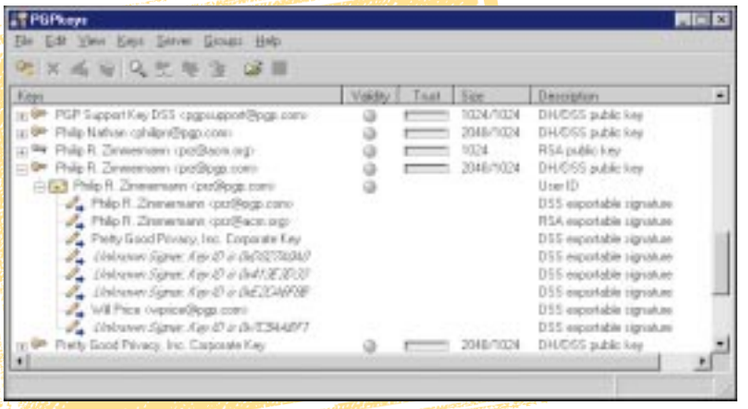
DSS

Podpis bez pera i papíru

Dnes se seznámíme s americkým vládním standardem digitálního podpisu DSS, který ve světě patří k nejpopulárnějším. Státním i komerčním institucím umožňuje digitálně podepisovat elektronickou poštu, dokumenty, programy, zkrátka vše, co má digitální podobu. Oč lehčeji by se nám s digitálním podpisem žilo, jsme naznačili na předcházejících stránkách.

Digitální podpisy jsou elektronickým protějškem ručně psaných podpisů. Jsou to složitě generovaná čísla, která nevypočítává člověk, ale mikroprocesor (nejčastěji čipové karty nebo PC). K výpočtu je potřeba také (pěkně dlouhé) tajné číslo, tzv. ***podepisovací klíč***, které si však člověk není schopen zapamatovat. Bývá proto uloženo na čipové kartě nebo v PC a chráněno nějakým PIN nebo přístupovým heslem daného uživatele. Digitální podpis ale – na rozdíl od toho klasického – závisí kromě podepisovacího klíče také zásadním způsobem na každém bitu (!!!) podepisované zprávy.



DSS se stává standardem mnoha aplikací; na obrázku vidíte několik klíčů a jejich podpisů v programu PGP v. 6.

Digitální podpisy mohou nahradit ruční podpisy, protože je může ověřit příjemce zprávy i jakákoli další osoba. Ověření umožňuje tzv. ***veřejný klíč***, který je zcela volně dostupný, a kdokoliv jím může kontrolovat správnost digitálního podpisu (opět to nedělá člověk, ale mikroprocesor). Digitální podpisy samozřejmě vylučují možnost padělání podpisu příjemcem podepsané zprávy nebo jakýmkoliv jiným útočníkem – najde se jistě spousta těch, kdo by chtěli padělat podpis banky na digitální bankovce nebo podpis klienta na příslušně modifikovaném bankovním převodu. Digitální podpisy ale zabraňují i tomu, aby sám jeho tvůrce odmítl již existující podpis (také v „digitálním světě“ by jistě člověk občas rád odvolal svůj podpis smlouvy, směnky, internetového nákupu apod.).

DSA – šifra, která nešifruje

Základem digitálních podpisů jsou asymetrické šifrovací algoritmy. Zmínili jsme se o nich už v několika článcích Chipu, a přejdeme proto rovnou k definici jednoho z nich. Jmenuje se ***Digital Signature Algorithm (DSA)*** a je popsán v dokumentu Digital Signature Standard (DSS, viz infotipy). Zkratky DSA a DSS se často zaměňují, ke zmatku by to však vést nemělo.

Asymetrický algoritmus DSA má jednu zvláštnost – umožňuje **pouze digitální podpis**, ale nedá se využít k šifrování dat (podle normy), jako je tomu u jiných asymetrických šifer (např. RSA, algoritmy eliptických křivek apod.). Je to dáno použitou matematikou pocházející z dílny NSA (National Security Agency), která si nepřála poskytnout národní standard pro asymetrické šifrování, ale jen pro podepisování.

Vznik algoritmu

Až do prosince 1990 Národní úřad pro standardizaci (NIST – National Institute of Standards and Technology), který měl vydání algoritmu digitálního podpisu na starosti, uvažoval, že navrhne algoritmus RSA, v té době de facto jediný průmyslový podepisovací standard v USA. O osm měsíců později, v srpnu 1991, se však rozhodl pro DSA, neboť NSA odepřela kvalitu RSA jakkoliv podpořit.

Účast NSA (jako bezpečnostního konzultanta NIST) v tomto procesu vyvolala vlnu nevole i kritiky samotného algoritmu. Kromě účelových námitek a senzačního nádechu kritik však tato bouře vedla NIST také k přidání nového parametru, který umožnil zvýšit kryptografickou sílu původního algoritmu. Původní návrh definoval modul (viz dále) o délce 512 bitů, konečná verze standardu umožňuje délku modulu zvyšovat v krocích po 64 bitech až na konečných 1024 bitů. Standard byl pak oficiálně přijat v roce 1994.

Ukázalo se, že to bylo prozíravé rozhodnutí. Dnes, i když žádný praktický útok na nižší modul není znám, se mnohem častěji používá modul 1024 bitů. Je po-

važován za naprosto bezpečný nejen v současnosti, ale i v horizontu mnoha desítek let. Díky tomu máme dnes k dispozici silný kryptografický nástroj pro digitální podpis, jehož kvalitu garantuje NSA. A to není špatné.
Navíc si další vývoj vyžádal také akceptaci algoritmu RSA, a tak v prosinci 1998 bylo navrženo, aby standard DSS byl aktualizován i o něj. V současné době je tento návrh v pracovní verzi (viz infotipy) a očekává se, že bude přijat. Jde pravděpodobně o důsledek tlaku americké asociace bank (RSA používá bankovní norma X9.31) a možná i blížícího se data expirace patentu RSA. DSA byl zahrnut do amerických bankovních norem ANSI, je používán jako běžný průmyslový standard v mnoha společnostech i aplikacích a na rozdíl od RSA nepodléhá licenčním poplatkům.

Co říká standard

Standard stanovuje, že digitální podpis je elektronická analogie psaného podpisu v tom, že může být použit pro důkaz příjemci nebo třetí straně, že zpráva v dané podobě byla skutečně podepsána svým původcem. Digitální podpis může být také pořízen pro uložená data nebo programy, takže později může být zkontrolována jejich integrita. Algoritmus DSA je použit jak k vytvoření, tak i ke kontrole digitálního podpisu. Každý signatář má tajný a veřejný klíč – tajný je použit k vytvoření podpisu, veřejný k jeho verifikaci.
Každý signatář si svůj tajný klíč chrání, protože při jeho odcizení zloděj získává možnost právoplatného digitálního podpisu za okradeného. Naproti tomu u párového veřejného klíče má signatář zájem na tom, aby se co nejvíce rozšířil, například v lokální síti nebo na internetu (viz třeba servery klíčů pro PGP na webové adrese *www.pgpi.com/products/keyservers.shtml*).
Kdo nezná tajný klíč signatáře, nemůže jeho jménem podepisovat. Naproti tomu každý může veřejným klíčem signatáře verifikovat správnost jeho podpisu. V tom spočívá ona asymetrie: tajným klíčem se podepisuje, veřejným ověřuje; podepisovat může jen vlastník tajného klíče, ověřovat může kdokoliv.
Poznamenejme ještě, že místo zprávy M se podepisuje a ověřuje jen její hašovací hodnota H(M). Jak víme z předchozích článků o hašovacích funkcích, je to naprosto dostatečné a bezpečné. Jako hašovací funkce je použita SHA-1, o níž jsme psali v minulém Chipu. A ještě jedno upozornění. Až si budete pročítat standard DSS (FIPS PUB 186), mějte na mysli, že původní hašovací funkce SHA (FIPS 180) je dnes nahrazena funkcí SHA-1 (FIPS 180-1) – viz též infotipy.

Namísto rukopisu tajný klíč

Abychom následující popis zjednodušili, vynecháme parametrizaci a popíšeme jen DSA s 1024bitovým modulem p. Úplný popis můžete najít na internetu (viz infotipy). DSA používá tyto parametry a klíče:

Parametry

- Veřejný modul **p**, což je 1024bitové prvočíslo v rozsahu $2^{1023} < p < 2^{1024}$.
- Veřejné 160bitové prvočíslo **q** v rozsahu $2^{159} < q < 2^{160}$, které je dělitelem čísla $p - 1$.
- Veřejné číslo **g**, které vznikne volbou přirozeného čísla **h** $(1 < h < p - 1)$ tak, že $g = h^{(p-1)/q} \bmod p > 1$.

(g je generátor cyklické podgrupy řádu q v grupě čísel 1 až p – 1.)

Klíče

- Tajný 160bitový klíč **x**, tj. číslo v rozsahu $0 < x < q$.
- Veřejný 1024bitový klíč **y** takový, že $y = g^x \bmod p$.

Čísla p, q, g (například pro účely certifikátů) označujeme jako ***parametry DSS***; jsou veřejné, a mohou být dokonce společné pro skupinu uživatelů (RSA podobnou vlastnost nemá, byla by to bezpečnostní slabina). Čísla y a x jsou skutečné ***klíče***. Povšimněte si, že tajný klíč má délku 160 bitů, což je na rozdíl od jiných asymetrických systémů velmi malé číslo (užitečné pro čipové karty). Na tajný klíč se jinak nekladou téměř žádné nároky, takže je možné, aby vznikal přímo hašováním passwordů, heslových frází apod.
Dále se zde používá 160bitový parametr **k** $(0 < k < q)$, který se generuje pro každý podpis zvlášť. Musí být generován náhodně a nesmí být prozrazen stejně jako tajný klíč x (při podepisování nové zprávy je generována nová hodnota k). Způsob generování uvedených parametrů i klíčů je poměrně podrobně definován v normě.

infotipy

Definice standardu SHA-1 (FIPS 180-1):
http://www.itl.nist.gov/div897/pubs/fip180-1.htm

Současná definice standardu DSS (FIPS 186):
http://www.itl.nist.gov/div897/pubs/fip186.htm
(Pozor! Zde jmenovaná hašovací funkce SHA byla aktualizována na SHA-1.)

Nový pracovní návrh DSS (nejnovější verze zahrnující i RSA; FIPS 186-1):
http://csrc.nist.gov/fips/fips1861.pdf

Vše o prvním digitálním podpisu mezinárodní dohody:
http://www.baltimore.com/clintonvisit98/

Račte se podepsat!

Jak se tedy vlastně podepíše zpráva **M**? Nejprve se vytvoří hašovací kód **m** = H(M) za použití funkce SHA-1. Poté se vygeneruje (buď náhodně, nebo normou stanoveným postupem) číslo **k** a vypočítá se dvojice čísel **(r, s)**, které tvoří podpis:
$r = (g^k \bmod p) \bmod q$,
$s = (k^{-1}(m + xr)) \bmod q$.
Čísla **r** a **s** se pak jako podpis připojí ke zprávě M a takto tvoří celek – zprávu s připojeným digitálním podpisem.
Ke vzorcům poznamenejme, že k^{-1} je multiplikativní inverzí čísla **k** v modulu **q**, tj. takové číslo $0 < k^{-1} < q$, pro něž platí $(k^{-1} * k) \bmod q = 1$.
Je nutné si uvědomit, že číslo **k** se druhé straně nijak nepředává a že ověřovatel podpisu je z hodnot **(r, s)** musí eliminovat. Úloha čísla **k** de facto spočívá v maskování tajného klíče **x** (hodnota **r** v rovnici pro **s**) při podepisování každé zprávy, a to vždy novým způsobem. Ověřovatel může zjistit, že tajný klíč **x** byl při tvorbě **(r, s)** použit, čímž potvrdí platnost podpisu, ale nemůže určit hodnotu **x** ani hodnotu **m**. Nemožnost určení hod-

noty **m** souvisí s tím, že DSS neumožňuje data šifrovat, ale jen podepisovat.

Jak se podpis ověří

Příjemce zprávy **M** si vypočte její hašovací hodnotu **m** = H(M) a dále z důvěryhodného zdroje musí získat parametry **p**, **q**, **g** a veřejný klíč signatáře **y**. Tato zdánlivě nevinná podmínka je klíčová pro zjištění digitální identity signatáře a její naplnění velmi ztěžuje masové nasazení jakýchkoliv asymetrických systémů. Proto také standard DSS způsob „důvěryhodného“ získání těchto hodnot nijak neřeší – tento problém ponechává certifikačním autoritám a různým systémům „infrastruktury veřejných klíčů“ (PKI, Public Key Infrastructure).

Vraťme se ale k ověření zprávy. Příjemce zkontroluje, že 0 < r, s < q, a vypočte pomocné proměnné:

$w = s^{-1} \bmod q$,

$u1 = mw \bmod q$,

$u2 = rw \bmod q$,

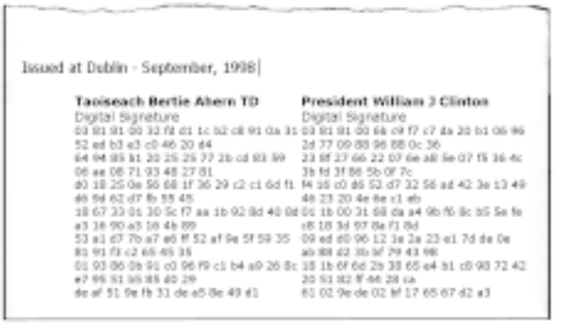
$v = (g^{u1} y^{u2} \bmod p) \bmod q$.

Je-li vše v pořádku, musí být **v** = **r**. Důkaz této rovnosti sice vyžaduje teorii čísel, ale není příliš obtížný. Zájemci ho naleznou v dodatku normy.

Výhody a nevýhody DSS

Bezpečnost DSA je dána tím, že využívá tzv. ***problém diskrétního logaritmu***. DSA je navržen profesionálně a zcela průhledně. Kryptologové jej považují za bezpečný s perspektivou mnoha desítek let a vůbec jim nevadí, že jeho návrh pochází od tajné služby.

Americký prezident a irský ministerský předseda digitálně podepisují komuniké o elektronickém obchodu...



... a takhle vypadají jejich digitální podpisy. (Pro pozorné čtenáře: zde byla použita šifra RSA, a podpis je proto tvořen pouze jedním číslem.)

Nevýhodou DSA je jednak nutnost generovat hodnotu **k** na každou zprávu, jednak o něco pomalejší verifikace podpisu než u jiných metod. Rychlost se však dohání různými triky, jako je možnost tabelovat hodnoty g^{u1} a y^{u2} (mod p mod q) předem pro všechny jednotkové vektory u1 a u2, předvypočítávat si sady hodnot **k** a **r** (všimněte si, že **r** vůbec nezávisí na zprávě, jen na **k**) apod. V současné době je mnoho digitálních podpisů vytvářeno čipovými kartami nebo softwarem PC a doba výpočtu je v obou případech (desetiny až jednotky sekund) zanedbatelná třeba vzhledem k době potřebné pro zasunutí čipové karty do snímače nebo vložení přístupového hesla.

Jednou z velkých výhod DSA je však to, že (například oproti RSA) jeho použití je zdarma. Například v nejnovější verzi známého programu PGP je použit právě DSA ve spojení s SHA-1 (dříve to byla kombinace RSA a MD5).

Závěr

Algoritmus DSA se dnes už široce používá pro digitální podpis v různém bezpečnostním softwaru a hardwaru. Byl přijat jako bankovní, průmyslový i státní standard a je považován za bezpečný. Budeme se s ním stále častěji setkávat v elektronickém obchodu, v bezpečnostních mechanismech operačních systémů a v mnoha různých aplikacích.

VLASTIMIL KLÍMA (*VKLIMA@DECROS.CZ*)

První digitální podpis na státní úrovni

Americký prezident Bill Clinton a irský ministerský předseda Bertie Ahern se 4. září 1998 zapsali do historie hned dvěma událostmi. Za prvé společně podepsali komuniké (dohodu) o podpoře pro elektronický obchod a za druhé toto komuniké podepsali digitálně.

Komuniké je zajímavé samo o sobě, neboť se vyjadřuje ke všem klíčovým otázkám elektronického obchodování. Například se říká, že klíčovou roli v elektronickém obchodě hraje liberalizace telekomunikačního trhu a že elektronický obchod zvýší životní úroveň obou států apod. Dále se prohlašuje, že role vlád spočívá ve vytvoření jasného a konzistentního právního rámce pro elektronický obchod a ve vytvoření konkurenčního prostředí, v kterém by se mohl rozvíjet a zajistit adekvátní ochranu veřejných zájmů v oblastech, jako je soukromí, intelektuální vlastnická práva, prevence proti podvodům, ochrana zákazníků a bezpečnost.

Komuniké se vyjadřuje i k tolik diskutovaným daním z elektronického obchodu, a dokonce i k systému doménových jmen, je poměrně obsáhlé (na tři strany) a celé si je můžete přečíst na *www.baltimore.com/clintonvisit98/communique.htm*/ nebo také na Chip CD v tomto čísle.