Vývoj v kryptografických technologiích

Ing. Jaroslav Pinkava, CSc.,
AEC spol. s r.o. & Norman Data Defense Czech Republic

Úvod

Jestliže bychom chtěli charakterizovat hlavní trendy, které v posledním roce (posledních letech) hýbou světem kryptografie, tak to nebudou ani nové principy šifrování, ani nově vzniklé algoritmy (i když některé se samozřejmě objevily) a ani nové směry v aplikacích. Rozhodně to však budou směry vytváření jednotných přístupů k využívání kryptografických postupů, tj. problematika konstituování kryptografických norem a doporučení. Níže uvedený přehled je dokladem těchto postupů.

S celkovým pohledem na tuto problematiku se čtenář může seznámit v přehledech [18] a [14], zde bude kladen důraz zejména na aktivity probíhající v uplynulém roce, resp. aktivity současné. S problematikou norem úzce souvisí i otázky certifikace kryptografických prostčředků (resp. prostředků pro elektronický podpis). Zde však pouze čtenáře odkáži na článek [12].

Normy pro základní kryptografické algoritmy

AES

Nová americká norma **AES**, kde výběr proběhl formou otevřené soutěže - výsledky byly oznámeny na podzim 2000.. Jedná se o algoritmus blokové šifry pracující s bloky otevřeného textu o délce 128 bitů. Algoritmus bude mít tři bezpečnostní úrovně (z hlediska délky použitého klíče – 128, 192 a 256 bitů). Původně bylo přihlášeno 15 algoritmů, z nichž bylo nejprve vybráno pět finalistů (Mars, RC6, Rijndael, Serpent a Twofish). Na podzim loňského roku byl vyhlášen vítěz – algoritmus ***Rijndael*** belgických autorů Joan Daemen, Vincent Rijmen a letos v únoru vyšel příslušný draft [17], který bude letos v létě následovat formálně vydaná norma. AES má zásadní význam pro budoucnost nejen americké, ale i mezinárodní aplikované kryptografie. Nyní probíhají práce zaměřené na stanovení různých pracovních módů, jako byly např. módy CBC, CFB, ECB pro DES (workshop k tomuto tématu se bude konat v srpnu 2001). S komplexními současnými plány NIST v oblasti kryptografie se lze seznámit na adrese [22].

Cryptonessie

V první polovině roku 2000 byl zahájen projekt NESSIE: *New European Schemes for Signatures, Integrity, and Encryption*. Cílem tohoto evropského projektu je přinést rozsáhlé portfolio tzv. kryptografických primitivů, které projdou procesem veřejné evaluace (viz webovské stránky iniciativy [15])..

Do konce září 2000 bylo třeba podat jednotlivé návrhy a v návaznosti na to se ve dnech 13-14. listopadu 2000 konala první pracovní konference (workshop) této iniciativy (Leuven, Belgie). Cílem iniciativy je vytvoření normativních dokumentů pro široké spektrum tzv. kryptografických primitivů:

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

V rámci každé třídy budou existovat dvě bezpečnostní úrovně (normální a vysoká). Na uvedené adrese je možné se seznámit z přijatými návrhy. V létě 2001 se má konat v pořadí druhá „lochnesská" konference, kde bude provedena první selekce podaných návrhů.Přehled návrhů lze nalézt na adrese: https://www.cosic.esat.kuleuven.ac.be/nessie/workshop/submissions.html spolu s odkazy na stránky, kde jsou umístěny jednotlivé dokumenty.

Toto velké množství různorodých návrhů (díky zadání celého konkursu) je odlišné nejen svým zaměřením, ale asi i kvalitou. Některé návrhy jsou hluboce rozpracovány, jiné přináší nové myšlenky, některé však zase budí dojem, že by neškodila přiložená hlubší analýza. Některé sekce také trpí malou konkurencí návrhů. Již dnes na základě vznesených přpomínek (např. algoritmus Nimbus) je jasné, které návrhy mají malé šance na své zařazení mezi ty vítězné.

Cryptrec

Japonská iniciativa CRYPTREC má obdobně široké zaměření jako Cryptonessie (viz [16]). Přijímání návrhů bylo uzavřeno teprve v lednu letošního roku (2001) a je proto ještě opravdu brzo odhadovat směry, kterými se bude tato iniciativa ubírat.

Algoritmy pro digitální podpis

V asymetrické kryptografii je základní iniciativou práce skupiny **IEEE P1363** [4]. Po několika letech intenzivních prací byla v září 2000 vydána norma *1363-2000 IEEE Standard Specifications for Public Key Cryptography.* Jejím obsahem je popis tří základních skupin kryptosystémů s veřejným klíčem:

a) kryptosystémy založené na úloze faktorizace (RSA, Rabin-Williams);
b) kryptosystémy založené na problému diskrétního logaritmu (DSA, Diffie-Hellmanovo schéma pro výměnu klíčů, El-Gamalovo šifrovací schéma);
c) kryptosystémy založené na úloze diskrétního logaritmu pro eliptické křivky.

V současné době je připravována další revize americké vládní normy NIST FIPS 186-2 – DSS (viz [21]). Budou vytvořeny (stejně jako u AES) tři úrovně bezpečnosti a pro každou z těchto úrovní bude definována potřebná délka klíče pro jednotlivá schémata digitálního podpisu. Zatímco pro eliptické křivky budou tyto délky čísla řádově stovková (jako potřebná délka klíče pro dosažení stejné úrovně bezpečnosti se uvádí zhruba dvojnásobek délky klíče pro symetrickou

kryptografii), tak pro schémata na bázi RSA a diskrétního logaritmu to budou čísla řádově v tisících až desetitisících bitů.

S rozvojem systémů však běží paralelně i rozvoj příslušných kryptoanalytických metod a s tím i zvyšující se nároky na tyto konkrétní praktické realizace. Např. dnes je velmi dobře znám Bleichenbacherův útok proti RSA algoritmu dle normy PKCS#1 v.1.5, který vedl k zásadnímu přepracování nejen této, ale i řady návazných norem. Existují však i jiné útoky.
V návaznosti na takovéto útoky je teoretiky moderní kryptologie dále precizován pojem bezpečnosti těchto kryptosystémů. Objevují se různé modely (např. tzv. random oracle model, který pomohl zkonstruovat vylepšenou variantu pro RSA - OAEP). Při konstrukci nových kryptosystémů na základě zmíněných modelů jsou sledovány především následující dva základní cíle:

a) zkonstrovat „bezpečnější“ schémata (v nějakém precizovaném smyslu),

b) zachovat efektivnost těchto schémat (tj. např. výpočetní náročnost nových schémat by měla být zhruba na stejné úrovni jako u původních schémat, totéž platí o délkách použitých klíčů, atd.).

V posledních dvou či tří letech se objevilo několik zajímavých publikací na toto téma (H. Cramer a V. Shoup; D. Pointcheval; M. Bellare a P. Rogaway atd.). V rámci pracovní skupiny IEEE P1363 (a rovněž evropské iniciativy Cryptonessie) - je projednáván komplexní model V. Shoupa - ACE. Tj. zmíněná problematika je ve stadiu přechodu od teoretických článků k začlenění do mezinárodních norem (podrobněji např. [19])..

XML – digitální podpis

Konzorcium World Wide Web (W3C – [24]) vytvořilo normalizovanou syntaxi pro strukturalizaci webových dokumentů – XML (Extensible Markup Language) [5]. V návaznosti na to probíhá vývoj syntaxe kompatibilní s XML, kterou lze použít pro reprezentaci podpisu zdrojů a syntaxe pro části protokolů a procedur při tvorbě a verifikaci takovýchto podpisů (viz [20]).

Digitální podpisy zaručují integritu dokumnetu, autentizaci podpisující strany a nepopiratelnost dat pohybujících se po Internetu. Tato vlastnost je zejména důležitá pro dokumenty, které jsou vyjádřením takových informací jako smlouvy, ceníky a různá prohlášení. Možnost adresovat dokumenty vytvořené v syntaxi XML je kritická pro celou řadu aplikací elektronického obchodu (včetně platebních nástrojů).

Cílem aktivit je vytvoření nezbytného modelu dat, syntaxe a metod zpracování, tak, aby bylo možné provázat digitální podpis s příslušným zdrojem v XML. Výchozí podmínky na XML na digitální podpis jsou zformulovány v RFC.2807 ([20]). Poukážeme především na dokument RFC.3075 (viz [20]), který specifikuje příslušnou syntaxi XML a pravidla pro vytváření a prezentaci digitálních podpisů. V dokumentu RFC.3076 (tamtéž) jsou definovány určité podmínky na podobu XML dokumentů. Jde o to, že dokumenty logicky ekvivalentní (z obsahového hlediska) se mohou lišit fyzickou reprezentací. Specifikace RFC.3076 definuje metodu generování jednotné fyzické reprezentace XML dokumentu – tzv. kanonickou formu. Potom (v zásadě) pokud mají dva dokumenty tutéž kanonickou formu, jsou i ekvivalentní z hlediska logického obsahu.

Evropské normy pro elektronický podpis

Celkový pohled

Práce probíhají ve dvou nezávislých pracovních skupinách: ETSI a CEN/ISSS. Nejprve ke skupině ETSI. Ta v roce 2000 zpracovala čtyři základní dokumenty zaměřené do dvou oblastí (kvalifikované certifikáty a časová razítka).
ETSI (2000):
a) problematika časových značek je řesena v rámci těchto okruhů:
Electronic Signature Formats.
Time Stamping Profile;
b) problematika kvalifikovaných certifikátů je řesena v rámci těchto okruhů:
Qualified Certificates Profile;
Policy Requirements for CSPs Issuing Qualified Certificates;
ETSI (2001):
ETSI v roce 2001 chystá vydání zhruba pěti nových dokumentů.
Policy requirements for CSPs issuing trusted time stamps
Policy requirements for CSPs, according to Art. 5.2 of the Directive
XML electronic signatures
Technical aspects of signature policies
Infrastructure and interoperability requirements for on-line validation of Certification Service Providers

Druhá pracovní skupina CEN/ISSS je časově oproti ETSI trochu ve skluzu, teprve první dokumenty se blíží do závěrečné fáze.
CEN/ISSS (2000-2001)
Security Requirements For Trustworthy Systems and Products
Security Requirements for Signature Creation Devices
Signature Creation Environment
Signature Verification Process nad Environment
Conformity Assessment of Products and Services for Electronic Signatures
Na finalizované dokumenty navazuje práce skupiny následujícími připravovanými materiály.
CEN/ISSS (2001-2002):
Extension of SSCD requirements towards specific applications/environments and towards e-commerce applications - Art5.2
Requirements for smart cards used as SSCD

Podrobněji se lze s obsahem těchto dokumentů seznámit např. v [10], [11] nebo na webovských stránkách [3] a [4].

Literatura

[1] Final Report ICTSB European Electronic Signature Standardization http://www.ict.etsi.org/eessi/Final-Report.pdf

[2] Směrnice EU o elektronickém podpisu – Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures http://www.ict.etsi.org/eessi/e-sign-directive.pdf

[3] webovské stránky ETSI : http://www.etsi.org/sec/el-sign.htm.

[4] webovské stránky CEN/ISSS: http://www.cenorm.be/isss/workshop/e-sign/ http://www.ni.din.de/index.php3

[5] J. Pinkava : Elektronický podpis a EU, DSM 2/2000

[6] Český zákon č. 227/2000 Sb. o elektronickém podpisu.

[7] Návrh české vyhlášky k ZoEP (ÚOOU), http://www.epodpis.cz

[8] Crypto-World (vychází 1x mesíčně v elektronické podobě), http://www.mujweb.cz/veda/gcucmp

[9] J. Pinkava: Moderní kryptografické algoritmy pro elektronický podpis, Seminář ČAČK, březen 2000

[10] J. Pinkava: různé články, CryptoWorld, http://www.mujweb.cz/veda/gcucmp

[11] J. Pinkava: Certifikační autorita. Bezpečné prostředí, Bezpečnost dát, Bratislava duben 2001

[12] J. Pinkava: Certifikace kryptografických prostředků a prostředků pro elektronický podpis, DSM 6/2000

[13] P. Vondruška: Typy elektronických podpisů, Bezpečnost dát, Bratislava duben 2001

[14] J. Pinkava: Normy pro kryptografii a návazné aplikace, DSM 2+3/2001

[15] webovské stránky Cryptonessie: https://www.cosic.esat.kuleuven.ac.be/nessie/

[16] webovské stránky Cryptrec: http://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html

[17] webovské stránky AES: http://www.nist.gov/aes

[18] J. Pinkava: *Přehled norem pro elektronický podpis a související okruhy problematik* – http://www.uoou.cz

[19] Jaroslav Pinkava: Prokazatelně bezpečná kryptografická schémata pro elektronický podpis, Kolokvium VA Brno, duben 2001

[20] webovské stránky: http://www.ietf.org/html.charters/xmldsig-charter.html

[21] FIPS 186-2, poslední verze americké vládní normy pro digitální podpis: http://csrc.ncsl.nist.gov/publications/fips/fips186-2/fips186-2.pdf

[22] NIST Cryptographic Toolkit: http://csrc.ncsl.nist.gov/encryption/index.html

[23] konzorcium World Wide Web Consortium –W3C - http://www.w3.org/