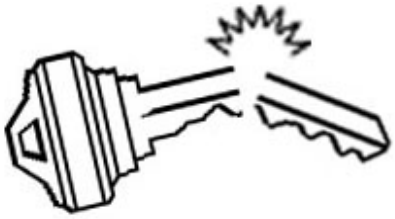
Crypto-World

Informační sešit GCUCMP

Ročník 2, číslo 9/2000 10.září 2000

9/2000

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

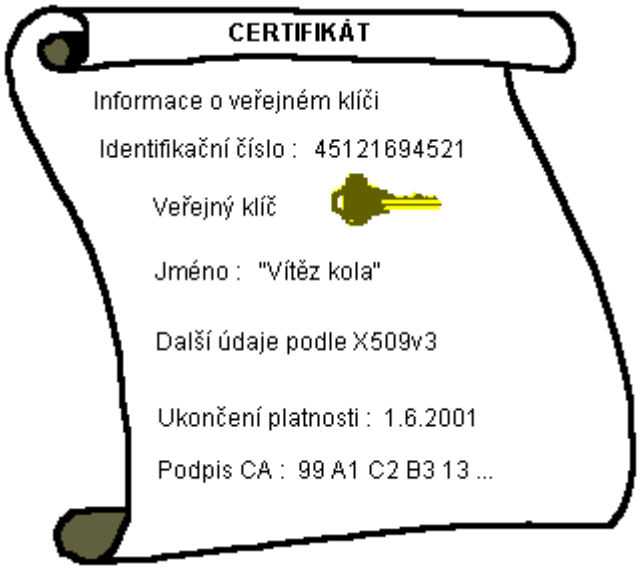


OBSAH : **Str.**

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

A. Soutěž
Mgr. Pavel Vondruška (NBÚ)

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



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

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

Část I. - Začínáme steganografií

Základní pojmy

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

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

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

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

Steganografie

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

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

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

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

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

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

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

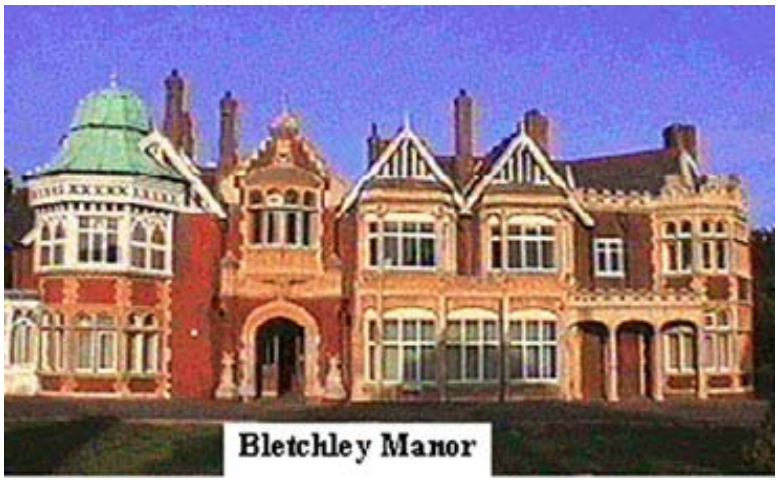
Na závěr jeden jednoduchý příklad. Přečtěte si znovu pozorně odstavec o tom, jak Demaratus informoval své krajany o nebezpečí perského vpádu. Budete-li číst pouze tučná písmena, získáte krátkou zprávu : "Jsem prozrazen. Končím tu." .

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

Úkol číslo jedna - utajení

Náš první úkol uvedeme citací ze staršího čísla tohoto e-zinu.
Crypto-World 2/2000 , Letem šifrovým světem, druhý odstavec, str. 9
Na adrese http://www.gchq.gov.uk/careers/ naleznete informace o volných místech v anglické GCHQ (Government Communications Headquarters). GCHQ chce obsadit celkem 100 svých volných míst. Hledají se především odborníci na komunikace, počítače, jazykoví odborníci a matematici. Matematikům se nabízí práce na : " analysis of complex signals, code-breaking techniques and code construction " (prostě luštění cizích zpráv). Stačí vyplnit přihlášku , dozvíte se , že přednost mají mladí zájemci s PhD, znalostmi jazyků ze specifikovaných oblastí (např. východní Evropa) a zájemci, kteří dokáží vyluštit text uložený na webovské stránce organizace (zájemce z ČR zklamu - požaduje se národnost anglická). O zkušebním textu se na jiném místě dozvíte pouze to, že jej musíte vyluštit do 25.2.2000, že je rozdělen do 5-ti částí, každá část obsahuje 5 znaků, každá část je zamaskována nebo přímo ukryta v jiné

části www stránky. Získané části je potřeba poskládat ve správném pořadí a tuto zprávu přiložit k žádosti o místo. Prozatím zaslalo správné řešení 14 žadatelů.



Ještě připomeňme, s kým máme tu čest :
GCHQ (Government Communications Headquarters) se proslavila už za 2. světové války. V té době ovšem působila pod názvem Government Code and & Cypher School - GC&CS, ale byla všeobecně známa pod názvem Bletchley Park podle místa svého tehdejšího sídla.

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

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

Přeji pěknou zábavu.

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

B. Přehled standardů pro elektronické podpisy (výběr)

Mgr. Pavel Vondruška (NBÚ)

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

UTAH

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

EVROPA - Německo

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

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

EVROPA - Ostatní

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

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

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

UNCITRAL

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

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

Směrnice EU (DIRECTIVE 1999/93/EC)

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

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

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

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

EESSI (European Electronic Signature Standardisation Initiative)

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

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

Nejdůležitější závěry dokumentu:

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

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

EESSI (Work-plan for ETSI electronic signature standardisation)

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

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

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

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

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

Česká republika

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

Přehled relevantních standardů a norem (výběr)

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

C. Kryptografie a normy

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

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

Úvod

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

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

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

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

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

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

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

PKCS

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

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

Dnes existují následující PKCS.

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

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

PKCS #1

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

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

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

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

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

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

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

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

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

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

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

Zpráva po vložení doplňku vypadá následovně:

$$\{00,02, PS,00, zpráva\} ,$$

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

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

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

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

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

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

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

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

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

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

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

Literatura

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

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

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

D. P=NP aneb jak si vydělat miliony

Mgr. Pavel Vondruška (NBÚ)

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

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

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

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

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

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

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

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

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

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

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

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

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

Příloha 1:

Vysvětlující příklad pojmu 3-SAT problému

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

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

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

Příloha 2:

Millennium Prize Problems

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

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

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

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

F. **Letem šifrovým světem**

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

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

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

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

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

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

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

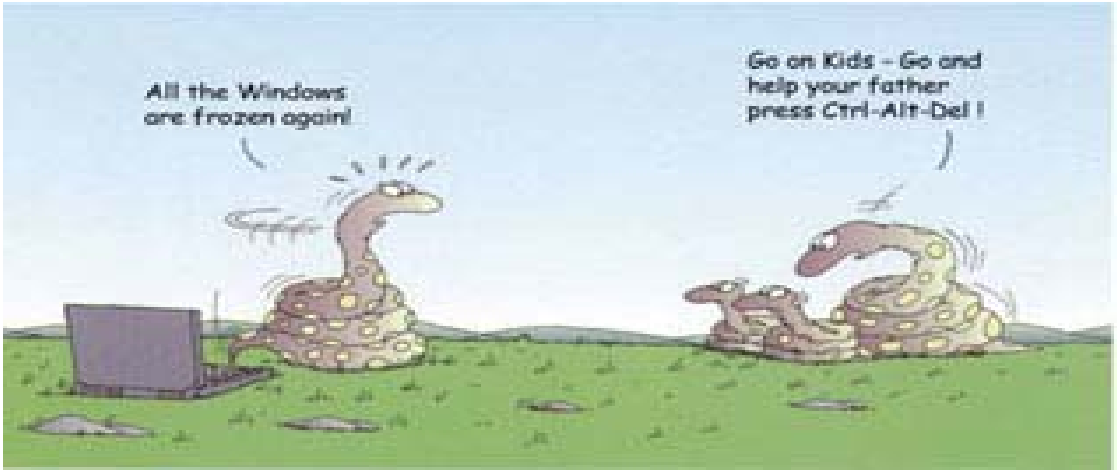
8. USA vyhlašuje nová pravidla v oblasti kryptologie:
   http://www.wired.com/news/politics/0,1283,37617,00.html
   Sdělení Bílého domu : http://cryptome.org/us-crypto-up.htm

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

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

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

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



G. Závěrečné informace

1.Sešit

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

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

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

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

http://cryptoworld.certifikuj.cz

2.Registrace - zrušení registrace

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

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

3.Spojení

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