépe luštily. Jedním z nejznámějších luštitelů nomenklátorů se stal Francouz Rossignol. O tom, že jeho výsledků si tehdejší král Ludvík XIII velice cenil, svědčí dochovaný záznam rozhovoru umírajícího krále. Na smrtelné posteli uvedl své manželce mezi osobami, které má podporovat jako nepostradatelné pro blaho státu také Rossignola. Rossignol navrhl metodu odstranění nedostatků tehdejších nomenklátorů. Doporučil promíchat číselné kódy. Nomenklátory se pak vytváří dva - jeden pro šifrování (výrazy seřazené abecedně) a druhý pro dešifraci (číselné kódy seřazeny vzestupně). Nomenklátory se dále zvětšovaly. Důvodem k většímu rozsahu byla skutečnost, že se prokázalo, že luštitelé jsou v případě používání malého počtu kódových slov stále schopni (po zachycení dostatečného počtu zpráv) korespondenci luštit. Základem jejich úspěchu byla opět

analýza frekventních slov a hlavně spojování událostí, které pravděpodobně šifrová zpráva obsahuje. Dvě podobné události a příslušné šifrové texty jsou pak klíčem k luštění. S nadsázkou lze říci, že luštitel se musí vcítit do role šifranta a pokusit se uhodnout, jak vypadá jim odesílaná zpráva v otevřené řeči. Ze šifrové zprávy pak dostane odhad jednotlivých kódů. Zda se mu to podařilo nebo ne, kontroluje podle druhé dvojice (situace a druhý šifrový text), kterou má k dispozici. Zdá se to složité, ale věřte, že to poměrně dobře funguje. Musíte mít jen fantazii, dostatek informací, čas a být schopni kombinovat spoustu detailů různorodého charakteru. V 18-tém století – tedy v době, kdy došlo k výše popsané bezpečnostní změně nomenklátorů, byli poměrně úspěšní i luštitelé pracující na dvoře Marie Terezie. Vídeň vděčila za své úspěchy na poli luštění velice prozíravé personální politice. Výcvik a školení luštitelů bylo přímo profesionálně připraveno. Mladí muži ve věku 20-ti let, kteří byli morálně bezúhonní a kteří hovořili plynně francouzsky a italsky a dále prokázali své schopnosti v algebře a matematice, byli zařazeni jako elévové do luštitelského oddělení. Po nějaké době se podrobili zkoušce v luštění lehkých nomenklátorů. Pokud neuspěli, byli převedeni na některý jiný úsek státní služby. Jestliže obstáli, byli zasvěceni do tajů luštění na další vyšší úrovni. Následovala povinná stáž v cizině z důvodu zdokonalení v cizích jazycích. Potom nastoupili svoji práci v tzv. černé komnatě a zde pracovali jako kryptoanalytici ve službách státu. Plat byl závislý na jejich výsledcích. Za každý vyluštěný systém jim náležela speciální odměna. Např. je dochovaný záznam za rok 1780, kdy bylo vyplaceno 15 odměn. Pokud se podařilo získat rakouské administrativě nomenklátor jinou cestou - tedy "nenápadně okopírovat", byla těmto analytikům též vyplacena malá odměna - jako odškodnění za to, že nemohli získat vyluštěním odměnu celou. Takto získanému nomenklátoru (obecně klíči) se říká v kryptoanalytickém slangu "kořist". Luštitelé, pokud mají takovouto „kořist“, vykonávají pak vlastně stejnou práci jako dešifranti. Přijatou zprávu podle "kořisti" převedou do otevřené řeči. Luštitelé tehdy pracovali vždy jeden týden a další týden měli volný. Jejich prestiž byla vysoká a byla to hlavní odměna za jejich práci. Císařovna Marie Terezie často rozmlouvala s pracovníky černé komnaty a o jejich práci se živě zajímala.

Jak čas plynul, stávaly se nomenklátory rozsáhlejší. Ve vytištěné podobě již nomenklátor vypadá jako kniha. Odtud nový název - **kódová kniha.** Ve skutečnosti je potřeba tisknout vždy pro každého uživatele knihy dvě. Jednu pro šifrování a druhou pro dešifrování zprávy. Hlavními nedostatky tohoto systému jsou :

- dlouhá a náročná přípravou kódu
- potřeba dokonalého utajení tisku těchto knih
- nákladná distribuce
- nutnost dlouhodobě používat jeden typ kódové knihy
- "ztráta" jediného exempláře kompromituje celý systém a je nutné přejít na novou kódovou knihu.

Co dále nahrává luštitelům k proniknutí do systému kódové knihy jsou chyby, které šifranti a dešifranti dělají. Je potřeba si uvědomit, že tito lidé nejsou kryptologové a chovají se podle předpisů a pokynů, které dostali. V kritických situacích nebo v situacích, se kterými návod nepočítá, se chovají podle svého uvážení a to může být zdrojem chyb, které může luštitel využít.

V dalším odstavci si popíšeme několik klasických chyb známých z I.světové války.

Po převzetí nové kódové knihy je v některém směru zaslána tatáž zpráva ještě pod starým kódem. Stávalo se to tehdy, když daný příjemce ještě novou kódovou knihu neobdržel. V případě, že knihy byly vyměněny z důvodu kompromitace původní knihy, má luštitel po dešifraci zprávy v původním kódu otevřený text a příslušný šifrový text podle druhé kódové knihy. Důsledek je zřejmý - je nutné začít tisknout nové kódové knihy.

Naprosto běžným nešvarem mezi šifranty (nejen v I.světové válce ☺) bylo zasílání přání k vánocům, velikonocům, svátkům ....Odhadnout obsah takovéto šifrové zprávy je pro luštitele přímo lahůdkou. Znalost obou textů (šifrového a příslušného otevřeného) je pro systém kódové knihy přímo vražedná.

Známé jsou případy, kdy byl odeslán otevřený text a následoval stejný text v zašifrované podobě. Ne všechny texty byly totiž zasílány šifrově a pokud vojáček přehlédl, že se jedná o tajnou zprávu, lekl se a honem všechno "napravil".

Pedagogicky "pěkné" jsou i dochované požadavky o opakování např. "...prosím zašli jen tu část od rozkazu k vyplutí" nebo "...nepřečetl jsem poslední blok, zašli od slova zítra...". Poučná jsou i hlášení typu "... v poslední zprávě jsi měl špatně kód, přehlédl ses, 15835 je "vojín" ne "velitel", to je o řádku níže - tedy 15836. Dej si příště pozor! Velitel šifrového oddělení …" .

Kryptoanalytikovi potom stačí pouze ověřit, že se v předchozích případech nejednalo o provokaci nebo pokus o zmatení nepřítele. Pokud takto získané kódy lze použít v dříve zachycené korespondenci, zapíše si je a může pokračovat v pokusu zrekonstruovat celou kódovou knihu.

Přes všechny tyto nedostatky byla kódová kniha nejrozšířenějším šifrovým systémem používaným za I.světové války. Vojenští velitelé se domnívali, že se jedná o použitelný systém a pokud budou schopni zajistit kontrolu všech kódových knih, že je bezpečný. Aby ztráta nějaké kódové knihy neohrozila celkovou komunikaci, byla vydávána obrovská spousta různých druhů knih. Byly vydány zvláštní knihy pro jednotlivé armády, zvláštní pro námořnictvo, pro generální štáb, pro diplomatickou poštu atd. V úvodu kódové zprávy se pak zapisovala tzv. hlavička, která určovala, která z knih se má použít k dešifrování a další služební údaje (zpravidla datum a celkový počet odeslaných skupin).

Než se sami pokusíte pokořit jednu zprávu zapsanou v kódu, seznamte se s příběhem německého diplomatického kódového systému 13042. Prolomení tohoto kódu změnilo dějiny Evropy.

Zimmermannův telegram

Nyní se seznámíme s jedním z mnoha fascinujících příběhů dějin šifrování. V tomto příběhu kryptologové, aniž by o tom veřejnost věděla, rozhodovali o dějinách celé Evropy.

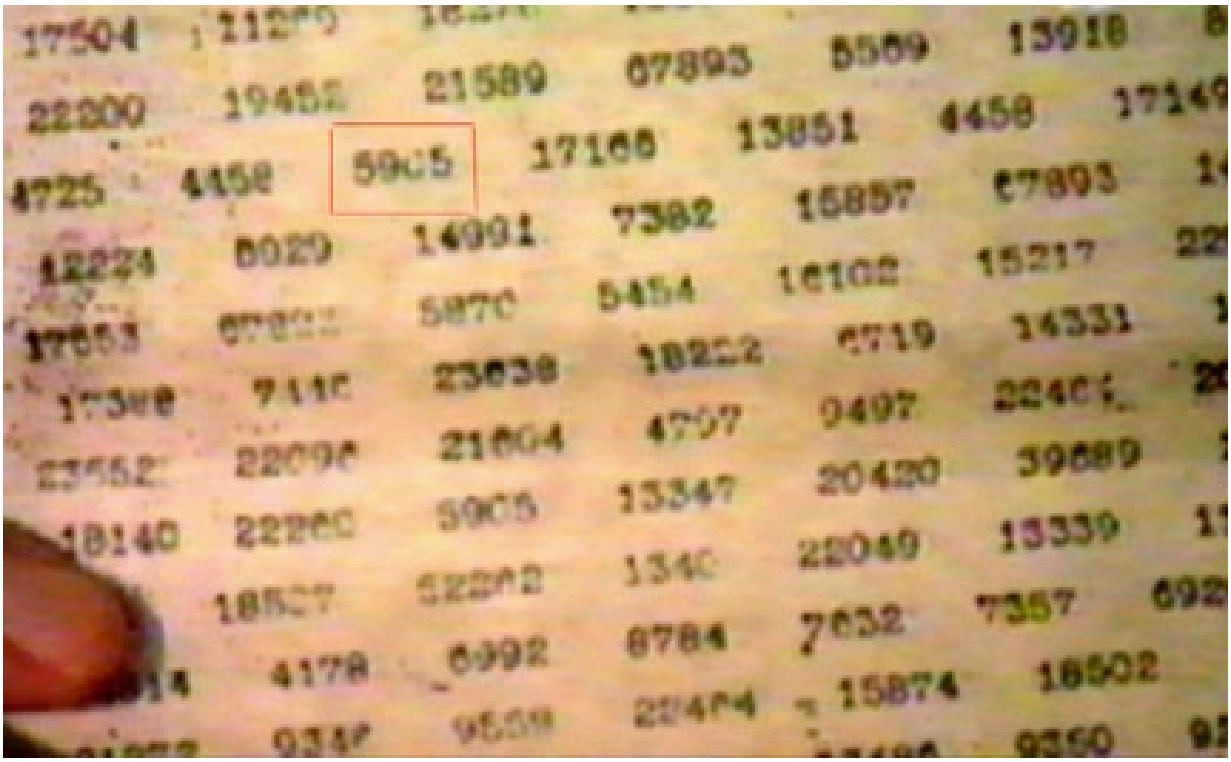
Začíná I.světová válka. Neuběhne ani dvacet hodin a vyplouvá britská loď s tajným cílem. V noci tajně zakotví u holandského břehu. Ze dna vyzdvihuje podmořský kabel vedoucí z Německa a přeřízne jej. Německo tak přichází o relativně bezpečné dálnopisné spojení se svými ambasádami a všechny depeše musí zasílat vzduchem - rádiem. Angličané tyto depeše zachycují a snaží se je vyluštit. Většina depeší je zašifrována podle různých kódových knih. Získanými telegramy se zabývá tzv. místnost č.40. V této místnosti je umístěno britské dešifrovací oddělení. Intenzívně zde od začátku války pracuje 40 lidí. Posuňme se na naší pouti historií dále. Je rok 1917. Po třech letech práce se kryptoanalytikům podařilo úspěšně proniknout do některých německých systémů. Na evropském válčišti zuří krutá válka, žádná ze stran nemůže získat rozhodující převahu. Válka zřejmě uvízla na mrtvém bodě, v zákopech umírají a strádají naprosto zbytečně tisíce lidí. Anglie žádá USA o pomoc. Spojené státy váhají, chtějí zůstat neutrální a do války se nechtějí zapojit. Angličanům je přitom jasné, že vstup USA do války by zásadním způsobem ovlivnil výsledek války. Němci naopak chtějí, aby USA zůstalo neutrální. Zlom nastává, když se novým německým ministrem zahraničí tává Zimmermann. V Německu se připravuje nová ofenzíva a současně bylo rozhodnuto zahájit bezpodmínečnou ponorkovou válku. Totální blokáda Anglie má přinést Německu převahu. Současně se však němečtí generálové bojí reakce USA.

Zimmermann vymýšlí plán, jak odvrátit pozornost USA od dění v Evropě. Jeho plán však bude díky luštitelům v místnosti č.40 odhalen a místo vítězství Německa vtáhne do války USA a přinese pád Německa a Rakouska-Uherska. O co šlo? Zimmermann chce využít dlouhodobých rozporů mezi Mexikem a USA o společnou hranici.Oznamuje proto mexické vládě, že Německo započne v nejbližší době totální blokádu Anglie. Německo má zájem, aby se vojska USA neobjevila na evropském válčišti. Nabízí tedy Mexiku dostatečné dodávky zbraní a jiného materiálu za slib, že Mexiko v případě, že by se Amerika chtěla zapojit do války v Evropě, zaútočí na jižní hranici USA. Amerika by pak určitě zůstala mimo evropské válčiště a snažila se vyřešit své vlastní problémy. Uvědomme si, že tehdejší USA ještě nebyly tou velmocí jakou jsou dnes a navíc přesun vojenských jednotek na evropské válčiště byl komplikovaným technickým problémem. Amerika by pravděpodobně zůstala v omezené válce o své hranice s Mexikem.

Telegram s touto naprosto neuvěřitelnou a supertajnou nabídkou byl odeslán z Berlína na německé velvyslanectví do Washingtonu rádiem 17.1.1917. Zde byl přepsán a poslán dálnopisem na zastupitelství v Mexiku a následně předán mexické vládě.

Ještě dříve, než se telegram dostal do Mexika, byl šifrový text k dispozici luštitelům v místnosti č.40. Luštitelé měli několik "kořistí", kódová kniha s kódem 13042 však k dispozici nebyla. Jednalo se o kód diplomatický a ten byl tedy pochopitelně méně dostupný než polní válečné kódy. Přesto se luštitelům podařilo knihu za tři roky pilné práce částečně rekonstruovat.

Odeslaný telegram obsahoval 150 kódů. Po převodu prvních kódů luštitelé pochopili, že zde mají něco velice důležitého:



Obr. č.1 Zimmermannův telegram

Zde jsou autentické kódy, které luštitelé horečně přepisovali ze své rekonstruované kódové knihy:

13347	vypuknutí
39689	USA
5905	válka (v telegramu vyznačeno červeným obdélníkem)
98092	ponorka

14936 neomezená
97556 Zimmerman

Vzrušením pravděpodobně nemohli dýchat. Pochopili, že to, co mají v ruce, je diplomatická bomba. Její zveřejnění by mohlo zatáhnout USA do války a to by znamenalo pro Němce jistou porážku. Ano, mají jasný důkaz, že Německo podněcuje válku na americké půdě!

Získaný otevřený text předali veliteli luštitelského oddělení admirálovi Hallovi. Ten věděl, že telegram nelze jen tak zveřejnit nebo předat USA. Nejprve se musí vyřešit věčné dilema kryptoanylýzy - jak využít získanou informaci, aby se protivník nedozvěděl, že jste prolomili jeho kód. Američané určitě obsah zveřejní a Angličané potřebují mít možnost monitorovat i nadále obsah německé diplomatické pošty. Hall vymyslel vynikající plán – přijtelnou legendu.

Musí Američany i Němce přesvědčit, že telegram získali již v otevřené podobě. Je pravděpodobné, že by Němci neuvěřili, že se jej podařilo získat na ambasádě ve Washingtonu. Budou tedy tvrdit, že se jej podařilo získat od podplacených státních úředníků, kteří se k němu dostali v Mexiku. Jenže byl zde problém. Hall měl k dispozici pouze ten telegram, který byl zaslán z Německa. Text poslaný telegrafem z Washingtonu se mohl lišit. Anglie tedy rychle úkoluje svého informátora v Mexiku (známého jen jako pana H). Agent musí získat telegram, který byl zaslán na ambasádu v Mexiku (za jakoukoliv cenu).
Pan H. se vloupal do telegrafní společnosti Western Union v Mexiku a zde skutečně kopii příslušného telegramu získal .

Text se opravdu lehce lišil (například byl podepsán již velvyslancem ve Washingtonu). Hall jásal - tyto rozdíly budou „důkazem“ , že Britové předali Američanům telegram získaný v Mexiku, nikoliv telegram, který byl poslán z Evropy do Ameriky.

Anglie předává telegram do USA a současně informuje, jak jej "získala".Američané a Němci legendě uvěří. Plán vyšel perfektně i z hlediska politického záměru. Američané po zveřejnění obsahu vycházejí do ulic a žádají vyhlášení války Německu, během šesti týdnů Amerika skutečně do války vstupuje. Z války v Evropě se tak stává první válka světová.

Zaměstnanci místnosti č.40 a další zasvěcenci ještě desítky let udrželi své tajemství. Nikdo mimo nich totiž netušil, že se jim podařilo změnit dějiny. Vstup USA do války zajistilo vítězství spojenců a záchranu bezpočtu životů v Evropě na obou stranách fronty.

Tolik historie. Než se pustíte do řešení našeho druhého úkolu, připomeňme, že kódové knihy nemusely být jen číselné, mohly být i textové. Kódy pak vypadaly např. takto ANLLL NHJKL OOPUJ ... Mohly vypadat také tak, jak je uvedeno ve vaší druhé úloze. V úvodu jsem slíbil, že úkoly budou letos lehké, a tak tedy napovím : je potřeba získat "kořist" :-) .

Úkol číslo 2 (kódová kniha):

NA-NIL-IN. HANE-AL-NEH BEH-BIH-KE-AS-CHINIGH A-KHA A-CHIN AH-NAH.
CHE-CHIL-BE-TAH-OLA YIL-DOI BE-LA-SANA TLA-GIN KLIZZIE-YAZZIE
LIN NO-DA-IH AH-JAD DIBEH-YAZZIE HUC-QUO A-WOH TLO-CHIN
A-KHA JAD-HO-LONI A-CHI TSAH WOL-LA-CHEE GLOE-IH BE-LA-SANA
NE-AHS-JAH A-CHIN CHA-GEE MA-E TKIN AH-LOSZ KLESH D-AH NIL-CHI-
TSOSIE. AL-TAH-JE-JAY YAH-DI-ZINI HA-HOL-ZIZ. ATSAH-BESH-LE-GAI A-KEH-
DI-GLINI TLO-CHIN A-CHIN BE AH-LOSZ SHI-DA DIBEH JAD-HO-LONI TSE-NILL.

Za úkol máte zaslat dešifrovaný text kódové zprávy (8 bodů) a zdroj (2 body), kde jste získali příslušnou "kořist". To je dnes vše.

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-1,2
Termín: do slosování budou zařazena všechna správná a úplná řešení, přijatá do 14.10.2001 !

Závěr:
„Obecný návod na luštění zašifrovaných zpráv neexistuje. Je nutné pozorně číst, hodně vědět, dívat se, přemýšlet a být připraven … „

B. Dostupnost informací o ukončení platnosti a zneplatnění kvalifikovného certifikátu (Mgr. Pavel Vondruška, ÚOOÚ)

Této problematice jsme se již po právní stránce dostatečně věnovali v předchozích číslech našeho e-zinu (Prokeš J.: Ukončení platnosti, zneplatnění (a zrušení) certifikátu, Crypto-World 5/2001 a 6/2001). Uvedené články se týkaly rozboru pojmů ukončení platnosti a zneplatnění kvalifikovaného certifikátu. Toto téma je však i nadále diskutované a setkávám se s ním prakticky na všech svých vystoupeních a prezentacích. Nejrozsáhlejší diskuse na toto téma proběhla v době příprav návrhu vyhlášky ÚOOÚ k zákonu o elektronickém podpisu. Možná bude dobré se ještě jednou u tohoto důležitého tématu zastavit.

V Zákoně o elektronickém podpise č.227/2000 je řešeno ukončení platnosti, zneplatnění a přístup k těmto informacím v následujících paragrafech:

§6, odst. 7
Poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty, musí neprodleně ukončit platnost certifikátu, pokud o to podepisující osoba požádá, nebo v případě, že byl certifikát vydán na základě nepravdivých nebo chybných údajů.
§6, odst.1 g)
zajistit provozování bezpečného a veřejně přístupného seznamu kvalifikovaných certifikátů, které byly zneplatněny, a to i dálkovým přístupem,
§15, odst. (2)
Seznam certifikátů podle § 6 odst. 1 písm. g) musí obsahovat přesný časový údaj, od kdy byl certifikát zneplatněn.

A jak dále upravuje otázku zveřejnění seznamu kvalifikovaných certifikatů, které byly zneplatněny, návrh vyhlášky k elektronickému podpisu?

§ 3
(6) Seznam kvalifikovaných certifikátů, které byly zneplatněny, je provozován tak, aby jeho dostupnost byla zajištěna dvěma nezávislými způsoby, z nichž nejméně jeden musí umožnit dálkový přístup a musí být nepřetržitě dostupný.
(7) Doba mezi ukončením platnosti kvalifikovaného certifikátu a zveřejněním údaje o ukončení této platnosti v seznamu kvalifikovaných certifikátů, které byly zneplatněny, může činit nejvýše 24 hodin. Tento údaj obsahuje číslo kvalifikovaného certifikátu unikátní u

daného poskytovatele certifikačních služeb, datum a čas s uvedením hodiny, minuty a sekundy, kdy je certifikát zneplatněn.

Námitky připomínkujících subjektů, ač různě zformulované, lze stručně vyjádřit takto:

Doba 24 hodin uvedená v § 3 odst. 7 návrhu vyhlášky je příliš dlouhá; doporučujeme 6 hodin (8 hodin, 12 hodin apod. – dle připomínkujícího subjektu)…

Nedozvěděl jsem se, o co opírali jednotliví diskutující své návrhy a proč si myslí, že právě jimi navrhovaná doba je ta dostačující. Úřad při stanovení doby 24 hodin (a to jako doby maximální) vycházel z dokumentů, které navazují na směrnici EU o elektronických podpisech. Konkrétně z dokumentu ETSI : ES 201 456 „Policy requirements for certification authorities issuing qualified certificates“. Upozorňujeme, že dokumenty ETSI jsou pro členské státy EU závazné, pro ČR významné z hlediska kompatibility.
Kdo je vlastně ETSI, že je pro nás v rozhodování v rámci našeho zmocnění takovou autoritou? ETSI - The European Telecommunications Standards Institute je nezisková organizace, která působí od roku 1988 s cílem připravovat telekomunikační standardy pro dlouhodobé využití. Je oficiálně uznána jak Evropskou komisí, tak i sekretariátem EFTA (European Free Trade Association). Sdružuje více než 789 členů z 52 zemí reprezentovaných správními orgány, provozovateli sítí, servisními organizacemi, výrobci, výzkumnými pracovišti i uživateli. Standardizace prostředků elektronického podpisu, včetně standardů pro činnost podpůrných infrastruktur (PKI), je v kompetenci technické komise TC SEC (Security), v jejímž rámci byla ustanovena samostatná pracovní skupina pro oblast elektronického podpisu (Working Group on Electronic Signatures and Infrastructures - ESI WG). Pro nás je tedy ETSI přirozenou autoritou a tam, kde jsme se museli v rámci svého zmocnění při přípravě vyhlášky rozhodnout pro nějakou volbu, snažili jsme se navrhnout řešení v souladu s jejími dokumenty.

Vraťme se ke zveřejňování informací o ukončení platnosti kvalifikovaného certifikátu. Většina současných aplikací používá při ověřování certifikátu informace ze seznamu zneplatněných certifikátů (dále CRL - Certificate Revocation List). Námitka oponentů, že doba 24 hodin mezi vydáním dvou následujících CRL je dlouhá, vychází pravděpodobně z nepřesné představy o skutečné praxi.

CRL (Certificate Revocation List) je definován např. v dokumentu RFC 2459. Perioda zveřejňování musí být uvedena v certifikační politice. Pro konkrétní certifikační politiky tedy může být stanovena doba kratší než navrhovaná doba 24 hodin a to vždy v souladu s tím, pro jakou agendu bude cerifikát používán a v souladu s rizikem zneužití. Například platební brána (Payment Gateways) pro platební obchodní protokol SET, používající VISA a MASTERCARD, provádí update CRL jednou za 24 hodin a to z příslušných VISA a MASTERCARD CRL serverů. CRL pro britskou hospodářskou komoru je v souladu s příslušnou certifikační politikou zveřejňováno jedenkráte za osm hodin atd. Doba 24 hodin je tedy dobou maximální a záleží na poskytovateli certifikačních služeb (dále jen PCS), jakou dobu zveřejňování CRL nabídne. Ve skutečnosti to bude záležet především na tom, o jaké certifikační politiky bude zájem a nakolik bude moci příslušný poskytovatel certifikačních služeb vyhovět. Z uvedeného příkladu nejrozšířenějších platebních karet je současně vidět, že stanovení kratšího limitu pro všechny agendy a aplikace by bylo zbytečné a ve svém důsledku by vedlo ke zbytečně vysoké ceně za certifikáty

Je však CRL jediná možnost, jak získat informaci o statutu kvalifikovaného certifikátu? Pro obchodování na burze by stahování CRL v několikahodinových intervalech skutečně nemuselo být to pravé. Zákon nařizuje PCS, který vydává kvalifikované certifikáty ještě další povinnost.

§6, odst.1 f) zajistit provozování bezpečného a veřejně přístupného seznamu vydaných kvalifikovaných certifikátů, a to i dálkovým přístupem, a údaje v něm obsažené při každé změně okamžitě aktualizovat,

V tomto seznamu zveřejňuje PCS informace o vydaných certifikátech. Pokud je jedním ze zveřejněných informací statut certifikátu – zákon to nikde neříká a je otázka zda je tedy zveřejňování této položky vynutitelné. Pokud však ukončení platnosti je součástí zveřejněných informací o certifikátu, pak pokud byla ukončena platnost některého z certifikátů, musí podle tohoto paragrafu být tato změna i zde zveřejněna a to okamžitě. Informace v této databázi je tedy aktuálnější než v té době zvěřejněný CRL. Existuje nějaký protokol, který by umožnil využívání informací z tohoto seznamu?

Ano, pro speciální aplikace je možné využít ON-linový protokol k těmto konkrétním datům. Takový protokol se nazývá **Online Certificate Status Protocol – OCSP**. Definován je např. v RFC 2560. Poskytovatel certifikačních služeb umístí svůj komunikační server do tzv. demilitarizované zóny a zde zveřejňuje seznam certifikátů podle §6, odst.1 f) se všemi předepsanými atributy (podle dokumentu ETSI : Electronic Signature Formats).

V souvislosti s výše uvedenými dvěma případy předávání informací o ukončení (zneplatnění) certifikátu ještě upozorním, že standardy vyžadují, aby v samotném kvalifikovaném certifikátu bylo vždy v „extenzích“ uvedeno distribuční místo seznamu certifikátů, které byly zneplatněny (tzv. CRLDP: CRL Distribution Point) a v případě OCSP protokolu přístup k poskytovaným informacím příslušného poskytovatele certifikačních služeb (tzv. AIA : Authority Information Access).

Poskytovatelé certifikačních služeb mohou dále nabídnout další službu spojenou s možností informovat o ukončení platnosti certifikátu také tímto jiným smluvním způsobem. Konkrétně se jedná o zasílání informací na adresu žadatele o tuto službu a to v okamžiku ukončení platnosti nějakého certifikátu. V takovém případě je nutné smluvně stanovit způsob a formát dodávané informace. Výhodou je, že příslušný subjekt může být vzhledem k získání aktuálních informací pasivní a přesto získá aktuální informace o ukončení platnosti každého certifikátu. Takovéto systémy nejsou zcela běžné a používají se pro velice speciální účely. Pokud vím, neexistuje žádný standardizovaný protokol pro takovouto službu.

Doufám, že tento krátký výčet služeb a možností spojených se získáním aktuálních informací o platnosti kvalifikovaných certifikátů celou záležitost alespoň částečně ozřejmil. Všechny dotazy na toto téma jsou vítány a rád je zodpovím.

C. Kryptografie a normy - Díl 9. Digitální certifikáty. Část 1. Pojem certifikátu. Úvodní poznámky.

Jaroslav Pinkava, AEC spol. s r.o. & Norman Data Defense Systems, CZ

l. Úvod

V tomto a několika následujících pokračováních seriálu Kryptografie a normy bude věnována pozornost problematice digitálních certifikátů.

Tento pojem je dnes velice často citován v návaznosti na problematiku elektronických podpisů. Např. v [1] se setkáme s následujícím přirovnáním : „Digitální certifikát slouží jako řidičský průkaz v digitálním světě." Digitální certifikát Vám umožní vstup do podnikové počítačové sítě, umožní Vám pracovat s Vaším bankovním účtem. Zároveň Vám však digitální certifikáty umožňují uvěřit si původ jiných dat (softwaru, digitálních dokumentů atd.), umožňují zavést kontrolu přístupu ke zdrojům, implementovat nepopiratelnost a další příbuzné vlastnosti.

Shrnutím výše uvedených poznámek se ukazuje, že digitální certifikáty nám poskytují jeden velice důležitý prvek bezpečnosti – **důvěru**. Základní dnes používaný přístup k vytváření digitálních certifikátů je popsán v normě ITU (International Telecommunications Union) X.509. Historicky existovalo několik verzí této normy (tak jak se v čase a vzhledem k potřebám praxe vyvíjela). Nejznámější a v praxi dnes také nejpoužívanější je verze 3, v současné době je připravována čtvrtá verze (již velice rozsáhlá) této normy.

Existují ale i jiné přístupy - např. tzv. *metacertikáty* (bohužel dřívější odkaz na webu http://www.mcg.org.br/index.html - již neplatí a novější se mi nepodařilo nalézt) a samozřejmě sem patří i odkaz na koncepci důvěry, kterou prosazovalo PGP. Koncepce X.509 však ve vztahu k praktickým aplikacím zvítězila a pro nová řešení je asi jedinou zvažovanou variantou.

Dnešní úvodní část bude věnována samotnému pojmu digitální certifikát a dalším úvodním poznámkám. V návazných částech to budou další podrobnosti k normě X.509 (to se týká současné verze a také verze, která je připravována). Následně přijdou na řadu materiály skupiny IETF-PKIX (ústřední část tohoto cyklu k digitálním certifikátům). Konečně na to naváží některé v současné době diskutované problematiky (jako kvalifikované certifikáty, některé novější poznatky k evropským normám, atd.)

2. Pojem digitálního certifikátu

Digitální certifikát je dokument vydaný důvěryhodnou institucí. V tomto dokumentu je obsaženo tvrzení, že k určité osobě (přesněji - k určitému jednoznačnému jménu – *distinguished name*) patřící veřejný klíč má určitou konkrétní (číselnou) hodnotu. Filosofie opřená o služby důvěryhodné třetí strany není nová, je to vlastně analogie notářského ověření papírového dokumentu. Příjemce papírového dokumentu ověřuje razítko notáře a interpretuje ho např. jako důkaz, že osoba podepsaná v dokumentu učinila tento podpis v přítomnosti důvěryhodné strany – notáře.

Vzhledem k digitálnímu certifikátu sehrává roli (která je paralelní k roli notáře) důvěryhodné strany instituce nazývaná **certifikační autoritou**.

Výše byl zmíněn veřejný klíč patřící určité osobě. Konkrétní číselná hodnota tohoto klíče je obsažena v digitálním certifikátu. K tomuto veřejnému klíči patří soukromý klíč (druhá dvojice páru klíčů ve smyslu pojmů asymetrické kryptografie – např. [2]) a tím již může výlučné disponovat pouze majitel tohoto klíče. Existuje pak řada prakticky používaných cest, které na základě této dvojice klíčů asymetrické kryptografie umožňují vytvářet cesty pro důvěryhodné transakce (digitální podpis, přenos klíčů pro symetrickou kryptografii atd.).

Uživatel (opírající se strana) musí mít důvěru v legitimnost takto získaného veřejného klíče. V opačném případě by mohl narušitel buď zaměnit veřejný klíč ležící někde v adresáři nebo by se mohl vydávat za někoho jiného. Pro tyto účely slouží právě certifikáty. Digitální certifikát označuje vlastníka veřejného klíče. Dovoluje verifikaci tvrzení, že daný veřejný klíč patří skutečně danému jedinci. Certifikáty pomáhají chránit se před možností, že někdo falzifikuje klíč s cílem vydávat se za někoho jiného. Ve své nejjednodušší podobě obsahují certifikáty veřejný klíč a jméno. Obecně užívané certifikáty obsahují rovněž:

- dobu vypršení platnosti
- jméno certifikační autority, která vydala certifikát
- pořadové číslo
- informaci o tom jak klíč má být používán
- nejdůležitější je digitální podpis vydavatele certifikátu

Certifikáty nesmí být možné padělat, musí být získány bezpečnou cestou a vytvářeny musí být tak, aby potenciální narušitel je nemohl zneužít. Vydání certifikátu musí rovněž probíhat bezpečným způsobem, musí být odolné proti možným útokům. Pokud by něčí soukromý klíč byl ztracen či kompromitován, pak ostatní uživatelé musí být včas varováni a nesmí již déle šifrovat zprávy neplatným veřejným klíčem nebo akceptovat zprávy podepsané tímto zkompromitovaným soukromým klíčem. Uživatelé musí své klíče mít bezpečně uloženy, na druhé straně musí mít tyto klíče k dispozici pro jejich legitimní používání. Klíče mají platit pouze do doby než vyprší jejich platnost. Doba platnosti musí být vhodně zvolena a bezpečně opublikována. Je třeba rovněž vzít do úvahy, že některé dokumenty budou mít zapotřebí ověřit platnost podpisu i po uplynutí doby platnosti daného veřejného klíče.

Nejrozšířenější akceptovaný formát pro certifikáty je definován mezinárodní normou ITU X.509. Tyto certifikáty mohou být pak čteny či psány libovolnou aplikací vytvořenou ve shodě s X.509. Normu X.509 využívá řada protokolů, např. PEM, PKCS, S-HTTP a SSL.
Certifikační autorita je organizace (důvěryhodná třetí strana), která podepisuje uživatelův veřejný klíč a jeho jméno (případně další doplňkové údaje jako doba platnosti) svým vlastním soukromým klíčem. Certifikát lze ověřit veřejným klíčem certifikační autority. Pokud chtějí nyní dva partneři spolu komunikovat, mohou se vzájemně autentizovat ověřením digitálního podpisu druhé strany veřejným klíčem partnera a posléze ověřením partnerova veřejného klíče verifikací digitálního podpisu certifikátu užitím veřejného klíče certifikační autority. Stačí pak důvěřovat veřejnému klíči certifikační autority. Tímto způsobem je redukován počet veřejných klíčů, kterým každý s uživatelů musí důvěřovat.

Certifikační autority často také provádí verifikaci klíčů, aby bylo zajištěni, že tyto klíče byly správně vygenerovány. Je jim důvěřováno, že správně provedou verifikaci. Na druhou stranu jim není sdělována žádná utajovaná informace (např. jiné uživatelovy utajované klíče).

Při větším počtu uživatelů jedna certifikační autorita nestačí. Veřejný klíč jedné certifikační autority může být certifikován jinou certifikační autoritou. Vytváří se tak sítě certifikačních autorit, které mohou mít různou hierarchickou strukturu.

Pro konkrétní certifikační autoritu je důležité jak postupuje při vydávání certifikátů, zejména pak, jak prověřuje oprávnění žadatele o certifikát. Některé certifikační autority mohou požadovat při identifikaci uživatele velmi málo, ale například banky nebudou zajisté chtít věřit certifikátům s nízkou úrovní jistoty. Každá certifikační autorita musí zveřejnit své požadavky na identifikaci klienta a svoji politiku v této oblasti (dokumenty CP – certifikační politika a CPS – certifikační prováděcí směrnice). Další strany tak mohou posoudit úroveň spolehlivosti certifikátů dané certifikační autority.

Důležitým souvisejícím pojmem je **seznam odvolaných certifikátů** (CRL – Certification Revocation List), což je seznam veřejných klíčů, které byly odvolány dříve než skončila doba jejich platnosti. Je řada důvodů, pro které mohl být klíč odvolán a umístěn v CRL. Klíč mohl být kompromitován. Klíč mohl být určen pro zaměstnance firmy, který mezitím z firmy odešel. Při ověřování podpisu je nutné si ověřit zda příslušný klíč není umístěn v CRL. CRL je provozován certifikační autoritou a obsahuje informaci o odvolaných klíčích, které byly původně certifikovány touto certifikační autoritou. Jsou zde umístěny pouze klíče, jejichž původní doba platnosti nevypršela (klíče s vypršenou dobou platnosti nesmí být akceptovány v žádném případě).

Vůbec jestliže certifikát má sloužit jako základní prvek důvěry, pak je třeba říci, že strana, která se o tento certifikát opírá, by měla učinit všechny dostupné kroky k tomu, aby si ověřila platnost tohoto certifikátu. K tomu je třeba minimálně zjistit, zda doba platnosti certifikátu nevypršela, zda daný certifikát byl platný v době jeho použití (nebyl na CRL) a zda byly platné i všechny návazné certifikáty příslušného řetězce certifikačních autorit. Toto za opírající se stranu často učiní jí používaný software, je však v jejím zájmu ověřit si zda vše proběhlo správnou cestou.

3. Jak je digitální certifikát vytvářen

K získání digitálního certifikátu lze použít dvě základní techniky.
- můžete si ho vytvořit sám (např. pomoci takových nástrojů jako je Internet Explorer, Natscape Navigator atd.)
- můžete požádat certifikační autoritu požádat o jeho vydání. Zase je to možné buď přímo (v praxi méně obvyklé) nebo prostřednictvím určitého (softwarového nástroje), který Vám vygeneruje žádost o certifikát.

Pokud požádáte o vydání certifikátů certifikační autoritu, musíte jí k tomu postoupit některé informace. jaké to budou údaje, zaleží na politice certifikační autority. Obvykle také CA vydává certifikáty různých tříd, kde se tyto požadavky v jednotlivých třídách různí (zpřísňují). Tak např. pro tzv. demo-certifikáty stačí zaslat požadavek obsahující vaši mailovou adresu. Naopak pro udělení certifikátu nejvyšších tříd je nezbytná Vaše osobní přítomnost na tzv. registrační autoritě, kam přinesete také příslušné požadované dokumenty.

Můžete si také sám vyrobit a podepsat digitální certifikát (tzv. self-signed certificate), ale je pak otázka, kdo bude tomuto certifikátu důvěřovat. Ověřující osoba bude samozřejmě vyžadovat, aby se k ní tento certifkát dostal důvěryhodnou cestou a v daném kontextu je toto

možné vlastně jen osobním předáním. Je zjevné, že tento postup (při vyšším počtu zainteresovaných stran) není příliš praktický.

4. PKI (Public Key Infrastructure)

S tímto pojmem se v návaznosti na problematiku digitálních certifikátů setkáváme velmi často. Pokud ovšem budeme hledat v literatuře jeho nějakou přesnější definici, nesetkáme se asi s okamžitým úspěchem. Pojem **PKI** je používán totiž často ve velice různorodých souvislostech. Je to (obecně řečeno) komplexní název pro celou řadu činností (v nejjednodušší podobě je to publikování veřejných klíčů asymetrické kryptografie). Přesnější formulace lze získat pro:

- **cíle PKI** – ustavit a ošetřovat důvěryhodné prostředí v síti.
- **prostředky PKI** – to jsou služby řídící práci s klíči a digitálními certifikáty (jako šifrování a digitální podpisy).

Jako **komponenty PKI** jsou v literatuře uváděny následující:

- certifikační autorita (CA);
- registrační autorita (RA);
- řízení práce s digitálními certifikáty (management);
- adresáře (databáze certifikátů);
- certifikační politiky a prováděcí směrnice (CP a CPS);
- navazující aplikace (např. šifrování mailů, přístupové mechanizmy atd.);
- celá řada dalších souvisejících pojmů (vlastní kryptografické jádro,...);

V praxi jsou dnes již používána různá řešení PKI. Je proto vhodné uvést určitá kriteria, která umožňují srovnávat jednotlivá tato řešení. Mezi nejčastěji citovaná patří následující:

- flexibilita, interoperabilita řešeni;
- bezpečnost CA, RA;
- snadnost použití (user friendly);
- snadnost úprav vzhledem k změnám (počtu uživatelů, hardwaru atd.);
- podpora bezpečnostní politiky organizace.

5. Literatura

[1] Feghhi, Jalal; Feghhi, Jalil, Williams, Peter: Digital certificates. Applied Internet Security, Addison-Wesley 1999, 456 pp.
[2] J. Pinkava: Úvod do kryptologie, květen 1998, http://crypto.aec.cz/ : Publications
[3] P. Vondruška: „Kde si mohu koupit elektronický podpis?“, Crypto-World 10/2000.
[4] J. Pinkava, P. Vondruška: Přednášky na semináři Bankovního institutu vysoká škola, 7.12.2000, http://www.mujweb.cz/veda/gcucmp/

D. E-Europe (přehled aktuální legislativy v ES)

Hobza Jan, ÚOOÚ, jan.hobza@uoou.cz

Blíží se druhé výročí přijetí Směrnice 1999/93 EC o zásadách Společenství pro elektronické podpisy vydané 13. prosince 1999. Tento dokument ukládá členským státům Evropské Unie přijmout právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí nejpozději do 19. července 2001. V současné době by tedy patnáctka členských států EU již měla mít přijatu adekvátní legislativní úpravu elektronického podpisu v souladu s danou směrnicí. To nás inspirovalo k určité inventuře v legislativě států evropského společenství. Následující řádky pak přináší stručný přehled výsledků legislativního stavu dosaženého v jednotlivých členských státech v souvislosti s tímto závazkem. Jedná se o stav k 15.9.2001. Podrobné informace k tomuto legislativnímu průzkumu budou zveřejněny na www stránce ÚOOÚ a nabídnuty k publikování v odborném tisku.

Stát
Datum Oficiální název příslušného právního dokumentu
Stručná charakteristika obsahu (nikoliv překlad)

Belgie
20.10.2000 Law introducing means of electronic signature into the legal procedure - **Zákon o změně základních právních předpisů v souvislosti s elektronickým podpisem**
14.6.2001 Draft Law on certification services - **Návrh zákona o certifikačních službách**

Dánsko
31.5.2000 Electronic Signature Act - **Zákon o elektronickém podpisu**

Finsko
1.1.2000 The Act on Electronic Service in the Administration - **Zákon o elektronické službě ve státní správě**
8.3.2001 Electronic Signature Act - **Zákon o elektronickém podpisu**

Francie
13.3.2000 Act adapting the right on proof and evidence to information technologies and on electronic signature - **Zákon adoptující do práva důkazy a svědectví založené na elektronických technologiích a elektronickém podpisu**
30.3.2001 Decree for the application of article 1316-4 of the civil code and relating to the signature electronic - **Vyhláška k aplikaci článku 1316-4 občanského zákoníku v souvislosti s elektronickým podpisem**

Holandsko
12.1.2001 Development plan of internet commerce - **Plán rozvoje internetového obchodu**
18.4.2001 Law on electronic government communications – **Zákon o elektronické státní komunikaci**
17.5.2001 Act on electronic signature – **Zákon o elektronickém podpisu**

Irsko
20.8.2000 Electronic Commerce Act - **Zákon o elektronickém obchodu**

Itálie

15.3.1997 Law on public administration - **Zákon o veřejné správě**

10.11. 1997 Presidential decree concerning the creation, storage and transmission of digital documents by means of computer-based systems - **Prezidentská vyhláška o tvorbě, ukládání a výměně digitálních dokumentů založených na počítačových systémech**

8.2.1999 The Technical rules for creation, storage and transmission of digital documents in the sense of the Presidential decree no. 513/97 - **Technická pravidla pro tvorbu, ukládání a výměnu digitálních dokumentů ve smyslu Prezidentské vyhlášky číslo 513/97**

Lucembursko

14.8.2000 Electronic Commerce Law - **Zákon o elektronickém obchodu**

1.1.2001 Order relating to the electronic signatures, the electronic payment and the creation of the committee for electronic commerce - **Nařízení vlády k elektronickému podpisu, elektronickým platbám a vytvoření výboru pro elektronický obchod**

Německo

22.5.2001 Law Governing Framework Conditions for Electronic Signatures and Amending Other regulations - **Zákon upravující základní podmínky elektronického podpisu a o změně některých dalších předpisů**

Portugalsko

2.8.1999 Digital Signature law - **Zákon o digitálním podpisu**

25.9.2000 Law on accreditation authority - **Zákon o akreditaci autority (PCS)**

29.8.2000 Administrative Rule on civil liability insurance of certification agencies – **Vládní nařízení o povinném pojištění certifikační agentury (PCS)**

Rakousko

1.1.2000 Federal Electronic Signature Law - **Federální zákon o elektronickém podpisu**

2.2.2000 Electronic Signature order - **Nařízení k federálnímu zákonu o elektronickém podpisu**

Řecko

28.9.1999 Presidential Decree on electronic signatures and related certification services - **Návrh vyhlášky Prezidenta republiky o elektronických podpisech a souvisejících certifikačních službách**

Španělsko

17.9.1999 Royal Decree on Digital Signatures - **Královský výnos k digitálním podpisům**

21.2.2000 Order on regulation of accreditation and certification - **Nařízení o regulaci akreditace a certifikace**

Švédsko

1.1.2001 Act on Qualified Electronic Signatures - **Zákon o kvalifikovaných elektronických podpisech**

Velká Británie

25.5.2000 The Electronic Communications Act - **Zákon o elektronické komunikaci**

E. Adaptivní útok na RSAES-OAEP (Optimal Asymmetric Encryption Padding) standardizovaný podle PKCS#1 verze 2.0 založený na vybraných šifrových textech

Bc. Jan Hobza, ÚOOÚ (jan.honza@uoou.cz)

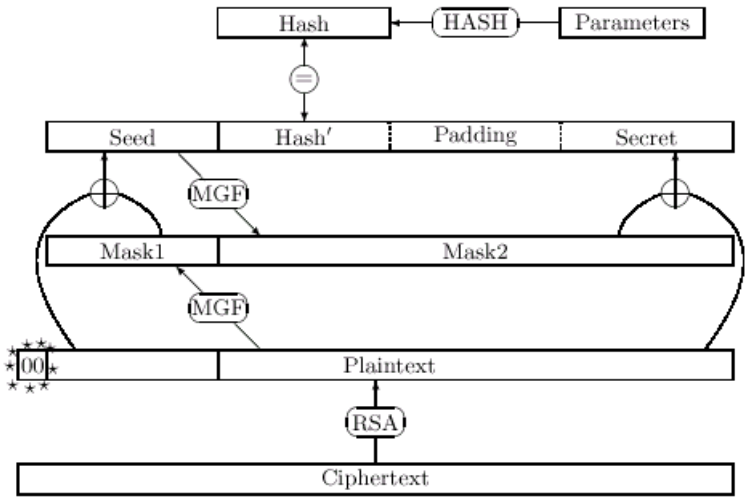
Na konferenci CRYPTO ’98 předvedl Daniel Bleichenbacher úspěšný adaptivní útok proti RSA používající standard PKCS#1, v1.5 [1]. K úspěchu při daném útoku (na 1024 bitový RSA modul) bylo třeba asi jeden milion modifikovaných šifrových textů. D. Bleichenbacher z tohoto útoku dovodil, že nejkritičtější fází je místo mezi dešifrováním textu a ověřováním integrity. Únik jakékoli informace z této fáze představuje bezpečnostní riziko pro celý algoritmus. Bleichenbacher navrhoval zavést vyšší redundanci dat, které je třeba při přijetí zkontrolovat.

Již v říjnu 1998 představily laboratoře RSA novou verzi standardu RSAES-OAEP (Optimal Asymmetric Encryption Padding), která měla odolat tomuto útoku. Oproti verzi 1.5 obsahuje tento standard dvojitou maskovací funkci pro vyšší redundanci dat a jsou zde nově upraveny chybové zprávy[2].

V úvodním odstavci kapitoly popisující schéma RSAES-OAEP se říká, že útok, založený na vybraných šifrových textech, je neefektivní proti schématu jako je RSAES-OAEP. Navzdory tomuto tvrzení James Manger z Telstra Research Laboratories předvedl na letošní konferenci Crypto 2001 v Kalifornii úspěšný útok i proti tomuto standardu. Sám zdůraznil, že ač samotný algoritmus může být bezpečný, některé jeho implementace umožňují dostatečný únik informací pro možný útok. Jím předvedený úspěšný útok vyžadoval se střední hodnotou pouze jeden tisíc dotazů pro modul RSA délky 1024 bitů.

Šifrování RSA-OAEP začíná zakódováním seedu, haše, doplňkových oktetů a utajovaných dat do oktetového řetězce. Maskovací operace náhodně promíchá tyto oktety, které pak představují binární reprezentaci modulu. Počet doplňkových oktetů (padding octets) se vybírá tak, že šifrování spotřebuje o jeden oktet méně než je uvedená binární reprezentace modulu. Jinými slovy, zakódovaná zprava je oktetový řetězec se stejnou délkou jako modul, ale vedoucí oktet je nastaven na ‘00’.

Následující obrázek znázorňuje proces dešifrování a dekódování RSAES-OAEP.



Šifrový text je převeden na otevřený text algoritmem RSA (umocnění soukromým exponentem , mod příslušný modul) a následuje konverze do oktetového řetězce. Maskovací funkce dále užije poslední významné bity otevřeného textu k odmaskování seedu. Maska získaná ze seedu odmaskuje haš, padding a utajovaná data. Integrita šifrového textu se potvrdí srovnáním odmaskovaného a nově vypočteného haše.

Samotný útok vychází z premisy, že útočník dokáže při testování modifikovaných šifrových textů rozpoznat chybu v konverzi čísla do oktetového řetězce od jiných chybových hlášení. Přes to, že se ve standardu PKCS#1 v2.0 výslovně říká: "Je důležité, aby chybová hlášení v krocích 4 (integer-to-octets konverze) a 5 (OAEP dekódování) byla stejná"[2], na následujících řádcích uvidíme, proč některé implementace budou náchylné k útokům.

Útočník může rozlišit o která chybová hlášení jde např. díky rozdílům v pravopisu. Velká písmena, pomlky a jiné mohou být dostatečným vodítkem pro útočníka. Dalším, pro nezkušené oko méně zřejmým vodítkem, může být časová odezva. I identické chybové hlášky mohou být útočníkem rozlišeny, pokud k nim dochází v různém časovém intervalu. Pro ilustraci, systém dokáže najít a nahlásit chybu integrity v průběhu OAEP-dekódování za delší čas než chybu v integer-to-octets konverzi. Rozdíl mezi těmito tvoří průběh dvou maskovacích funkcí[3].

Pokud útočník dokáže definovat příslušné chybové hlášení (chyba při konverzi čísla do oktetového řetězce - integer-to-octets conversion), postupuje dále podobným způsobem dělení intervalů jako u Bleichenbacherova útoku. Podrobný popis samotného útoku lze nalézt ve sborníku konference Crypto 2001.

Možným řešením těchto nedostatků je zavedení vyšší nečitelnosti chybových hlášení, resp. nečitelnosti jejich původu. James Manger též navrhuje ignorovat strukturu otevřeného textu, tedy ignorovat jeho nejvýznamnější oktet v průběhu dešifrování[3]. Tato modifikace by ale popřela hlavní výhodu OAEP. Laboratoře RSA řeší tuto situaci v připravovaném standardu PKCS#1 v2.1, jehož draft č.2 je již k dispozici. V tomto dokumentu se přiklánějí k prvnímu návrhu řešení; uvádí se zde, že chybová hlášení z konverze čísla na oktetové řetězce musí být nerozeznatelná od ostatních a především časová odezva nesmí umožňovat určení původu chyby[4].

Literatura

[1] D. Bleichenbacher: Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1. In Hugo Krawczyk (ed.), Advances in Cryptology { CRYPTO '98, pages 1{12, Berlin, Springer, 1998 (Lecture Notes in Computer Science, vol. 1462).
[2] PKCS #1 v2.0: RSA Cryptography Standard, 1 October 1998.
http://www.rsasecurity.com/rsalabs/pkcs
[3] James Manger: A Chosen Ciphertext Attack on RSA Optimal Asymmetric Encryption Padding (OAEP) as Standardized in PKCS #1 v2.0Advances in Cryptology. In J. Killian (ed.) Advances in Cryptology - CRYPTO 2001 (Lecture Notes in Computer Science. VOL. 2139)
[4] PKCS #1 v2.1 draft 2: RSA Cryptography Standard, 5 January 2001.
http://www.rsasecurity.com/rsalabs/pkcs

F. Letem šifrovým světem

1. V minulém čísle jsme vás seznámili s příběhem ruského programátora Skljarova, který je stíhán za to, že vytvořil program odstraňující ochranu proti kopírování z formátu Adobe Acrobat eBook. Neuběhl ani měsíc a prestižní časopis Technology Review uvedl (viz. http://www.techreview.com/web/roush/roush083001.asp), že se blíže nejmenovanému americkému kryptologovi podařilo obdobně odstranit ochranu proti kopírování formátu MS Reader. Tento ochranný formát elektronických knih od firmy Microsoft byl dosud považován za vysoce kvalitní. Uvedený kryptolog nepočítá se zveřejněním svého postupu, bojí se totiž podobného soudního obvinění a stíhání, jako postihlo Skljarova. Soud se Skljarovem tedy byl v každém případě „úspěšný" – veřejnost je zastrašena a nedovolí si ukázat na chyby v bezpečnostních produktech…Domníval jsem se, že ze vstupem do 21.století se situace změní. Veřejně publikované algoritmy se stanou po seriozní analýze standardy. Ochrana založená pouze na utajování algoritmu je předem odsouzena k nezdaru. Amerika v této oblasti vždy zaujímala zvláštní politiku. Nejprve dlouhodobý zákaz vývozu silné kryptografie měl za následek vznik silných firem zabývajících se kryptografií v Evropě a nyní se zase může stát, že americké produkty a aplikace používající kryptografii budou nedůvěryhodné. Celou situaci může navíc výrazně ovlivnit připravovaný kontraverzní SSSCA zákon (viz. níže).

2. Začátkem srpna byl oznámeno, že byl rozbit šifrovací protokol podle standardu 802.11 (Wireless LAN Encryption Standard) používaný pro zabezpečení radiového propojení počítačů v síti LAN. Chybu odhalil jeden student z Rice University. Na adrese http://slashdot.org/articles/01/08/09/1758200.shtml lze najít technické detaily příslušného útoku.

3. Code Talkers – příběhy indiánů z kmene Navajů za druhé světové války a jimi používanou kódovou knihu jsme vám v našm e-zinu představili již v loňském roce. O něco rozšířenější verzi si můžete v současné době přečíst na http://www.root.cz , kde je ve třech dílech popisována tato část americké historie, která je zajímavá i z pohledu kryptografie. Jednotlivé části byly publikovány 3.9., 10.9. a 17.9. Mediální zájem o tyto příběhy zapříčinilo natáčení filmu Windtalkers. Film se začne promítat v USA 9.11.2001. Režisér John Woo, který jej natočil, se proslavil akčními filmy (Zlomený šíp, Tváří v tvář, …). Film popisuje, jak za války americká armáda využívala indiány z kmene Navajo, aby jejich prostřednictvím předávala tajné zprávy. V upoutávce k filmu se píše, že jazyk těchto indiánů je tak složitý, že funguje lépe než klasické šifry. Aby mohla být metoda předávání zpráv utajena, muselo být zajištěno, aby se nikdo z Navajů nedostal do rukou Japoncům. Každému "tlumočníkovi" byl přidělen voják, který jej v případě zajetí měl zastřelit. Film sleduje příběh jednoho takového páru a ukazuje, jak je složité zlikvidovat člověka, který se mezitím stal vaším přítelem. V titulních rolích se představí Nicolas Cage a Christian Slater. Další informace k filmu Windtalkers můžete najít na této adrese http://movies.yahoo.com/shop?d=hv&cf=info&id=1805535156 nebo na http://us.imdb.com/Title?0245562

4. Dne 23.8. byla vysílána od 15:10 do 16.00 na frekvenci Svobodné Evropy (Český rozhlas 6) v diskusním pořadu „Odpoledni LIVE - Na rovinu" beseda o kryptologii. Redaktorka Lucie Vopálenská zde rozmlouvala 50 minut s pány Vondruškou, Rosou, Matyášem a Benešem o historii, současnosti a problémech kryptologie. Repríza pořadu byla uvedena v neděli 26.8. v 16:10. Část záznamu z tohoto vystoupení je dostupná na adrese: http://www.i.cz/doc/cr6.mp3

5. Ještě před dvěma týdny byla podpora nového, velice kontroverzního a přísného zákona SSSCA (Security Systems Standards and Certification Act) velice malá. Zdá se, že události posledních dnů o jeho přijetí rozhodnou. Zákon navrhuje a předkládá předseda Obchodního výboru Senátu USA - Fritz Hollings. Podle tohoto zákona je fakticky zakázáno vytvořit (ač třeba jen pro vlastní potřebu) nějaký šifrový software… Plyne to např. z odstavce 101, písmena a) , který říká:
„Zákon poruší každý, kdo vyrobí, importuje, veřejně nabízí, poskytuje nebo jakkoli šíří interaktivní elektronické zařízení, které neobsahuje a neprovozuje bezpečnostní technologie schválené státem …“
Celé znění návrhu : http://cryptome.org/sssca.htm
http://www.nullify.org/sssca-draft.pdf
http://sites.inka.de/risctaker/sssca-draft.pdf
http://www.parrhesia.com/sssca-draft.pdf
http://gnu-darwin.sourceforge.net/sssca-draft.pdf (2.5MB)
Další podrobnější (ač trochu jednostranné) informace naleznete v článku Ladislava Zajíčka : SSSCA — Orwellův zlý sen se naplňuje http://www.lupa.cz/clanek.phtml?show=1766

6. Sedmého září vydal Evropský parlament již dlouho očekávanou závěrečnou zprávu k „špionážnímu“ systému Echelon (globální systém pro odposlouchávání soukromé a komerční komunikace). Celou velice obsáhlou a ve všech ohledech zajímavou zprávu najdete uloženu na adrese: http://cryptome.org/echelon-ep-fin.htm

7. V USA byly zveřejněny zajímavé informace o průniku pracovníků FBI do hackerské komunity v této zemi. Článek v Computerworldu popisuje způsob, jak členové tohoto malého týmu nejprve získávali svými vědomostmi ocenění v hackerské komunitě a postupně se zúčastnili i hacků vybraných serverů včetně státních.Uvedeny jsou zde i důvody a cíle celé akce:
http://www.computerworld.com/cwi/story/0,1199,NAV47_STO63711,00.html

8. Procesor označený jako XPP má být v současné době nejvýkonnějším procesorem na světě - při taktovaní na frekvenci 100 MHz dosáhne výkon až 60 tisíc MIPS, což představuje 80-ti násobek výkonu 1,3 GHz Pentia 4. Zvládne 60 miliard instrukcí za jednu sekundu! S takto výkonným procesorem by mohla být provedena faktorizace čísla RSA-155 (tedy 512 bitů) za pouhých 50 dnů! Procesor připravuje dosud úplně neznámá společnost PACT se sídlem v Mnichově. Společnost založil v roce 1996 Martin Vorbach. Architektura nového čipu se nazývá eXtreme Processor Platform (XPP). Samotný čip má rozměry 39 x 39 mm a využívá 1521 pinový ball-grid array (BGA) obal. Celý přístup k řešení problému je v XPP architektuře, která je odlišná od běžně používané von Neumannovské architektury.

9. Zdrojový kód Windows CE byl zveřejněn! Od srpna tohoto roku může každý (přesněji každý, kdo má registrovaný účet na Hotmailu - registrace v Passportu) nahlédnout do zdrojového kódu Windows CE. Zatím byl tento kód přístupný jenom výrobcům hardwaru a to až po vyřízení příslušných formalit. Jestliže chcete nahlédnout do zdrojového kódu, potřebujete k tomu minimálně zkušební verzi Platform Builderu (1,7 GB na disku, 9,5 GB plná instalace) a eMbedded Visual Tools (800 MB). Podporované jsou Windows 2000 a NT 4.0 se Service Packem 5 a vyšším.

10. Anti - kopírovací CD. Společnost Macrovision testuje novou technologii, která má být implementovaná do CD nosičů. Výsledkem mají být nové anti-kopírovací CD nosiče. Zkoušky probíhají dobře a nové CD nosiče by se měli už brzy objevit v obchodech. Hudební nakladatelství se tak chtějí bránit proti nelegálnímu kopírovaní jimi prodávané hudby. Právě tato nová technologie by měla zabránit vyrábění kopií na osobních počítačích. Otázkou zůstává, jak dlouho použitá technologie Macrovisionu zůstane "nepřekonatelná". Hudební průmysl se o implementaci technologie, které dokáže zabránit kopírovaní na obyčejném PC, snaží už několik let. Velkým problémem je zachování kompatibility se starými přehrávači a se zachováním kvality přehrávaných dat. V některých zemích se společnosti dostali dokonce i do soudního sporu - uživatelé si totiž nemohli "chráněné" nosiče na svých hifi věžích přehrát. Nově testovaná technologie má předchozí problémy zvládnout. Technologii vyvinula pro Macrovision izraelská firma TTR Technologies.V každém souboru je jakýsi digitální rušič, při přehrávaní v normálním CD přehrávači uživatel neregistruje nic, pokud je však skladba zkopírovaná do digitální formy na harddisk, její kvalita je díky implementovanému rušení velice špatná.

11. Již jste četli o „ilegálních“ prvočíslech? Znáte práce matematika Philla Carmodyho? Pokud ne, prosím - poslužte si: http://asdf.org/~fatphil/maths/#Smallest
http://www.theregister.co.uk/content/6/21591.html
http://www.theregister.co.uk/content/archive/17681.html

12. Firma NetLine Communications Technologies z Tel Avivu uvedla na trh C-Guard. Tento přístroj je schopný umlčet všechny typy mobilních telefonů, které fungují na frekvenci 900 a 1800 Mhz a nacházející se od něj ve vzdálenosti do 20 metrů. Přístroj vysílá rušivý signál a zabraňuje tak mobilu odšifrovat signál pocházející z mobilní sítě a způsobí tak jeho odpojení. Jedná se o první komerčně nabízený přístroj tohoto typu. Jeho cena se bude pohybovat kolem 50 000 Kč. Doplňuje tak komerčně dostupnou nabídku "protimobilních přístrojů" od firmy Q-Zone (na dané ploše sníží zvuk zvonění nebo přepne na vibrace) a Zetron (upozorňuje na přítomnost zapnutých mobilních telefonů).

O čem jsme psali v září roku 1999 a 2000

Crypto-World 9/1999
A. Nový šifrový standard AES 1-2
B. O novém bezpečnostním problému v produktech Microsoftu 3-5
C. HPUX a UNIX Crypt Algoritmus 5
D. Letem "šifrovým" světem 5-7

Crypto-World 9/2000
A. Soutež ! Část I. - Začínáme steganografií 2 – 5
B. Přehled standardu pro elektronické podpisy (výběr) (P.Vondruška)6 – 9
C. Kryptografie a normy I. (PKCS #1) (J.Pinkava) 10-13
D. P=NP aneb jak si vydělat milióny (P.Vondruška) 14-16
E. Hrajeme si s mobilními telefony (tipy a triky) 17
F. Letem šifrovým světem 18-19
+ příloha : gold_bug.rtf (The Gold Bug od Edgara Allana Poea)

VOLNÁ MÍSTA

Zajímavá práce v oblasti počítačové bezpečnosti!

- Zajímáte se o perspektivní oblast bezpečnostních informačních technologií a systémů ?
- Hledáte pestrou a tvůrčí práci s možností seznámit se s moderními a rychle se rozvíjejícími technologiemi?
- Chcete pracovat v týmu zkušených profesionálů?

Oblast bezpečnosti informačních technologií (IT security) je jedním z nejdynamičtěji se rozvíjejících oborů. Dříve exotikou zavánějící pojmy jako počítačové viry, elektronický podpis, hackeři či kryptologie se dnes již staly běžnou součástí každodenního „provozu“ v oblasti IT.

Pokud se chcete věnovat oblasti IT security na více než sto procent, máte možnost získat perspektivní zaměstnání u společností AEC, spol. s r.o. (www.aec.cz).

Případné dotazy a informace k daným technickým pozicím rádi zodpovíme a poskytneme na e-mailu firmy AEC – miroslava.dohnalova@aec.cz nebo na telefonní lince 05/41235445.

"Codebreaker"-Don't you Mess Around With Me!"

Pat Benatar opens the General Session at the RSA Conference 2001 with her rendition of "Codebreaker"

Your mail is like a tidal wave, spinning over my head
Drownin' me in your viruses, better left unread
You're the right kind of hacker, to release my new technology
The invincible cracker, that you think you were born to be

You're a Codebreaker
Crash Maker, File Taker
Don't you mess around with me!
You're a Codebreaker
Name Faker, Risk Taker
Don't you mess around - NO NO NO!

Your pranks have set my net on fire, and it's taken its toll
We set a trap on the wire, now we're takin back control
You're the right kind of hacker, to release my new technology
The invincible cracker, that you think you were born to be

You're a Codebreaker
Crash Maker, File Taker
Don't you mess around with me!
You're a Codebreaker
Name Faker, Risk Taker
Don't you mess around - NO NO NO!

You're the right kind of hacker, and you'll pay the penalty
The invincible cracker, that you know you were born to be

You're a Codebreaker
Crash Maker, File Taker
Don't you mess around with me!
You're a Codebreaker
Name Faker, Risk Taker
Don't you mess around - NO NO NO!

You're a Codebreaker
Crash Maker, File Taker
Don't you mess around with me!
You're a Codebreaker
Name Faker, Risk Taker
Codebreaker!

G. 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