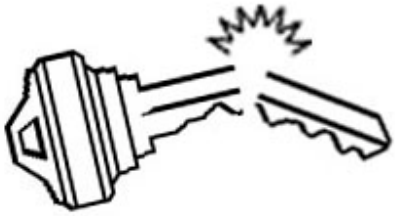
Informační sešit GCUCMP
Crypto-World 4/2000

Připravil : Mgr.Pavel Vondruška,
člen GCUCMP, IACR, ISACA.
Sešit rozesílán registrovaným čtenářům,
registrace na adrese pavel.vondruska@post.cz , subject : Crypto-World
sešity najdete také na adrese www.mujweb.cz/veda/gcucmp
(102 e-mail výtisků)
Uzávěrka 7.4.2000



POČET REGISTROVANÝCH ODBĚRATELŮ PŘESÁHL 100 !

Děkujeme !

OBSAH : **Str.**

A. Prohlášení odborné skupiny pro zpracování pozměňovacích návrhů k předloze zákona o elektronickém podpisu

Prostřednictvím médií se patrně již mnozí setkali s informacemi o přípravě zákona o elektronickém podpisu. **Cílem tohoto prohlášení je doplnit již zveřejněné informace a poukázat na závažné problémy, které se při přípravě zákona vyskytly a které měly bohužel negativní dopad na jeho současné znění.** Po určitou dobu vznikaly dokonce návrhy dva, jeden v Úřadu pro státní informační systém (ÚSIS), druhý jako poslanecká iniciativa. Oba návrhy byly odborné veřejnosti známy, oba byly odborníky připomínkovány. Tyto připomínky a porovnání obou návrhů byly publikovány v odborném tisku. Vzhledem k tomu, že dokončení vládního návrhu, byť podle názoru některých expertů v určitých aspektech kvalitnějšího, bylo stále v nedohlednu, odborná veřejnost přivítala poslaneckou iniciativu, která dávala možnost přijetí zákona v rozumném časovém horizontu.

Zde je nutné vysoce ocenit zásadní roli Sdružení pro informační společnost (SPIS), které iniciovalo vznik poslaneckého návrhu, a pro poslance-předkladatele zajistilo zpracování textu návrhu zákona. Za tuto aktivitu patří SPIS velký dík. Bohužel SPIS neměl příliš šťastnou ruku při výběru osoby, která návrh zpracovala. Docent Smejkal je jistě známým mediálním propagátorem myšlenky zákona o elektronickém podpisu, ovšem, jak se ukázalo v průběhu zpracování návrhu zákona, zároveň člověkem, který není schopen komunikace s odbornou veřejností. Již od září loňského roku řada odborníků upozorňovala SPIS **i docenta Smejkala** na zásadní nedostatky předlohy (například prostřednictvím diskusního fóra na webových stránkách SPIS), neakceptování reálného stavu a možností současných technologií, postupů při aplikaci elektronického podpisu, nesoulad s tehdy ještě připravovanou směrnicí EU o elektronických podpisech atd. Bohužel ve valné většině bezúspěšně.

Jako poslední možnost kvalitativní změny byl chápán projev poslance Mlynáře při prvním čtení v PSP, ve kterém avizoval vznik odborné skupiny a dopracování zákona do žádoucí podoby (připomeňme, že vláda vyslovila nesouhlas s původní předlohou). V té době prezentovali zájem na vzniku a činnosti odborné skupiny jak předkladatelé, tak SPIS a ÚSIS. Skupina nevznikla jmenováním členů, nereprezentuje žádný existující subjekt, či zájmovou skupinu. Jedná se o odborníky, kteří se dané problematice systematicky věnují a které buď oslovil ÚSIS, nebo kteří se ke spolupráci sami přihlásili. V průběhu třech týdnů, které měla skupina k dispozici, byl návrh zásadně přepracován a bylo dosaženo všeobecného konsensu ohledně jeho znění. S původním textem měl nově zpracovaný návrh velmi málo společného. Výsledek činnosti skupiny, tj. nový text návrhu zákona, na jehož základě měly být zpracovány pozměňovací návrhy pro projednávání v hospodářském výboru a následně ve 2. čtení v PSP, byl 7. března prostřednictvím SPIS předán předkladatelům. Tímto okamžikem přestala mít skupina na další osud návrhu jakýkoliv přímý vliv.

Za této situace se stalo něco naprosto nepochopitelného. Návrh připravený odbornou skupinou začal ve spolupráci s předkladateli „upravovat“ , a to i po stránce ryze odborné, opět docent Smejkal! Výsledkem jsou nejen právnické, ale také odborné úpravy, které žádným způsobem nerespektují dosažený konsensus odborné skupiny, v mnoha případech spíše připomínají snahu zasáhnout do znění návrhu za každou cenu tak, aby se co nejvíce podobal původní předloze. Tyto změny bohužel nereflektují možnosti současných technologií a jejich hlavním rysem je na jedné straně zesílení pravomocí centrálního úřadu a na druhé straně zeslabení jeho povinností. Snaha o centralizaci ovšem není podložena reálnými možnostmi aplikace v současných technologických podmínkách. Bohužel je nezbytné konstatovat, že tento postup při „dopracování“ návrhu měl plnou podporu jednoho z předkladatelů, poslance Mlynáře.

Došlo tak k opětovnému zanesení chyb, které byly návrhu vytýkány po celou dobu jeho zpracovávání. Stalo se tak opět bez odborné diskuse, podle pouhého uvážení autora původního návrhu. Tento postup považuje odborná skupina za nekorektní. Návrh zákona se opětovně dostal do podoby, ve které jej nelze doporučit k přijetí parlamentem.

Záměrem členů skupiny není vzbudit dojem, že jimi navržené znění návrhu je bezchybné **a jediné možné.** Důrazně však protestují proti způsobu, kdy jim nebyl dán žádný prostor pro obhajobu vlastní práce a následné změny byly učiněny bez jakéhokoliv dialogu s nimi a značně neodborným způsobem.

Odborná skupina si uvědomuje, že toto prohlášení přichází do jisté míry pozdě. Důvodem byla ovšem dobrá vůle jejích členů nevytahovat na povrch odborné problémy, vůle, která byla podporována sliby SPIS o možnostech změny způsobu práce při přípravě návrhu zákona. Opakované nenaplnění těchto slibů, ať již v důsledku přecenění vlastních možností, či z jiných důvodů, skupinu vede k vydání tohoto prohlášení. Motivem jejího dosavadního mlčení o uvedených problémech byla i snaha nezpochybnit nutnost přijetí zákona o elektronickém podpisu a nevyvolat nedůvěru k používání elektronického podpisu.

Členové skupiny jsou otevřeni diskusi s těmi, kdo zastávají v této oblasti odlišné názory. Diskutovat však není s kým. Připustíme-li, že zde existují dvě strany s rozdílným pohledem na to, jak by měl zákon o elektronickém podpisu vypadat, pak jednu z těchto dvou stran představuje pouze jediná osoba, a to osoba nekomunikující.

Za této situace je odborná skupina nucena veřejně prohlásit, že se současným zněním návrhu zákona o elektronickém podpisu nesouhlasí, a to pro jeho závažné nedostatky. Rovněž se ohrazuje proti způsobu, jakým bylo naloženo s výsledky její práce.

Návrh zákona bude PSP projednávat ve druhém čtení v polovině května. Je tedy stále otevřena možnost text dopracovat do přijatelné podoby. Najde-li skupina v PSP partnera, který bude ochoten s ní v této věci komunikovat, je k takové spolupráci připravena. Cíl je jediný – kvalitní a použitelný zákon o elektronickém podpisu.

Toto prohlášení nevyjadřuje pouze názor členů odborné skupiny, ale i názor jiných uznávaných odborníků v oblasti elektronického podpisu, jejichž jména jsou připojena.

Mgr. Pavel Vondruška, Ing. Dr. Petr Hanáček, Ing. Jiří Mrnuštík, Ing. Daniel Cvrček, Ing.Jaroslav Pinkava,CSc., Mgr. Antonín Beneš, RNDr. Petr Tesař, Doc. Ing. Jan Staudek, CSc., Jiří Peterka nezávislý konzultant publicista, odborný pracovník MFF UK Praha.

Všichni, kteří mají zájem studovat problematiku zákona o elektronickém podpisu a kterým jeho stav není lhostejný, se mohou zúčastnit diskuse o tomto zákonu a problematice s ním svázané na těchto stránkách. Vítáme hlasy všech, kteří souhlasí s prohlášením odborné skupiny. Svůj souhlas a tím i připojení Vašeho podpisu zašlete na adresu mailto:jiri.mrnustik@aec.cz . Podpisy dalších osob budou postupně přidávány do tohoto dokumentu.

Další informace je možno získat na adrese http://www.e-commerce.cz/akce/zep/ nebo na adrese http://www.trustcert.cz/

****

Za Vaši podporu a zaslaný souhlas na výše uvedenou adresu předem děkujeme!

Mgr. Pavel Vondruška

B. Fermatova čísla

Mgr. Pavel Vondruška, NBÚ

Doplnění a upřesnění dat k přednášce :
Netradiční pohled na bezpečnost RSA (Rozvoj teorie prvočísel, otevřené problémy a vztah k bezpečnosti RSA a faktorizaci), Pavel Vondruška, MFF UK 28.3.2000, celá přednáška bude dostupná od 20.4.2000 na http://www.mujweb.cz/veda/gcucmp/mff/prvocisla.htm

Pierre de Fermat (1601-1665)

Definice :

$$F_m = 2^{2^m} + 1$$

Tabulka prvních Fermatových čísel

m	Známý rozklad F_m
0	3
1	5
2	7
3	257
4	65537
5	641*6700417
6	274177* 67280421310721
7	59649589127497217* 5704689200685129054721
8	1238926361552897* P_{62}
9	2424833*7455602825647884208337395736200454918783366345657* P_{99}
10	45592577*6487031809*4659775785220018543264560743076778192897* P_{252}
11	319489*974849*167988556341760475137*3560841906445833920513* P_{564}
12	114689*26017793*63766529*190274191361*1256132134125569* C_{1187}
13	2710954639361*2663848877152141313*3603109844542291969*319546020820551643220672513* C_{2391}
14	Složené C_{4933}
15	1214251009*2327042503868417* C_{9840}
16	825753601* C_{19720}
17	31065037602817* C_{39444}
18	13631489* C_{78906}
19	70525124609*646730219521* C_{157804}
20	Složené C_{315653}
21	4485296422913*C
22	Složené $C_{1262612}$

Symbol P_k v tabulce označuje prvočíslo o k dekadických cifrách, zatímco C_k označuje složené číslo o k dekadických cifrách, pro něž neznáme žádný netriviální rozklad.

Při studiu dokonalých čísel, která souvisí s Mersennovými prvočísly si Fermat položil otázku, zda čísla tvaru 2^n+1 jsou prvočísla . Vyslovil chybnou hypotézu, že čísla tvaru F_m = (2 na 2^m) + 1 jsou všechna prvočísla.

Jak píše C.Pomerance ve svém vynikajícím článku, jsou dějiny rozkladu Fermatových čísel jakýmsi mikrokosem historie faktorizace.
Fermat věděl, že **F_0 až F_4** jsou prvočísla, a domníval se, že i všechna ostatní čísla v posloupnosti F_m jsou prvočíselná.

$\mathbf{F_5}$ však rozložil Euler pomocí zesíleného Fermatova tvrzení, které dokázal v roce 1878 E.A.Lucas a podle něhož každý prvočinitel p čísla F_p je tvaru $p=1 \bmod 2^{2m+1}$, kde m je alespoň 2.

Tato myšlenka byla použita i k rozkladu čísla $\mathbf{F_6}$ v roce 1880 (Landry) a k získání dalších malých prvočinitelů více jak 80 Fermatových čísel, která již nejsou uvedena v tabulce.
Fermatovo číslo $\mathbf{F_7}$ bylo rozloženo pomocí Brillhartovy-Morrisonovy faktorizační metody řetězových zlomků.

Brent a Pollard přizpůsobili Pollardovu metodu k rozkladu $\mathbf{F_8}$.

$\mathbf{F_9}$ - dle Pomerance je tento rozklad nad síly kvadratického síta , metoda eliptických křivek nebyla vhodná, je určena pro malý prvočinitel cca do 30-ti cifer).Rozklad se podařil na jaře roku 1990 bratrům Lenstrům a M.Manassovi (přesněji již v době rozkladu se vědělo, že se jedná o číslo složené, znal se jeho sedmiciferný prvočinitel, ale předmětem rozkladu byl zbývající činitel o 148 cifrách, jehož rozklad nebyl znám). K rozkladu byla použita Pollardova metoda.

$\mathbf{F_{10}}$ a $\mathbf{F_{11}}$ rozložil Brent pomocí Lenstrovy metody eliptických křivek.

$\mathbf{F_{14}}$, $\mathbf{F_{20}}$ a $\mathbf{F_{22}}$ jsou čísla složená, ale zatím neznáme žádné prvočinitele těchto čísel. To, že jsou složená, plyne z tzv. Pepinova kritéria :

$\mathbf{F_m}$ je prvočíslo právě tehdy, když $3^{(F_m-1)/2} \equiv -1 \bmod F_m$

Otevřený problém:
$\mathbf{F_{31}}$ je nejmenší Fermatovo číslo, o němž nevíme , zda je prvočíslo nebo složené číslo. V současné době se mnoho teoretických matematiků domnívá, že každé Fermatovo číslo po $\mathbf{F_4}$ je složené.

Největší Fermatova čísla, která se podařilo rozložit
$\mathbf{F_{303088}}$ - 1998 - Young , dělitel $3*2^{303093}+1$
$\mathbf{F_{382447}}$ - 1999 - Cosgrave , Gallot, dělitel $3*2^{382449}+1$

Celkový přehled (stav k 13.2.2000):

Číslo	$\mathbf{F_m}$
Prvočíslo	m= 0, 1, 2, 3, 4
Kompletně rozložené čísla	m= 5, 6, 7, 8 (mají 2 dělitele), 9 (3 dělitele), 10 (4), 11 (5)
Částečně rozložené , známe 5 dělitelů	m=12
Částečně rozložené , známe 4 dělitele	m=13
Částečně rozložené , známe 3 dělitele	m=15,25
Částečně rozložené , známe 2 dělitele	m=16,18,19,27,30,36,38,52,77,147,150,416
Částečně rozložené , známe 1dělitele	m=17,21,23,26,28,29,32,37,39,42,55,58 a dále 129 hodnot z intervalu (58, 382447>
Složené, ale nepodařilo se rozložit	m=14,20,22,24
Neznámý charakter	m=31,33,34,35,40,41,43,44,45,46,47,48,…

Poslední dosažený výsledek :
11.2.2000 - Rachel Lewis nalezl dělitele $57*2^{146223}+1$ Fermatova čísla $\mathbf{F_{146221}}$.
K získání dělitele použil program Proth.exe od Yvese Gallota. Celkem je to již osmý dělitel některého z Fermatových čísel nalezený tímto programem.

Literatura :

[1] A tale of two sieves. Notices Amer. Math. Soc. 43 (1996), 1473-1485 (originál článku je přístupný na adrese http://www.ams.org/publications/notices/199612/pomerance.html, český překlad viz. PMFA, ročník 43 (1998), č.1)

[2] M. A. Morrison and J. Brillhart, A method of factorization and the factorization of F_7, Math. Comp. 29 (1975), 183-205.

[3] R.P.Brent, J.M.Pollard: Factorization of the eight Fermat number. Math. Comp. 36 (1981), 627-630.

[4] Wilfrid Keller, Prime factors k. 2^m+1 of Fermat numbers F_m and complete factoring status http://vamri.xray.ufl.edu/proths/fermat.html

C. Lekce pro tajné agenty - č.1 : "Neztrácejte své laptopy "

Během března se podařilo ztratit britským agentům hned dva laptopy, které obsahovaly tajné informace. Prvý případ se stal v noci ze 3.3 na 4.3, kdy důstojník MI5 holdoval alkoholu v Rebato's tapas baru, který se nachází blízko hlavní budovy MI6. V počítači měl uloženy dokumenty, které souvisely s choulostivými otázkami mírového postupu v Severním Irsku. Agent nebyl schopen říci, kde o počítač skutečně přišel. Ztrátu ohlásil až 4.3 s tím, že se domnívá, že jej zanechal v taxíku, kterým se nechal odvézt z baru domů. MI6 událost utajilo a pokusilo se anonymně získat laptop zpět. V novinách uveřejnili jeho přesný popis s tím, že se jedná o počítač ve kterém jsou důležité vědecké poznámky a žádali o jeho navrácení. Tento trik se zdařil a počítač byl vrácen zpět 16-tého března.

Druhý případ se odehrál 26-tého března večer. Scénář je podobný. Pracovník MI6 se při cestě z práce zdržel v jednom z podniků. Také on neví přesně, kde jeho počítač v ceně 2000 liber mohl zůstat. V laptopu byly tentokráte data, která se týkají detailů činnosti tajných agentů pracujících v cizině.

Ředitele MI6 Richarda Dearloveho čeká poněkud nepříjemná povinnost, má podat vysvětlení k těmto případům přímo ministerskému předsedovi Tonymu Blairovi

D. Opět INRIA !

Ing.Jaroslav Pinkava, CSc., AEC Brno

V čísle 10/99 jsme Vás informovali o úspěchu francouzské instituce INRIA (France's National Institute for Research in Computer Science and Control), kde skupina výzkumníků při použití 740 počítačů z 20 zemí světa v průběhu 40 dnů rozbila eliptický kryptosystém ECC2-97. Tento kryptosystém je součástí výzvy firmy Certicom (ECC Challenge) z roku 1997, kdy byla opublikována celá serie úloh z rostoucí obtížností (číslo 97 označuje délku použitého prvočísla).

Nyní byla vyřešena úloha ECC2K-108:

http://cristal.inria.fr/~harley/ecdl7/

Poznámka: V současnosti je připravován projekt CABAL773 řízený Arjenem Lenstrou a Bruce Dodsonem. Jeho cílem je faktorizace 2^773+1 pomocí algoritmu SNFS.
Podrobnosti http://www.lehigh.edu/~bad0/cabal773.html

E. Nový efektivní kryptosystém s veřejným klíčem na světě?

Ing.Jaroslav Pinkava, CSc., AEC Brno

Na webovské stránce http://www.ecstr.com/ se můžete seznámit s prvními informacemi ohledně nového kryptosystému s veřejným klíčem, který autoři Arjen Lenstra a Eric Verheul nazvali XTR. Kryptosystém vychází z klasického Diffie-Hellmanova kryptosystému, avšak velice chytrou cestou redukuje nezbytnou délku klíče. Cílem autorů bylo nalézt metodu, která má délku klíče přibližně stejnou jako je délka klíče pro eliptické kryptosystémy (při shodné bezpečnosti), avšak na bázi úlohy klasického diskrétního logaritmu.

F. CODE TALKERS

Díl I. - Vznik nové šifrové techniky

Mgr. Pavel Vondruška, NBÚ

CHOCTAW CODE TALKERS

První světová válka končí. Boje na západní frontě však stále ještě zuří. Jsme v zákopech na frontě v Mouse-Argonne ve Francii. Francouzské jednotky společně s pomocným praporem amerických vojáků se ocitly v částečném obklíčení. Jsou ve velice špatné pozici. Bez spojení není velení a zde se to projevuje na koordinaci akcí jednotlivých oddílů. Velitelé těchto oddílů pochopili, že Němci znají jejich kódy a jsou napojeni na jejich telefonní linky. Veškeré zprávy předávají spojky, které musí doslova pod střelbou nepřítele přebíhat mezi jednotlivými oddíly. Být takovou spojkou je zlé, ze čtyř pokusů je vždy jeden voják zajat nebo přímo zastřelen.Vzhledem k tomu je celá koordinace obrany ochromena. Nejhorší je, že oddíl nemůže komunikovat se svým hlavním velením, které leží mimo dokončující se obklíčení, tam spojky nemohou.

Velitel jednoho z oddílů Lawrence při kontrole pozic zaslechl dva vojáky Solomona Lewisa a Mitchella Bobba, jak se spolu baví ve svém rodném jazyce - jazyce severoamerického indiánského kmene Choctaw. Napadla jej spásná myšlenka, zavolal k sobě Bobba Mitchella a důkladně jej vyzpovídal. Dozvěděl se přesně, co potřeboval. V praporu je ještě několik indiánů z tohoto kmene, všichni mluví mimo své řeči i plynně anglicky. A co bylo nejlepší, Bobb věděl, že na velitelství také slouží dva indiáni z jejich kmene.

Velitel Lawrence ihned pochopil, jak může využít této informace. Indiány Choctaws rozmístil mezi svá stanoviště a nechal zavolat na hlavní stan. Tento okamžik byl kritický - najde se někdo, kdo pochopí, že se jedná o indiánskou řeč a sežene někoho ze sloužících indiánů. Vše dobře dopadlo. Na velitelství byl přiveden Smithville Ben Carterby .

První "kódované" spojení v indiánské řeči bylo navázáno. Bobb přeložil plán svého velitele do svého rodného jazyka a Ben zase přeložil zpět tento plán do angličtiny a předal na hlavním velitelství. Jazyk indiánů byl chudý, a proto museli vše opisovat (kulomet, letadlo, tank, plyn). Jejich řeč však byla pro Němce zcela nepochopitelná a těžko přepisovatelná do hláskové podoby. Velitelství souhlasilo a plán mohl začít.

Němci sice zachytili nový kód, ale nemohli jej rozluštit. Během 24 hodin se začal na celém úseku tento indiánský "kód" používat. Koordinace jednotlivých oddílů se začala projevovat, velitelé jednotlivých úseků nyní mohli bez strachu z vyzrazení popsat, kde je kolik munice, lidí, kam bude zaměřen dělostřelecký úder a kdy bude potřeba koordinovat protiútok. Během 72 hodin mohl začít protiútok, který Němce zahnal a obklíčenou jednotku vysvobodil.

Využití tohoto jazyka bylo omezeno jen na tuto událost a po vyrovnání fronty přešli Američané a Francouzi zpět na svůj kódový systém.

Velitel Lawrence svolal všech osm (podle jiných zdrojů celkem čtrnáct) indiánů z kmene Choctaw a poděkoval jim, uložil jim mlčení o celé události a řekl, že za svůj čin dostanou medaile.

Medailí se ale indiáni nedočkali, teprve v roce 1986 během každoročních indiánských oslav "Choctaw Labor Day Festival" byla udělena medaile rodinám těchto "mluvčích v kódech". Bylo to vůbec první oficiální uznání těmto mužům. A teprve tehdy se svět dozvěděl o jejich osudech. Třetího listopadu 1989 pak francouzská vláda ocenila důležitou roli těchto mužů a udělila jim nejvyšší francouzské vyznamenání "Chevalier de L'Ordre National du Merite".

O tom, jak vypadalo samotné "šifrování", nemáme mnoho informací. Jak již víme, řeč severoamerických indiánů neobsahovala vojenské termíny, a tak bylo pro určité výrazy potřeba vytvořit kód - opisný tvar. V memorandu veliteli 142.pěchotního pluku píše 23.1.1919 generál třicáté šesté divize, že jako některé kódy byla použita tato spojení : dělostřelectvo - indiánskou řečí "velká pistole" , kulomet - indiánskou řečí "malá pistol střílející rychle" a pro jednotlivé oddíly se používalo indiánskou řečí "jedna, dvě nebo tři zrna klasu".

Na závěr si dovolíme uvést jména těchto mužů, kteří, aniž by o tom věděli, začali psát novou historii amerického šifrování. Jednalo se o novou metodu využití kódů v neznámém nebo málo známém jazyce. Zprávy byly předávány pouze telefonicky nebo rádiem a právě zde se využilo to, že přepis indiánského jazyka vzhledem k atypické výslovnosti je pro netrénovaného člověka nesmírně těžký. Další výhodou byl velice rychlý způsob šifrování a dešifrování. Celkem lze říci, že tak bylo dosaženo relativně slušné bezpečnosti.

Zatímco na tuto příhodu se na mnoho let zapomnělo, velitelství americké armády tento způsob šifrování využilo během druhé světové války. Indiáni - "mluvčí v kódech" byli speciálně vycvičeni. Dá se říci, že tato šifrovací metoda ovlivnila výsledek války v Tichomoří ve prospěch USA.

Jména prvních mluvčích v kódech ("Code Talkers")

Albert Billy, Mitchell Bobb, Victor Brown, Ben Caterby, James Edwards, Tobias Frazer, Ben Hampton, Solomon Louis, Pete Maytubby, Jeff Nelson, Joseph Oklahombi, Robert Taylor, Calvin Wilson a Walter Veach.

COMANCHE CODE TALKERS

Je druhá světová válka. Snad vlivem nečekaného úspěchu, kterého dosáhli koncem prvé světové války indiáni severoamerického kmene Choctaw, se rozhodlo velení Signal Corpsu americké armády do svých řad povolat komančské indiány. Sedmnáct z nich bylo vybráno a vycvičeno. Sami se dohodli na jistých kódech, kterými označovali věci a situace, které v jejich jazyce nebyly. Například posah-tai-vo (bláznivý bílý muž) bylo kódové označení pro Adolfa Hitlera. Slovo letadlo v komančské řeči již existovalo, ale bombardovací letadlo v tomto jazyce nebylo. Indiáni se dohodli na označení "těhotné letadlo" atd.

Tato jednotka byla nasazena v roce 1944 v Evropě. Indiáni byli jako spojaři rozmístěni v poli a svá hlášení předávali pomocí vysílačky na velitelství, kde jiný indián zase text převáděl do anglické řeči. Jejich hlášení nebyla nikdy rozluštěna.

Na jejich příběhy z doby osvobozování Evropy se zapomnělo, jejich jména jsou ale známa. Tito muži se jmenovali :
Charles Chibitty, Haddon Codynah, Robert Holder, Forrest Kassanavoid, Wellington Mihecoby, Edward Nahquaddy, Perry Noyabad, Clifford Otitovo, Simmons Parker, Melvin Permansu, Elhin Red Elk, Roderick Red Elk, Larry Saupitty, Morris (Sunrise) Tabbyetchy, Tony Tabbytite, Ralph Wahnee a Willie Yackeschi.

Důvod, proč se o nich po válce nemluvilo, je zcela prozaický. Americká armáda ještě začátkem šedesátých let uvažovala o případném použití kódové řeči v nějakém málo používaném indiánském jazyce.

Ocenění se dočkali až třetího listopadu 1989, kdy francouzská vláda ocenila důležitou roli těchto mužů a udělila jim nejvyšší francouzské vyznamenání "Chevalier de L'Ordre National du Merite". Tři poslední žijící muži z této skupiny (Charles Chibitty, Roderick Red Elk a Forrest Kassanavoid) se zúčastnili tohoto slavnostního ceremoniálu a vyznamenání jménem všech převzali.

Význam těchto 17-ti mužů ale nelze přeceňovat. Dokonce ani konstatování, že se Němcům nepodařilo jejich "šifry" rozluštit, nic neříká. Na frontě se používala spousta různých šifrových systémů. Spojení s různými stupni velení mělo odlišné šifrovací techniky, odlišné šifry se používaly pro různé stupně utajení, podle naléhavosti se také používala různá spojení. Zachycených kódových zpráv těchto indiánů mělo dešifrovací oddělení jen malé množství a nevyplatilo se jim zabývat se těmito šiframi.

Jiná situace byla v Tichomoří, kde indiáni kmene Navajo byli nasazeni téměř masově a sehráli důležitou roli v předávání tajných zpráv. Těmto indiánům a jejich kódové řeči je věnován druhý díl.

Příště :

II. díl YIL-TAS GLOE-IH-DOT-SAHI UT-ZAH (code will success)

G. Letem šifrovým světem

1. Mezinárodní konference EUROCRYPT´2000 se koná od 14.5 do 18.5 v Bruggách (Belgie). Konferenci pořádá IACR ve spolupráci s belgickou odbornou skupinou COSIC. Všechny potřebné informace najdete na adrese http://www.esat.kuleuven.ac.be/cosic/eurocrypt2000
   Od současného organizačního výboru je velice milá zmínka o loňské konferenci EUROCRYPT´1999, která se konala v Praze a pořádala ji ve spolupráci s IACR právě naše odborná skupina GCUCMP. Loňskou konferenci dále připomíná i mapa na webu konference. Mapa představuje stát, kde se letošní konference koná a Praha zde slouží jako orientační bod pro loňské účastníky

2. Česká asociace pro čipové karty (ČAČK) a Asociace firem pro ochranu informací (AFOI) pořádá seminář ELEKTRONICKÝ PODPIS. Seminář se koná 17.dubna 2000 od 9.00 hod tradičně v hotelu Olšanka. Závazná přihláška mhruby@mbox.vol.cz . Další informace na ČAČK, Budovatelská 4821, 730 05 Zlín.

3. Šifrovací přístroj Enigma byl ukraden (ČTK, 2.4.2000) . Přímo z muzea v Bletchley Parku (hrabství Buckinghamshire), kde za války bylo legendární anglické středisko pro analýzu a luštění německých tajných kódů, byl odcizen šifrovací stroj Enigma. Enigma je určitě nejznámější šifrovací přístroj všech dob. Němci jej používali v průběhu celé druhé světové války a o domnívali se o něm, že jeho kód je neluštitelný. Ředitelka muzea v Bletchley Parku přirovnala zmizení stroje ke krádeži obrazu francouzského impresionisty Cézanna z oxfordského muzea. Odhadovaná cena zařízení je 300 000 USD.

4. 8.mezinárodní veletrh informačních a komunikačních technologií ComNet Prague 2000 se koná 23.-25.května 2000 na výstavišti Praha (Holešovice). Doprovodná konference ComNet Prague 2000 se koná v hotelu Diplomat. Obsah přednášek se dotýká tématu elektronického obchodu a jeho bezpečnosti.
   http://www.comnet-prague.cz

5. Na adrese http://zive.cpress.cz/forum/vypsat.asp/id=11073&all=true najdete zajímavý článek od Jana Vaňhary : Jak mi v Americe vybrali účet z české karty. Článek vyšel 21.3.2000. S chutí jsem si přečetl i následující obsáhlou diskusi, která dílem poukazuje na opravdové problémy kolem používání kreditních karet a dílem ukazují znalosti a představy "průměrného" uživatele internetu. Doporučuji přečíst.

6. Z adresy ftp://entropia.com/gimps/prime4.txt si můžete stáhnout dosud největší známé prvočíslo $2^{6\ 972\ 593}$-1 (třicáté osmé Mersennovo prvočíslo). Toto prvočíslo je prvé megaprvočíslo, tedy prvočíslo, které má více jak milión cifer (přesně 2 098 960!), druhé největší známé prvočíslo $2^{3\ 021\ 377}$-1 (třicáté sedmé Mersennovo prvočíslo) má "jen" 909 526 cifer. Toto prvočíslo Vám při tisku (bold 10) zabere cca 110 stránek A4.
   Další informace http://homepages.go.com/~joekorovin/Mersenne.html

7. Výsledky dosažené v jednotlivých projektech týkajících se hledání velkých prvočísel lze najít na následujících adresách :
   Prvočíselná dvojčata : http://www.serve.com/cnash/twinsearch.html
   Cunningham project : http://www.cerias.purdue.edu/homes/ssw/cun/index.html
   Mersennova prvočísla : http://homepages.go.com/~joekorovin/Mersenne.html
   Faktoriálová prvočísla : http://www.hut.fi/~nkuosa/primeform
   Trojčata CC2K : http://www.geocities.com/Area51/Portal/3360/
   Dvojitá Mersenova čísla: http://www.ltkz.demon.co.uk/ar2/mm61.htm
   Lucas-Lehmerův test : http://www.utm.edu/research/primes/notes/proofs/LucasLehmer.html

8. Zájemci o informace na téma uvolnění vývozu silné kryptografie najdou řadu zajímavých dat v článku : Cryptography and Liberty 2000, An International Survey of Encryption Policy http://www2.epic.org/reports/crypto2000/overview.html

9. 30.3.2000 byl na webu "živě" uveřejněn článek Michala A.Valáška „ Co by měl znát správný hacker na internetu“. Doporučuji také přečíst všechny příspěvky v doprovodné diskusi. http://zive.cpress.cz/r-art.asp/id=11362

10. Kerberos (client-server, autentizační protokol) je nyní součástí Windows 2000. Microsoft bohužel jeho implementaci tvůrčím způsobem upravil, takže sice dosáhl nekompatibility s jinými servery než se softwarem od Microsoftu, ale současně díky tomu nikdo nemůže zaručit, že tato úprava je bezpečná …
    Bruce Schneier , http://www.counterpane.com/crypto-gram-0003.html

H. 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 články a další související témata :

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

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

Spojení :

!!!!! - prosím následující adresu v souvislosti s časopisem již nepoužívat !!!
hruby@gcucmp.cz (Group of Cryptology Union of Czech Mathematicians and Physicists)
- oficiální e-mail adresa kryptologické sekce JČMF

důvodem je, že tato adresa již není pod mojí kontrolou a může se stát, že Vaše pošta se ke mně nedostane !

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, stačí 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.