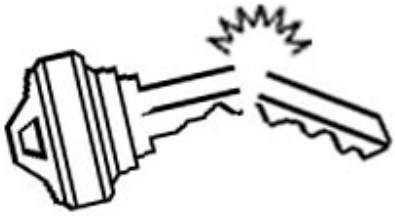
Informační sešit GCUCMP
Crypto-World 5/2000

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
(107 e-mail výtisků)
Uzávěrka 7.5.2000



POČET REGISTROVANÝCH ODBĚRATELŮ PŘESÁHL 100 !

Děkujeme !

OBSAH : **Str.**

A. Statistický rozbor prvého známého megaprvočísla

RNDr.Petr Tesař (I.CA) , Mgr.Pavel Vondruška (NBÚ)

Na adrese ftp://entropia.com/gimps/prime4.txt je dostupné dosud největší známé prvočíslo $2^{6\,972\,593}-1$. Toto prvočíslo je prvé známé 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. Pro lepší představu o jeho velikosti uvedeme, že při tisku (bold 10) zabere cca 110 stránek A4. Při zápisu do řady, kde jedna číslice je široká 1 mm a mezery mezi číslicemi zanedbáme, by bylo toto číslo více jak 2 km dlouhé. Číslo patří do souboru Mersennových prvočísel a je pravděpodobně třicátým osmým nebo třicátým devátým prvočíslem z tohoto souboru. Další podrobnosti jsou uvedeny v následujícím přehledovém článku Mersennova prvočísla.

Rozhodli jsme se podrobit toto megaprvočíslo statistickému rozboru. Otázkou tedy bylo, zda vykazuje ve svém dekadickém vyjádření nějaké statistické nepravidelnosti.

Dívejme se na naše prvočíslo jako na posloupnost znaků nula až devět. Celková délka této posloupnosti je 2098960 číslic.

Výskyt jednotlivých číslic je následující

"0" = 210190, "1" = 210744, "2" = 209678, "3" = 209382, "4" = 209832,
"5" = 209863, "6" = 210356, "7" = 209314, "8" = 209961, "9" = 209640.

Testujme hypotézu o rovnoměrném výskytu jednotlivých číslic pomocí známého χ-kvadrát kritéria. Hodnota statistiky je 8.302 . Kritická hodnota na hladině významnosti 0.05 je 16.919 , a proto můžeme na této hladině významnosti přijmout hypotézu o rovnoměrném rozdělení výskytu všech číslic v našem prvočíslu.

Obdobně testujme hypotézu o rovnoměrném rozdělení výskytu všech možných dvojic čísel (00 až 99) čili tak zvaných bigramů. Řetězová varianta bere každé číslo dvakrát - jednou na nižším místě bigramu, jednou na vyšším místě dalšího bigramu (samozřejmě kromě prvního a posledního čísla posloupnosti, která se vyskytují pouze v jednom bigramu). Neřetězová varianta bere každé číslo pouze jednou - bigramy se nepřekrývají a v našem případě je jich přesně 1049480. Hodnoty χ-kvadrát kritéria a příslušné kritické hodnoty na hladině 0.05 jsou:

	Řetězové bigramy	Neřetězové bigramy
Hodnota statistiky =	79.308	77.356
Kritická hodnota =	113.145	123.225

Obě hypotézy se tedy na hladině významnosti 0.05 přijímají.

V kryptologii se jako kritérium nerovnoměrnosti používá index coincidence (IC), což je zhruba řečeno - součet kvadrátů relativních četností všech hodnot znaku. Rovnoměrně rozdělená posloupnost z deseti různých znaků má IC okolo hodnoty 0.1. Pro naši posloupnost bylo vypočteno IC = 0.999999667. Kritická hodnota na hladině významnosti 0.05 je 0.1000003325. Lze tedy konstatovat, že i podle tohoto kritéria je přijata hypotéza o rovnoměrném rozdělení výskytu jednotlivých číslic.

Velmi zajímavou charakteristikou je výskyt opakování různě dlouhých podřetězců. Z teorie náhodných výběrů s vracením můžeme zhruba odhadnout pravděpodobnost výskytu alespoň jednoho opakování určené délky ve sledované posloupnosti.

Náhodný výběr s vracením :

Délka opakovaného řetězce	Pravděpodobnost alespoň jednoho opakování
10	1 - 2.1E-96
11	0.99999999973
12	0.8895
13	0.1977
14	0.0218
15	0.0022

Testované megaprvočíslo:

Délka opakovaného řetězce	Počet opakování
10	161
11	13
12	2
13	1
14 a více	0

Nejdelší opakující se řetězec je " 7 6 0 6 8 7 8 5 2 2 1 5 2 ".
První výskyt je na 23896 řádu (umístění nejpravější dvojky). Druhý výskyt je na 379360 řádu.

Shoda s teorií náhodných výběrů s vracením je viditelně dobrá.

Závěr :

Největší známé prvočíslo interpretované jako posloupnost znaků nula až devět se jeví jako náhodná posloupnost s rovnoměrným rozdělením výskytu jednotlivých znaků.

B. Mersennova prvočísla

Mgr.Pavel Vondruška (NBÚ)

Mersennova prvočísla jsou prvočísla speciálního tvaru, a to $M_n = 2^n - 1$. Aby číslo uvedeného tvaru mohlo být prvočíslo, musí být exponent n prvočíslem. Jedná se ovšem jen o podmínku nutnou.

Začátkem 17-tého století vyslovil francouzský matematik (a teolog) Marin MERSENNE (1588 - 1648) hypotézu, že pro n menší jak 258 jsou čísla tvaru $M_n = 2^n - 1$ prvočísly, právě pro n= 1, 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257

Prvočísla tvaru $M_n = 2^n - 1$ se v současné době na jeho počest nazývají Mersennova prvočísla.

Mersennova prvočísla se zapisují vzestupně do tabulky a je zvykem je označovat pořadovým číslem v této tabulce. Tabulka dosud nalezených Mersennových prvočísel je uvedena jako příloha k tomuto článku.

Vraťme se k Mersennově hypotéze. Hypotéza byla v následujících letech testována mnoha matematiky a postupně se podařilo odstranit chyby, které obsahovala.

V intervalu 1-257 byla vynechána celkem 3 Mersennova prvočísla a naopak dvě z uvedených čísel jsou čísla složená:

- vynechána byla deváté, desáté a jedenácté Mersennovo prvočísla , tedy M_{61} , M_{89} a M_{107} (přičemž pro n=61 , $M_{61} = 2^{61} - 1$ bylo dokázáno , že je prvočíslo teprve v roce 1883)
- složená čísla jsou naopak M_{67} a M_{257} (Číslo $M_{67} = 2^{67} - 1 = 193707721 * 761838257287$ rozložil Cole roku 1903)

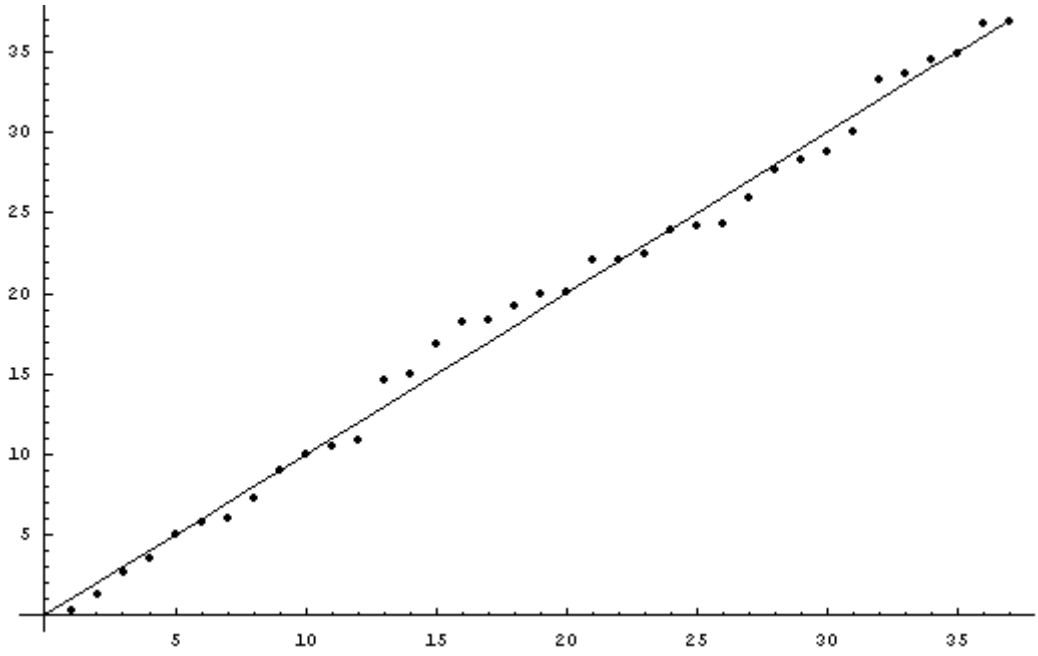
Důležitým kritériem, zda Mersennovo číslo je nebo není prvočíslo, je **Lucas (1870)-Lehmerův (1930) test.** Síla tohoto testu je mimo jiné v tom, že jej lze snadno realizovat pomocí výpočetní techniky.

Lucas-Lehmerův test :
Nechť n je liché prvočíslo. Pak je M_n prvočíslem právě tehdy, když dělí číslo S(n-2), kde $S(0)=4$, $S(k+1) = S(k)^2 - 2$.
Podrobnosti (včetně vysvětlení použitého značení) naleznete např. na URL adrese
http://www.utm.edu/research/primes/notes/proofs/LucasLehmer.html

Koncem roku 1998 bylo nalezeno celkem 37 Mersennových prvočísel. Na základě rozboru všech těchto prvočísel byla vytvořena hypotéza o jejich rozložení a byly experimentálně určeny parametry lineární funkce, která určuje závislost exponentu n Mersennova čísla na jeho pořadí v tabulce (tzv "lineární hypotéza"). Z této "lineární hypotézy" se dalo očekávat, že třicáté osmé Mersennovo prvočíslo bude mít exponent přibližně roven 4,699,385. Při systematickém prohledávání vhodných kandidátů bylo v prosinci roku 1999 objeveno nové Mersennovo prvočíslo (v současné době označováno jako třicáté osmé). Jenže jeho exponent je 6972593 , což by bylo v dobré shodě pro třicáté deváté Mersennovo prvočíslo (předpověď z lineární hypotézy je : 6,935,171). Řada odborníků se tedy domnívá, že při prohledávání prostoru kandidátů na třicáté osmé Mersennovo prvočíslo

se podařilo příslušnou hodnotu "přeskočit" . Na projektu se podílely stovky dobrovolníků, kteří hypotézu testovali na svých PC a je tedy možné, že některý z dobrovolníků "selhal". V současné době je celý prostor znovu prohledáván. V každém případě poslední objevené Mersennovo prvočíslo je největším známým prvočíslem a je prvým megaprvočíslem - tedy prvočíslem, které má ve svém dekadickém zápisu více jak milión cifer.

Příloha 1 : "Lineární hypotéza" rozložení Mersennových prvočísel



$e^G \log_2 n - 1.462$ With Respect to N, and the Line y = x

(G je Eulerova gamma funkce (0.5772156649…) a e je základ přirozeného logaritmu (2.718281828…))

Očekávané hodnoty exponentu n pro n-té Mersennovo prvočíslo, vypočtené podle "Lineární hypotézy"

N	exponent n v 2^n-1
38	4,699,385
39	6,935,171
40	10,234,658
41	15,103,913
42	22,289,772
43	32,894,385
44	48,544,264
45	71,639,751
50	501,458,270
55	3,510,067,986
60	24,569,496,568
65	171,979,620,925

Příloha 2 : Tabulka všech dosud nalezených Mersennových prvočísel

Pořadí N	n	Cifer	Rok	Objevil
1	1	1	-	Starověké Řecko
2	3	1	-	Starověké Řecko
3	5	2	-	Starověké Řecko
4	7	3	-	Starověké Řecko
5	13	4	1456	?
6	17	6	1588	Cataldi
7	19	6	1588	Cataldi
8	31	10	1772	Euler
9	61	19	1883	Pervušin
10	89	27	1911	Powers
11	107	33	1914	Powers
12	127	39	1876	Lucas
13	521	157	1952	Robinson
14	607	183	1952	Robinson
15	1279	386	1952	Robinson
16	2203	664	1952	Robinson
17	2281	687	1952	Robinson
18	3217	969	1957	Riesel
19	4253	1281	1961	Hurwitz
20	4423	1332	1961	Hurwitz
21	9689	2917	1963	Gillies
22	9941	2993	1963	Gillies
23	11213	3376	1963	Gillies
24	19937	6002	1971	Tucker
25	21701	6533	1978	Noll,Nickel
26	23209	6987	1979	Noll
27	44497	13395	1979	Nelson, Slowinski
28	86243	25962	1982	Slowinski
29	110503	33256	1988	Colquitt, Welsh
30	132049	39751	1983	Slowinski
31	216091	65050	1985	Slowinski
32	756839	227832	1992	Slowinski, Gage
33	859433	258716	1994	Slowinski, Gage
34	1257787	378623	1996	Slowinski, Gage
35	1398269	420921	1996	GIMPS
36	2976221	895932	1997	GIMPS
37	3021377	909,526	1998	GIMPS
38	6972593	2,098,960	1999	GIMPS, Cray

Literatura :

Mersennova prvočísla - přehled : http://homepages.go.com/~joekorovin/Mersenne.html
Uloženo celé 38 Mersennovo prvočíslo ftp://entropia.com/gimps/prime4.txt
Lucas-Lehmer test : http://www.utm.edu/research/primes/notes/proofs/LucasLehmer.html
Caldwell, Chris K. "Mersenne Primes: History, Theorems and Lists." Prime Pages (1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.utm.edu/research/primes/mersenne.shtml
Caldwell, Chris K. "The Largest Known Prime by Year: A Brief History." Prime Pages (1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.utm.edu/research/primes/notes/by_year.html
Caldwell, Chris K. "Where is the next larger Mersenne prime?" Prime Pages (1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.utm.edu/research/primes/notes/faq/NextMersenne.html
Caldwell, Chris K. "Lucas-Lehmer Theorem." Prime Pages (1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.utm.edu/research/primes/notes/proofs/LucasLehmer.html
Caldwell, Chris K. "Modular restrictions on Mersenne divisors." Prime Pages (1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.utm.edu/research/primes/notes/proofs/MerDiv.html
Caldwell, Chris K. "Prime-square Mersenne divisors are Wieferich." Prime Pages (1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.utm.edu/research/primes/notes/proofs/SquareMerDiv.html
Kurowski, Scott. "Current Internet PrimeNet Server World Test Status." Entropia.com (November 22, 1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://entropia.com/primenet
O'Connor, John J., and Robertson, Edmund F. "Prime numbers." The MacTutor History of Mathematics Archive (December 1996). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www-history.mcs.st-andrews.ac.uk/history/HistTopics/Prime_numbers.html
Williams, Hugh C. Édouard Lucas and Primality Testing. New York: John Wiley & Sons, Inc., 1998.
Wiman, Lucas, et al. "The Mersenne Prime Mailing List FAQ." Mersenne FAQ (1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.tasam.com/~lrwiman/faq-mers
Woltman, George. "38th Mersenne Prime Discovered." Mersenne.org (June 30, 1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.mersenne.org/6972593.htm
Woltman, George. "Mersenne Prime Search." Mersenne.org (October 4, 1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.mersenne.org/prime.htm
Woltman, George. "Mersenne Search Status." Mersenne.org (November 17, 1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.mersenne.org/status.htm

C. Quantum Random Number Generator

RNDr. Jaroslav HRUBY, CSc., GCUCMP

Abstract

Celý článek je uveden jako zvláštní příloha k tomuto sešitu - soubor QNG.PDF.

Příloha je distribuována společně se sešitem 5/2000. Zde jen upoutávka v podobě malé ukázky.

A physical quantum random number generator based on the random events which are realized by the choice of single photons between the two outputs of a beamsplitter is presented.

The data generated from this quantum generator sucessfully passed DIEHARD statistical tests and also cryptological tests (QUT Brisbane, Information research centre) for measuring the randomness of large binary streams. The author of the DIEHARD statistical tests G.Marsaglia (http://stat.fsu.edu/geo)

The research in this direction is in progress. We conclude, we demonstrated a random number generator using a basic quantum process with super small correlation between succesive bits. Such generator behaves like a perfect random source, **which is better then other for us known physical random sources**.

D. Sdružení pro bezpečnost informačních technologií a informačních systémů (BITIS)

Registrace Stanov sdružení uskutečnilo MV ČR v lednu 2000. Prvé valné hromady (12.4.2000), kde byl zvolen výbor sdružení, se zúčastnilo přes 20 odborníků v této oblasti.

Plný název tohoto nového občanského sdružení je :
Sdružení pro bezpečnost informačních technologií a informačních systémů (dále jen BITIS).

Cílem a posláním sdružení je

a) sdružit odborníky z oblasti bezpečnosti informačních technologií a informačních systémů, kteří chtějí rozvíjet komplexní ochranu a bezpečnost informací a dat v IT a IS, v telekomunikační, výpočetní, fyzické, administrativní, legislativní a morálně-etické oblasti
b) organizovat pro členy odborné aktivity
c) pořádat presentační aktivity pro širší odbornou veřejnost
d) je chránit společné zájmy členů před nekompetentním a neetickým.chováním
e) je zprostředkovat některé související činnosti, k nimž např. patří vypracování posudků a stanovisek, konzultace k vyhledávání dodavatelů služeb, know-how a bezpečnostních produktů a styk a spolupráce s dalšími relevantními subjekty, českými i zahraničními.

Základní odbornou aktivitou BITIS jsou interní semináře z oblasti informační bezpečnosti, které slouží zejména k diskusi a výměně názorů k aktuálním odborným problémům a s tím souvisejícím legislativně-právním aspektům .
K prezentaci činnosti BITIS pro ostatní odbornou veřejnost (včetně manažerů) slouží veřejné semináře o informační bezpečnosti a další odborně zaměřené akce.

Prvou veřejnou akcí tohoto sdružení bylo spolupořádání přednášky významného izraelského kryptologa prof. Beni Arazi, "Architektura pro implementaci algoritmů kryptografie eliptických křivek". Přednáška se konala dne 20. dubna 2000 od 16.00 hod. ve velké zasedací síni rektorátu ČVUT v Praze 6 a odběratelé sešitu GCUCMP byli o ní včas informováni pomocí e-mailu.

Předsedou sdružení byl zvolen :	Doc. Ing. Jiří PŘIBYL, CSc.
Sekretář :	Doc. Oldřich PEKÁREK, CSc.
Pokladník :	Mgr. Pavel VONDRUŠKA
Dalšími členy výboru byli zvoleni :	
	Ing. František HRON, Ing. František FENCL,
	Mgr. Jan JANEČKO, Ing.Jindřich KODL,CSc

Sídlem BITIS je Katedra telekomunikační techniky FEL ČVUT v Praha 6 - Dejvice, Technická 2, PSČ 166 27.

V nejbližší době bude zřízena informační www stránka BITIS. Tato adresa bude zveřejněna v některém z příštích sešitů.

E. CODE TALKERS
Díl II. - YIL-TAS GLOE-IH-DOT-SAHI UT-ZAH
(code will success)

Mgr. Pavel Vondruška, NBÚ

Guadalcanal, Tarawa, Peleliu, Iwo Jima - místa, kde se za druhé světové války proslavili indiáni z kmena Navajo, kteří zde ve službách amerického námořnictva působili jako "code talkers" (mluvčí v kódech). Přenášeli důležité strategické zprávy pomocí rádia nebo telefonu, sloužili ve všech šesti námořních divizích americké armády. Šifrové zprávy, které předávali, se nepodařilo Japoncům nikdy vyluštit. Šéf japonské luštitelské služby za druhé světové války, generál Seizo Aisue, prohlásil, že za druhé světové války se jejich službě podařilo rozluštit postupně všechny šifry amerického letectva a část šifer námořnictva, ale šifrám námořnictva, které používalo v radiovém provozu, nerozuměli a nevěděli, co s nimi. Americké velení v sedmdesátých letech prohlásilo, že nejtajnější a nejúspěšnější americkou zbraní v Pacifiku byli právě indiánští "mluvčí v kódech" z kmene Navajo. Ještě více jak dvacet let po válce byly následující informace o výcviku a nasazení těchto indiánů klasifikované stupněm tajné a veřejnost o vynikajících úspěších těchto mužů nic nevěděla. V současné době jsou již všechny informace uvolněny, včetně původní kódové knihy, kterou indiáni za války používali. Následující řádky jsou věnovány všem těm, kteří za války pomohli své vlasti a museli po dlouhou dobu zůstat v anonymitě bez jakéhokoliv veřejného ocenění.

S myšlenkou využít indiány z kmene Navajo pro přenos tajných informací přišel Philip Johnston. Byla to ta správná osoba ve správné době na správném místě. Bojoval v prvé světové válce a věděl, že zde bylo s úspěchem využito indiánů k přenosu tajných zpráv. Jeho otec byl misionář v indiánské rezervaci kmene Navajo. Jako dítě se zde naučil plynně mluvit jejich obtížnou řečí. Byl tak jeden z mála asi třiceti bělochů, kteří tuto řeč ovládali. Indiáni z tohoto kmene žili velice izolovaně a nekomunikovali ani s ostatními indiánskými kmeny. Uvědomoval si, že řeč Navajů je velice obtížná, a to především svojí speciální výslovností. Například samohlásky indiáni vyslovovali deseti velice podobnými způsoby. Řeč neměla psanou podobu, ale kdyby byla slova zapsána, bylo by nutné označit tyto rozdíly ve výslovnosti. Prostý přepis několika rozdílných slov tak totiž mohl být identický (např. "bito" je voda a "bitó" je pomerančová šťáva, "bita" je mezi a "bitá" je křídlo).

Tabulka č.1 : Možná výslovnost hlásky "a"

a-	short and low in pitch
aa-	long and low in pitch
a-	a rise in pitch and short
aa-	a rise in pitch and long
a-	short, high and nasal
a-	short and nasal
aa-	long, high and nasal
aa-	long and nasal
aa-	falling tone
aa-	falling nasal

Právě tato vlastnost se zdála Philipu Johnstonovi velice vhodná pro tajnou komunikaci. Přepis zachycené komunikace je pro netrénovaného člověka bez znalosti

významu slov v podstatě nemožný. Řeč Navajů měla ještě jednu význačnou vlastnost - nepřebírala slova z jiných jazyků a pro nová slova si volili vlastní kombinace.

V březnu 1942 se Philipu Johnstonovi podařilo přemluvit generála Claytona B.Vogela, aby mu umožnil předvést využití utajeného přenosu pomocí indiánských mluvčích. Během prezentace Navajové přenesli bez chyby tří řádkovou zprávu během dvaceti vteřin. Při použití kryptografického zařízení, které námořnictvo používalo, trval celý přenos zašifrování, přenosu a dešifrování třicet minut. Na konci prezentace bylo všem přítomným vysvětleno, že v reálném provozu nebude jen použit překlad do indiánské řeči, ale bude vytvořena kódová kniha v indiánské řeči, která se bude při přenosu používat. Prezentace byla úspěšná a Philip Johnston dostal za úkol vycvičit prvních třicet indiánů a vytvořit kódovou knihu. Pilotní program mohl začít.

Získat třicet vhodných rekrutů nebylo však jednoduché. (V roce 1942 žilo přibližně 50 000 Navajů, v roce 1945 sloužilo u námořnictva 540 indiánů - ne všichni ale jako "code talkers", těch bylo podle různých údajů něco mezi 375 až 420). Především zde byla jazyková bariéra - řada indiánů totiž neuměla anglicky. Řada indiánů také jít do války za bělochy nechtěla - ještě stále doznívala vzpomínka na utrpení jejich dědů. Navajové po prohrané indiánské válce v roce 1860-63 se museli přestěhovat o 300 mílí dále k pevnosti Fort Sumner, kde měli být převychováni a zcivilizováni. Tento pochod indiáni nazývali "Long Walk". Pochod byl nesmírně obtížný a mnoho indiánů během něj zemřelo. Řada indiánů měla zájem pomoci, ale komisi, která je odváděla, se zdáli příliš mladí. Indiáni neměli žádné doklady a nevěděli, kdy se narodili. Vypráví se historka, že komise indiány jednoduše vážila a kdo byl příliš lehký, toho neodvedla. Indiáni nevěděli, kam mají být odvedeni. Popletli si slova marine (námořnictvo) a submarine (ponorka) a hrozně se báli, že půjdou sloužit pod vodu. Indiáni byli nejprve odvedeni do sběrného tábora, kde byli cvičeni v běžných vojenských dovednostech. Seznamovali je s technikou (včetně zápalek, rádia, vysílačky). Indiáni nebyli dobrými vojáky (dle velitelů), nechápali, proč musejí poslouchat své nadřízené, opouštěli kasárna, v noci několikráte vykradli kantýnu, zajímali se o ženy důstojníků, jejich hygiena nebyla valná, vojenské boty nečistili a na nástup chodili ustrojeni podle počasí. Ti, kteří prošli tímto vstupním táborem se dostali do tábora Pendleton, blízko San Diega. Zde začal jejich výcvik spojařů.

Společně s 29-ti prvními Navaji vytvořil Philip Johnston první kódovou knihu. Obsahovala něco málo přes dvě stě slov. Kniha obsahovala hláskovou abecedu, nejpoužívanější názvy zbraní, názvy států a nejpoužívanější vojenské termíny. Slova byla volena tak, aby si je indiáni dobře zapamatovali.

Hlásková abeceda byla vytvořena podle tohoto schématu :

A - slovo v angličtině od A - ant (mravenec) kód : Wol-La-Che (mravenec v řeči Navajů). Tedy kdykoliv bylo použito slovo Wol-La-Che znamenalo to písmeno A.

Názvy států byly také pro indiány lehce zapamatovatelné :

Amerika - naše matka , Afrika - černí , Aljaška - zima, Japonsko - šikmé oči.

Některá slova byla vybrána na základě souzvuku , tedy tak, aby si je indiáni lehce pamatovali:

Dispatch - dog is patch (samozřejmě řečeno indiánskou řečí)

Belong - long bee , district - deer is strict atd.

Názvy zbraní, které indiáni neznali, byly kódovány podle "podobnosti" :

Letadlo - pták, bomba - vejce, loď - ryba atd.

Na konci pilotního projektu (po výcviku prvních třiceti mužů) byla opět provedena prezentace. Tentokráte se jí zúčastnili i američtí kryptologové. Zvukové záznamy, které jim předložili, nebyli schopni zařadit a přepsat do správného textu. K jazyku se vyjádřili, že připomíná nejspíše hebrejštinu. Po seznámení se s kódovou knihou bylo doporučeno ji

rozšířit. Především bylo ke každému písmenu zavedeno více slov. Rozšířen byl i slovník o další frekventní slova. Nasazení systému však bylo schváleno.

Kódová kniha byla podle těchto připomínek upravena a byla rozšířena na 450 výrazů.

Příloha č.2: Ukázka začátku hláskovací tabulky

Písmeno	kód	pomocné slovo
A	WOL-LA-CHEE	ANT
A	BE-LA-SANA	APPLE
A	TSE-NILL	AXE
B	NA-HASH-CHID	BADGER
B	SHUSH	BEAR
B	TOISH-JEH	BARREL
C	MOASI	CAT
C	TLA-GIN	COAL
C	BA-GOSHI	COW
D	BE	DEER
D	CHINDI	DEVIL
D	LHA-CHA-EH	DOG

Photo of Navajo Code Talkers in formation at Camp Pendelton, California
Local call number Philip Johnston Physical description Black-and-white photograph, 8 x 13.5 cm. Reproduction requires permission of the repository.

Výcvik indiánů v táboře Pendelton

Indiáni byli začátkem roku 1943 připraveni k nasazení k námořním divizím a dále bylo rozhodnuto o přijetí dalších stovek nových rekrutů, určených pro výcvik v přenášení kódových zpráv.
Celý program byl přísně tajný a jen málo lidí vědělo, o co opravdu jde. Američané, kteří zachytili vysílání Navajů, si např. často mysleli, že se jedná o vysílání Japonců na americké frekvenci.

Pokračování příště : Díl III. : Od Iwo Jimy k mluvící loutce firmy Hasbro

F. Letem šifrovým světem

1. Ve dnech 30.-31.května 2000 se bude konat v Míčovně Pražského hradu mezinárodní konference - Finanční služby ve virtuálním prostředí.. Hlavní přednášky přednesou :
   L.Strous (Nizozemí) : Audit IS a informační bezpečnost v De Nederlandsche Bank
   S.Katsikas (Řecko): Role PKI v E-Commerce.
   Z českých odborníků zde promluví:
   T.Ivanovský - Finanční služby prostřednictvím mobilních telefonů
   Z.Kaplan - Řízení bezpečnosti na úrovni vrcholových vedoucích pracovníků.
   V.Matyáš - Biometrie
   E.Racková, F.Stolle - Penetrační testování - praktické zkušenosti.
   Konferenci pořádá společnost Tate International, s.r.o., vydavatel časopisu DSM.
   Další informace tel.: 02/57920319-20, http://www.dsm.tate.cz

2. V sešitě 2/2000 jsme otiskli důkaz Velké Fermatovy věty (FLT), který předložil veřejnosti 23.1.2000 k odborné diskusi profesor Victor Sorokin. Tento důkaz byl zajímavý především proto, že byl založen čistě na algebraických tvrzeních a byl sympaticky krátký. V současné době jediný uznaný důkaz FLT od Andrew Willese (z roku 1994) je značně komplikovaný a je založen na důkaze Taniyamovy-Shimurovy hypotézy o modulárních formách eliptických křivek (podrobnosti viz např. sešit 2/2000). Důkaz Victora Sorokina, jak někteří doufali, mohl připomínat myšlenkový postup Pierre de Fermata při formulaci tohoto slavného problému. Bohužel se ukázalo, že v předloženém důkazu je chyba. Chybu jako prvý objevil Paul Dreyer. Profesor Sorokin se pokusil chybu odstranit, ale nakonec během března rezignoval a účastníkům diskusní skupiny rozeslal e-mail, ve kterém přiznává, že důkaz je chybný a problém, na který byl upozorněn, nelze odstranit (v jednom okamžiku byla rovnice zaměněna za identitu).

3. Evropská Unie stanoví nová - volnější pravidla pro vývoz kryptografických prostředků! Evropská unie odsouhlasila uvolnění pravidel pro vývoz kryptografických zařízení do 25-ti zemí světa (15 zemí EU a dále 10 jiných zemí -- USA, Japonsko, Kanada, Švýcarsko, Austrálie, Nový Zéland, Norsko, Česká republika, Maďarsko a Polsko). Státy, do nichž je povolen vývoz, dohromady tvoří více než 80% světového trhu s kryptografickými zařízeními. Toto uvolnění opět staví vývozce z USA do nevýhodnější pozice než vývozce EU a to i přes značně uvolněná pravidla vývozu USA, která byla schválena letos v lednu.
   Wall Street Journal 28.4.2000,
   http://interactive.wsj.com/articles/SB956867771608897487.htm

4. Společnosti Oskar, Ericsson a České vysoké učení technické (ČVUT) podepsaly dohodu o založení "Centra pro výzkum a vývoj" v prostorách ČVUT v Praze. Moderní centrum bude sloužit především k vývoji aplikací a služeb v oblasti bezdrátových telekomunikací. Jedním z cílů je uvést Českou republiku do popředí v oblasti aplikací a služeb pro UMTS, třetí generaci bezdrátových technologií. Společnosti Oskar a Ericsson rovněž prostřednictvím Centra poskytnou prostředky na stipendijní programy pro studenty ČVUT.

   Po dokončení se Centrum stane základnou poskytující nejaktuálnější data pro výzkum mobilních bezdrátových technologií v České republice. Centrum zahájí provoz do 31.prosince 2000.

5. Na konferenci Fast Software Encryption Workshop 2000 (10.-12.4.2000, New York City) publikoval Adi Shamir, Alex Biryukov a David Wagner nový útok na silnější verzi šifrového algoritmu A5/1, který se používá ve 130 milionech GSM mobilních telefonů, včetně ČR. Dříve publikovaný útok vyžadoval záznam 2 minut šifrového spojení a následnou analýzou (doba 1 s) byl získán klíč. Nově publikovaný útok umožňuje ze záznamu dvou vteřin spojení (!) získat klíč. Analýza trvá cca 4 minuty a vyžaduje běžné PC (500 Mhz) vybavené 4 pevnými disky, každý o kapacitě 73 GB. Jejich přednáška je dostupná od 27.4.2000 na adrese :
   http://cryptome.org/a5.ps , http://cryptome.or/a5.zip
   Některé základní informace o předchozím útoku jsou dostupné i v našem sešitě 1/2000 (Soukromí uživatelů GSM ohroženo).

6. IACR (International Association for Cryptologic Research, organizátor konferencí EUROCRYPT a CRYPTO), zavedla na své webovské stránce novou službu. Jedná se o tzv. kryptologický archív, kde jsou ukládány v elektronické podobě významné články, které poskytli k veřejnému použití členové IACR. Přesná URL adresa je :
   http://eprint.iacr.org/2000/

7. ZDnet zveřejnil obsah tajné interní zprávy Microsoftu, ze které vyplývá nutnost opravit přes 63 000 chyb ve Windows 2000. Marc Lucovsky, vedoucí vývojového týmu Windows, rozeslal svým podřízeným výzvu k urychlenému opravení desítek tisíc chyb ve finálním kódu Windows 2000. Podle zprávy obsahují Windows 2000 celkem 21 000 odložených chyb, které mohou způsobit vážné problémy nebo jenom dělají něco jiného, než by měly; 27 000 chyb se týká špatné optimalizace a nedodělků. Při nákupu Windows 2000 se tedy můžete setkat celkem s 65 000 potencionálními problémy, z nichž 28 000 může podle odborníků způsobit reálnou hrozbu k ohrožení vašich dat.
   Zdroj : Mery Jo Foley , "Can Microsoft squash 63,000 bugs in Win2K?"
   http://www.zdnet.com/pcweek/stories/news/0,4153,2436920,00.html

8. Přibližně v půlce dubna se rozhořela nová mediální aféra (informace na News.COM a ZDNN) , která nejdříve vinila Microsoft ze zabudování zadních vrátek do produktu FrontPage97 (možná i Frontpage98).
   Co bylo podstatou ? Součástí FP97 a FP98 instalace je knihovna Dvwssr.dll - nachází se vždy ve v_vti_bin/_vti_aut adresáři a je tedy přístupná z Internetu. Zároveň je tento modul zodpovědný za browsing funkci (tj. prohlížení obsahů FP webů). Právě v této knihovně lze najít text (dle prvních tvrzení univerzální heslo) "Netscape engineers are weenies!" .

   Pochopitelně se ukázalo, že o zadní vrátka nejde. Tento text vepsal do zdrojového kódu jeden z programátorů, který byl již unaven soubojem mezi firmou Microsoft a Netscape a chtěl "zesměšnit" své protihráče u Netscapu.

   Celá aféra měla i kladnou stránku - během "propírání" bezpečnosti tohoto produktu bylo objeveno několik významných slabin tohoto produktu a doufejme, že budou brzy odstraněny.

   Chci však upozornit ještě na jeden aspekt celé "aféry" a to z hlediska bezpečnosti. Je potřeba si položit otázku, jak funguje "výstupní" kontrola u Microsoftu. Opravdu si může každý programátor do zdrojového textu zařadit, co se mu zlíbí? Nebo jsou již zdrojové texty tak složité, že efektivní kontrola není možná? Obě možnosti jsou z hlediska bezpečnosti znepokojující a naznačují, že Microsoft své produkty chápe především jako produkty komerční a bezpečnost je až na dalším místě.

9. V době, kdy dopisuji tento sešit, řádí ve světě nový virus I Love You (a jeho roztomilé mutace). Vzhledem k mediální popularitě k němu asi moc nového nenapíši. Uvedu tedy alespoň užitečnou adresu : http://servery.cz/index.php3?include=virus.inc , kde je uložen návod na jeho odstranění z napadeného PC.

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 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

Upozornění :

!!!!! - 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 !

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.