Moderní kryptografické metody

Návrat šampiona

Náš minikurz moderní počítačové kryptografie dnes pokračuje asymetrickými šiframi. Ukážeme si nejprve, že nejsou všemocné a že se prakticky používají pouze v kombinaci se symetrickými šiframi. Dále se budeme věnovat algoritmu RSA a skupině standardů, které vznikly jako první pro realizaci kryptosystémů s veřejným klíčem a které mají dodnes dominantní postavení.

Symbióza rivalů

V minulém čísle jsme hovořili o proudových a blokových šifrách. Blokové šifry nevznikly z rozmaru milionářů, ale proto, že se postupem času objevily stavební prvky, které poskytovaly silnější a přesvědčivější kryptologicko-bezpečnostní vlastnosti, než bylo zvykem u proudových šifer. Přesto byly blokové šifry prostřednictvím modů činnosti, o nichž jsme minule hovořili, “ohnuty" tak, aby šifrovaly proudově. Docílilo se tak nejen nových možností, specifických pro blokové šifry, ale zejména nové kvality proudového šifrování.

Podobně tomu bylo se symetrickými a asymetrickými šiframi, o nichž jsme se zmínili v červnovém Chipu. S vynálezem asymetrických šifer (šifer s veřejným klíčem) také nebyly zapomenuty symetrické šifry, tentokrát ale z jiného důvodu – byla jím rychlost šifrování. Ta je totiž u všech kvalitních asymetrických šifer tak mizerná, že nelze šifrovat velké objemy dat. Jenže asymetrické šifry jsou nezastupitelné pro digitální podpis a často výhodné i pro klíčové hospodářství. Proto byly vynalezeny hašovací funkce, resp. přišlo se na jejich nové využití. Díky nim nemusíme asymetrickou šifru vytvářející digitální podpis aplikovat na celý (například gigabajtový) soubor, ale pouze na jeho jedinečnou haš (hašovací hodnotu, kód) o délce většinou 128 nebo 160 bitů. Aplikace asymetrického systému se tak redukovala na jedinou šifrovací operaci.

Ale co dělat v případě šifrování vlastních dat, která musí být přenášena značnou rychlostí třeba na internetu? Také v tomto případě se našlo řešení. Asymetricky se zašifruje jenom náhodný řetězec, který se předá protistraně před vlastní šifrovanou komunikací. Tento řetězec se pak u protistrany rozšifruje a interpretuje jako klíč pro symetrický šifrovací systém. Vlastní data se pak šifrují starým dobrým symetrickým algoritmem. Jak je vidět, nic není samo o sobě lepší ani horší, ale z každého nástroje se v aplikacích využívají ty nejvýhodnější stránky.

Výměna klíčů a digitální podpis

Pro další výklad si tedy zapamatujme, že využití asymetrických šifer je v zásadě dvojího druhu. První použití je pro šifrování symetrických klíčů. Asymetrická šifra v tomto případě zpracovává jen data, která jsou, jak jsme si řekli před chvílí, interpretována jako klíče pro symetrické šifry. Častěji se proto toto využití asymetrických šifer nazývá výměnou klíčů (ustavením klíčů, dohodou klíčů) a předává se tak klíč pro společnou symetrickou šifru, která bude později použita k šifrování následných dat. Způsob dohody symetrické šifry leží o vrstvu výše. Součástí této dohody v příslušném komunikačním protokolu (například SSL nebo TLS) je pak nejen typ symetrické šifry, ale i délka klíče, dále typ asymetrických šifer pro výměnu klíčů a pro podpis, jejich parametry, typ autentizace atd. Nejčastější dohadované délky klíčů v současných protokolech jsou 40, 56, 128, 192 a v brzké budoucnosti to bude i 256 bitů (k bezpečné délce klíče jsme se vyjadřovali v minulém dílu).

Druhé použití asymetrických šifer se hodilo při realizaci digitálního podpisu. Asymetrická šifra v tomto případě opět nezpracovává vlastní podepisovaný soubor dat, ale (až na výjimky) pouze jeho hašovací hodnotu. Připomeňme si, že v tomto případě se většinou jedná o data délky 128 nebo 160 bitů (výjimečně 256 a 320 bitů).

Jak vidíme, v obou dvou hlavních použitích asymetrických šifer se jedná o data velmi krátkých délek, směšných oproti milionům megabajtů dat, která denně proběhnou internetem v zašifrované podobě nebo která se digitálně podepisují. Čas, který se tak ušetří, znamená v těchto případech peníze víc než kdy jindy...

RSA znovu na scéně

Abychom mohli ukázat, jak se realizuje digitální podpis a výměna klíčů v praxi, vybrali jsme konkrétní asymetrický systém – RSA. Už jeho historie je sama o sobě zajímavá, ale určitě má před sebou také velkou budoucnost.

Po svém objevu (1977, blíže viz infotipy) byl tento algoritmus patentován – to je u algoritmu sice kuriózní, ale v zemi jeho vzniku (USA) možné. Logicky proto byla k jeho komerčnímu využití založena příslušná společnost (RSA Data Security Inc.) a za jeho použití v USA se pak musely platit licenční poplatky, což nebylo právě příjemné. Řekněme, že tato skutečnost “nějak unikla" programátorovi Philipu Zimmermannovi, jehož napadlo, že by mohl napsat software pro utajení a digitální podpis elektronické pošty (byl to jeho osobní protest proti připravovanému zákonu o odposlechu). Ve svém programu PGP (Pretty Good Privacy, blíže viz infotipy) tedy “bezděky” použil i algoritmus RSA; ke vší smůle se jeho software navíc “nějak dostal" také za hranice USA.

Znamenalo to hned dvojí faux pas. Za prvé porušení autorských práv na použití RSA a za druhé porušení velmi tvrdých zákonů o zákazu vývozu zbraní z USA (program PGP realizoval silnou kryptografii, a byl proto “zbraní" ve smyslu vývozních omezení). Zimmermannovi hrozilo vězení. Avšak následné soudní spory a masivní protivládní mediální kampaň udělaly své – Zimmermannovo vyšetřování bylo zastaveno, společnost RSA dosáhla mimosoudní dohody a ustoupila od žaloby. Algoritmus RSA a program PGP tím sice získaly ohromnou reklamu, kterou by nikdy jejich tvůrci nemohli zaplatit, a staly se dominujícími, ale bylo to stále málo. Šifra RSA víceméně živořila a také program PGP se dále vyvíjel klikatými cestičkami.

Použití algoritmu RSA dostalo nový impulz s masovým rozšířením internetu a elektronické pošty a následným podpisem smluv o použití RSA v poštovních klientech a internetových prohlížečích. Záhy na to byla RSA Data Security Inc. koupena společností Security Dynamics Inc. (nyní přejmenovanou na RSA Security Inc.), která byla známa a obchodně byla úspěšnější zejména díky svým autentizačním tokenům velikosti kalkulačky. Myšlenkově jednoduchá “hračička" realizující symetrický algoritmus DES (s 56bitovým klíčem) tak přispěla k obchodnímu pokoření společnosti svázané s geniálním objevem asymetrického algoritmu! Také původní datové formáty PEM (Privacy Enhanced Mail) a PGP, využívající RSA, se nepříliš rozšířily a v současné době se používají zejména formáty a protokoly S/MIME a SSL.

Čas postupoval a šifra RSA získala díky rozšiřování internetu výsadní komerční postavení a stala se standardem asymetrické šifry i v bankovních normách. Neměla však stále podporu ve státních standardizačních dokumentech, a dokonce došlo i k jejímu “odstrčení" algoritmem DSA (blíže viz infotipy), který byl schválen americkým standardizačním úřadem NIST pro digitální podpis v roce 1994. Neustále bobtnající internet však potřeboval také algoritmus na výměnu klíčů. Na to DSA nestačil, protože byl určen jen pro digitální podpis. A tak se pro výměnu klíčů používaly algoritmy Diffie-Hellman (blíže viz infotipy) a RSA. Zatím neoficiálně.

Léta plynula a mezitím vznikla úplně nová větev v asymetrických algoritmech – kryptografické algoritmy realizované na tzv. eliptických křivkách. Zároveň se přiblížil konec platnosti patentu na RSA (v září 2000). A tak se americký NIST rozhodl udělal další zlomové rozhodnutí – v lednu 2000 vydal normu pro digitální podpis (FIPS PUB 186-2), která zrovnoprávňuje hned všechny tři uvedené techniky pro digitální podpis – DSA, RSA i ECDSA (to je DSA, realizovaný na zmíněných eliptických křivkách).

Důsledky tohoto kroku jsou dalekosáhlé. V každém případě je to pocta kryptografické kvalitě algoritmu RSA a dále uznání “statu quo”, že RSA je průmyslovým a bankovním standardem (pro podpis i pro výměnu klíčů). Zároveň je to ale i krok k volné soutěži RSA a nové slibné technologie eliptických křivek (pro digitální podpis i pro výměnu klíčů). RSA se tak “se státním razítkem" vrací do velké hry o tvář budoucí aplikované kryptografie. Nejsou to jen prázdná slova – jde o čistý byznys zahrnující celou oblast elektronického obchodu, mobilních telefonů, elektronických peněženek, čipových karet, elektronického podpisu atd.

RSA a standardy PKCS

Pro implementaci algoritmu RSA a později i příbuzných šifrovacích technik musela firma RSA (nyní je to divize “RSA Laboratories" společnosti RSA Security Inc.) vydat řadu standardů, které přesně definovaly použití algoritmu RSA a související formáty různých datových struktur. Tyto standardy, známé jako normy PKCS (Public-Key Cryptography Standards, blíže viz infotipy), začaly vznikat v roce 1991 jako výsledek práce malé skupiny nadšených implementátorů kryptografie s veřejným klíčem. První oficiální vydání přišlo ale až v roce 1993 a od té doby se počet těchto standardů mění (vznikají nové a některé zanikly) a v rámci každého standardu postupně vznikají nové revize.

Dosud bylo vydáno 15 těchto standardů (PKCS#1 až PKCS#15) a jejich současný stav vidíte v připojené tabulce. Poněvadž začínaly jako první, staly se PKCS základem i mnoha jiných

standardů, např. pro elektronickou poštu, internetové prohlížeče či v oblasti bankovnictví. Dnes jsou tyto standardy vytvářeny v širším kontextu, aby se dosáhlo co největší interoperability; navíc nejsou jedinými standardy na tomto poli a soutěží s řadou dalších. Jsou ale zatím ve výše uvedených oblastech dominantní, a tak jsou zahrnuty nebo jsou kompatibilní s dalšími formálními i neformálními standardy, včetně dokumentů skupiny ANSI X9 (bankovní oblast), PKIX (infrastruktura veřejných klíčů), SET (platební transakce), S/MIME (elektronická pošta), SSL (internetové prohlížeče), IEEE P1363 (skupina prestižního amerického institutu IEEE, pracující na standardech různých kryptografických technik).

Shrnutí

V oblasti asymetrických šifer jde v současné době o dvě služby – digitální podpis a výměnu klíčů. Od algoritmu k realizaci je však poměrně daleko, a tak nepochybně přežijí jen ty algoritmy, které jsou podporovány uznávanými standardy, a to nejlépe od státních nebo mezinárodních institucí. Jednou z takových skupin standardů je série PKCS, která se týká využití algoritmu RSA.

Vlastimil Klíma
(v.klima@decros.cz)

Normy PKCS

Název standardu	Poznámka
PKCS #1: RSA Cryptography Standard	Základní dokument, který definuje zejména základní operace RSA, strukturu veřejného a privátního klíče a kódování (konverzi) vstupně-výstupních dat. Platná verze: 2.0 z 1. 10. 1998, připravuje se verze 2.1.
PKCS #2	Byl zrušen, je zahrnut v PKCS#1.
PKCS #3: Diffie-Hellman Key Agreement Standard	Popisuje implementaci Diffieho-Hellmanova algoritmu pro výměnu klíčů. Platná verze: 1.4. z 1. 11. 1993.
PKCS #4	Byl zrušen, je zahrnut v PKCS#1.
PKCS #5: Password-Based Cryptography Standard	Protože uživatelská hesla jsou často používána ve funkci symetrických klíčů, ale většinou je takto nelze použít přímo, standard popisuje způsob práce s nimi a jejich použití v různých kryptografických technikách (solení, MAC). Platná verze: 2.0. z 25. 3. 1999.
PKCS #6: Extended-Certificate Syntax Standard	Tento standard popisuje syntaxi tzv. rozšířených certifikátů, které se skládají z klasického certifikátu podle uznávané normy X.509, ale navíc jsou k němu připojeny další informace, a tento datový obsah je podepsán vydavatelem certifikátu. Záměrem bylo přidat informace k prvotní “chudší" verzi certifikátu X.509, což bylo ale později vyřešeno zahrnutím přídavných informací (tzv. extensions) přímo do normy X.509 v.3. Platná verze: 1.5 z 1. 11. 1993; standard zatím platí, ale od jeho použití se bude z výše uvedených důvodů ustupovat.
PKCS #7: Cryptographic Message Syntax Standard	Definuje šest základních typů datových struktur (např. data, podepsaná data, šifrovaná data a digitální obálky) umožňujících vnořování, které jsou klíčové pro použití zejména pro další protokoly, například S/MIME.

	Ve verzi 1.6 se ustupuje od podpory PEM a PKCS#6, a naopak se podporuje SET a X.509 v.3. Ve verzi 2.0 se předpokládá podpora pro symetrické klíčové hospodářství (!) a také změna identifikace vlastníků veřejného klíče ze současné metody podle vydavatele a sériového čísla na novější metodu podle jména vlastníka klíče. Platná verze: 1.5 z 1. 11. 1993. Byla oznámena revize 1.6 z 13. 5. 1997, která ale není oficiální, a připravuje se zásadní revize 2.0.
PKCS #8: Private-Key Information Syntax Standard	Privátní klíče asymetrických systémů musí být někde uloženy. Aby byly chráněny, jsou opět šifrovány – tentokrát symetrickými algoritmy. Standard definuje, jak se to dělá, a odpovídající datové struktury. Typicky se zde využívá PKCS#5. Platná verze: 1.2 z 1. 11. 1993.
PKCS #9: Selected Attribute Types	Standard definuje vybrané datové typy a objektové identifikátory pro ostatní normy PKCS#6, #7, #8 a #10. Verze 2.0 obsahuje dva zcela nové pojmy (pkcsEntity a naturalPerson) a datové struktury pro podporu PKCS #7, digitálně podepsaných zpráv pomocí S/MIME CMS, žádostí o certifikáty podle PKCS #10, výměnu osobních informací podle PKCS #12 a pro podporu kryptografických tokenů podle PKCS #15. Platná verze: 2.0 z 25. 2. 2000.
PKCS #10: Certification Request Syntax Standard	Definuje syntaxi žádosti o certifikát. Žádost se skládá z údajů o žadateli, jeho veřejného klíče a volitelně z řady dalších atributů. Certifikát je vydán podle normy X.509. S normou těsně souvisí PKCS #7 a PKCS #9. Uvažuje se i podpora PKI podle RFC 2510 (Internet X.509 Public Key Infrastructure – Certificate Management Protocols. March 1999). Platná verze: 1.7 z 26. 5. 2000.
PKCS #11: Cryptographic Token Interface Standard	Tento standard specifikuje aplikační interfejs Cryptoki na obecné moduly nebo zařízení, která obsahují kryptografické informace (klíče) nebo vykonávají kryptografické funkce. Je to API například na čipové karty nebo HW šifrovací zařízení. Proto se jedná o mimořádně důležitý standard pro budoucí aplikace. Je používán zejména prohlížečem Netscape, naproti tomu Microsoft o podpoře PKCS#11 neuvažuje, protože má vlastní kryptografické API (MS CAPI). Platná verze: 2.10 z prosince 1999.
PKCS #12: Personal Information Exchange Syntax Standard	Popisuje syntaxi pro ukládání nebo přenos osobních informací, jako jsou například privátní klíče uživatelů, certifikáty a různé další tajné informace. Standard umožní, aby různá zařízení, programy, internetové kiosky, browsery apod. mohly importovat a exportovat tyto osobní informace. Standard podporuje různé metody šifrování i zajištění integrity dat a

	navazuje na PKCS #8. Platná verze: 1.0 z 24. 6. 1999.
PKCS #13: Elliptic Curve Cryptography Standard	Nejedná se vlastně o standard, ale teprve o zahájený projekt. Výsledkem bude nejspíše podpora standardu IEEE P1363. Až bude vydán, bude se zabývat různými aspekty kryptografie realizované na eliptických křivkách (ECC) a zahrne všechny detaily. Podobně jako řada PKCS byla vytvořena pro realizaci RSA a souvisejících technik, standardy P1363 jsou de facto mírně konkurenčním projektem, protože se týkají oblasti ECC. Protože zahrnují také RSA, lze PKCS#13 chápat jako “přemosťující" dokument. Plán projektu je z 12. 1. 1998.
PKCS #14: Pseudorandom Number Generation Standard	Tento standard je zatím ve fázi příprav, nicméně ze současného stavu je vidět, že se bude generováním (pseudo)náhodných čísel zabývat velmi podrobně a bude přínosný. Plán projektu (verze 1.0) pochází z roku 1998, zatím je pouze v powerpointové prezentaci.
PKCS #15: Cryptographic Token Information Format Standard	Tento dokument je zamýšlen jako standard, který zajistí, aby uživatel mohl používat kryptografické tokeny (opět zejména čipové karty) k vlastní identifikaci (nebo prezentování certifikátu) nebo kryptografickým operacím. Reaguje na všeobecnou nekompatibilitu programů a čipových karet, a proto se zaměřuje na datové formáty. Zejména specifikuje adresářový a souborový formát pro ukládání zmíněných informací. Platná verze: 1.1 z 6. 6. 2000.