Co je nového v kryptografii v roce 2000?

Ing. Jaroslav Pinkava, CSc.

(e-mail: Jaroslav.Pinkava@aec.cz)

Úvod

Cílem předloženého materiálu je dát určitý přehled o současném dění v kryptografii. Každá takováto práce se musí nutně jednotlivými okruhy problémů zabývat pouze stručně a poukázat jen na některé základní aspekty problematik. V závěru je proto dán poměrně široký seznam zdrojů (literatura a Internet), kde zainteresovaný čtenář nalezne další podrobnosti. Pokud se týče informací pro vstupní přehled do problematiky odkazuji na práci [17], kde lze nalézt definice příslušných pojmů i popisy základních kryptografických algoritmů. Pro každého, kdo se zajímá o aktuální informace z kryptologie, doporučuji Cryptogram Bruce Schneiera [22] a Crypto-World (v českém jazyce) Pavla Vondrušky [24]. Zájemcům o hlubší studium kryptologické problematiky doporučuji knihu [13], kterou lze celou nalézt on-line na Internetu.

Další odstavce obsahují některé nové poznatky, skutečnosti, které se objevily v průběhu posledního roku. Týká se to samozřemě jak symetrické tak i asymetrické kryptografie. Středem pozornosti v posledním období je speciálně i problematika elektronických podpisů.

3-DES

Algoritmus DES již ukončil svou životnost i jako americká vládní norma. Do doby než bude schválen chystaný Avanced Encryption Standard (AES) byl vydán NIST dokument FIPS-PUB-46-3 [4], který ustavuje jako současně platnou normu algoritmus 3-DES. Fakticky tak dochází pouze ke schválení již existujícího status-quo. Algoritmus 3-DES byl převzán z již déle platné finanční normy ANSI X9.52.Souběžně s touto normou (rovněž v říjnu 1999) byl vydán materiál NIST [11] popisující velice důkladně validaci jednotlivých operačních módů algoritmu.

Postup při zašifrování 64-bitového bloku otevřeného textu ***I*** na 64-bitový blok ***O*** šifrového textu je dán následovně:

$$O = E_{K3}(D_{K2}(E_{K1}(I))).$$

Dešifrace je pak logicky popsána vzorcem:

$$O = D_{K1}(E_{K2}(D_{K3}(I)))$$

Norma specifikuje tři varianty pro použití klíče $(K1, K2, K3)$:

1. $K1, K2$ a $K3$ jsou nezávislé klíče;
2. $K1$ a $K2$ jsou nezávislé klíče a $K3 = K1$;
3. $K1 = K2 = K3$.

Celková délka použitého klíče je tedy v jednotlivých variantách 168, 112 a 56 bitů.

AES

V roce 1996 inicioval NIST program AES – formou veřejné výzvy na vytvoření kryptografického algoritmu na principu blokové šifry. Oproti stávajícím algoritmům má tanto nový typ algoritmu zpracovávat bloky otevřeného textu v délce 128 bitů a musí umožňovat práci s klíči v délkách 128, 192 a 256 bitů. V roce 1998 bylo akceptováno celkem 15 kandidátů, přitom v roce 1999 z nich bylo vybráno 5 finalistů.

Třetí AES konference (AES3) se konala 13-14. dubna 2000 v New Yorku. Zúčastnilo se jí vice než 250 lidí z cca. 25 zemí. Obsahem konference bylo provedení druhého cyklu

technické analýzy finalistů (5 algoritmů: MARS, RC6™, Rijndael,Serpent, Twofish). Je k dispozici elektronická verze konfernečních materiálů [1].

Vítěz zatím nebyl oznámen, čeká se, že příslušná informace bude zveřejněna v průběhu letošního léta.

Z komentářů Bruce Schneiera ([22], April 2000): Z kryptoanalytických útoků se zdá být nejvíce postižen algoritmus RC6 (bylo ukázáno, jak rozbít tento algoritmus při jeho redukci na 15 cyklů z celkových 20 cyklů). Z těchto útoků naopak nejlépe vyšly algoritmy Serpent a Twofish. Samozřejmě žádný z útoků není aplikovatelný na plné verze algoritmů.

Co se týká rychlosti, pak na tom jsou nejlépe Rijndael a Twofish, naopak Serpent je nejpomalejší na většině softwarových technologických platforem. V hardwaru jsou na tom nejlépe Rijndael a Serpent, Mars je velice pomalý.

Schneier doporučuje z dalšího zvažování eliminovat algoritmy Mars a RC6 (oba jsou dle jeho názoru poměrně nevhodné pro hardware a nelze je vhodně umístit na malé čipové karty). Pozn.: Samozřejmě je třeba vzít na zřetel, že B. Schneier je autorem jednoho z návrhů (algoritmus Twofish).

P1363

Výsledky pracovní skupiny IEEE P1363 (lit.[15]) jsou v oblasti asymetrické kryptografie současným nejvýznamějším počinem. Od svého vzniku byla tato práce orientována na vytvoření základní normy pro tři rodiny kryptografických systémů s veřejným klíčem: Jsou to algoritmy, jejichž bezpečnost je založena na složitosti úlohy faktorizace velkých čísel (známý RSA algoritmus, Rabin-Williamsův algoritmus). Dále jsou to algoritmy spočívající z hlediska bezpečnosti na složitosti úlohy diskrétního logaritmu a konečně algoritmy eliptické kryptografie, jejichž bezpečnost je obdobně opřena o složitost řešení úlohy eliptického diskrétního logaritmu. Jsou zde pokryty všechny tři základní oblasti asymetrické kryptografie: algoritmy pro výměnu klíčů, digitální podpis a šifrování.

V letošním roce byl schválen poslední (třináctý) draft zpracovaných materiálů jako norma IEEE a tato norma bude v brzké době oficiálně vydána.

Práce skupiny však tímto nekončí. Již se rozběhly práce na dokumentu: IEEE P1363a: Standard Specifications for Public-Key Cryptography: Additional Techniques, jehož obsahem bude řada doplňkových technik (v současné době je k dispozici již třetí verze). Po ukončení těchto prací by se stávající doplněk měl stát součástí hlavního materiálu.

P1363 a nové algoritmy

V současné době se rozjíždí práce na dalším významném projektu. Byla vytvořena tzv. „The Study Group for Future Public-Key Cryptography Standards" (lit. [16]), jejímž cílem je jak adekvátní popis nových aplikací asymetrické kryptografie, tak i adaptace dalších nových rodin kryptografických algoritmů. Jedná se např. o popis autentizace na bázi hesla a sím souvisejícími protokoly pro výměnu klíčů, identifikační schemata, prahové schema digitálního podpisu a jiné. Níže jsou stručně zmíněny dva z těchto nových přístupů (kryptosystémy NTRU a ACE). V letošním roce má k nim přibýt také některý ze systémů rozvíjených německými kryptology. Odpovídající citace lze nalézt v článku [25]. Tyto kryptosystémy jsou konstruovány nad imaginárními kvadratickými tělesy a mají mít určité výhodné vlastnosti a to jak z hlediska rychlosti, tak i z hlediska délky klíče. Např. systém ze zmíněného článku poskytuje stejnou bezpečnost při délce klíče 341 bitů jakou má RSA při délce klíče 1024 bitů. Přitom má umožňovat výrazně rychlejší implementace.

NTRU

Jako jeden z příspěvků pro další práce skupiny P1363 byl přijat materiál [10]. Na webovské stránce firmy NTRU Cryptosystems,Inc.[14] je tento systém inzerován dokonce

jako současný nejrychlejší kryptosystém s veřejným klíčem, který je až 100 krát rychlejší než jeho konkurenti. NTRU pracuje pouze s malými čísly a proto umožňuje relativně rychlé implementace. Např. pro RSA při délce klíče N je složitost práce odpovídajícího kryptografického algoritmu popsána výrazem $O(N^3)$, zatímco pro NTRU výrazem $O(N^2)$, resp dokonce O(N log N) – dle způsobu implementace. Ovšem z hlediska kryptografické odolnosti je délka klíče kryptosystému NTRU srovnatelná se systémem RSA (resp. se systémy na bázi diskrétního logaritmu), tj. v současnosti délka klíče v mezích 1000-2000 bitů poskytuje dostatečnou bezpečnost (eliptické křivky požadují pro odpovídající bezpečnost délku klíče cca 180-200 bitů).

ACE

Velice zajímavým příspěvkem pro P1363 je článek [22], iniciovaný původními články R. Cramera a V.Shoupa [2,3]. Je zde popsán tzv. Advanced Cryptographic Engine (ACE), který specifikuje jak šifrování tak i digitální podpis pomocí algoritmu s veřejným klíčem. Schéma je přitom popsáno natolik detailně, aby byla zabezpečena interoperabilita mezi jeho jednotlivými implementacemi. Schéma má navíc jednu zásadní výhodu – tzv. prokazatelnou bezpečnost (za určitých přesně definovaných požadavků , týká se to zejména tzv. adaptivních útoků [9]).

DSS

V posledních dvou letech prošla norma Digital Signature Standard (DSS) [5].dvojí reedicí. Koncem roku 1998 (FIPS 186-1) zde byl doplněn algoritmus RSA (dle formulace z normy ANSI X9.31) a v lednu tohoto roku (FIPS 186-2) byla norma doplněna celou sadou eliptických křivek. Eliptické křivky jsou definovány pro oba typy těles (binární a prvočíslená tělesa) a byly generovány tzv. prokazatelně náhodně. Obdobnou cestou jdou i materiály SECG (aktivita firmy Certicom – lit.[26]).

Samotný původní algoritmus DSA (na bázi diskrétního logaritmu) však nedoznal změn z hlediska doporučované délky klíče. S tím polemizuje např. článek [12], ve kterém je řečeno, že použité délky parametrů (p má délku 1024 bitů, q délku 160 bitů) budou bezpečné nejdéle do roku 2002 z hlediska velikosti použitého pole (resp. do roku 2013 z hlediska použité hashovací funkce a do roku 2026 z hlediska velikosti podgrupy).

Kryptoanalýza – výzvy Certicomu a RSA

Kryptoanalytické metody jsou samozřejmě výzvou schopnostem výpočetní techniky již sami o sobě. Protože je však i v zájmu producentů kryptografických technologií mít možnosti výpočetní techniky zmapovány velice důkladně, existují takovéto výzvy dokonce v oficiální podobě. Na webovských stránkách firem RSA a Certicom lze nalézt celou serií úloh v rámci taovýchto výzev (challenge), přitom jednotlivé úlohy (a i ceny) jsou odstupňovány dle jejich rostoucí složitosti. Kryptografickou veřejností jsou sledovány dosažené výsledky také proto, že umožňují lépe zmapovat současné možnosti výpočetní techniky a učinit tak i možné závěry o budoucím vývoji v tomto směru. V srpnu roku 1999 tak bylo poprvé rozbito RSA s klíčem v délce 512 bitů. Pro kryptosystémy na bázi eliptických křivek byly v poslední době dosaženy dva takovéto výsledky: v září 1999 byl rozbit ECC2-97 (binární těleso, obecná křivka) a v březnu 2000 ECC2K-108 (binární těleso, Koblitzova křivka). Čísla 97 a 108 značí přitom odpovídající počet bitů klíče eliptického kryptosystému. Podrobnosti a další odkazy viz [24].

Elektronický podpis – Směrnice EU

Celá řada velice zajímavých dokumentů se objevila v souvislosti s úsilím Evropské Unie o zavedení technologií elektronických podpisů. Je to především Směrnice EU pro elektronický podpis [6], která po několikaleté veřejné diskusi byla schválena v prosinci 1999. Tato

směrnice vytváří základ nu pro elektronický podpis především z hlediska legislativního. Jednotlivé členské země EU mají do poloviny roku 2001 upravit své zákony pro tuto oblast tak, aby splňovaly podmínky stanovené touto směrnicí.

Základním výchozím dokumentem z hlediska přípravy evropských norem pro elektronické podpisy je materiál EESSI [7]. V květnu tohoto roku byl schválen rovněž velice důležitý dokument „Electronic Signature Formats“ (lit. [8]). Obsahuje řadu velice užitečných podnětů zejména z hlediska aplikace tzv. časových značek pro elektronické podpisy. Na základě těchto doporučení bude např. možné archivovat elektronický podpis i několik desetiletí, aniž by tento podpis ztratil svoji právní platnost. Některé úvodní poznámky k problematice norem pro oblast elektronických podpisů lze nalézt v [20].

Zákon o elektronickém podpisu v ČR

V květnu tohoto roku proběhl druhým čtením parlamentu ČR návrh zákona o elektronickém podpisu. Formulace zákona vychází již ze Směrnice EU pro elektronický podpis, jinou otázkou je však, zda se zákonodárcům podaří zformulovat i příslušná administrativní východiska tak, abychom se brzy dočkali elektronických podpisů i v praxi (elektronických podpisů v komplexní podobě, tj. včetně odpovídajících legislativních důsledků). Zájemcům doporučuji [18] a také http://www.trustcert.cz.

Délky kryptografických klíčů

Na toto velice zajímavé téma se v poslední době objevily hned dva zásadní články. Autoři Lenstra a Verheul [12] na základě hluboce sofistikované analýzy dochází přitom k poměrně velice přísným odhadům (viz také výše poznámka k DSA). Autor dále dochází k následujícím doporučením pro rok 2020 (aby bezpečnost elektronické informace byla garantována pro období 20 let). Symetrické klíče by měly mít minimálně délku 86 bitů, modul RSA minimálně 1881 bitů, analogicky i modul pro diskrétní logaritmus, pro eliptické křivky by měla být minimální délka klíče 161 bitů (pokud nedojde k významnému kryptoanalytickému pokroku).

S těmito odhady polemizuje R. Silverman [23], který je považuje za přiliš přísné. Poukazuje zejména na to, že dnes neexistuje takový hardware s jehož pomocí by se dal uskutečnit požadovaný pokrok v kryptoanalýze. Dochází proto k závěru, že např. délka klíče 1024 bitů pro algoritmus RSA zůstává dostatečně bezpečná. Je ovšem třeba také vidět, že pan Silverman je pracovník firmy RSA, které se nepříznivé odhady Arjena Lenstry přímo dotýkají. Viz také článek [21].

Literatura

[1] AES: http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf

[2] Cramer, R.; Shoup, V.: A practical public key cryptosystem provaby secure against adaptive chosen ciphertext attack, In Advances in Cryptology – Crypto 98, pp.13-25

[3] Cramer, R.; Shoup, V.: Signature schemes based on the strong RSA assumption, In 6th ACM Conf. On Computer and Communications Security, 1999

[4] Data Encryption Standard (DES), FIPS-PUB 46-3, October 1999

[5] Digital Signature Standard (DSS), FIPS PUB 186-2, NIST, January 2000

[6] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, http://europa.eu.int/comm/dg15/en/media/sign/ind ex.htm

[7] EESSI: Final Report of the EESSI Expert Team 20th July 1999, http://www.ict.etsi.org/eessi/Final-Report.doc

[8] ETSI ES 201 733, V1.1.3 (200-05), Electronic Signature Formats, http://www.etsi.org/sec/el-sign.htm

[9] Goldwasser, S.; Micali, S.; Rivest, R.: A digital signature scheme secure against adaptive chosen-message attacks, SIAM J. Comput., 17, pp. 281-308, 1988
[10] Hoffstein, Jeffrey, Pipher, Jill; Silverman, Joseph H.: NTRU. A Ring-Based Publi Key Cryptosystem, IEEE P1363 submission
[11] Keller, Sharon S.: Modes of Operation Validation system for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures, NIST Special Publication 800-20.
[12] Lenstra Arjen K.; Verheul Eric R. : Selecting Cryptographic Key Sisez, November 1999, (http://www.pwcglobal.com/cce.)
[13] Menezes, Alfred J.; van Oorschoot, Paul C.; Vanstone: Handbook of Applied Cryptography, 1997, http://www.cacr.math.uwaterloo.ca/hac/
[14] NTRU: http://www.ntru.com/
[15] P1363: http://grouper.ieee.org/groups/1363
[16] P1363, Study Group: http://grouper.ieee.org/groups/1363/StudyGroup/index.html
[17] Pinkava, J.: Úvod do kryptologie, http://www.aec.cz
[18] Pinkava, J.: Elektronický podpis a Evropská Unie, DSM 2/2000
[19] Pinkava, J.: Digitální a elektronický podpis ve světě a v EU. Legislativní a standardizační aspekty. Seminář AFOI, únor 2000
[20] Pinkava J.: Moderní kryptografické algoritmy pro elektronický podpis, Seminář ČAČK, duben 2000
[21] Pinkava, J.: Jak je to s bezpečností eliptických kryptosystémů, Crypto World
[22] B: Schneier: Cryptogram: http://www.counterpane.com
[22] Thomas Schweinberger; Victor Shoup: ACE: The Advanced Cryptographic Engine, March 1, 2000.
[23] Silverman, Robert D.: A Cost-Based Security Analysis of Symmetric and Asymmetric Key Length, Bulletin RSA, April 2000
[24] Vondruška, P.: Crypto World, http://www.mujweb.cz/veda/gcucmp
[25] Paulus, S.; Takagi, T.: A New Public-Key Cryptosystem over a Quadratic Order with Quadratic Decryption Time, Journal of Cryptology, Vol. 13, Number 2, Spring 2000
[26] SECG: http://www.secg.org/