Crypto-World

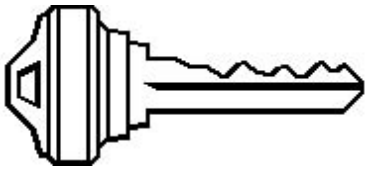
Informační sešit GCUCMP

1999

Ročník 1

Crypto-World 1999
Informační sešit GCUCMP

Připravil : Mgr.Pavel Vondruška,
člen IACR, GCUCMP

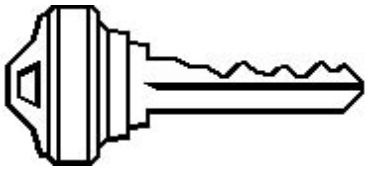


Obsah: str.

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

Crypto-World 9/99
Informační sešit GCUCMP

Připravil : Mgr.Pavel Vondruška,
člen IACR, GCUCMP
Uzávěrka 7.9.99
(25 e-mail výtisků)



Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (internet, noviny). Oficiální informační sešit je primárně určený pro členy "Kryptologické sekce Jednoty matematicko-fyzikální " (GCUCMP). Pokud má někdo zájem o tyto informace, stačí se zaregistrovat e-mailem na adrese hruby@gcucmp.cz (subject : Crypto-World). Informační sešit je bezplatně rozesílán v elektronické podobě e-mailem.
Případné chyby a nepřesnosti jsou dílem P.Vondrušky a GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

OBSAH : **Str.**

A. Nový šifrový standard AES

AES (Advenced Encryption Standard) – algoritmus, který má nahradit dosavadní standard DES . Jaký je vlastně aktuální stav ve vyhledávání nového šifrového standardu?

Historie :
1997 – americká vláda (přesněji NIST) vypisuje „soutěž“ na vytvoření nového komerčního standardu pro symetrické šifrování
1998 , červen – uzávěrka pro podání návrhu, celkem bylo předloženo 15 kandidátů (CAST-256, CRYPTON, DEAL, DFC, E2, FROG, HPC, LOKI97, MAGENTA, MARS, RC6, RIJNDAEL, SAFER+, SERPENT, TWOFISH) , NIST rozhodne vyhodnotit tyto návrhy a přijmout do dalšího kola jen 5 kandidátů
1998, srpen – první konference , kde se hodnotí podané návrhy (Californie, USA)

1999, duben – druhá konference (Řím, Itálie), rozhodnuto, že konec připomínek k jednotlivým algoritmům bude v červnu 1999
1999, srpen – NIST ohlašuje výběr následujících kandidátů:

1) **Mars** – vytvořeno rozsáhlým týmem odborníků IBM (reprezentován Nevenko Zunicem)
2) **Rijndael -** připravil vynikající tým belgických kryptologů (Vincent Rijmen, Joan Daemen)
3) **RC6** – od RSA Data Security (Burt Kaliski, podílel se i slavný Ron Rivest)
4) **Serpent** – navržený trojicí velice známých kryptologů - Ross Andrsonem, Eli Bihamem, Lars Knudsenem
5) **Twofish** – návrh firmy Counterpane System (prezident firmy Bruce Schneier)

(Pozn. s většinou uvedených kryptologů - jste se mohli osobně setkat v Praze letos v květnu na konferenci Eurocrypt´99 . Barevnou fotku všech účastníků konference si lze u mne zdarma vyzvednout).

NIST publikovalo velice rozsáhlou zprávu (52 stran), ve které zdůvodňuje výběr těchto kandidátů, a proč nebyly přijaty ostatní algoritmy. Tato zpráva je k dispozici na adrese :

http://csrc.nist.gov/encryption/aes/round2/round2.htm#NIST

Dalším krokem bude výběr ze zbývajících kandidátů.

Dohodnutý časový harmonogram:

1) Na „7-th Fast Software Encryption workshopu“ v dubnu roku 2000 budou komentovány vlastnosti uvedených kandidátů.
2) Připomínky bude dále možné na NIST předkládat do 15.května roku 2000 a potom NIST ohlásí, který z algoritmů se stál jediným kandidátem na nový komerční standard.
3) AES dále bude podroben formálnímu vládnímu schvalovacímu procesu a výsledky budou zpracovány ve FIPS (Federal Information Processing Standard).
4) Pokud vše proběhne úspěšně, tak v létě roku 2001 bude ohlášen nový standard šifrového algoritmu pro všechny komerční mezinárodní aplikace.

Připomeňme závěrem, že vybraný standard má být velice flexibilní, lehce implementovatelný, má pracovat s 32-bitovým mikroprocesorem, 64-bitovým procesorem, ale i 8-bitovým (v tzv. režimu smart card). AES má být 128-bitová bloková šifra, musí podporovat klíče délky 128, 192 a 256 bitů. Výběr takového algoritmu, který je určen pro všechny typy aplikací a nasazení (klasický software pro PC, terminály pro elektronickou komerci, čipové karty) není opravdu lehký. Autoři tvrdí , že nově vzniklý standard by snad mohl být standardem pro celé 21-století !

Pokud chcete zaslat nějaké komentáře nebo připomínky k výběru kandidátů , případně ukázat jejich slabost (!), lze je odeslat do NIST dokonce pomocí e-mailu. Přesné instrukce najdete na :
http://www.nist.gov/aes

B. O novém bezpečnostním problému v produktech Microsoftu

1.Historie
Na konferenci CRYPTO v létě roku 1998 oznámil britský kryptolog Nicko van Someran, že při analýze zdrojového kódu Windows - bezpečnostního driveru ADVAPI.DLL, který kontroluje povolení bezpečnostních funkcí včetně Microsoft Cryptographic API (MS-CAPI), objevil, že driver obsahuje dva různé klíče. Jeden slouží Microsoftu ke kontrole (podpisu) použití kryptologických funkcí a ve svém důsledku ke kontrole U.S.exportu silných kryptologických funkcí. Existenci druhého klíče nedokázal objasnit.
Na letošní konferenci CRYPTO ´99 v Santa Barbaře oznámil kanadský matematik Andrew Fernandez, že při analýze service Packu 5.0 pro Windows NT 4.0 získal pomocí odšifrování pomocných debugging informací v souboru _CProvVerifyImage@8 interní označení obou dvou výše jmenovaných klíčů. Jeden z klíčů se jmenuje _KEY a druhý _NSAKEY. Tato skutečnost vyvolala na internetu debatu a spekulace o tom, že Microsoft umožnil NSA pomocí zadních vrátek vstup k právě choulostivému modulu, který slouží k šifrování. Spekulace vycházely především z názvu pro druhý klíč a z nedávno odhalené aféry, kdy známý výrobce šifrových zařízení Crypto AG ve svých výrobcích zadní vrátka pro NSA měl.
Microsoft proto 3.9.1999 reagoval oficiální tiskovou zprávou, ve které vysvětluje, že se jedná pouze o záložní klíč, a protože slouží ke kontrole exportu silné kryptografie, která podléhá kontrole vlády, byl "vhodně" nazván _NSAKEY.

2. Odhalení názvu druhého klíče

Uvedený postup provedl Andrew Fernandez z firmy Cryptonym a je popsán např. v dokumetu uloženém na (http://www.cryptonym.com/hottopics/msft-nsa.html)

Před zavedením CSP	v	ADVAPI32.DLL
adresa 0x77DF5530	->	A9 F1 CB 3F DB 97 F5 ... ...
adresa 0x77DF55D0	->	90 C6 5F 68 6B 9B D4 ... ...

Po dešifrování pomocí algoritmu RC4		dostaname
A2 17 9C 98 CA	=>	R S A 1 ... 00 01 00 01 ... (+veřejný klíč)
A0 15 9E 9A CB	=>	R S A 1 ... 00 01 00 01 ... (+veřejný klíč)

Service Pack 5 pro NT4.0		v debugging symbolech v modulu ProvVerifyImage@8"
Adresa 0x77DF5530	<-	mají data označení "_KEY"
Adresa 0x77DF55D0	<-	mají data označení "_NSAKEY"

3. Bezpečnostní problém v systému Windows
Bez ohledu na to, co existence druhého klíče s "podezřelým" názvem znamená, je nutné se podívat, jaké jsou možné důsledky tohoto faktu.

Existence dvou klíčů je prokázána v následujících verzích Win95 SR2, Win98, Win98gold, WinNT4 (všechny verze) a Win2000 (sestavení 2072, RC1). Ve Win2000 byly nalezeny dokonce tři klíče, k tomuto faktu zatím nebylo vydáno žádné oficiální prohlášení.
K čemu vlastně slouží klíč v systému Windows? Microsoft CryptoApi povolí ISVs (Independent Software Vendors) dynamické natažení CSPs (Cryptographic Service Providers) po ověření, že je digitálně podepsán klíčem Microsoft. Pokud CSPs není podepsán nelze použít šifrové rozhraní. Toto bylo zavedeno v souvislosti s kontrolou exportu kryptografie z USA. Jestliže někdo chce nahradit CSPs vlastním rozhraním nebo rozhraním s delšími-silnějšími klíči, musí být toto rozhraní podepsáno digitálním podpisem Microsoftu a to jej udělí jen, je-li použití poveleno v souladu s restrikcemi americké vlády.
Pokusy, které v posledních dnech byly provedeny, ukázaly, že CSPs nemusí být podepsán prvním klíčem (ozanačení KEY), ale k povolení načtení do paměti stačí podpis _NSAKEY. Dále se prokázalo, že veřejný klíč _NSAKEY lze nahradit jiným veřejným klíčem, a pokud je soukromým klíčem podepsán modul CSPs, lze jej provozovat.

4. Popis bezpečnostního útoku
Útok 1 (neúspěšný):
Použít vlastní CSP podepsané soukromým klíčem.
Přepsat "_KEY" vlastním odpovídajícím veřejným klíčem...
... Windows přestanou pracovat , neboť nemohou ověřit vlastní bezpečnostní podsystém

Útok 2 (úspěšný !) :
Použít vlastní CSP podepsané soukromým klíčem.
Přepsat "_NSAKEY" vlastním odpovídajícím veřejným klíčem...
... Windows pracují dále, neboť k ověření bezpečnostního subsystému je k dispozici _KEY (klíč Microsoftu)

CSP pracuje , protože Windows se pokusily jej verifikovat užitím "_KEY" a protože byly neúspěšné, pokusily se je verifikovat pomocí "_NSAKEY" (obsahuje již náš veřejný klíč).

Výsledek:
Windows CryptoAPI systém je funkční
klíč _NSAKEY je odstraněn
uživatel může použít CSP, bez podpisu klíčem _KEY (Microsoftu) nebo vlastníkem klíče _NSAKEY (Microsoft / NSA ?)

Že uvedený útok je reálný potvrzuje již zveřejněný program na serveru firmy Cryptonym, který si lze pro demonstrační použití dokonce stáhnout. Program je určen pro Windows NT 4.0.

5.Závěr
Vzhledem k uvedenému útoku plyne, že:
- Microsoft ztratil možnost kontrolovat použití silné kryptografie ve svých produktech. Přesněji - uživatel může použít vlastní CryptoApi bez podpisu firmou Microsoft a tedy bez ohledu na exportní omezení a jeho kontrolu americkou vládou.
- Potenciálně je možné ve vašem počítači nahradit _NSAKEY jiným klíčem a nahradit CryptoApi jiným CryptoApi , podepsaným výše zmíněným vnuceným klíčem . Toto nové CryptoApi může mimo předchozích funkcí vykonávat i jiné nedokumentované úkoly, které mohou sloužit útočníkovi k získání cenných informací o datech na vašem počítači

Literatura:

1. Tiskové prohlášení firmy Microsoft 3.9.99
   www.micosoft.com/presspass/press/1999/sept99/rsapr.htm
2. The New York Times, September 4, 1999 , John Markoff, A Mysterious Component Roils Microsoft http://www.nytimes.com/library/tech/99/09/biztech/articles/04soft.html
3. The New York Times, September 4, 1999 , Peter Wayner, Why a Small Software Label Raised Eyebrows , http://www.nytimes.com/library/tech/99/09/cyber/articles/04soft-side.html
4. Duncan Campbell, NSA Builds Security Access Into Windows
5. A. Fernandez, Microsoft, the nSA, and You
   http://www.cryptonym.com/hottopics/msft-nsa.html
6. R. Cooper, Is the NSA in Microsoft - Who killed JFK?
   http://ntbugtraq.ntadvice.com/default.asp?sid=1pid=47&aid=52
7. S. Kettmann, J. Glave, MS Denies Windows "Spy Key"
   http://www.wired.com/news/news/technology/story/21577.html

A další …

C. HPUX a UNIX Crypt Algoritmus

HPUX je šifrový algoritmus implementovaný v operačním systému Solaris a Crypt je šifrový algoritmus implementovaný v operačním systému UNIX. Ve skutečnosti se jedná o stejné algoritmy. V manuálech k těmto operačním systémům můžeme najít úplně rozdílné hodnocení těchto systémů !

V manuálu Solaris 2.6 Crypt můžeme číst : „ crypt je implementací jedno-rotorového zařízení založeného na bázi německého přístroje Enigma, ale s 256-elementy rotoru. Metody útoku na takovýto algoritmus jsou obecně známy, crypt poskytuje jen minimální bezpečnost.“
V manuálu HPUX 10.20 můžeme číst : „ crypt je implementací jedno-rotorového zařízení založeného na bázi německého přístroje Enigma, ale s 256-elementy rotoru. Metody útoku na takovýto algoritmus jsou známé , práce, které je třeba vzít do úvahy s těmito útoky, jsou však velmi rozsáhlé.“
Čteme-li manuál HPUX dále , najdeme vyjádření, že crypt chrání adekvátním způsobem vaše soubory. Je smutné, když šifrový algoritmus, který umí „breaknout“ (rozluštit) každý student kryptografie za domácí úkol, je doporučen dodavatelem operačního systému k ochraně dat!
http://www.counterpane.com

D. Letem "šifrovým" světem

1) Na adrese
http://www.ntsecurity.net/forums/2cents/news.asp?IDF=118&TB=news
je uvedeno tvrzení, že šifrový algoritmus EFS (Encrypting File Systém) vestavěný do Microsoft Windows 2000 byl „rozbit“. Microsoft ve své odpovědi tvrdí, že systém samotný nebyl „rozbit“, ale bylo využito toho, že uživatelé systém špatně používají (jedná se o možnost využití EFS recovery key) …
http://www.microsoft.com/security/bulletins/win2kefs.asp

2) Objevila se nová verze známého viru Melisa. K šíření využívá slabin Microsoft Outlook. Vir ničí operační systém Windows. Na internetu najdeme jízlivé komentáře, které dodávají, že práce, kterou Melisa provádí je "chytrá a aktuální ".
http://www.computerworld.com/home/print.nsf/all/990719B50A

3) V Kalifornii byla přijata nová verze zákona o digitálním podpisu. Digitální podpis je nyní uznáván jako podpis, který lze právně použít k podpisu obchodních kontraktů .
http://www.computerworld.com/home/news.nsf/all/9907294dig

4) Útok "hrubou silou" (totální zkoušky klíčů) na soubor zašifrovaný pomocí programu ZIP je samozřejmě možný (odmyslíme-li otázku strojového času) a jednoduchý (na internetu je spousta programů, které lze úspěšně použít. Na níže uvedené adrese se však objevila novinka, která využívá možnosti útoku ze znalosti otevřeného textu (known-plaintext attack). Velice zajímavé je, že k útoku stačí znalost 13-ti bytů ! Zájemci mohou navštívit adresu :
http://www.unix-ag.uni-kl.de/~conrad/krypto/pkcrack.html a pokud vlastníte 30 ecash (digitálních peněz) můžete si stáhnout verzi pro UNIX nebo DOS.

5) Po úspěšném útoku hackerů na poštovní server Microsoftu koncem minulého měsíce se řada lidí ohlíží po jiném "bezpečném" poštovním serveru. Vzhledem k tomu, že hackeři stáhli úplný seznam všech uživatelů včetně hesel a vzhledem k tomu, že pro zapomnětlivé je na Hotmailu přímo vestavěná možnost jak heslo (při znalosti jistých údajů o majiteli účtu) získat, rozhodl jsem se tuto adresu vyškrtnout ze seznamu mnou používaných adres. Současně doporučuji používat pro důvěrnou poštu následující server : "Hushmail".
Hushmail je typu serveru Hotmail, ale používá šifrování. Pro komunikaci je implementován protokol SSL (z prohlížeče) na server a následně šifrování zpráv pomocí kvalitního programu Blowfish . RSA v SSL používá klíč délky 1024 bitů ! Zdrojový kód lze také získat a stáhnout z níže uvedeného serveru (poslední verze je 1.04) a vytvořit si vlastní silnou kryto-aplikaci (nepodléhá vývozním restrikcím !).
http://www.wired.com/news/news/email/explodeinfobeat/technology/story/19804.html
Hushmail homepage: **http://www.hushmail.com/**
Technická podpora: **https://www.hushmail.com/tech_description.htm**
Zdrojový kód: **http://www.cypherpunks.ai/~hush/**

6) Francie změnila svoji politiku restrikcí na poli šifrování. Ministerský předseda Lionel Jospin oznámil, že Francie obrací svoji dlouhotrvající tradiční domácí restriktivní politiku směrem k volnému používání silných šifer až do délky klíče 128 bitů. Do té doby Francie umožňovala na domácím poli používat volně jen šifry do 40 bitů klíče. Jedná se pravděpodobně o rozhodnutí, které bylo provedeno na základě informací o existenci a využívání špionážního systému ECHELON.
http://jya.com/jospin-coup.htm

7) Na základě zprávy odborného orgánu EP (Evropského parlamentu) STOA, která byla publikována v dubnu 1999 (zpráva se krátce nazývá "Interception Capabilities 2000", nebo jen IC2000 , **http://www.iptvreports.mcmail.com/stoa_cover.htm**), byla přehodnocena německá vládní politika v oblasti kryptologie a ochrany dat. Německá vláda přijala zásadní dokument o principech šifrové politiky "Eckpunkte der deutschen Kryptopolitik", který je svým obsahem ve světě zcela ojedinělý (**http://www.bmwi.de/presse/1999/0602.html**). Tento dokument zásadně mění vládní postoj k silné kryptografii. Některé základní informace lze nalézt např. v V.Klíma : "Velký bratr všechno slyší", CHIP 8/99 nebo mohu předat svůj pracovní překlad kompletního vládního prohlášení.

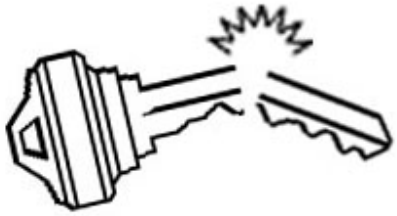
8) Švédsko. Podle časopisu Datateknik (10/99, **http://www.datateknik.se**) švédské ministerstvo studuje zprávu STOA IC2000 a švédská vláda pověřila tajnou polici SAPO, aby vyšetřila průmyslovou špionáž, která je vedena proti švédským národním a průmyslovým zájmům. Zahrnuje to systém ECHELON a dohodu UKUSA.
Snad již reakcí na výsledky tohoto šetření je liberalizace švédského exportu šifrových zařízení (z 23.7.1999) a obecně povolení exportu silné kryptologie s klíči do 128 bitů (mimo vyjmenované státy).
http://www.ud.se/pressinf/pressmed/1999/juni/990623_5.htm

9) CGHQ britský ekvivalent NSA se bude stěhovat. Nová budova má plánovanou kapacitu pro 4500 lidí (v originále for 4,500 eavesdroppers and code-breakers) a bude dokončena v roce 2002. V areálu bude místo pro 1750 služebních aut a náklady jsou stanoveny na 300 miliónů liber šterlinků.
http://www.guardianunlimited.co.uk/Archive/Article/0,4273,3862710,00.html

10) INVEX Computer Brno´99 se již tradičně uskuteční v týdnu od 4.10 do 8.10.1999. Ve stánku DSM se konají každý den od 13.00 hod. do 16.00 hod. neformální odborná setkání, která budou koncipována jako odborné přednášky zástupců jednotlivých firem. Mottem setkání je slogan "O informační bezpečnosti - netradičně". Na akci je nutné se předem registrovat u DSM.

Crypto-World 10/99
Informační sešit GCUCMP

Připravil : Mgr.Pavel Vondruška,
člen IACR, GCUCMP
(31 e-mail výtisků)
Uzávěrka 3.10.99



Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (internet, noviny). Oficiální informační sešit je primárně určený pro členy "Kryptologické sekce Jednoty matematicko-fyzikální " (GCUCMP). Pokud má někdo zájem o tyto informace, stačí se zaregistrovat e-mailem na adrese hruby@gcucmp.cz **(subject : Crypto-World). Informační sešit je bezplatně rozesílán v elektronické podobě e-mailem.**
Případné chyby a nepřesnosti jsou dílem P.Vondrušky a GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

OBSAH : **Str.**

Logo z minulého čísla - klíč - bylo po připomínce jednoho z Vás, že klíč značí spíše zvýšenou odolnost proti útokům, ale obsah sešitu spíše poukazuje na bezpečnostní slabiny - změněno (Petře, Je to OK ?). Logo vymyslel můj syn a druhý mi pomohl s jeho realizací a já jim za to slíbil, že to v sešitu napíši. Tedy logo dle návrhu Petra Vondrušky (11 let), grafická úprava Pavel Vondruška (13 let).

A. Microsoft Back Orifice 2000

Z bezpečnostního hlediska se jedná o nové veliké riziko pro počítače připojené na internet. Kusé informace, které se tu a tam objevují , doplníme alespoň úplným oficiálním zněním tiskového prohlášení firmy Microsoft z 31.8.1999 viz www.microsoft.cz, anglická verze je umístěna mezi tiskovými prohlášeními na www.microsoft.com . Pro zájemce jsou připojeny odkazy na www stránky, kde jsou uvedeny rozsáhlejší informace.

Co by měli zákazníci vědět o „BackOrifice 2000“

BackOrifice 2000 (BO2K) je nepřátelský škodlivý program, který měl být uveden do oběhu okolo 10. července t. r. Jeho autoři se jistě pokusí vyvolat okolo něj hysterii. Uživatelé se před ním mohou chránit dodržováním běžných pravidel bezpečné práce s počítačem. Ačkoliv program ještě nebyl do oběhu uveden, společnost Microsoft pečlivě sleduje situaci a vynasnaží se poskytovat informace, které umožní uživatelům pochopit podstatu programu a ochrany proti němu, jakmile se objeví.

Následují odpovědi na nejčastější otázky ohledně programu BO2K.

Co je BO2K za program?
BO2K je program, který po nainstalování na počítač s Windows umožňuje dálkové ovládání počítače jiným uživatelem. Software pro dálkové ovládání počítače není sám o sobě nikterak závadný (škodlivý) a mnoho takových programů se legálně prodává a je využíváno např. správci výpočetních systémů. BO2K se odlišuje tím, že má sloužit k poškozování uživatelů a má utajené funkce, které nemají jiný účel než stížit jeho odhalení.

Jaké nebezpečí od tohoto programu hrozí?
Je-li BO2K instalován na počítači, „útočník“ může s počítačem dělat cokoliv, co může udělat oprávněný uživatel z klávesnice. Může tedy i spouštět programy, tvořit nebo mazat soubory, odesílat a přijímat data apod.

Jak se tento program může dostat do mého počítače?
Jako kterýkoliv jiný program, BO2K musí být na počítač nainstalován. Nelze ho tam jakkoliv nenápadně „vsunout“. Existují pouze dva způsoby, jak může být instalován:
Umožníte-li člověku, který ho chce na váš počítač nainstalovat, fyzický přístup k vašemu počítači (tj. zná-li vaše přihlašovací heslo, nebo pustíte-li ho k zprovozněnému počítači). Pokud vás nějak přiměje, abyste si ho nainstalovali sami. Toto je známo jako tzv. technika Trojského koně. Může vám být např. zaslán e-mail s přílohou, která se tváří jako hra, ale ve skutečnosti nainstaluje na váš počítač BackOrifice.

Jak předejít instalování BO2K na můj počítač?
Nemusíte podnikat žádná mimořádná opatření. Pouze dodržujte běžné postupy pro bezpečnou práci s počítačem:
nikomu nikdy nesdělujte svoje přístupové heslo a vždy uzamkněte počítač, když od něj odcházíte nikdy nespouštějte software z neověřených zdrojů udržujte neustále aktuální verze vašeho antivirového příp. i jiného bezpečnostního software

Pokud se již BO2K do mého počítače dostal, jak se ho zbavím?
Výrobci antivirového software a utilit pro indikaci nežádoucích aktivit v počítači pozorně očekávají objevení BO2K a jsou připraveni co nejrychleji vyvinout software k jeho detekci a odstranění. Microsoft s nimi úzce spolupracuje a je připraven jim asistovat. Při uvedení

předchůdce BO2K byly obranné prostředky k dispozici během několika dní a stejný termín lze předpokládat i v současné situaci.

Využívá BO2K nějakých mezer v zabezpečení Windows nebo Windows NT?
Nikoliv. Programy jako BO2K mohou být vytvořeny pro jakýkoliv operační systém – tento byl napsán zrovna pro Windows a Windows NT. V jakémkoliv operačním programu můžete spustit program, který může dělat všechno to, co může dělat uživatel přímou obsluhou počítače. A pokud vás někdo lstí přinutí spustit destruktivní program, ten pak může smazat vaše data, pozměnit údaje nebo umožnit někomu dalšímu zadání dalších příkazů.
Software typu Trojského koně nenapadá technologii, ale uživatele. V případě, že by BackOrifice využíval nějaké bezpečnostní mezery ve Windows nebo Windows NT, Microsoft by okamžitě tuto mezeru opravil a zabránil tak funkci programu. Autoři BackOrifice si však uvědomili, že je snazší se zaměřit na lidi a přimět je ke spuštění škodlivého software, než se zaměřit na technologii.

Je BO2K něco jako virus Mellisa?
Jenom v tom smyslu, že oba jsou tzv. Trojské koně a vykonávají „záškodnické“ akce, a ani jeden z nich nevyužívá jakékoliv případné chyby v produktech společnosti Microsoft.

Co v souvislosti s BO2K podniká společnost Microsoft?
Microsoft pečlivě sleduje situaci a cítí se povinen pomoci uživatelům zajistit bezpečnou a radostnou práci s počítačem:
experti společnosti Microsoft na bezpečnost jsou připraveni okamžitě po objevení se software BO2K přesně zjistit jak pracuje a jaké prostředky lze použít k ochraně před jeho účinky
Microsoft spolupracuje s ostatními firmami, zabývajícími se bezpečností počítačů – zejména s výrobci antivirového software, utilit pro detekci nežádoucích aktivit počítače a dalších bezpečnostních produktů – na tom, aby software pro detekci a odstranění BO2K byl dostupný co nejdříve Microsoft poskytne svým zákazníkům maximální množství dostupných informací o tomto programu.

Další informace:
http://www.bo2k.com/
http://www.zdnet.com/zdnn/stories/news/0,4586,2127049,00.html
http://www.infoworld.com/cgi-bin/displayArchive.pl?/99/30/o03-30.36.htm
http://www.microsoft.com/smsmgmt/techdetails/remote.asp
http://www.cultdeadcow.com/news/pr19990719.html

B. Šifrování disku pod Linuxem

To: cypherpunks@algebra.com
From: "Doobee R.Tzeck" <doobee@ccc.de>
Subject: Encrypting your Disks with Linux

Je mnoho možností jak šifrovat data na disku v OS Linux. Šifrování dat na disku potom chrání vaše data proti klasickým útokům, jako přihlášení se vaším jménem, nabootování z jiného volumu a přimontování vašeho disku ke svému, chrání samozřejmě vaše data při ztrátě laptopu. Otázku jakou metodu použít, si položil "Doobee R.Tzeck" <doobee@ccc.de> a shromáždil informace o dostupných šifrovacích programech disku pro

LINUX. Potom se obrátil na diskusní fórum cypherpunks@algebra.com se žádostí, zda může někdo kvalifikovaně k těmto systémům něco říci.

Pro náš sešit jsem přepsal některé základní informace. V případě, že se na diskusním fóru objeví některá informace o slabosti některého z dále předkládaných systémů a já ji zachytím, budu se snažit o ní informovat. Dnes tedy jen základní přehled.

Přehled šifrování v Linuxu :

1. Loopback Encryption http://drt.ailis.de/crypto/linux-disk.html#loopback
2. Encrypted Home Directorys http://drt.ailis.de/crypto/linux-disk.html#ehd
3. CFS - Cryptographic File Systém http://drt.ailis.de/crypto/linux-disk.html#cfs
4. TCFS - Transparent Cryptographic Filesystem http://drt.ailis.de/crypto/linux-disk.html#tcfs
5. ppdd - Practical Privacy Disc Driver http://drt.ailis.de/crypto/linux-disk.html#ppdd
6. sfs - Steganographic File System for Linux http://drt.ailis.de/crypto/linux-disk.html#sfs
7. StegFS - A Steganographic File System for Linux http://drt.ailis.de/crypto/linux-disk.html#stegfs
8. BestCrypt http://drt.ailis.de/crypto/linux-disk.html#bestcrypt

1. The Kernel Loopback Encrypting Block device

Jedná se o klasickou metodu šifrování partitions v Linuxu. Před instalací je nutno použít poslední patch kernelu. Lze jej stáhnout např. z http://www.kerneli.org . Co je podle mne velice zajímavé, že nový patch umožňuje používat následující šifry DFC, MARS, RC6, Serpent, CAST 128, IDEA, Twofish, Blowfish. Jak vidíte většinu tvoří kandidáti na AES - nový šifrový standard (viz. např minulé číslo našeho sešitu Crypto-World 9/99 - Nový šifrový standard AES)..

2. Encrypted Home Directorys Patch

Umožňuje šifrování adresářů užitím loopback encryption, ale pro více uživatelů .Je to výhodné pokud váš počítač je sdílen více uživateli.
Jak to funguje je popsáno v : http://members.home.net/id-est/

3. CFS - Cryptographic File System

CFS byl "zlomen" Matt Blazem. Více o CFS např. ve "A Cryptographic File System for Unix" by Matt Blaze ftp://research.att.com/dist/mab/ .CFS podporuje DES (považovaný již za nepříliš bezpečný), 3DES (který je ovšem pomalý), MacGuffin (ten je již ale rozbit), SAFER-SAK-128 (ovšem v neobvyklém tvaru), Blowfish (který se obecně považuje za bezpečný, ale zde je nějaký problém s uložením P-boxů a S-boxů v systémovém archívu - dokonce tu snad chybí …). Mimo bezpečnosti je zde ještě problém s rychlostí , kopie dat se několikráte vyměňují mezi jádrem a uživatelským prostorem. Při šifrování velkého objemu dat je tato metoda nevhodná.

4. TCFS - Transparent Cryptographic Filesystem

TCFS byl vyvinut na univerzitě v Salerno (Itálie). Je hluboko zaintegrován v systému, šifrové služby a systémová práce se soubory jsou kompletně transparentní pro užití v uživatelských aplikacích. Je nutné mít nainstalovaný poslední patch 2.0.x Kernel. Aplikacemi je zatím málo používán. Nevýhodou je minimální podpora klíčového hospodářství. Je zde jen nějaký

prozatimní " Placebo-key management" dodávaný s TCFS ale ten používá jen přihlašovací heslo a jedno heslo na šifrování.
Některé z možných problémů jsou diskutovány na : http://tcfs.dia.unisa.it/tcfs-faq.html.
Domácí stránka TCFS je umístěna zde :http://tcfs.dia.unisa.it/

5. ppdd - Practical Privacy Disc Driver
ppdd je dobře vystavěný systém na šifrování vašeho disku. Jeho autorem je for Allan Latham. Sám píše, že " … ppdd se užívá k šifrování souborů pod Linuxem. Využívá vysoce kvalitní šifrovací techniky pro velké volumy, lehce se instaluje. …" . Chránit lze např. root tak, že po naběhnutí systému, mohou být různé části chráněny jinými přístupovými právy. Je ideální pro víceuživatelský systém. Práce se zašifrovanými soubory je samozřejmě pomalejší. Např. u Pentia 100 Mhz, 32 MB RAM, IDE řadič je propustnost 50%. Ovšem již na dual PII/266 Mhz,256 MB RAM, IDE řadič byl sice zápis na zašifrovaném volumu 2x pomalejší, ale čtení zašifrovaných dat již bylo 4x rychlejší …
Další podrobné informace můžete nalézt na :
http://drt.ailis.de/crypto/Specification.txt
http://drt.ailis.de/crypto/ppdd.man.html
http://linux01.gwdg.de/~alatham/ppdd.html
ftp://ftp.gwdg.de/pub/linux/misc/ppdd
http://drt.ailis.de/crypto/ppddhow.txt (podrobnosti k instalaci)

6. sfs - steganographic file system for Linux
Teoretickým východiskem byl článek Ross Anderson, Roger Needham and Adi Shamir "The Steganographic File System" (http://drt.ailis.de/crypto/sfs3.ps.gz) . Prvou implementaci napsal Carl van Schaik and Paul Smeddle. Aby nemohla být data lehce napadnutelná, je zde např. zabudována myšlenka automatického přešifrování (utajení dat) každý den , podle určité skryté informace. Autoři o programu píší, že neručí za případnou ztrátu vašich dat, že se jedná vlastně o experiment Připomínají, že neručí za to jak silnou šifrovou metodu jste použili - s ohledem na platný řád v zemi, kde žijete a kde jsou možná určitá omezení.
Domácí stránka této problematiky je na : http://leg.uct.ac.za/~carl/vs3fs/ (patches pro Linux 2.0 and 2.1). Peter Schneider-Kamp updatoval program pro verzi 2.2. Tento update lze nalézt na adrese: http://www.linux-security.org/sfs/
Problému je také věnována stránka: http://drt.ailis.de/public_html/crypto/sfspatch-2.2.10.tar.gz

7. StegFS - A Steganographic File System for Linux
Andrew McDonald a Markus Kuhn vytvořili vlastní implementaci šifrování dat na základě steganografických metod. Jejich základní myšlenka také vychází z již citovaného článku Anderson, Needhama a Shamira. Tvrdí, že sfs je "vadné". Jejich systém StegFS se zdá být opravdu vypracovaný a zdá se, že je v praxi dobře použitelný a "lepší" než sfs.
StegFS má svoji stránku na http://ban.joh.cam.ac.uk/~adm36/StegFS/

8. BestCrypt
Jedná se o komerční program pro zašifrování disku pod Linuxem. Jeho verze existují též pod operačními systémy MS Windows a MacOS .
Informace na : http://www.jetico.com/

C. Microsoft Point-to-Point Tunneling Protocol (PPTP)

Counterpane Systems and L0pht Heavy Industries Announce Analysis of Microsoft PPTP Version 2 By Bruce Schneier

Plné znění této přednášky lze najít na http://www.counterpane.com/pptpv2-paper.html .
Zde jen některé detaily.

V roce1998, Bruce Schneier and Mudge provedli analýzu protokolu PPTP od firmy Microsoft. My (píše B.Schneier) jsme nalezli vážné chyby v následujících oblastech :

- password hashing -- slabý algoritmus umožňující útočníkovi seznámit se s uživatelskými hesly
- Challenge/Reply Authentication Protocol -- chyba umožňuje útočníkovi tvářit se jako server
- encryption -- chyba v implementaci umožňuje obnovit zašifrovaná data
- encryption key -- obecná hesla poskytují napadnutelné klíče, i když je použito šifrování s klíčem délky 128-bit
- control channel -- neautentizované zprávy umožňují útočníkovi zaútočit na PPTP server

Detaily z analýzy provedené v roce 1998 jsou umístěny v tiskové zprávě na našem serveru (http://www.counterpane.com/) a ve FAQ.

Na základě naší analýzy Microsoft realizoval upgrade protokolu. Tento upgrade je použitelný pro Windows 95, Windows98, a Windows NT jako DUN 1.3. Microsoft tak zvýšil upgradem bezpečnost svého protokolu.

O analýze nového upraveného protokolu vzhledem k přesnosti již původní originální text :

The weaker LAN Manager hash is no longer sent along with the stronger Windows NT hash. This is to prevent automatic password crackers like L0phtcrack (http://www.l0pht.com/l0phtcrack)
from first breaking the weaker LAN Manager hash and then using that information to break the stronger NT hash. An authentication scheme for the server has been introduced. This is to prevent malicious servers from asquerading as legitimate servers.
The change password packets from MS-CHAPv1 have been replaced by a single change password packet in MS-CHAPv2. This is to prevent the active attack of spoofing MS-CHAP failure packets. MPPE uses unique keys in each direction. This is to prevent the trivial cryptanalytic attack of XORing the text stream in each direction to remove the effects of the encryption.

The software is more robust against denial-of-service attacks, and does not leak as much information about its status.

These changes address most of the major security weaknesses of the orginal protocol. However, the revised protocol is still vulnerable to offline password-guessing attacks from hacker tools such as L0phtcrack**. At this point we still do not recommend Microsoft PPTP for applications where security is a factor.**

D. Letem "šifrovým" světem

1) Několik lidí se pozastavilo nad tím, že v čísle 9/99 jsem tak rezolutně vystoupil proti poštovnímu serveru HOTMAIL a zrušil jsem svoji adresu na tomto serveru.
Můj postoj snad osvětlí následující krátký komentář. Z článků, které se objevily během tohoto měsíce na internetu vyplývá, že chyba na serveru HOTMAIL dovolila číst bez hesla všechny e-mailové zprávy po delší dobu a nejednalo se o náhodný průnik na poštovní server. Je více jak pravděpodobné, že hackerské společenství o chybě na serveru vědělo a umělo ji využívat již dávno před tím, než byla tato chyba odhalena.
http://207.82.250.251/cgi-bin/start?curmbox=ACTIVE&js=no&login=username
http://www.wired.com/news/news/technology/story/21503.html
http://www.msnbc.com/news/306093.asp
http://www.zdnet.com.au/zdnn/stories/zdnn_display/0,3440,2324361,00.html
http://news.excite.com/news/zd/990901/10/the-bug-syndrome
http://news.excite.com/news/zd/990901/06/how-hotmail-blew
http://www.salon.com/tech/log/1999/09/02/hotmail_hack/print.html

2) Firma Microsoft vyvinula k zajištění digitální hudby speciální bezpečnostní formát - Windows Media Audio (WMA), zabezpečenou alternativu MP3. O tom, že právě bezpečnost není doménou firmy Microsoft svědčí to, že byl do dvou dnů po jeho uveřejnění již rozbit.
http://www.wired.com/news/news/technology/story/21325.html
http://www.news.com/News/Item/0,4,0-40672,00.html?st.ne.lh..ni
http://www.msnbc.com/news/302195.asp

3) Bezpečnost NT.
Bruce Schneier v článku o Microsoft Orifice 2000 (časopis "Crypto-Gram 8/99")se zmínil, že aby byl operační systém Windows NT opravdu bezpečný, bylo by potřeba provést více jak 300 úprav. Na svém webu (http://www.counterpane.com) Bruce Schneier píše :

"Mnoho lidí se pozastavilo nad mou poznámkou o bezpečnosti grafického operačního systému NT a potřebě nastavit více jak 300 bezpečnostních změn. Předložil jsem tedy tento odhad diskusní skupině na Usenetu (comp.os.ms-windows.nt.admin.security) a ptal se kolik tedy je potřeba nastavit bezpečnostních opatření. Diskusní skupina se ujednotila, že počet změn je kdesi mezi 50 a 3000, a tedy můj odhad 300 nebyl nerozumný . Pokud si to chce někdo ověřit, doporučuji
http://people.hp.se/stnor/ nebo http://www.trustedsystems.com/NSAGuide.htm "
- konec citace .

4) Microsoft se snaží zvýšit svoji vážnost na poli bezpečnosti například i následující akcí. Microsoft umístil beta verzi svého nového grafického operačního systém Windows 2000 a vyzval hackery, aby se do něj pokusily "vloupat". Útok hackerů byl neúspěšný. (Možnost útoku byla ovšem časově omezena).
http://www.zdnet.com/zdnn/stories/news/0,4586,2309474,00.html?chkpt=hpqs014
http://www.windows2000test.com/

5) Oficiální bezpečnostní politika firmy Microsoft je popsána ve sděleních "white paper" na serveru microsoftu. Mezi tato sdělení přibyla dvě následující:
Základy bezpečnosti: http://www.microsoft.com/security/resources/security101wp.asp
Microsoft Office 2000 Macro Security White Paper :
http://officeupdate.microsoft.com/2000/downloadDetails/o2ksec.htm

6) Za jediný měsíc, kdy je na tuzemském trhu k dispozici sada kancelářského softwaru Office 2000 v české verzi, se prodal rekordní počet 31 000 licencí (mimochodem instalační sada nyní již obsahuje 4 plná CD)! http://www.microsoft.cz/

7) Skupina českých hackerů CzERT pozměnila (již potřetí) www stránku banky UNION. Tentokráte přejmenovali banku na RUIN banku a umístili zde fotografii nahé ženy, která strká ruku do zadnice koně, s nadpisem "Ředitelka ústavu" a textem : "Tady lovím vaše investice a úspory ! " . Pokud se chcete pokochat jak vypadaly stránky před útokem a po útoku této skupiny, doporučuji navštívit archiv průniků této skupiny (jsou zde informace i útoku na servery policie, ministerstva zdravotnictví apod.). Archiv je umístěn na http://www.hysteria.sk .

8) Těsně před uzávěrkou jsem dostal upozornění od J.Pinkavy na velice zajímavou informaci, která se týká odolnosti eliptických křivek. Celý text je uveden v závěru jako samostatná příloha :
"INRIA leads nearly 200 international scientists in cracking code following challenge by Canadian company Certicom"

9) Ještě jednou připomínám INVEX Computer Brno´99 začíná dnes tj. 4.10 a trvá do 8.10.1999. Ve stánku DSM se konají každý den od 13.00 hod. do 16.00 hod. neformální odborná setkání, která budou koncipována jako odborné přednášky zástupců jednotlivých firem. Mottem setkání je slogan "O informační bezpečnosti - netradičně". Na akci je nutné se pro veliký zájem předem registrovat u DSM a nebo se na místě vnutit.

10) Problém Y2K (přechod na rok 2000) a Windows. Těm, kteří to neví, připomínám že je potřeba doinstalovat patche do jednotlivých verzí Windows, aby (v případě, že váš BIOS je OK) jste mohli v roce 2000 dále bez potíží používat svůj oblíbený operační systém. Tentokráte musím firmu Microsoft pochválit. Na serveru http://www.microsoft.com/year2000 jsou k dispozici všechny patche pro jednotlivé verze Windows. Nejsou nijak malé (až několik megabyte). Nicméně konec roku se blíží, a tak doporučuji stáhnout a nainstalovat.

11) A tuhle znáte …
Z oficiálního sdělení firmy Microsoft... Pokud nebude verze Windows 2000 v prodeji do konce tohoto roku 1999 , bude v prodeji v lednu roku 1900.

Příloha č.1

http://www.inria.fr/Actualites/pre55-eng.html

INRIA leads nearly 200 international scientists in cracking code following challenge by Canadian company Certicom

Paris, September 28. 1999 - A new code-cracking challenge set by Certicom has been successfully overcome using 740 computers in 20 countries over a period of 40 days. The code, ECC2-97, is based on a technique known as elliptic curves.

Led by Robert Harley, a member of the Cristal project at INRIA, France's National Institute for Research in Computer Science and Control, the 195 researchers involved showed that a 97-bit encryption system based on elliptic curves is more difficult to crack than a 512-bit system based on integers such as RSA-155.

Encryption systems based on elliptic curves have been known since the mid-1980s, but have only recently been adopted by leading encryption companies such as RSA Security Inc. Certicom issued its "ECC Challenge" in November 1997, specifying a series of challenges of increasing difficulty. The company offers prizes up to US$100,000. The aim of the challenge is to encourage research in the field of elliptic curves and their applications in encryption, and to strengthen arguments in favor of using elliptic curve cryptography instead of systems based on integer factorization.

The challenge dubbed "ECC2-97" took place in a set of about 10^29 points on an elliptic curve chosen by Certicom. To solve the problem, participants first computed 119,248,522,782,547 (more than 10^14) using open-source software developed by Harley. Among these points, they screened 127,492 "distinctive" points and collected them on a Alpha Linux workstation at INRIA where further processing revealed two twin points. Finally Harley computed the solution using information associated with these two points, thus nailing the problem.

The solution was found after less than one third of the predicted computation. The probability of finding the answer so quickly was less than one in ten. Two other twins were detected a few hours after the first - a less than one in 100 probability! Nevertheless the computing power used, around 16,000 MIPS/years, was twice as much as that used for the factorization of RSA-155 announced by Herman Te Riele of CWI (Amsterdam) and his colleagues on 26 August 1999.

"These results strengthen our confidence in codes based on properly-chosen elliptic curves," said Harley. "This needs to be taken into account in standards for security and confidentiality on the Internet."

According to Andrew Odlyzko, Head of Mathematics and Cryptography Research, at AT&T Labs, the code-cracking operation was "a great achievement that demonstrates the value of fruitfully harnessing some of the huge computational power of the Internet that is idle most of the time". He added: "It validates theoretical security predictions, and demonstrates the need to keep increasing cryptographic key sizes to protect against growing threats."

Arjen K. Lenstra, Vice President at Citibanks's Corporate Technology Office in New York and one of the main contributors to the recent successful attack on the RSA-155 challenge, compared the two computational efforts and noted that the present result makes 160-bit ECC keys look even better compared to 1024-bit RSA keys, from a security point of view. "Ideally we would like new theoretical advances to further reinforce these practical results, although such advances appear out of reach for the moment."

Out of the $5000 prize money, the team members will give $4,000 to the Free Software Foundation to encourage the creation of new free software. The remaining $1,000 go to the team members who identified the twin points. Both were in fact found by Paul Bourke using a network of Alpha workstations, mainly used for studying pulsars at the Centre of Astrophysics at Swinburne University in Australia.

The most active teams in the project were:

Astrophysics & Supercomputing	Australia
INRIA	France
University of New South Wales	Australia
"Friends of Rohit Khare"	USA and France
Ecole Polytechnique	France
Compaq	USA and Italy
Technischen Universitat Wien	Autriche
University of Vermont	USA
"WinTeam"	International
British Telecom Labs	UK
Internet Security Systems	UK
Rupture Dot Net	USA
"Jabberwocky"	USA
Ecole Normale Superieure de Paris	France

For a complete list of participants consult the project's Web pages.

Further information:
The ECDL Project
http://cristal.inria.fr/~harley/ecdl/

The Certicom ECC Challenge
http://www.certicom.com/chal/

Technical contact:
Robert Harley, INRIA :
33 1 39 63 51 57 - Robert.Harley@inria.fr

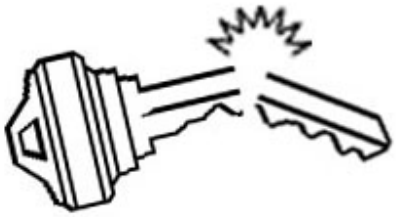
Media contacts:
Christine Genest, INRIA :
33 1 39 63 55 18 - Christine.Genest@inria.fr
Sylvie Baranger, Andrew Lloyd & Associates :
33 1 43 22 79 56 - sylvie@ala.com

Data k příloze poskytl :
Ing.Jaroslav Pinkava, CSc. (člen IACR, GCUCMP)
AEC Ltd.
Bayerova 30 tel./fax: +420 (0)5 4123 5466-7 / 41235038
602 00 Brno mobil: 0602 845 027
Czech Republic HotLine: +420 (0)5 4123 5468

INTERNET: e-mail : jaroslav.pinkava@aec.cz

Crypto-World 11/99
Informační sešit GCUCMP

Připravil : Mgr.Pavel Vondruška,
člen IACR, GCUCMP
(35 e-mail výtisků)
Uzávěrka 1.11.99



Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (internet, noviny) nebo se jedná o původní články podepsané autory. Oficiální informační sešit je primárně určený pro členy "Kryptologické sekce Jednoty matematicko-fyzikální " (GCUCMP). Pokud má někdo zájem o tyto informace, stačí se zaregistrovat e-mailem na adrese hruby@gcucmp.cz (subject : Crypto-World). Informační sešit je bezplatně rozesílán v elektronické podobě e-mailem.
Případné chyby a nepřesnosti jsou dílem P.Vondrušky a GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

OBSAH : **Str.**

A. Jak je to s bezpečností eliptických kryptosystémů?

Ing. Jaroslav Pinkava, CSc., AEC Ltd., Brno

Užití eliptických křivek pro návrh kryptosystému s veřejným klíčem poprvé navrhli pánové Victor Miller a Neal Koblitz zhruba uprostřed osmdesátých let. Jedná se v zásadě o analog již existujících systémů s veřejným klíčem; přitom modulární aritmetika je nahrazena aritmetikou budovanou na základě operací s body na eliptické křivce.

Tak jako u jiných kryptosystémů (RSA, systémy na bázi úlohy diskrétního logaritmu) spočívá bezpečnost eliptických kryptosystémů v obtížnosti řešení příslušného matematického problému. Zde se jedná o řešení úlohy diskrétního logaritmu pro eliptické křivky. V současné době je tato úloha podstatně obtížněji řešitelná než je úloha klasického diskrétního logaritmu. V důsledku toho lze konstruovat bezpečné kryptosystémy s výrazně kratší délkou klíče. To vede mimo jiné k implementacím s menšími nároky na paměť, implementacím, které jsou současně i výrazně rychlejší ve srovnání např. s kryptosystémy na bázi diskrétního logaritmu. Teoretická konstrukce přitom umožňuje vytvořit systémy zcela analogické klasickým modelům (šifrování – El Gamal, digitální podpis – DSA a výměna klíčů – Diffie-Hellman). Někteří odborníci hovoří o kryptosystémech na bázi eliptických křivek jako o nové generaci kryptosystémů s veřejným klíčem. Výrazným subjektem podílejícím se jak na teoretickém výzkumu eliptických kryptosystémů tak i na vývoji příslušných realizačních prostředků (hardware i software) je firma Certicom (http://www.certicom.com). V České republice poprvé realizovala eliptické kryptosystémy a do svých produktů implementovala brněnská firma AEC (http://www.aec.cz).

Přitom samozřejmě pro dostatečně malé rozměry klíčů (stejně jako tomu je pro všechny existující kryptosystémy) jsme schopni úlohu diskrétního logaritmu pro eliptické křivky řešit. Základní otázky, které se v této souvislosti nabízí, jsou tedy následující.

Jaké k tomu můžeme použít prostředky (algoritmy) ? Kde leží současné výpočetní meze těchto algoritmů, tj. jaké délky klíčů lze dnes již považovat za bezpečné (a to i s určitým výhledem na perspektivní rozvoj výpočetních možností)? Jaké jsou srovnatelné délky klíčů (při stejné bezpečnosti) pro eliptické křivky a např. pro RSA nebo systémy na bázi diskrétního logaritmu?

Nejprve jedna technická poznámka. Z hlediska implementací systémů na bázi jak klasického diskrétního logaritmu, tak i eliptického diskrétního logaritmu lze zvažovat v zásadě dva druhy těles, ve kterých bude příslušná aritmetika realizována. Jsou to tělesa charakteristiky 2 (tj. tělesa mající 2^n prvků) a prvočíselná tělesa. Pro klasické kryptosystémy na bázi diskrétního logaritmu se ukázala tělesa charakteristiky 2 jako nevhodná varianta – existuje řada technických prostředků k výraznému zvýšení efektivity řešení příslušné matematické úlohy kryptoanalýzy.

Na rozdíl od toho pro úlohu eliptického diskrétního logaritmu žádné postupy vedoucí k efektivnějšímu řešení pro tělesa charakteristiky dvě známa nejsou a jsou proto používány souběžně oba typy implementací, každý z těchto typů má výhody pro určitý typ realizací. Obvykle se uvádí, že eliptické křivky v prvočíselných tělesech jsou vhodnější pro softwarové realizace, zatímco eliptické křivky v tělesech charakteristiky dvě jsou vhodnější pro hardwarové realizace.

Nyní k matematické úloze řešení úlohy eliptického diskrétního logaritmu. Zde existuje několik algoritmů, jejichž výpočetní složitost lze popsat ve tvaru druhé odmocniny z N, kde N je počet bodů příslušné eliptické křivky. Jsou to zejména Pollardova ρ-metoda a Pollardova λ-metoda. Složitost z nich nejefektivnější Pollardovy ρ-metody je daná výrazem $(\pi N/4)^{1/2}$.

Obecně pro řešení úlohy eliptického diskrétního logaritmu není znám žádný algoritmus mající subexponenciální výpočetní složitost jako je tomu pro řešení úlohy faktorizace (RSA) nebo řešení úlohy klasického diskrétního logaritmu. Existují však určité speciální případy

(speciální typy eliptických křivek), kde takovéto postupy existují. Např. v roce 1991 pánové Alfred Menezes, Tatsuaki Okamoto, a Scott Vanstone přišli se subexponenciálním algoritmem pro tzv. supersingulární eliptické křivky (MOV útok) a v roce 1997 byl nalezen algoritmus s lineární (!) výpočetní složitostí pro eliptické křivky s tzv. stopou-1 (trace-1). Podobné útoky jsou stále předmětem úvah odborníků, jsou však obvykle orientovány na speciální případy eliptických křivek.

Z tohoto důvodu je také v současnosti doporučováno používat eliptické křivky s náhodně generovanými parametry, kde pravděpodobnost existence podobných útoků je minimální. Zejména atraktivním postupem je možnost generovat parametry eliptické křivky tzv. prokazatelně náhodně. Konstruktér eliptické křivky se takto může vyhnout potenciálním obviněním ze strany uživatele, že vložil do hodnot parametrů určitá zadní vrátka, která mu umožňuji proniknout snadněji za bezpečnostní hranice systému. Pro konstrukci eliptických křivek je nezbytné pro stanovení konkrétních hodnot parametrů mít k dispozici prostředek pro výpočet počtu bodů dané eliptické křivky. Obecně toto řeší tzv. Schoofův algoritmus, který však není tak jednoduché implementovat. Proto také v současnosti jsou již k dispozici určité doporučené množiny parametrů (NIST, SECG – viz dále).

Srovnatelná bezpečnost různých kryptosystémů při různých délkách klíčů:

Blokové šifry	Eliptické křivky	RSA/DL (klasický diskrétní logaritmus)
56	112	512
64	128	768
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

Již delší dobu probíhá tzv. RSA Factoring Challenge sponzorovaná RSA Security, Inc. (http.//www.rsasecurity.com) V srpnu 1999 byl v tomto směru získán význačný výsledek, bylo rozbito RSA s délkou klíče 512 bitů (mj. tato délka klíče je stále používána v řadě komerčních systémů, zejména systémů pro elektronický obchod).

Analogický výsledek byl získán francouzským vládním institutem INRIA, kdy při použití 740 počítačů v 20 zemích byl za 40 dnů rozbit 97-bitový eliptický kryptosystém (Certicom Elliptic Challenge). Tento výsledek byl popsán v minulém čísle informačního sešitu (Crypto-World 10/99).

Pokud srovnáme dosažené výsledky s výše uvedenou tabulkou můžeme zcela jednoznačně zhodnotit jejich význam pro bezpečnost příslušných kryptosystémů. Doplníme-li tyto informace o známý výsledek rozbití DES (56-bitová bloková šifra), máme vlastně plnou charakterizaci současných možností.

Proto také doporučované hodnoty délek příslušných klíčů se dnes pohybují (tabulka) od třetího řádku níže. Přitom v tabulce první řádek vlastně charakterizuje již dosažené výsledky (s výjimkou eliptických křivek, kde realizace příslušných kryptoanalytických metod je asi přeci jen ještě obtížnější než dávají odhady v tabulce). Druhý řádek charakterizuje již mez, která sice zatím v praxi dosažena ještě nebyla, avšak lze předpokládat, že např. v dalších dvaceti či možná deseti letech dosažena bude. Ani jedny z těchto hodnot parametrů nejsou tudíž doporučovány pro praktické použití.

Samozřejmě v budoucnu lze předpokládat, že budou v tomto směru dosaženy další výsledky dokumentující postup výpočetních možností lidské společnosti. Pokud však nebudou získány zásadní matematické výsledky umožňující zcela nový pohled na úlohu elitptického diskrétního logaritmu (nebo nebude např. zrealizován kvantový počítač), lze tyto výpočetní možnosti určitým způsobem predikovat. Odsud lze potom také odvodit doporučení pro bezpečné délky klíčů. To je také cílem výše zmíněných „výzev“ (challenge) organizovaných firmami RSA a Certicom.

V současné době již existuje řada plnohodnotných norem pro vytváření kryptosystémů na bázi eliptických křivek. Jedná se především o materiály vytvořené skupinou IEEE P1363, které jsou zpracovány s velkou důkladností a vytváří základní východiska pro budování konkrétních kryptosystémů. Dále jsou to normy vytvořené pro finanční sféru (ANSI X9.62 a ANSI X9.63), které dále konkretizují postupy při vytváření digitálních podpisů a definují postupy pro výměnu a přenos klíčů. Konkrétní volbou parametrů pro eliptické kryptosystémy se zabývají materiály skupiny SECG (Certicom, http://www.secg.org) a v květnu 1999 vydaná příslušná doporučení amerického vládního úřadu NIST.

V materiálech SECG lze nalézt řadu dalších hodnotných informací ve vztahu k různým bezpečnostním problémům při realizacích eliptických kryptosystémů.

B. Známý problém přístupu k zabezpečeným serverům pomocí protokolu https s aplikací Internet Explorer 5 v systému Windows NT 4.0 s aktualizací SP4

Přístup k zabezpečeným serverům pomocí protokolu https (tj. bezpečný SSL protokol) může s aplikací Internet Explorer 5 nainstalovanou v systému Windows NT 4.0 s aktualizací Service Pack 4 nefungovat.

Jestliže nainstalujete systém Windows NT 4.0 a dále aktualizaci Service Pack 4 a poté aplikaci Internet Explorer 5.0, nebude pravděpodobně možné získat přístup k zabezpečeným serverům. To je způsobeno souborem s názvem schannel.dll. Česká verze aktualizace Service Pack 4 instaluje nesprávnou verzi tohoto souboru, která nepracuje správně s aplikací Internet Explorer 5. Tento problém lze vyřešit zkopírováním správné verze daného souboru do systému Windows NT.

Soubor schannel.dll je umístěn v adresáři \winnt\system32. Existuje několik způsobů řešení tohoto problému:

1) Instalace aplikace Internet Explorer 4.0 Problém lze vyřešit tak, že nejprve nainstalujete aplikaci Internet Explorer 4.0, a poté provedete aktualizaci na verzi Internet Explorer 5. Aplikace Internet Explorer 4.0 zkopíruje do systému správný soubor, a verze Internet Explorer 5 jej zachová.

2) Instalace aplikace Internet Explorer 5 do systému Windows NT s aktualizací Service Pack 3. Pokud aplikaci Internet Explorer 5 nainstalujete do systému Windows NT 4.0 s aktualizací Service Pack 3, aplikace Internet Explorer 5 do systému zkopíruje správný soubor. Jestliže později provedete aktualizaci na Service Pack 4, správný soubor bude v systému zachován.

3) Zkopírování souboru schannel.dll do adresáře \winnt\system32 Problém lze vyřešit ručním zkopírováním správné verze souboru schannel.dll do adresáře \winnt\system32. Správnou verzi daného souboru (jedná se o soubor s číslem verze rovným nebo vyšším než 1877.1) můžete získat z anglické verze aktualizace Service Pack 4 systému Windows NT 4.0 nebo z jiného PC, kde již je nainstalován správný soubor např. pomocí metody 1 nebo 2.

C. Y2Kcount.exe - Trojský kůň v počítačích

Společnost Microsoft varuje své zákazníky, že zatím neznámý pachatel zneužil její e-mailovou adresu a distribuuje elektronickou poštu s virem typu trojského koně (Y2Kcount.exe).

Ve středu 15. září byla společnost Microsoft Corporation upozorněna, že jejím zákazníkům někdo distribuuje elektronickou poštu vydávající se za časomíru poskytovanou společností Microsoft, která má odpočítávat čas, jenž zbývá do roku 2000.
Tuto elektronickou poštu neposílala společnost Microsoft a distribuovaná příloha není program pro odpočítávání času zbývajícího do roku 2000, ale vir typu trojského koně, nazvaný Y2Kcount.exe. Odesílatel pošty zneužil e-mailovou adresu společnosti Microsoft:
Support@Microsoft.com

Společnost Microsoft má pro uživatele několik užitečných informací: zásadně nedistribuuje software elektronickou poštou, updaty související s rokem 2000 lze nalézt pouze na jejích webových stránkách (http://www.microsoft.com/y2k/) nebo fyzicky na CD ROM nosiči jako je např. Microsoft Year 2000 Resource CD. Upgrady distribuuje přes Internet. Při tomto způsobu distribuce je software dostupný na webových stránkách společnosti Microsoft na adrese http://www.microsoft.com/ nebo na FTP serveru na adrese ftp://ftp.microsoft.com.

Microsoft příležitostně zasílá zákazníkům elektronickou poštu, aby je informoval o dostupnosti upgradů. V elektronické poště jsou však uvedeny pouze odkazy na místa, odkud si je možné tento software stáhnout. Tyto odkazy se vždy týkají webových stránek nebo FTP serveru, nikdy ne serverů třetích stran. K digitálnímu podpisu produktů společnosti Microsoft vždy používá autentický kód. Zákazníci tak mají jistotu, že produkty nebyly poškozeny. Pokud obdržíte e-mail, ve kterém se bude uvádět, že obsahuje software společnosti Microsoft, zásadně neotevírejte přílohu. Nejjistější věc, kterou můžete udělat, je tuto zprávu kompletně vymazat.

E-mailová zpráva, kterou v žádném případě nedistribuuje společnost
Microsoft, vypadá takto:

From: support@microsoft.com
Sender: support@microsoft.com
Subject: Microsoft Announcement
Date: Wed, 15 Sep 1999 00:49:57 +0200

Další informace (mimo tohoto oficiálního prohlášení firmy Microsoft) můžete najít na:
http://www.wired.com/news/print_version/technology/story/21823.html?wnpg=all
http://www.zdnet.com/zdnn/stories/news/0,4586,1017257,00.html

D. Matematické principy informační bezpečnosti

RNDr. Jiří Souček, DrSc., MÚ ČSAV

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

Identifikace: MAT069
Zajišťuje: MUKU
Vyučující: Jiří Souček, Tonda Beneš
Rozsah: 0/2 Z, 0/2 Z
Konání: každé úterý 17:20 seminární místnost KSI (Malá Strana)

Konkrétní témata přednášek budou vyhlašovány v průběhu semestru.

Přehled již uskutečněných přednášek:
12. 10. Ondřej Pangrác: Diferenční kryptoanalýza I. (DES 4,6 rund)
19. 10. Ondřej Pangrác: Diferenční kryptoanalýza II. (DES 16 rund)
26. 10. Ondřej Pangrác: Lineární kryptoanalýza
2. 11. Tonda Beneš : Faktorizační metody

E. Letem "šifrovým" světem

1. Sešit GCUCMP dosáhl svého rekordního nákladu 35 registrovaných e-mail odběratelů.

2. Na internetu je asi od poloviny tohoto měsíce k dispozici nově přepracovaná stránka NBÚ (Národní bezpečnostní úřad). Obsahuje přehled příslušných zákonů, vyhlášek a nařízení, strukturu úřadu, náplň práce jednotlivých odborů, kontaktní adresy, seznam akreditovaných psychologických pracovišť, akreditovaných zdravotnických pracovišť, certifikované technické prostředky apod. Celkově lze říci, že stránka obsahuje všechny základní veřejné informace o úřadu a i grafická úroveň je dobrá. Stránka obsahuje překlepy (techické, Ptaha, Csc., v anglické verzi číslování prázdných odstavců … , atd.), ale snad budou tyto chyby brzy odstraněny.
   http://www.nbu.cz/

3. Organizátoři nejvýznamnější kryptologické konference v Evropě - EUROCRYPT 2000 - oznámili konečný termín a místo konání . Konference se bude konat od 14.5 do 18.5.2000 v Bruggách v Belgii. Informace o konferenci lze najít na následující stránce :
   http://www.esat.kuleuven.ac.be/cosic/eurocrypt2000/ . Současně organizátoři upozorňují, že 3.11.1999 končí termín k odevzdání příspěvků na konferenci.

4. Ve dnech 29.9 až 1.10.1999 se konal ve Švédsku v Royal Institute of Technology (KTH, Stockholm) PKCS WORKSHOP '99. V seznamu účastníků bohužel chybí zástupci z České republiky. Jednotlivé přednášky a další dokumenty jsou k dispozici na adrese :
   http://www.rsasecurity.com/rsalabs/pkcs/

5. Tento měsíc se uskutečnila konference "International Association for Counterterrorism and Security Professionals". Na téma počítačová kriminalita zde zaznělo hodně odstrašujících případů a historek z celého světa. Pokud máte o tyto informace zájem, naleznete je na adresách :
   http://www.iacsp.com/
   http://www.wired.com/news/news/politics/story/22146.html

6. Firma AMD vyvinula novou technologii, kterou nazvala "Magic Packet", pomocí které lze po síti "vzbudit" nebo "uspat" procesor - PC nebo dokonce vypnout PC (ATX board). V této technologii se vůbec neuvažuje o zabezpečení tohoto procesu. Takže jistě již někde hackeři vyvíjí program, kterým budou moci tato PC v síti vypínat …
   http://www.amd.com/products/npd/overview/20212.html

7. 18.10.99 oficiálně odstartoval v USA- Kalifornii projekt , jenž si klade za cíl využívat pro bezpečnou komunikaci digitální podpis. Digitální podpis zde má již ze zákona stejnou váhu jako podpis "manuální". V tomto projektu se jedná především o komunikaci mezi státními orgány a občany a o zavedení celé nové oblasti elektronických služeb. Jako certifikační autorita byla vybrána známá firma Verisign Inc. Jako zajímavost uveďme, že se stát dokonce zajímá i o možnost použít digitální podpis k zabezpečení voleb přes internet. Ředitel firmy Verisign - pan Sclavos - prozradil, že firma spolupracuje na podobném projektu (využití digitálního podpisu) také v dalších státech Oregonu, New Jersey, Utahu a Washingtonu.
   http://cnn.com/TECH/computing/9910/19/california.digital.idg/index.html

8. Než začnete používat (a důvěřovat) různým "anonym serverům", přečtěte si informaci od Richarda Smithe, která je uvedena na přiložených www adresách. "Anonym servery" jsou servery poskytující službu, která umožňuje se přes ně připojit na jinou www adresu a poskytovaná služba má dále zajistit, že informace o vašem připojení (především Vaše IP adresa) se vymaskuje a na cílovém serveru nelze informace o Vás získat (dostupné mají být pouze informace o "anonymním" serveru, přes který jste se přihlásili). Jistě nejznámější (a to i mezi naší studentskou populací) je server Anonymizer , další významné servery, které poskytují tyto služby, jsou Bell Labs, Naval RL, Aixs.

   Anonymizer (http://www.anonymizer.com/)
   Bell Labs (http://www.bell-labs.com/project/lpwa)
   Naval Research Laboratory (http://www.onion-router.net)
   Aixs (http://aixs.net/aixs/)

   Pan Smith ve svém článku popisuje, jak během několika hodin se mu podařilo dokázat, že ve službách všech výše uvedených "anonym serverů" je chyba a lze na cílovém serveru Vaši IP adresu získat. Přesné detaily (použitý browser, demo programu, podmínky, popis chyb - na různých serverech jsou chyby a tedy metody získání IP různé) viz. jeho článek.
   http://www.tiac.net/users/smiths/anon/anonprob.htm
   http://www.tiac.net/users/smiths/anon/test.htm

9. Odvolací soud souhlasil s novým slyšením v Bernsteinově procesu. Ten je obviněn za to, že letos v květnu tvrdil, že šifrovací programy jsou jen algoritmy a slouží k vyjádření myšlenek matematickým vzorcem a jako takové je nemůže vláda potlačovat a regulovat.
   http://www.techserver.com/noframes/story/0,2294,500040274-500065347-500103132-0,00.html

10. A tuhle znáte …
    Víte co se stane, když v budově Microsoftu praskne žárovka a na chodbě nastane tma ? Nic, nikdo žárovku nevymění, protože Microsoft prohlásí tmu za standard.

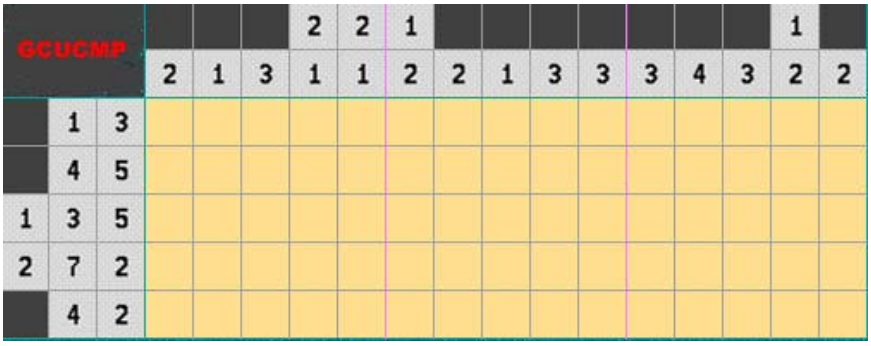
F. Trocha zábavy na závěr (malované křížovky)

Descartes Enigma je hra, v níž máte odhalit skrytý obrazec pomocí klíčů, které Vám dávají informace o jednotlivých blocích čtverečků v každém řádku a sloupci.

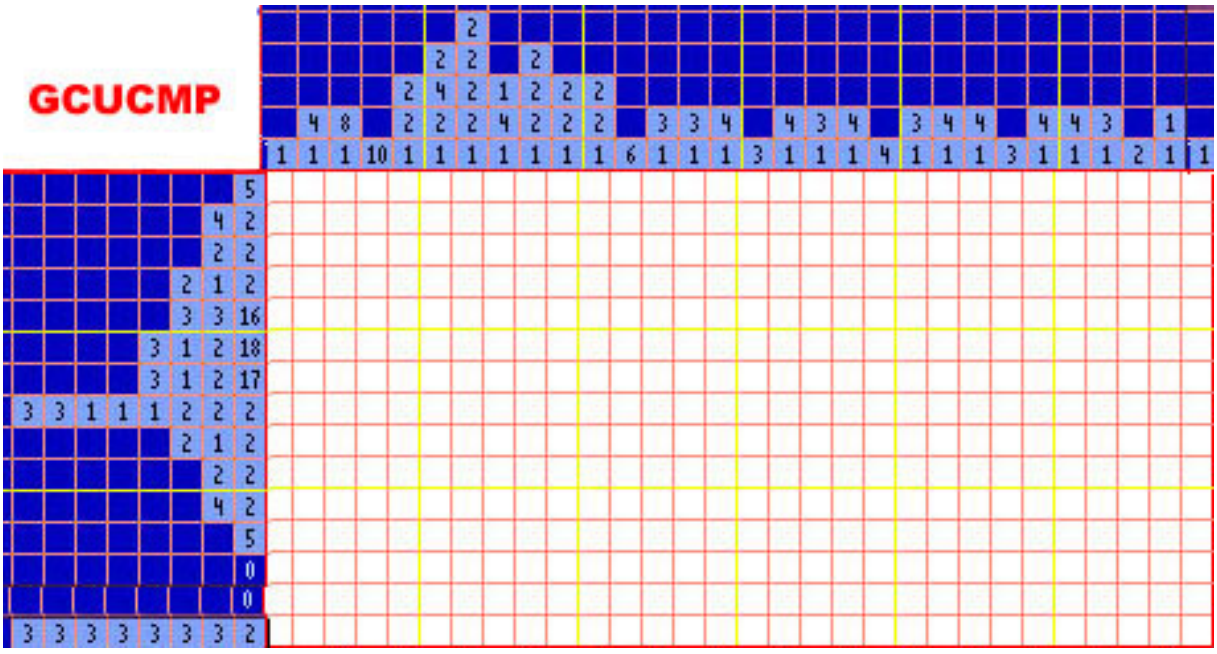
Postup:

1. Je potřeba vymalovat takový počet za sebou jdoucích políček, kolik určuje číslo zadané v řádku nebo sloupci.
2. Jestliže je v řádku nebo ve sloupci zadané více jak jedno číslo, je potřeba mezi nimi vynechat vždy nejméně jedno políčko nevyplněné (počet prázdných políček není tedy zadaný)

Tento typ hry byl ve skutečnosti vymyšlen v Japonsku panem Tetsuya Nishio a ve Spojených státech velmi zpopularizován časopisem World of Puzzles. Na Slovensku se prodávají tyto hlavolamy pod jménem malované křížovky a jsou poměrně populární.
Ve volném času si jednu lehkou vyzkoušejte :

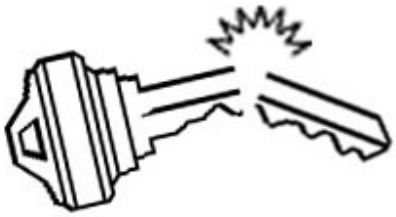


A pokud máte zájem, je zde ještě jedna (delší a těžší), výsledkem je obrazec.



Crypto-World 12/99
Informační sešit GCUCMP

Připravil : Mgr.Pavel Vondruška,
člen IACR, GCUCMP
(47 e-mail výtisků)
Uzávěrka 5.12.99



Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (internet, noviny) nebo se jedná o původní články podepsané autory. Oficiální informační sešit je primárně určený pro členy "Kryptologické sekce Jednoty matematicko-fyzikální " (GCUCMP). Pokud má někdo zájem o tyto informace, stačí se zaregistrovat e-mailem na adrese hruby@gcucmp.cz (subject : Crypto-World). Informační sešit je bezplatně rozesílán v elektronické podobě e-mailem.
Případné chyby a nepřesnosti jsou dílem P.Vondrušky a GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

OBSAH : **Str.**

A. Microsoft nás zbavil další iluze !

Mgr. Pavel Vondruška, NBÚ ČR

Také svým zákazníkům, kolegům a vůbec svému okolí pracně vysvětlujete, že virus se dá chytit jen tak a tak a např. že pouhým přečtením e-mailu jej nemohou získat ? Virus se přece šíří pouze v příloze a my jej sami aktivujeme tím, že přílohu spustíme. Takže se nebojte, pouhým čtením e-mailu se virus šířit nemůže … Jenže ono to už neplatí !!!
Kdosi (zpravidla se říká, že student, nějaký recesista nebo majitel antivirové firmy) napsal nový "chytrý" virus (spíše červa), který využívá skripty vložené do HTML kódu. Účinky a možnosti těchto skriptů jsou velice omezeny, přesto se podařilo najít bezpečnostní trhlinku a na jejím základě virus napsat. Virus byl napsán pro VB Script (ne pro JavaScript nebo Jscript). Ohroženi jsou tedy potenciálně pouze ti, kteří nějaký mailer interpretující HTML a podporující VB Scripty využívá. VB Script je podporován pouze v produktech Microsoftu. Speciálně jsou tedy ohroženi uživatelé rozšířených mailerů Outlook a Outlook Express. Virus se šíří e-mailem s nadpisem "BubbleBoy is back!" Ten si po odklepnutí zapíše svůj kód na disk (to skripty v zásadě dělat nemají), kód je pak automaticky inicializován při restartu počítače. Červ se dále automaticky rozešle na všechny adresy, které najde v uživatelově adresáři (proto červ), smaže existující e-maily (proto virus). Jeho název je zvolen podle subjectu, který používá, tedy BubbleBoy. Microsoft tentokráte reagoval na bezpečnostní chybu rychle a na svém webu umístil bezpečnostní patch (záplatu). Tento patch lze stáhnout z adresy http://www.microsoft.com/security/Bulletins/ms99-032.asp .
Samotný viruso-červ není ani tak nebezpečný, je lehce odhalitelný, jeho význam je především v tom, že pomohl odhalit bezpečnostní nedostatek v produktech Microsoftu a hlavně v tom, že padl další mýtus a to, že "přečtením e-mailu nelze získat virus".

Další doplňující informace lze zjistit na :
http://www.wired.com/news/story/0,1240,32434,00.html
http://www.wired.com/news/technology/0,1282,32529,00.html
http://www.europe.datafellows.com/v-descs/bubb-boy.htm

Mimochodem, když už jsme u těch záplat - patchů - stáhli jste si již záplatu pro problém Y2K (přechod na rok 2000) ve Windows? Na serveru http://www.microsoft.com/year2000 jsou k dispozici všechny patche pro jednotlivé verze Windows.

A ještě jedna poznámka, zajímali jste se již někdy, kolik těch záplat v produktech Microsoftu už asi je ? Bruce Schneier odhadl, že jen bezpečnostních záplat a dodatečných nastavení je pro Windows NT asi 300 … V polemice, kterou tento jeho odhad vyvolal, pak odborníci vyslovili různé odhady a to od padesáti do tří tisíc … (viz Crypto-World 10/99).

B. Matematické principy informační bezpečnosti

RNDr. Jiří Souček, DrSc., MÚ ČSAV

Identifikace: MAT069
Konání: každé úterý 17:20 seminární místnost KSI (Malá Strana)

Každé úterý se koná dvouhodinová přednáška (seminář) v seminární místnosti KSI MFF UK na Malé straně (druhé poschodí, katedra systémového inženýrství). Seminář vychází z praktických úloh, na semináři přednáší přední odborníci v dané oblasti. Seminář je vhodný pro studenty a bude probírána daná problematika od počátku. Na seminář je volný přístup pro členy GCUCMP a další zájemce o konkrétní témata.

Přehled již uskutečněných přednášek:

12.10. Ondřej Pangrác:	Diferenční kryptoanalýza I. (DES 4,6 rund)
19.10. Ondřej Pangrác:	Diferenční kryptoanalýza II. (DES 16 rund)
26.10. Ondřej Pangrác:	Lineární kryptoanalýza
2.11. Tonda Beneš :	Faktorizační metody I.
9.11. Tonda Beneš :	Faktorizační metody II.*
16.11. Jaroslav Hrubý:	Kvanová kryptolgie
23.11. Pavel Vondruška:	TWINKLE**
30.11. Pavel Kaňkovský:	Informační toky

Zbývající přednášky:

7.12. Jaroslav Pinkava:	Softwarové pseudogenerátory
14.12. Jaroslav Hrubý:	Kvantové počítání
21.12. Jiří Souček:	Závěrečný seminář

(Případné změny v přednáškách budou domluveny na semináři 7.12.99)

* Na vyžádání lze zaslat elektronickou verzi přílohy k semináři (Faktorizace)
** Na vyžádání lze zaslat elektronickou verzi přednášky (TWINKLE)

C. Pod stromeček nové síťové karty

Mgr. Pavel Vondruška, NBÚ ČR

Pokud Vaše společnost plánuje "přezbrojení" na nový operační systém Windows 2000, musíte do finanční kalkulace rovnou zahrnout i nákup nových síťových karet od firmy 3Com. Firma 3Com totiž uzavřela s firmou Microsoft strategickou dohodu na vývoj rozhraní umožňující hardwarové zrychlení klíčových operací mezi síťovou kartou a jádrem Windows 2000 týkajících se TCP/IP protokolu a síťové bezpečnosti. Toto rozhraní významně odlehčí zatížení CPU na hostitelském počítači, čímž se zvýší propustnost sítě a rychlost vlastního PC.

Nová rodina karet 3COM-3XP je osazena speciálním čipovým obvodem (ASIC), který obsahuje integrovaný procesor 3XP. Právě tento procesor umožňuje vylepšený výkon a snižuje zatížení při využití klíčových síťových úkolů pod Windows 2000. Karta se bude vyrábět ve verzi 10/100 PCI.
http://www.3com.com

D. Konec filatelie

Ing. Jiří Němejc CSc., GESTO Communications

Od července 1999 je možné frankovat zásilky americké pošty USPS (US Postal Service) elektronicky. Známky se tisknou jako 2-dimensionální čárový kód, který obsahuje údaje potřebné pro účtování a sledování procesu doručení, přičemž tato data jsou digitálně podepsána. Aplikace IBIP (Information Based Indicia Program) je založena na využití certifikátů a digitálního podpisu. Celou rozsáhlou bezpečnostní infrastrukturu pro USPS vybudovala a komponenty pro ni dodala americká firma Cylink. PKI je implementována na systému clusterů serverů Sun Enterprise a produktu CryptoServer. Architektura je distribuovaná se zajištěným zálohováním, transakčním zpracováním, vysokou dostupností a výkonem. Obsahuje certifikační autority, registrační servery a je dimenzována pro řádově stovky milionů certifikátů (aby byla dostupná všem uživatelům USPS nejen v USA). Infrastruktura je určena i pro další aplikace.

Druhým společným projektem Cylink a USPS ve spolupráci s IPC (International Postal Corporation) je "PostECS" (Electronic Courier Service). Jde o elektronickou obdobu kurýrní pošty, která je však digitálně podepsaná a šifrovaná (event. s dalšími přidanými službami). Privátní klíče jsou zpracovávány v kryptografických smart kartách (PrivateCard). Garantem z hlediska certifikátu a údajů o odeslání je opět příslušná pošta. Pilotní projekt probíhá s účastí tří pošt: USPS, Canada Post Corporation, La Post (Francie).

http://56.0.78.92/html/ibimain.html
http://www.usps.gov/news/press/99/99066new.htm
http://www.cylink.com/news/press/pressrels/80999.htm
http://www.usps.gov/dtf/1dtfelectronic.html
http://www.usps.gov/dtf/28short11.htm
http://www.usps.gov/postecs/
http://www.postescanada.ca/CPC2/eps/postecs/eleccour.html
http://pcworld.com/pcwtoday/article/0%2C1510%2C7655%2C00.html

E. Y2K (Problém roku 2000)

Mgr. Pavel Vondruška, NBÚ ČR

O tomto problému již bylo napsáno tolik, že napsat něco nového a chytrého teď , necelý měsíc před prověrkou, zda jsme my a naše okolí připraveni, snad ani nejde. Přesto v tomto čísle o tomto problému něco musí být napsáno (jak by náš sešit vypadal …), a tak snad jen pár historicko-právních poznámek..

Na úrovni státních orgánů se tímto problémem v USA začali oficiálně zabývat již v roce 1995. Následovala Velká Británie (1996) a potom v rychlém sledu další státy např. 1997 Mexiko, Tunis atd. Rok 1998 byl ve vývoji zlomový. V tomto roce se problémem již zabývala většina států celého světa a vznikala první koordinační a krizová centra. V USA byl přijat 14.6.1998 zákon o "Y2K", který platí po dobu 3 let. Zajímavý aspekt je doktrína, která říká, že soukromé podniky musí v této oblasti bezpodmínečně poslouchat stát, a dále doktrína, která říká, že žádný subjekt se nesmí spoléhat na jiný subjekt a musí se postarat sám o sebe . Smysl druhé doktríny je v zabránění možných dlouhodobých následných právních sporů o náhradách škody. Koncem roku - 11.12.1998 na půdě OSN zaznělo, že státy sdružené v OSN musí ve své legislativě zakotvit nebo alespoň deklarovat, že se nezbavují odpovědnosti za možné dopady na obyvatelstvo (především za energetiku, dodávky vody, tepla apod.) a to i v oblastech, které nejsou ve vlastnictví státu, ale v soukromých rukou. Současně byl náš stát koncem roku 1998 ambasádou USA požádán, aby celý problém začal urychleně na úrovni státu také řešit.

Dne 1.2.1999 bylo konečně zřízeno Národní koordinační centrum i v České republice. Pro dotazy občanů a firem byla zřízena zelená linka 0800 11 2000 , kde je možné zdarma získat všechny základní informace. Stát se zavázal koncem roku vystupňovat mediální kampaň, která informuje občany o možných dopadech problému Y2K na domácnosti. Do 15.12.99 bychom pak měli všichni najít ve svých schránkách letáček s informacemi, jak se máme připravit na překonání možných problémů.

31.12.1999 ve 23.59 pohlaďme své počítače, mikrovlnky, automatické pračky a popřejme jim do nového roku vše nejlepší. Ty chytřejší se nám za to určitě v roce 2000 odvděčí.

F. PATÁLIE SE SYSTÉMEM MICKEYSOFT FRITÉZA

CyberSpace.cz - the future of M.A.T.R.I.X)
(Silvestrovské čtení)

Píše se rok 2000, rok vítězného tažení operačního systému Mickeysoft Windows CE do našich obýváků, kuchyní i ložnic a už i my máme doma několik zařízení nové generace. Po cestě z práce domů jsem dostal chuť na hranolky a koupil si jich pytlík, těšíc se na dobrou večeři. Příprava měla být snadná a jednoduchá - naše fritéza je vybavená poslední verzí operačního systému, pochopitelně včetně pěti nejdůležitějších softwarových záplat. Osud tomu však chtěl jinak.

Položil jsem pytlík s hranolkami na linku, zapnul přístroj pomocí tlačítka "Zažehnout" a už po necelých třech minutách (můj osobní rekord, měl jsem skutečně hlad) a dvou resetech (znáte to, klasický trojhmat Ctrl+Alt+Hranolek) jsem z menu vydoloval program fritování. A kruciš, v tom spěchu jsem zapomněl odpojit friťák z lokálního Mickeysoft Kitchenetu. Ta mrcha to stihla, spojila se s ledničkou a zahlásila: "Jste si jist, že chcete fritovat hranolky, když v lednici žádné nemáte?" a nabídla mi tlačítka "Ne" a "Storno". S odevzdaných povzdechem vkládám hranolky do ledničky, zavírám dveře, čekám pět vteřin až blikne zelená kontrolka, signalizující aktualizaci databáze potravin v Kitchenetu a vytahuji pochoutku zpět.

Po dalším startu už fritéza neprotestovala a na jejím displeji konečně naskočil známý "Průvodce fritováním". Pravda, těsně po záruce přestala fungovat vestavěná váha a hned po ní se odebral do věčných lovišť i scanner, takže mne navíc čekaly kroky "Nakreslete typický tvar hranolku", "Zadejte počet hranolků" či "Určete délku nejdelšího a nejkratšího hranolku", ale na to už jsem byl připravený - odhad mám skvělý a navíc jako jediný z rodiny celkem obstojně kreslím, takže napůl syrové a napůl spálené hranolky jsme měli zatím pouze dvakrát.

Mnohem větší obavy jsem měl z neblaze proslulé databáze olejů. Svoji drahou ženu jsem už sice naučil kupovat na její vkus poněkud předražené flašky s logem "Mickeysoft Kitchen 2000 compatible", ale jeden nikdy neví, zrovna včera jsem ve špajzu zahlédl novou láhev Lukany a nebyl jem si jist, zda se nejednalo o nějakou levnější noname verzi… Bohužel mé tušení bylo správné a na displeji se proto vynořila obávaná hláška "Neočekávaná chyba při detekci oleje, aktualizujte prosím seznam ovladačů a spusťte průvodce fritováním znovu."

Ještě že olej byl v novém balení, které mívá ve špuntu mikročip s ovladačem. Špunt, proboha kde je ten špunt ?! Určitě bude v šuplíku. V šuplíku bylo mnoho špuntů, máme moderní domácnost… Po deseti minutách, kdy jsem na snímač fritézy přiložil dva tucty mikročipů ve vršcích ze sirupů, moštů, piv a minerálek jsem propadl totální beznaději. Pravda, jeden z moštů označil Mickeysoft Fritéza CE za kompatibilní s obecným rostlinným olejem, ale po loňské zkušenosti s kuřecími prsíčky na octu už má důvěra v odhady fritézy značně poklesla.

Vypnul jsem proto strojek jak jinak než pomocí tlačítka "Zažehnout" a hladově si namazal osvědčený chleba se sádlem. Domácí sádlo bez identifikačního čipu máme od rodičů a starý nemoderní nůž jsme naštěstí ještě nevyhodili. I když, při vytahování sklenice se sádlem z ledničky se mi na její dvířka promítla za zvuků rolniček reklama na nový kráječ na chleba kompatibilní se sadou Mickeysoft Kitchen 2000. Prý mimo krájení umí navíc vyřezávat betlémy z překližky…

(převzato ze serveru www.tombo.cz bez redakční úpravy)

G. **Letem "šifrovým světem"**

1. Zákon o elektronickém podpisu, jehož znění inicioval SPIS (Sdružení pro informační společnost) inicioval a jehož autory jsou doc. Smejkal a doc. Mates , je vystaven na internetových adresách, mj.
   http://www.spis.cz/ , http://www.apek.cz/digitpodpis.html
   Na adrese "spisu" je dále k dispozici rozsáhlá a velice zajímavá diskuse k předloze tohoto zákona. Diskuse byla uzavřena 15.10.99 v 16.30 hod. Reakce na podněty a připomínky měly být vyvěšeny během 44 týdne , dnes (49 týden) ještě stále nejsou k dispozici.

2. Při spolupráci Windows NT se zařízeními řízenými pomocí Windows CE (viz bod F "silvestrovské čtení") Microsoft zašifrová vaše heslo. To je jistě chvályhodné, ale je zarážející, že k tomu zvolil následující algoritmus (toto již není silvestrovské čtení!) :
   XOR vašeho hesla s "susageP" . Tedy se slovem Pegasus napsaným obráceně (Pegasus je pracovní název Windows CE ….).
   http://www.cegadgets.com/artsusageP.htm

3. Na internetu se objevil nový elektronický časopis "Skytale". Časopis se zabývá obecně informační bezpečností. Právě vyšlo prvé číslo. Texty je možné stáhnout z webu nebo si je nechat elektronicky zasílat na uvedenou e-mail adresu. Texty jsou uvedeny ve formátu TXT, HTML nebo PDF.
   Více informací, prvé číslo časopisu, registraci apod. lze najít na adrese :
   http://www.isrc.qut.edu.au/skytale

4. (Jaroslav Pinkava) Čerstvé informace k chystaným úpravám v americkém zákonodárství
   -nedochází k plnému uvolnění amerického vývozu
   -neomezeně lze vyvážet produkty obsahující symetrické šifry s maximální délkou klíče 64 bitů a asymetrické šifry s maximální délkou klíče 1024 bitů
   -dochází k určité liberalizaci formulace komu lze dovážet produkty s neomezenou délkou klíče (dříve to např. v České republice byly pouze finanční a příbuzné instituce).
   http://cryptome.org/ear-crypto.htm
   http://www.usatoday.com
   http://www.cdt.org/crypto/regs112399.shtml

5. (Jiří Němejc) Daňové přiznání v elektronické formě, kryptograficky zabezpečené lze podat v Brazílii a Izraeli přes Internet. Aplikace byla vytvořena pro brazilskou vládu firmou Cylink (Algorithmic Research). Základní bezpečnostní komponentou je standardní produkt "Private Wire". Daňové přiznání podalo elektronicky v roce 1997 (pilot) 500 000 brazilských poplatníků, v roce 1998 2,5 milionu a letos se očekává 7,5 milionu on-line podaných přiznání. (A jako minulý rok bude zřejmě jejich většina podána v průběhu posledních 2 dnů lhůty).
   http://www.cylink.com/news/press/pressrels/81899.htm

6. (METRO 29.11.1999) - "Prvá vlašťovka" problému Y2K přiletěla do americké Filadelfie, kde 500 občanů dostalo 26.11.99 upozornění, že budou povoláni jako členové soudních porot v příštím roce - 1900. Městský komisař pro soudní poroty M. McAllister oznámil, že byla provedena příslušná opatření, aby se již tento problém nevyskytl.

7. (DSM 5/99) Společnost SGI oznámila instalaci prvního 128 procesorového serveru pracujícího pod operačním systémem Linux. Předinstalovaným softwarem je SGI Linux Enviroment s Red Hat Linux 6.0. Počítač je umístěn v Ohio Supercomputer Centru ve městě Columbus.

8. Jste připraveni i na 29.2.2000 ? A bude vůbec tento den v příštím kalendářním roce ? Odpovězte tedy rychle na otázku : "Je rok 2000 přestupný nebo ne ? " .
   Řešení : Platí pravidlo, že rok je přestupný tehdy, je-li dělitelný 4. Výjimkou jsou roky dělitelné 100, pokud nejsou dělitelné 400. Rok 2000 je tedy výjimkou z výjimky (rok 1900 přestupný nebyl, rok 2000 tedy je přestupný).

9. Na závěr jedna zajímavost: víte o tom, že 21. století nezačíná rokem 2000, ale až rokem 2001?

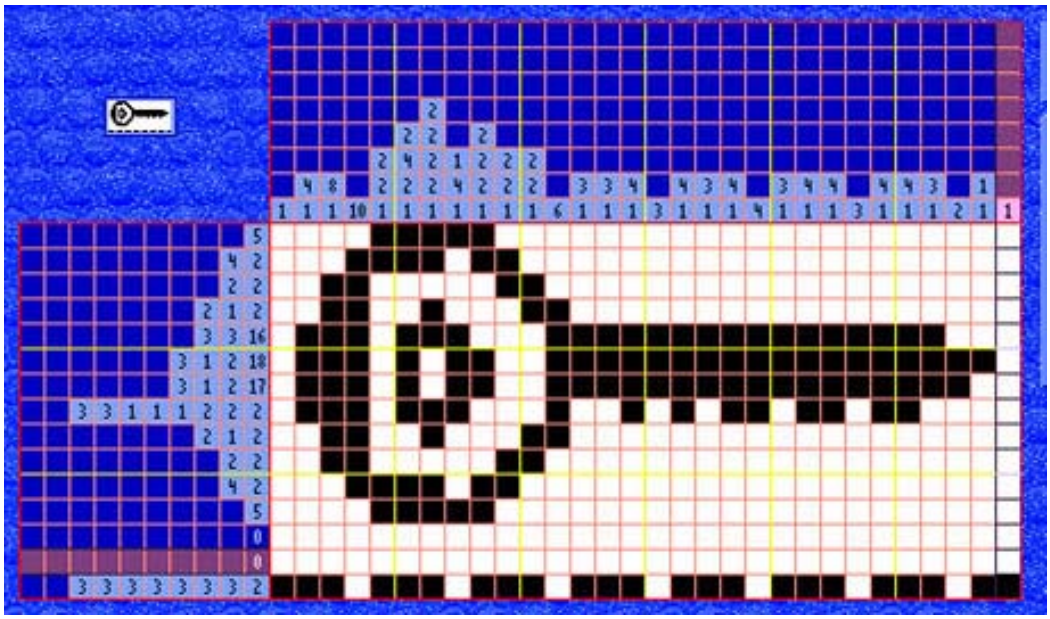
10. A úplně na samý závěr malá statistika vztahující se k našemu sešitu:

Sešit	**výtisků***	**autoři**	**velikost**	**Počet stran**
9/99	25	Vondruška	84992	7
10/99	31	Vondruška,Pinkava	130048	10
11/99	36	Vondruška,Souček,Pinkava	205312	9
12/99	47	Vondruška,Souček,Pinkava,Němejc	337920	9

* počet "výtisků" v době oficiálního rozeslání sešitu

H. **Řešení malované křížovky z minulého čísla**

Descartes Enigma (malovaná křížovka) je hra, v níž máte odhalit skrytý obrazec pomocí klíčů, které Vám dávají informace o jednotlivých blocích čtverečků v každém řádku a sloupci. Tuto velice zajímavou hru jsme Vám představili v minulém čísle 11/99. Zde uvádíme řešení malované křížovky z minulého čísla :



S přáním všeho nejlepšího v celém příštím roce ~~**1900**~~ **2000** se s Vámi loučí autoři tohoto sešitu.
(Pokud vše dobře dopadne, tak se těšíme na shledání v příštím miléniu).