Crypto-World

Informační sešit GCUCMP

Ročník 6, číslo 6/2004 **15. červen 2004**

6/2004

Připravil : Mgr.Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(550 registrovaných odběratelů)

Obsah : **Str.**

(články neprocházejí jazykovou korekturou)

A. Měsíc prvočísel
Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.

Svět prvočísel (a s jistou nadsázkou celý náš svět) se od května do června 2004 výrazně změnil. Začalo to nenápadně – nejprve bylo oznámeno nalezení nového největšího známého prvočísla, pak následovalo překvapující oznámení o vyřešení otázky počtu prvočíselných dvojčat. Těsně před přípravou tohoto čísla se objevila informace, že byla vyřešena Riemannova hypotéza - hypotéza, která má význam v teorii prvočíselnosti a která patřila do souboru sedmi nejsložitějších nevyřešených matematických problémů.

1. Mersennovo prvočíslo nalezeno

Mersennova prvočísla jsou prvočísla speciálního tvaru: $M(n) = 2^n - 1$. Doposud bylo takovýchto prvočísel známo 40. Čtyřicáté Mersennovo prvočíslo bylo objeveno loni v listopadu. Bylo dosud největším známým prvočíslem (lze jej zapsat pomocí 6 320 430 dekadických cifer).

Dne 22.5.2004 bylo oficiálně oznámeno nalezení 41. Mersennova prvočísla a po kontrole správnosti byla 29.5 zveřejněna jeho hodnota - je jím $2^{24\,036\,583}-1$. Toto číslo se stalo největším v současnosti známým prvočíslem - lze jej zapsat pomocí 7 235 733 dekadických cifer (mimochodem odborníci předpokládali, že bude výrazně větší a k jeho zápisu bude potřeba přes devět milionů číslic). K nalezení bylo použita kapacita 240 000 PC, kterou dobrovolníci v rámci projektu GIMPS poskytli. Odměna 100.000 USD, kterou věnuje organizace Electronic Frontier Foundation za nalezení prvočísla, k jehož zapsání bude potřeba 10 miliónů cifer, tak stále ještě nebude vyplacena a čeká pravděpodobně na toho, kdo nalezne 42. Merssennovo prvočíslo. Číslo si můžete v dekadickém tvaru stáhnout z http://mersenne.org/prime7.htm .

Protože jsme se Mersennovými prvočísly již dříve důkladně zabývali (viz [1], [2], [3], [4]) , tak se dnes spokojíme pouze s výše uvedeným krátkým konstatováním o nalezení tohoto nového velikána. Pokud by vás zajímala struktura tohoto čísla, pak v následujícím článku se můžete dočíst, jak dopadl statistický rozbor na náhodné rozdělení číslic v jeho zápisu.

Starší informace věnované Mersennovým prvočíslům:

[1] Vondruška,P: Mersennova prvočísla, Crypto-World 5/2004, 7.5.2000, http://www.crypto-world.info/casop2/crypto05_00.pdf

[2] Tesař,P., Vondruška,P.: Statistický rozbor prvého známého megaprvočísla, Crypto-World 5/2004, 7.5.2000, http://www.crypto-world.info/casop2/crypto05_00.pdf

[3] Vondruška,P.: Mersennovo prvočíslo nalezeno?, ROOT.CZ, 16.11.2001, http://www.root.cz/clanek/937

[4] Vondruška,P.: Za nalezení Mersennova prvočísla bude vyplaceno 100.000 dolarů, Technet.idnes.cz, 21.11.2003, http://technet.idnes.cz/novinky/mersenn_prvocisla031121.html

Informace o projektu hledání Mersennových prvočísel naleznete zde:
[5] http://www.mersenne.org/prime.htm

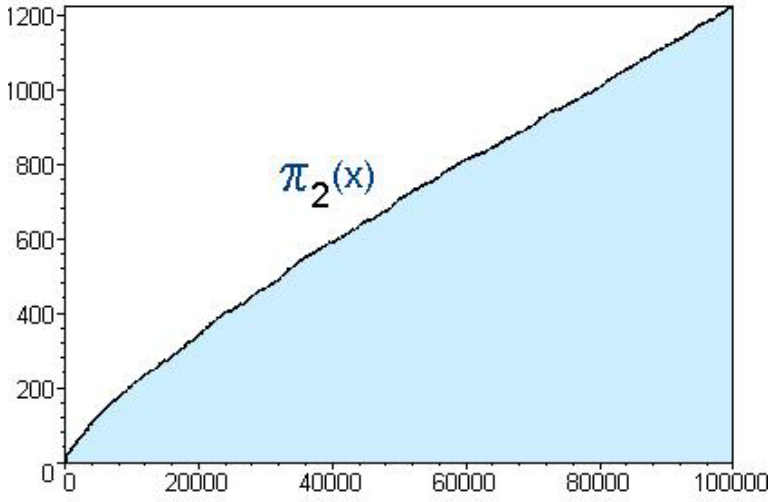
2. Prvočíselná dvojčata

Koncem května 2004 profesor Richard Arenstorf z Vanderbiltovy univerzity publikoval 38-ti stránkovou studii, ve které pomocí klasické číselné teorie dokazuje, že **prvočíselných dvojčat je nekonečně mnoho**. Podařilo se mu tak vyřešit jeden ze známých otevřených problémů teorie čísel.

O co v tomto problému šlo? Prvočíselný,í dvojčaty nazýváme taková prvočísla a,b, jejichž rozdíl je 2 . Tedy např. (3,5) , (5,7), (11,13), (29,31), ….(1 000 000 000 061, 1 000 000 000 063)…..

Asi vás ihned napadne, že najít „velká“ prvočíselná dvojčata je těžší a těžší. Jinými slovy - je jich stále méně a méně. Pomocí počítačů se podařilo najít opravdová „odrostlá dvojčátka“, která se dají napsat pomocí desítek tisíc dekadických cifer. Mezi největší známé prvočíselná dvojčata patří

361 700 055 * 2^{39020} +1 a 361 700 055 * 2^{39020} –1 (1999, H.Lifschitz)
665 551 035 * 2^{80025} +1 a 665 551 035 * 2^{80025} –1 (2000, Carmody, 24098 dekadických číslic)
33 218 925 * 2^{169690} +1 a 33 218 925 * 2^{169690} -1 (2002, 51090 dekadických číslic)



Počet prvočíselných dvojčat menších než x

Hledání prvočíselných dvojčat a stanovení jejich počtu se stalo otevřenou výzvou pro matematiky 20.století. Během století bylo vysloveno a výpočtem ověřeno několik odhadů, které se týkají výskytu prvočíselných dvojčat.

Hypotéza 1:
V intervalu <1,n> leží přibližně n/ $(\ln n)^2$ prvočíselných dvojic.

Hypotéza 2:.
Pro náhodně zvolené prvočíslo p z intervalu <1,n> je pravděpodobnost toho, že p+2 je také prvočíslo je : 1,32032*n / $(\ln n)^2$.

Výše uvedené odhady byly potvrzeny výpočtem pro velké soubory čísel. Odhady velice přesně korespondují s výpočty provedenými na PC.

Jako příklad si uvedeme shodu počtu předpověděných (P) a nalezených (N) prvočíselných dvojčat v různých intervalech délky 150 000.

Interval	P	N
100 000 000 , 100 150 000	584	601
1 000 000 000 , 1 000 150 000	461	466
10 000 000 000 , 10 000 150 000	374	389
100 000 000 000 , 100 000 150 000	309	276
1 000 000 000 000, 1 000 000 150 000	259	276
10 000 000 000 000, 10 000 000 150 000	221	208
100 000 000 000 000 , 100 000 000 150 000	191	186
1 000 000 000 000 000 , 1 000 000 000 150 000	166	161

Z výpočtu je zřejmé, že počet prvočíselných dvojčat „pravidelně“ klesá. Nabízí se tedy otázka, zda existuje nějaké velké číslo K, pro nějž platí, že všechna prvočíselná dvojčata jsou menší než tato konstanta. Jinými slovy, zda existuje pouze konečně mnoho prvočíselných dvojčat, nebo zda jich je nekonečné množství.

Hypotéza 3:.

Prvočíselných dvojčat je konečně mnoho.

Přiznávám, že předchozí úvaha, která vyústila ve formulaci hypotézy o konečnosti prvočíselných dvojčat, je poněkud zjednodušená a zavádějící. Obdobnou argumentaci bychom totiž mohli použít i na prvočísla. Také jejich počet s rostoucím n klesá a prvočísla jsou rozložena řidčeji a řidčeji. Přesto je velice jednoduché ukázat, že jich je nekonečně mnoho.

Věta : Prvočísel je nekonečně mnoho.
Důkaz sporem: Nechť je prvočísel konečně mnoho, označme jejich počet jako n. Sestrojme z těchto n prvočísel následující číslo: $p_1 * p_2 * p_3 *_{\dots} * p_n + 1$ (součin všech prvočísel + 1). Toto číslo je prvočíslo, ale je odlišné od všech n prvočísel. Prvočísel by tedy muselo být n +1 a to je spor s předpokladem, že prvočísel je n.

V čem je tedy rozdíl mezi prvočísly a prvočíselnými dvojčaty, že vznikla hypotéza o možné konečnosti počtu dvojčat? V čem se tak zásadně liší posloupnosti, které bychom vytvořili z prvočísel resp. prvočíselných dvojčat?

Významný rozdíl mezi posloupností všech prvočísel a posloupností prvočíselných dvojčat je v tom, že harmonická prvočíselná řada diverguje, ale řada složená ze všech prvočíselných dvojčat konverguje. Kupříkladu mezi prvočísly a přirozenými čísly není v tomto smyslu významný rozdíl, obě příslušné harmonické řady divergují.

Konveregenci harmonické řady prvočíselných dvojčat :
(1/3 + 1/5) + (1/5 + 1/7) + (1/11 + 1/13) + (1/17 + 1/19) + ... dokázal v roce 1919 matematik Brun.

Během dvacátého století byly objeveny jisté indicie, že by tato řada mohla být nekonečná a naše hypotéza 3 je pravděpodobně neplatná.

Součet řady byl nazván Brunova konstanta. V únoru 1999 stanovil Thomas Nicley hodnotu Brunovy konstanty na 1,902 160 582 3 … . Pro ty, kteří často pokládají otázku: „K čemu to je?“, odpovím jednou zajímavostí. Při výpočtech na odhadu této konstanty objevil Thomas Nicley chybu v procesoru Intel Pentium.

Vraťme se však k prvočíselným dvojčatům a k otázce jejich konečnosti či nekonečnosti.
V květnu 2004 profesor Richard Arenstorf ve své práci tento sto let starý problém s konečnou platností vyřešil.

Věta:.

Prvočíselných dvojčat je nekonečně mnoho.

Důkaz:
[1] Richard Arenstorf : There Are Infinitely Many Prime Twins ,
http://arxiv.org/PS_cache/math/pdf/0405/0405509.pdf
[2]http://www.math.vanderbilt.edu/faculty/Arenstorf.html .

3. Riemannova hypotéza

Na matematické konferenci v Paříži 24.5.2000 (podobně jako sto let předtím (8.8.1900), kdy David Hilbert vyhlásil program řešení otevřených problémů) CMI (Clay Mathematics Institut of Cambridge) vyhlásil sedm matematických problémů tisíciletí - "Millennium Prize Problems". Tentokráte je však připraven i fond se sedmi milióny dolarů. Za řešení každého z problémů je vypsána odměna a to jeden milión dolarů! Všeobecně se očekávalo, že nebudou vyplaceny příliš brzy. Přesto již téměř přesně po čtyřech letech oznámil Luis de Branges de Bourcia, profesor matematiky Purdueovy univerzity, že vyřešil čtvrtý z předložených problémů - tzv. Riemannovu hypotézu. Riemannova hypotéza souvisí s nulovými body Riemannovy zeta-funkce v komplexní rovině. Pokud bude potvrzeno, že v důkazu není chyba, může to mít obrovský dopad pro teorii prvočísel, speciálně při dokazování, zda je číslo prvočíslem.

Speciálně Miller v roce 1976 dokázal, že tzv. prvočíselnost (tj. určení zda je nebo není číslo prvočíslem) lze řešit v polynomiálním čase (G.L.Miller. Riemann´s hypothesis and tests for primality. J.Comput. Systém Sci, 1976)! Ovšem v důkazu předpokládal, že platí Riemannova hypotéza.

Pokud se chcete dozvědět něco více o prvním z problémů tisíciletí (zda platí P=NP a co znamená, že úloha je řešitelná nebo není řešitelná v polynomiálním čase), doporučuji čtyři roky starý článek z našeho e-zinu:
Vondruška,P: P=NP aneb jak si vydělat miliony, Crypto-World 9/2004,
http://www.crypto-world.info/casop2/crypto09_00.pdf .

Pokud jde o Riemannovu hypotézu, doporučuji originální článek Apology for the proof of the Riemann hypothesis od řešitele tohoto problému.
Michael Kanellos: Riemann hypothesis proven?, 9.6.2004, News Com,
http://news.com.com/Riemann+hypothesis+proven%3F/2100-7348_3-5229702.html
Louis de Branges de Bourcia : Apology for the proof of the Riemann hypothesis,
http://www.math.purdue.edu/ftp_pub/branges/apology.pdf

Poznámka (doplněno 30.6.2004):
Mathworld hedline news 30.6.2004 zveřejnil informaci o tom, že Riemannova hypotéza dokázána nebyla. Zpráva, která 8.6 a 9.6 obletěla celý svět a ze které jsem při přípravě tohoto článku vycházel je tedy mylná. Autoři doslova píší, že se jednalo o hodně povyku o ničem.
[3] http://mathworld.wolfram.com/

B. Statistický rozbor největšího prvočísla
RNDr. Petr Tesař, PVT PROKOM, a.s.

Na adrese http://mersenne.org/prime7.htm je dostupné dosud největší známé prvočíslo 2 na 24036583 - 1 (dále v textu také MP). Exponent tohoto prvočísla (24036583) je rovněž prvočíslo a je to tedy tzv. Mersennovo prvočíslo. MP je obrovské, jeho dekadický zápis má 7235733 cifer. Odborníci nicméně předpokládali, že by mohlo mít přes 10 miliónů cifer. Odměna 100.000 USD, kterou věnuje organizace Electronic Frontier Foundation za nalezení prvočísla k jehož zapsání bude potřeba 10 miliónu cifer tak stále ještě nebude vyplacena.

Pro lepší představu o jeho velikosti uvedeme, že při tisku (bold 10) zabere cca 380 stránek A4. Při zápisu do řady, kde jedna číslice je široká 1 mm a mezery mezi číslicemi zanedbáme, by bylo toto číslo více jak 7.2 km dlouhé. To je pro představu vzdušná vzdálenost z Petřínské rozhledny na náměstí v Horoměřicích. Příslušný exponent patří do souboru Mersennových prvočísel a je jedenačtyřicátým zjištěným zástupcem těchto v kryptologii velmi užitečných čísel..

Obdobně jako u prvního zjištěného megaprvočísla (prvočíslo s více jak miliónem cifer) byl proveden statistický rozbor, a byla položena otázka zda MP vykazuje ve svém dekadickém vyjádření nějaké statistické nepravidelnosti. Použitá metodika testování byla převzata z předchozího rozboru, který byl publikován v Crypto-Worldu č. 5/2000.

Dívejme se na naše prvočíslo jako na posloupnost znaků nula až devět. Celková délka této posloupnosti je 7 235 733 cifer.

Výskyt jednotlivých číslic je následující:

"0" = 722613, "1" = 723188, "2" = 722754, "3" = 722181, "4" = 723758,
"5" = 724196, "6" = 723856, "7" = 724543, "8" = 723551, "9" = 725093 .

.

Testujme hypotézu o rovnoměrném výskytu jednotlivých číslic pomocí známého χ-kvadrát kritéria. Hodnota statistiky je 10.272 . 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 3617866. Hodnoty χ-kvadrát kritéria a příslušné kritické hodnoty na hladině významnosti 0.05 a na hladině významnosti 0.01 jsou:

	Řetězové bigramy	Neřetězové bigramy
Hodnota statistiky =	119.187	94.827
Kritická hodnota na h.v. 0.05 =	113.145	123.225
Kritická hodnota na h.v. 0.01 =	128.299	134.642

Obě hypotézy se na hladině významnosti 0.01 přijímají. Nicméně hypotéza o rovnoměrném rozdělení řetězových bigramů je na hladině významnosti 0.05 zamítnuta. Hladina významnosti se volí typicky 0.05 nebo 0,01 s tím, že při 0.05 je testovací podmínka „přísnější“. Protože test řetězových bigramů vyhověl na hladině 0.01 a všechny ostatní testy dokonce na hladině významnosti 0.05, můžeme s malým přimhouřením oka hypotézu rovnoměrného výskytu cifer přijmout.

V kryptologii se jako kritérium nerovnoměrnosti používá index coincidence (IC), což je zhruba řečeno - součet kvadrátů relativních četností všech hodnot znaků. Rovnoměrně rozdělená posloupnost z deseti různých znaků má IC okolo hodnoty 0.1. Pro naši posloupnost bylo vypočteno IC = 0.1000000176. Kritická hodnota na hladině významnosti 0.05 je 0.1000000965. 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.

Délka opakovaného řetězce	Pravděpodobnost výskytu alespoň jednoho opakování
10	1 - (E-1136)
11	1 - (E-113)
12	1 - 4.3E-12
13	0.9270
14	0.2303
15	0.0258
16	0.0026

V další tabulce jsou konkrétní počty opakování zjištěné v MP:

Délka opakovaného řetězce	Počet opakování
10	2048
11	371
12	36
13	3
14	1
15 a více	0

Nejdelší opakující se řetězec má délku 14 cifer a to: " **9 0 6 0 4 4 3 2 9 5 9 8 2 1** ".
První výskyt je na 4 493 327 řádu (umístění nejpravější jedničky). Druhý výskyt je na 4 788 086 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.

C. Program STORK - vstupní dokumenty, příprava E-CRYPT Část 2

Jaroslav Pinkava, PVT a.s.

1. Úvod

V první části článku o nové evropské iniciativě v kryptografické problematice **E-CRYPT**. (http://www.stork.eu.org/documents.html) byl zmíněn výchozí roční projekt **STORK** (začal v červenci roku 2003), který byl součástí pátého rámcového programu a kde byly zpracovány vstupní dokumenty:

1. New trends in Cryptology
2. Research agenda for the Future of Cryptology
3. Open Problems in Cryptology,

publikovány byly v květnu a červnu 2003 (viz lit. [2], [3], [4]).
Každý ze tří výše zmíněných dokumentů (pro jednoduchost dalších odkazů, které budou časté, je označíme – v té posloupnosti, jak jsou výše uvedeny - jako materiály **M1, M2, M3**) má obdobnou strukturu:

1. Úvodní kapitola
2. Kryptografie v informační společnosti
3. Kryptografické protokoly
4. Kryptografické techniky
5. Matematické základy

V první části článku byly popsány problematiky – kryptografie v informační společnosti + kryptografické protokoly. V této druhé části článku bude popsána problematika kryptografických technik a problematika matematických základů kryptografie.

2. Kryptografické techniky

Materiál M1 je členěn v této kapitole následovně:

4.1 Symetrická kryptografie
4.2 Asymetrická kryptografie
4.3 Implementační aspekty a realizace
4.4 Některé techniky útoků

K bodu 4.1: Nejprve se autoři zmiňují o základních podstatných rozdílech mezi proudovými a blokovými šiframi. *Blokové šifry* jsou obvykle pomalejší a jsou složitější v implementaci. Jsou však podstatně flexibilnější, umožňují použití různých módů a konec konců mohou i fungovat v módu proudové šifry, zatímco obráceně to možné není. Jsou zde zmíněny významní reprezentanti – DES, AES resp. další jako Triple-DES, IDEA, RC5 atd. Norma DES byla používána od roku 1977, za dobu své existence měla velký význam pro rozvoj různých technik konstrukce obdobných algoritmů i technik kryptoanalýzy (diferenciální a lineární kryptoanalýza ale i další - jako útoky pomocí vyšších diferencí, interpolační útoky, některé statistické metody a také útoky proti klíčovým schématům). Je zde poznamenáno, že v

současné době neexistuje přístup, který by umožnil využít některou z popsaných cest vzhledem k algoritmu AES. Je to dáno především tím, že AES využívá kombinace různých algebraických struktur. V posledních letech jsou také vyvíjeny techniky tzv. nepodmíněných bezpečných důkazů (unconditional security proof techniques), které mají za cíl zhodnotit určitou část konstrukce blokové šifry (resp. módu). Zde je nějaká úroveň kryptografická konstrukce modelována jako pseudonáhodná funkce (permutace) a její chování je pak porovnáváno s ideální náhodnou funkcí (permutací).

Přestože tedy existuje celá řada hodnotících postupů, soudí autoři materiálu, že – např. ve srovnání s kryptografií veřejného klíče – je zde ještě stále mnoho problémů, kterými je třeba se z hlediska výzkumu zabývat. Jsou zde jmenovány:

- současný stav bezpečnostních důkazů (existují pouze částečné techniky);
- samotné AES je třeba hlouběji analyzovat , rozšíření algebraických a statistických technik;
- přestože již bylo publikováno více schémat blokových šifer, jsou svou konstrukcí obdobné a ne dostatečným způsobem různorodé;
- studium módů šifer si také vyžaduje hlubší pozornost (mj. bezpečnostní modely ve smyslu paradigmatu Luby-Rackoff).

Dále se zde autoři zabývají *proudovými šiframi*, které nacházejí své použití především v různých telekomunikačních aplikacích (mobilní telefony, radia), kde je snaha minimalizovat hardwarové nároky (GSM, GPRS). Zmíněn je proprietární algoritmus RC4 (společnost RSA), který je často takto používán nebo jsou zmíněny další algoritmy jako SEAL, SCREAM a SNOW. Řada proudových šifer svou konstrukcí vychází z využití lineárních registrů se zpětnou vazbou, kde jsou garantovány globální statistické vlastnosti a délka periody. Existuje zde dnes celá řada zvažovaných útoků (korelační útoky, útok "rozděl a panuj" a další). V projektu NESSIE se ukázalo, že všechny zde navrhované proudové šifry byly zranitelnější více než se původně předpokládalo (např. SEAT verze 3 byla rozbita úplně).

Důležitou podtřídou jsou *samosynchronizující se proudové šifry*, které jsou odolné vůči chybám jednotlivých bitů při přenosu dat. Jediným zde rozšířeným praktickým příkladem je CFB mód blokové šifry.

Do tohoto odstavce patří i postupy pro *generování pseudonáhodných čísel* (pseudonáhodných binárních posloupností). Klíčovým je pojem pseudonáhodného generátoru (PRNG) definovaný následovně:

- číslo x_0 (seed);
- iterace $x_i = f(x_{i-1}),\ i = 1,...,n$
- výstupní posloupnost $b(x_1), b(x_2),...,b(x_n)$.

Existují specifické požadavky na konstrukce takovýchto PRNG, teorie ukázala na jejich blízký vztah k existenci jednosměrné funkce. Existujícími příklady prokazatelně bezpečných PRNG (za určitých předpokladů) jsou generátory jako Blum-Blum-Shubův generátor či generátor Blum-Micali. Bloková šifra v čítačovém módu (counter mode) je také příkladem prokazatelně bezpečného PRNG.

Pseudonáhodné funkce (PRF) se opírají i o použití klíče, zobrazují obecně n bitů na m bitů. Jsou vlastně určitým zobecněním pojmu bloková šifra (bloková šifra je PRF při $n=m$). Nachází využití v rámci některých protokolů typu výzva-odpověď, při konstrukcích náhodných řetězců, při tvorbě kryptografických hashů a autentizačních kódů atd.

Speciální třídu tvoří *kryptografické hashovací funkce*. V dnešní kryptografii jsou široce používány (vytváření otisků zprávy – message digest). Jejich použití zaručuje datům jejich integritu a to je důležité pro celou řadu aplikací, příkladem jsou schémata digitálních podpisů.

Při analýze těchto funkcí existuje rovněž celá řada důležitých otevřených problémů (prokazatelná bezpečnost, vztah ke konstrukcím blokových šifer atd.).

Poslední zde zmíněnou třídu kryptografických primitivů tvoří *autentizační kódy zpráv* (MAC – message authentication codes). Je to vlastně určitá speciální podtřída hashovacích funkcí, podstatnou vlastností je zde závislost na klíči.

K bodu 4.2: Díky různým normotvorným iniciativám (RSA PKCS, ISO, IEEE P1363, CRYPTREC, NESSIE) by se zdálo, že problematika *asymetrické kryptografie* je vyřešena. Klíčový pojem bezpečnosti těchto šifer však zůstává stále nedořešenou otázkou. V podstatě je dnes řešena standardním postupem – převodem na poukázání výpočetní složitosti nebo obtížnosti řešení nějakého známého algoritmického problému (faktorizace, diskrétní logaritmus atd.). Status této výpočetní složitosti však podléhá dynamickým změnám a je často obtížné srovnávat různé typy algoritmů (např. právě složitost faktorizace a složitost výpočtu diskrétního logaritmu). Pro řešení těchto otázek byl zkonstruován (Bellare a Rogaway) model náhodného oráklu. Není to však univerzální prostředek pro řešení nastolených otázek.
Nejvíce používané schéma – kryptosystém RSA – má dnes již celou řadu alternativ a právě hledání a analýza těchto alternativ je dnes hlavním předmětem výzkumu. Důvodů je několik (je dobré mít k dipozici různé typy schémat, problematickým momentem je požadovaná délka klíče pro RSA – dnes minimálně 1024 bitů, pro dlouhodobé aplikace ještě podstatně větší, efektivnost implementací).

Jsou tedy hledány schémata s kratší požadovanou délkou klíče. Příkladem je eliptická kryptografie, schémata XTR, LUC. Existuje snaha vytvořit svým způsobem "ideální konstrukci" založenu na NP-těžkých úlohách. Příkladem je NTRU či obdobné mřížové systémy (ale – poznámka autora – nedávno bylo prokázáno, že NTRU lze řešit pomocí kvantového počítače, zatímco totéž neplatí pro NP-těžké úlohy obecně), dále schémata opírající se o NP-těžké úlohy z teorie kódů – McEliece/Niederreiter či schémata založená na polynomiálních rovnicích s více proměnnými v konečných tělesech (Matsumoto-Imai). Ve všech těchto modelech však délka klíče není zanedbatelná a např. konkurenceschopná ve srovnání s eliptickou kryptografií.

Důležitou součástí asymetrické kryptografie je problematika *digitálních podpisů.* Význam bezpečnosti, který je problematický pro celou asymetrickou kryptografii (viz výše) zde má ještě komplikovanější situaci. Důležitým pojmem je zde *nepopiratelnost*, ten kdo podepíše zprávu, nesmí později tento podpis popřít. Je však poměrně složité provést odpovídající bezpečnostní analýzu tohoto pojmu a materiál konstatuje, že to nebylo dosud vyhovujícím způsobem provedeno. Dnes je pro podpis používáno nejčastěji schéma RSA. Jsou hledány alternativní řešení (eliptické křivky, NTRU,..) založená na efektivnějších operacích (ve srovnání s modulárním umocňováním pro RSA).

V řadě aplikací je vhodné použít digitální podpisy se specifickými vlastnostmi (např. následující typy podpisů – signature – proxy, designated-verifier, undeniable, blind, ring/goup, short, identity-based).

K bodu 4.3: Problematika *implementací je* samozřejmě klíčovou otázkou pro nasazení v praktických aplikacích. Autoři rozlišují tři základní typy platforem:

- softwarové implementace využívající HW obecného určení;
- implementace na bázi speciálního HW (ASIC, FPGA);
- "zapuštěné" softwarové implementace (např. čipové karty).

Základním nezbytně zvažovaným aspektem bezpečnosti implementací je skutečnost, že zde dochází k určitým typům úniků informací (příkladem jsou postranní kanály).

Při práci s HW samozřejmě sledovaným momentem je jeho efektivnost. Např. programovatelná pole (FPGA) mají oproti speciálním integrovaným obvodům (ASIC) několik výhod – nižší cena výchozího návrhu, možnost změn návrhu, na druhou stranu však mají vyšší spotřebu energie a vyšší cenu na jednotku.

Stejně tak softwarové implementace jsou posuzovány z hlediska jejich efektivnosti. Náročnost některých kryptoschémat je v tomto směru značná. Jako příklad je uváděno RSA, kde podle autorů je reálné, že v nepříliš vzdálené budoucnosti bude požadována délka klíče 3072-4096 bitů. Samozřejmě rychlé implementace jak v SW tak i v HW budou vždy výhodnější cestou.

Technologie čipových karet je dnes stále důležitější oblastí kryptografických aplikací. Je zde řešena celá řada souvisejících specifických otázek v návaznosti na vlastnosti implementací a efektivnosti těchto implementací. Příkladem je použití kryptografických koprocesorů, jejichž cílem je rychlé zpracování modulárních násobků (algoritmy Montgomery, Sedlak, aj.). Dnešní využití čipových karet v širších PKI modelech přináší rovněž potřebu řešit další specifické otázky (GSM SIM karty, WAP Identity module, Mastercard a VISA – EMV atd.).

K bodu 4.4: Analýza postranních kanálů vyžaduje znalosti několika oborů – elektronika, kryptografie, zpracování signálu a statistika. Dnes jsou zejména známy následující typy útoků : DPA (diferenciální analýza spotřeby proudu), její varianta SPA a také analýza časů. V posledním období se objevuje také elektromagnetická analýza, má stejné techniky jako DPA či SPA, ale jsou zde měřeny jiné veličiny. Tyto útoky jsou směrovány jak na implementace blokových šifer, tak i hashovacích funkcí a stejně tak i na asymetrickou kryptografii. Stále jsou rozpracovávány různé (maskovací) techniky jak čelit těmto útokům. Bohužel složitější přístupy pro útoky z postranních kanálů jsou stále úspěšné a dokáží překonat veškeré známé ochranné techniky a je tudíž nezbytná v tomto směru budoucí hluboká spolupráce kryptografických a inženýrských specialistů.

Kromě pasivních útoků (podstata spočívá v měření nějakých veličin) existují i aktivní modely útoků – záměrná vyvolání chyb, poruch. V současnosti v podstatě chybí detailní analýza příslušných s tím souvisejících teoreticko-bezpečnostních vlastností.

V závěru kapitoly jsou zmíněny některé specifické techniky. Mezi ně patří (zatím ještě diskutované – z hlediska reálnosti) využití kvantových počítačů. Kvantová teorie informací naproti tomu již v kryptografii své pevné místo nachází (příkladem – pozn. autora – je spuštění první počítačové sítě používají kvantovou kryptografii). pro kryptoanalýzu je důležité zvážit i možnosti za tímto účelem speciálně vyvinutého HW (známým příkladem je EFF DES key search machine, zařízení, které v roce 1998 našlo klíč DES pro výzvu firmy RSA -RSA DES Challenge - za 56 hodin). Jiným příkladem je známé Shamirovo TWINKLE, které směřovalo na kryptoanalýzu algoritmu RSA (prezentováno poprvé v rump session na Eurocryptu 1999 v Praze). V posledních letech se objevila celá řada dalších návrhů v tomto směru (využití FPGA, Bernsteinův návrh pro řešení maticového kroku v algoritmu síta číselného tělesa, němečtí autoři Geiselman a Steinwandt atd.). Autoři materiálu soudí, že tyto návrhy svým způsobem povedou k ohrožení bezpečnosti RSA s délkou klíče 1024 bitů.

Materiál M2 je členěn shodným způsobem:

4.1 Symetrická kryptografie
4.2 Asymetrická kryptografie
4.3 Implementační aspekty a realizace
4.4 Některé techniky útoků

K bodu 4.1: Jako stěžejní oblast výzkumu pro blokové šifry je zde zmíněna kryptoanalýza AES a obdobných blokových šifer. Dnes existují určité heuristické důkazy, že proti AES není diferenční a lineární kryptoanalýza aplikovatelná, přesto na nezbytnost dalších analýz v tomto směru kladou autoři materiálu velký důraz. Další doporučenou oblastí výzkumu jsou postupy vedoucích k novým cestám při navrhování konstrukčních částí blokových šifer. Ve vztahu ke kryptoanalýze je zde zmíněn (kromě postupů, které lze převést z kryptoanalýza blokových šifer) útok autorů Courtois a Meier. Potřeba nových algoritmů proudových šifer (vycházejících např. z algoritmů SCREAM a SNOW v.2 pro softwarová řešení) je vysoce aktuální (zejména pro návrh HW řešení). Zmíněna je zde také problematika samosynchronizujících se proudových šifer, i když je zde poukázáno na to, že není jasná jejich aktuální potřeba v praxi.

Pro generátory náhodných znaků (PRNG) existuje volné pole výzkumu zejména pro analýzu bezpečnosti generátorů vycházejících z kryptografických primitivů. Zatímco pro PRNG opírající se o modely z teorie čísel byly řada výsledků již získána, pro primitivy opírající se např. o blokovou šifru obdobné bezpečnostní důkazy chybí. Totéž se týká i pseudonáhodných funkcí.

Představitelem nové cesty konstrukcí hashovacích funkcí je algoritmus Whirlpool (iniciativa NESSIE). Jsou zkoumány návrhy hashovacích funkcí, které se opírají o využití algoritmu blokové šifry. Existuje zde řada dalších důležitých výzkumných problémů (otázky kolizí, důkazy bezpečnosti,...).

Pro autentizační kódy zpráv (MAC) je doporučováno hledání cest pro navrhování nových typů algoritmů. Dále je to obdobně problematika důkazů bezpečnosti, vztah k blokovým šifrám atd.

Operačními módy se výzkum začal intenzivněji zabývat teprve v posledních několika letech. Existující důkazy bezpečnosti však nelze stále považovat za uspokojující, zejména vzhledem k používaným v praxi produktům. Jsou také zkoumány nové návrhy módů.

K bodu 4.2: Model náhodného oráklu je pro prokazování bezpečnosti ústředním pojmem. S tím souvisí i několik autory doporučených teoretických otázek, na které dnes zatím odpovědi neexistují. Např. Cramer-Shoupův kryptosystém je prokazatelně bezpečný na základě rozhodovacího předpokladu: Existuje obdobný efektivní kryptosystém prokazatelně bezpečný na základě výpočetního předpokladu (v obou případech bez využití náhodného oráklu)?
Alternativy RSA – jak je to s jejich výpočetními předpoklady? Lze nalézt nová alternativní schémata dostatečně výpočetně efektivní nebo nalézt nové výpočetně obtížné problémy, které by byly použitelné pro kryptografii?

A také samozřejmě ve vztahu ke kvantovým počítačům – nalézt v tomto smyslu odolné kryptografické primitivy.

Zájem je i na vývoji různých speciálních kryptografických asymetrických technik (homomorfní schémata, schéma Boneh-Franklina, schémata opírající se o totožnost,...).
Co s týká digitálních podpisů, zde např. v současné době existuje pouze jediné prokazatelně bezpečné schéma v standardním modelu (vychází z RSA). Je otázkou zda existují jiná taková schémata (použitelná v praxi). Podpisová schémata alternativních konstrukcí (oproti RSA) s celou řadou různorodých požadovaných vlastností vzhledem k dokazování bezpečnosti stále chybí.

K bodu 4.3: Efektivní HW je dnes vyvinut pro konstrukci schémat RSA resp. DSA. Je zmíněna potřeba obdobného vývoje pro další třídy schémat (eliptické křivky, mřížové algoritmy, uzlíčkové šifry). Také vývoj algoritmů vhodných zejména pro HW implementace je doporučovaným předmětem výzkumných prací. To se týká i postupů používaných pro čipové karty (příkladem zde použitým je RSA s větší délkou klíče – 2048 bitů).

K bodu 4.4: Útoky z postranních kanálů jsou dnes velmi vážnou hrozbou v řadě aplikací, souvisí samozřejmě s použitou implementací. V počátečním stadiu jsou analýzy opírající se o využití elektromagnetického vyzařování. Neexistují postupy (maskovací techniky) odolávající útokům používajících korelací vyšších řádů. Z hlediska praxe není jasný vztah mezi maskovacími technikami booleovského a aritmetického typu. Zajímavým výzkumným směrem je také zkoumání existence odpovídajících bezpečnostních důkazů ve vztahu k únikům informací z postranních kanálů.

Vynucované chyby – z hlediska bezpečnostních vlastností (např. při prokazování bezpečnosti) jsou zatím velice málo brány na zřetel.

Kvantová teorie a kryptografie – zde existuje celá řada zajímavých oblastí výzkumu. Dopad existence reálného kvantového počítače na dnešní kryptografii byl již zmíněn. Důsledkem neexistence kvantového bit-commitment je existence větších možností eventuálního "kvantového" útočníka. Kvantová kryptografie směřuje již do praxe, samozřejmě zde existuje celá řada otázek (protokoly, implementační technologie,...). Jsou zkoumány možnosti využít v kryptografii další kvantové postupy (teleportace, ...).

Materiál M3 je členěn v této kapitole následovně:

4.1 Symetrická kryptologie
4.2 Asymetrická kryptografie
4.3 Implementační aspekty a realizace
4.4 Speciální techniky útoků

K bodu 4.1: Zmíněno:

- studium AES – odolnost proti útokům, bezpečnostní důkazy, analýza algebraické struktury AES, kombinace existujících přístupů k útokům, kvadratické rovnice (přístup, který navrhl Pieprzyk)
- studium ostatních typů blokových šifer - návrhy konstrukce, S-boxy, optimální počty iterací, odolnost proti útokům z postranních kanálů atd.

Co se týká proudových šifer, NESSIE v tomto směru neuspěla, návrh moderní proudové šifry, který by vyhovoval současným požadavkům je vysoce aktuální otázkou.
Pro náhodné generátory – žádoucí by např. bylo odvození náhodného generátoru ze symetrického primitivu a to tak, že pokud budeme schopni odlišit výstup z PRNG od náhodného výstupu, zároveň to povede k rozbití příslušného symetrického primitivu.

Pro hashovací funkce – žádoucí je další analýza rodiny hashovacích funkcí SHA, dále např. analýza bezpečnostních důkazů v modelu náhodného oráklu atd.
Několik zajímavých otevřených otázek jmenují autoři v návaznosti na problematiku operačních módů (tzv. "tweakable" blokové šifry, módy vhodné pro šifrování sektorů na disku,...).

K bodu 4.2: Pojem prokazatelné bezpečnosti ovlivňuje stále více celou asymetrickou kryptografii. Pojem sám však navozuje celou řadu s ním souvisejících a doposud nevyřešených otázek. Uspokojujícím není také stav současných modelů a ani nebyla vyřešena otázka existence některých schémat. Např. mezi otevřené otázky patří nalezení prokazatelně bezpečného schématu, které by vycházelo z RSA či z úlohy faktorizace a další. Hledání alternativ k RSA je i pro praxi vysoce důležitou otázkou (délka klíče RSA – nároky se stále zvyšují). Prokazatelně bezpečné podpisové schéma (opírající se o RSA či DL) je v oblasti podpisových schémat také otevřenou výzkumnou otázkou a stejně tak i hledání alternativ k RSA.

K bodu 4.3: Kromě ASIC a FPGA se objevují další nové HW platformy (rekonfigurovatelná zařízení obsahující programovatelný procesor aj.). Optimalizační přístupy pro implementace na takovýchto HW platformách jsou intenzivně studovány. Stejně tak je analýze podrobována (z řady úhlů) bezpečnost těchto implementací. Zmíněna je např. problematika bezkontaktních čipových karet. Problematika samotných čipových karet obsahuje řadu otázek, které souvisí s implementací kryptografických algoritmů (generování klíče na kartě, bezpečnost implementace, optimalizace z hlediska výkonu, testovací postupy, atd.).

K bodu 4.4: Zde je citována zejména otázka postranních kanálů, útoků z nich a odpovídajících protiopatření. Rovněž tak i aktivní útoky vyžadují pozornost kryptografické veřejnosti.

¨ Kvantová teorie je bohatým zdrojem nových problémů pro kryptografii. Otevřené otázky se týkají samozřejmě existence kvantových počítačů, vývoje algoritmů pro tyto počítače a dopadu vlastností těchto algoritmů na celou dnešní "klasickou" kryptografii.
V kvantové kryptografii také nebylo řečeno závěrečné slovo. Objevují se nové protokoly a i dřívější návrhy vyžadují pečlivou bezpečnostní analýzu.

Kvantová teleportace je použitelná např. pro konstrukci schématu, které je obdobné jednorázovému heslu.

Poslední slovo nepochybně neřekly konstrukce speciálního HW pro použití v kryptoanalytických postupech.

3. Matematické základy

Problematika je rozdělena (**materiál M1**) následovně:

5.1 Teorie výpočtů
5.2 Kombinatorika v konečných tělesech
5.3 Algoritmická teorie čísel
5.4 Kombinatorická teorie grup

K bodu 5.1: *Teorie výpočetní složitosti* z hlediska kryptografie může dát odpověď na její základní otázku: Je bezpečná kryptografie z teoretického hlediska možná? Kryptografie vyžaduje existenci jednosměrných funkcí, funkce, které jdou snadno spočítat, ale je obtížné je invertovat. Existence jednosměrných funkcí implikuje, že P ≠ NP a byla by tak vyřešena jedna z nejobtížnějších otázek teorie výpočtů. Bohužel zatím jsme stále daleko od důkazu existence takovýchto funkcí a také zatím více-méně troskotá snaha vytvářet kryptografii založenou na NP-těžkých úlohách.

Existuje však již dnes celá řada dílčích vazeb mezi kryptografií a teorií výpočtů (modely založené na předpokladu, že jednosměrná funkce existuje, vztahy různých předpokladů v asymetrické kryptografii, techniky nulových znalostí, analýza protokolů,...).

Vztah *teorie informace* a kryptografie je datován od doby vzniku dnes již klasické Shannonovy práce (40 léta minulého století). V posledních dvaceti letech zde však byla získána celá řada dalších zajímavých výsledků. Souvisí např. s protokoly pro nepodmíněnou bezpečnou výměnu klíčů a distribuci klíčů či obecněji pro problém výpočtů více stran (multiparty computation).

K bodu 5.2: *Konečná tělesa* se objevují v celé řadě kryptografických problematik. Příkladem jsou eliptické křivky, schémata pro sdílení klíčů, S-boxy blokových šifer, okruh modulo součin dvou prvočísel (algoritmus RSA) atd. V posledních letech byla řada nových výsledků získána zejména v návaznosti na konstrukce S-boxů blokových šifer (studium nelinearity).

K bodu 5.3: Problém *faktorizace* celého čísla je dnes pravděpodobně nejznámějším problémem *algoritmické teorie čísel*. Nejrychlejším dnešním algoritmem zůstává síto číselného tělesa (NFS – Number Field Sieve). Tento algoritmus má několik částí, každá z nich je podrobována důkladné analýze a v posledních letech zde došlo k celé řadě vylepšení. Blízkou úlohou je úloha řešení *diskrétního logaritmu*. Také zde hlavní roli hrají algoritmy síto tělesa funkcí a síto číselného tělesa.

Algebraické křivky nad konečnými tělesy vstoupily do kryptografie díky eliptické kryptografii (resp. dnes je to i hypereliptická kryptografie). Výzkum je orientován na tyto úlohy: výpočet řádu bodu (kardinalita jakobiánu), algoritmy pro řešení diskrétního logaritmu (některé speciální typy křivek byly takto "rozbity"), párování – velice zajímavá nová oblast kryptografie se zajímavými aplikacemi – např. tzv. kryptografie veřejných klíčů založená na totožnosti (identity-based), hypereliptické křivky.
V materiálu jsou zmíněny i další oblasti algoritmické teorie čísel – *geometrie čísel*, *systémy opírající se o polynomiální rovnice více proměnných*.

K bodu 5.4: Vzhledem k známému Shorovu algoritmu, který pomocí kvantového počítače rozbíjí RSA (a existují obdobné algoritmy rozbíjející další systémy s veřejným klíčem) je samozřejmě důležitým probléme nalézt takové kryptografické systémy s veřejným klíčem, které by odolaly útokům vedeným s pomocí kvantových počítačů (sic!). Autoři v této souvislosti zmiňují několik možných cest.

Materiál M2 členěn následovně:

5.1 Teorie výpočtů
5.2 Teorie informace
5.3 Algoritmická teorie čísel
5.4 Kombinatorika v konečných tělesech
5.5 Kombinatorická teorie grup

K bodu 5.1: Dlouhodobým cílem je samozřejmě otázka zda platí nerovnice $P \neq NP$. Zatím však jsme od tohoto cíle asi hodně vzdáleni. Existuje však i řada konkrétnějších otázek. Autoři zde zmiňují např. konstrukce kryptografických primitivů z jednosměrných funkcí (pseudonáhodné generátory a podpisová schémata), únik informací z různých konkrétních jednosměrných funkcí, analýza nedávno publikovaných nových kryptosystémů (RSAP, Pointcheval), protokoly,

K bodu 5.2: Zde autoři hovoří o problematice dlouhodobé bezpečnosti používaných kryptografických technik a potřebě bezpečnosti používaných protokolů, studiu univerzálních hashovacích funkcí a dalších otázkách.

K bodu 5.3: V algoritmické teorii čísel je velkým existujícím problémem bezpečnost RSA a DL (diskrétního logaritmu) v konečných tělesech a na eliptických křivkách (resp. nalezení úspěšného útoku). Stanovení řádu hyperelipticých křivek je doposud úspěšně řešeno jen částečně. Jsou hledány další grupy, kde by bylo možné využití kryptografie založené na DL.
Polynomy více proměnných (algoritmy Sflash a Quartz v NESSIE) jsou zatím z hlediska využití v kryptologii málo prozkoumány. V algoritmu NTRU není dořešena k plné spokojenosti otázka podpisového schématu. Existují další přístupy ke konstrukci algoritmů s veřejným klíčem (problém batohu, Poly cracker, uzlíčkové algoritmy,..), je otázkou nakolik důležitým bude jejich budoucí přínos.

K bodu 5.4: Problematika konstrukce S-boxů s těmi či jinými pro kryptografii důležitými vlastnostmi stále zaměstnává hlavy odborníků. V budoucnu bude existovat řada nových myšlenek vztahujících se k útokům na blokové šifry, budou mít nepochybně dopad na konstrukční kriteria. Zajímavá je souvislost S-boxů a permutačních polynomů.

K bodu 5.5: Kombinatorická teorie grup se v současné době zdá být vhodným kandidátem pro konstrukci nových kryptografických systémů s veřejným klíčem. Existuje několik návrhů, ale výzkumy jsou teprve v počátcích.

Materiál M3 je členěn následovně:

5.1 Teorie výpočetní složitosti
5.2 Teorie informace
5.3 Algoritmická teorie čísel
5.4 Kombinatorika v konečných tělesech

K bodu 5.1: Kromě otázky P ≠ NP je zde jmenováno 10 konkrétnějších otázek. Např.

- zkonstruujte funkci f, pro kterou poměr složitostí výpočtu f a f^{-1} je větší než konstanta,
- stanovte "přesný" vztah výpočetní složitosti úlohy faktorizace a úlohy diskrétního logaritmu.

K bodu 5.2: Výčet otevřených problému zahrnuje např. otázku vztahu klasické a kvantové teorie z několika hledisek (např. generování společného klíče, dohoda na klíči).

K bodu 5.3: Mezi konstruktivními problémy jsou jmenovány např.:

- otázka důkazu, že systémy v praxi používané jsou skutečně odolné proti útokům;
- nalezení výkonnějších současných i navrhovaných systémů;

Z hlediska kryptoanalýzy existuje celá řada nedořešených otázek:

- analýza existujících systémů;
- odolnost proti útokům z postranních kanálů;

a dlouhá řada konkrétních problémů souvisejících s jednotlivými schématy.

K bodu 5.4: V této oblasti jsou očekávány i výsledky nových typů, např. nové kryptosystémy, nové techniky pro analýzu blokových šifer, dále hlubší studium S-boxů atd.

Závěr:

Lze dnes asi těžko odhadnout, která z citovaných oblastí kryptologie se bude vyvíjet (z hlediska dosažených výzkumných výsledků) rychleji či kde to naopak potrvá a nové teoretické skutečnosti se objeví později. Materiály STORK však jsou významným inspiračním zdrojem pro současné i budoucí generace kryptologů.

Literatura:

[1] Information Society Technologies, 2003-2004 Workprogramme, http://www.stork.eu.org/FP6/SP1-Priority-2-ist.doc
[2] http://www.stork.eu.org/documents/ENS-D4-1_4.pdf
[3] http://www.stork.eu.org/documents/RUB-D5-2_1.pdf
[4] http://www.stork.eu.org/documents/RUB-D6-2_1.pdf
[5] http://www.stork.eu.org/documents/KUL-D2_3-1_11.pdf
[6] Birjukov, Alex: Block Ciphers and Stream Ciphers: The State of the Art, http://eprint.iacr.org/2004/094.pdf

D. Letem šifrovým světem

Průběžně můžete sledovat novinky a zajímavosti ze světa kryptografie, informační bezpečnosti a příslušných standardů na http://www.crypto-world.info/news/index.php . Novinky v tomto měsíci pro vás již tradičně vybrali : Vlastimil Klíma, Jaroslav Pinkava, Tomáš Rosa a Pavel Vondruška.

Přístupy k novinkám se začátkem měsíce června ustálily na 200 denně a hojně začal být využíván RSS kanál. Novinky ze stránky Crypto-Worldu jsou pravidelně přebírány i na informačním portálu : http://www.pravednes.cz/index.jsp?panel=secur v sekci Bezpečnost.

Výběr z novinek, které byly v tomto období nejčtenější

Zajímavý e-volební systém umožňující kontrolu bez odhalení hlasu

http://news.com.com/2100-1028-5227789.html

Kryptolog a vynálezce tohoto systému David Chaum použil dva proužky papíru a kryptolografii k tomu, aby si volič mohl ověřit, zda jeho hlas byl nebo nebyl ve volbách zmanipulován. Systém byl poprvé předveden na konferenci E-voting. Problém následné manipulace s elektronickými hlasy nebyl dosud úspěšně vyřešen. Chaum založil firmu, která má prodávat HW. Bohužel ani tento systém neřeší všechny problémy spojené s e-volbami. Je to však zajímavý krůček dopředu.

Riemann hypothesis proven? (By Michael Kanellos).

http://news.com.com/Riemann+hypothesis+proven%3F/2100-7348_3-5229702.html

Mathematician at Purdue University claims to have come up with a proof for the Riemann hypothesis, often called the greatest unsolved math problem, though the work has yet to be peer-reviewed.

Více k tomuto tématu viz úvodní článek tohoto e-zinu.

Bezdrátové sítě a penetrační testy

http://www.securityfocus.com/infocus/1783

První část třídílného seriálu věnovaného nové problematice - penetračním testům v bezdrátových sítích. Jsou zde popsány tři základní typy útoků a některé další specifické momenty, které by měl brát na zřetel administrátor bezdrátové sítě. V připravované druhé části by některé hackerské techniky měly být popsány důkladněji a zároveň by zde mělo být objasněno jak identifikovat a využít slabá místa.

Neodborná instalace podnikových bezdrátových sítí bezpečnostním problémem

http://www.theregister.co.uk/2004/06/10/wlan_security_gartner/

Podnikové bezdrátové sítě budou v nejbližších několika letech bezpečnostním problémem. I přes přípravu zlepšených bezpečnostních standardů zůstává totiž hlavním problémem neodpovídající politika a neodborná instalace. Hackeři se mohou do sítí dostat přes nechráněné přístupové body a budou těžko detekovatelní.

Ztracené notebooky obsahují neuvěřitelné poklady

http://www.pointsec.com/news/news_pressrelease.asp?PressID=2004_June_8

Například přístupová hesla s administrátorskými právy k bezpečnému intranetu jedné z největších evropských finančních institucí (tohle konkrétně stálo pět liber) a tuny dalších informací. Průzkum prováděla společnost Pointsec Mobile Technologies, která v aukcích nakupovala notebooky ze ztrát a nálezů například z letišť apod.

O čem jsme psali v červnu 2000 - 2003

Crypto-World 6/2000

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

Crypto-World 6/2001

Příloha : priloha6.zip

(fotografie Security 2001, témata přednášek na konferenci Eurocrypt´2001)

Crypto-World 6/2002

Crypto-World 6/2003

E. Závěrečné informace

1. Sešit

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

Články neprocházejí jazykovou kontrolou!

Adresa URL, na níž můžete najít tento sešit (nejdříve 21 dní po jeho rozeslání) a předchozí sešity GCUCMP, informace o přednáškách z kryptologie na MFF UK, některé články a další související témata :

http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci **o zasílání** tohoto sešitu se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci formulář na http://crypto-world.info . Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání sešitu.

Ke **zrušení registrace** stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info . Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byl sešit zasílán.

3. Spojení

běžná komunikace, zasílání příspěvků k otištění , informace
pavel.vondruska@crypto-world.info
pavel.vondruska@ct.cz