Kryptologie pro praxi – Jak Diffie zaspal

V květnu navštívil Prahu Whitfield Diffie, žijící legenda kryptografie a spoluautor stěžejní koncepce asymetrických schémat (viz [1], ST 8/2003 a ST 5/2004). Podíváme-li se ovšem trochu do historie kryptografie, nelze přehlédnout, že zatímco pánové Diffie a Hellman koncepci asymetrické kryptografie popsali, slávu a peníze na ní získali spíše jejich kolegové Rivest, Shamir a Adleman, jejichž metoda RSA [3] vyšla až o dva roky později. Že to trochu trápí i samotného Diffieho, svědčí skutečnost, že při odpovědi na otázku: „Co byste dnes udělal jinak?“ se řeč téměř okamžitě stočí k tématu prohraného konkurenčního zápasu mezi schématy z rodiny Diffie-Hellman (viz protokol D-H a ElGamalovy algoritmy, ST 5/2004 a ST 6/2004) a schématem RSA (ST 3/2004).

Zápas, který se nikdy nekonal

Jak víte z tohoto seriálu [4], jsou schémata z rodiny Diffie-Hellman založena na problému diskrétního logaritmu, zatímco matematický problém garantující bezpečnost RSA se nazývá e-tá diskrétní odmocnina. Obě úlohy můžeme zadat nad mnoha různými algebraickými strukturami (viz například ST 10/2005), některé z nich přitom vedou na jednodušší, jiné zase na složitější instance těchto problémů. Pro příklad vyjdeme z operace násobení modulo celé číslo. Problémem diskrétního logaritmu je pak pro dané celé číslo y, $0 < y < p$, nalézt celé číslo x, $0 < x < p$, splňující rovnici $g^x \bmod p = y$. Přitom p je prvočíslo a g generátor grupy Z_p^*. V některých kryptografických schématech nevyužíváme celou grupu Z_p^*, nýbrž jen nějakou její cyklickou podgrupu velkého prvočíselného řádu. Úloha e-té diskrétní odmocniny je schématem RSA zadána následovně: pro dané celé číslo y, $0 < y < N$, najít celé číslo x, $0 < x < N$, splňující rovnici $x^e \bmod N = y$. Přitom N a e jsou celá kladná čísla splňující $\gcd(e, \phi(N)) = 1$, kde ϕ je Eulerova funkce a gcd je největší společný dělitel. Záměrně zde nepředepisujeme, že N je prvočíslo, neboť v tomto případě by šla úloha triviálně řešit, a tudíž by v kryptografii byla nepoužitelná. Snadno se o tom přesvědčíme. Je-li N prvočíslo, potom podle Fermatovy věty pro všechna celá y, $\gcd(y, N) = 1$, platí $y^{N-1} \bmod N = 1$. Označme d celé číslo splňující $ed = 1 + k(N-1)$, kde k je celé číslo. Takové d existuje, protože podle zadání máme $\gcd(e, \phi(N)) = \gcd(e, N-1) = 1$, takže d snadno vypočteme pomocí rozšířeného Euklidova algoritmu. Nyní můžeme pro x psát $x = y^d \bmod N$, neboť platí $(y^d \bmod N)^e \bmod N = y^{de} \bmod N = y^{1+k(N-1)} \bmod N = y*(y^{N-1})^k \bmod N = y*1^k \bmod N = y$.

Má-li být úloha e-té diskrétní odmocniny náležitě složitá, potom musí být obtížné ze znalosti jejího zadání určit celé číslo λ, pro které pro všechna přirozená k a celá y, $0 < y < N$, platí $y^{1+k\lambda} \bmod N = y$. To lze zajistit pouze pro N složená z velkých prvočíselných faktorů. Strukturu N pak musíme pro zajištění bezpečnosti utajit. A v tom to právě podle Diffieho vězí. V případě zadání problému diskrétního logaritmu nemusí zůstat o hodnotách p a g nic skryto, zatímco v případě e-té diskrétní odmocniny musíme utajit řadu strukturálních vlastností čísla N. To by samo o sobě

nemuselo být tak zlé, nebýt ovšem toho, že ve struktuře veřejných parametrů asymetrických systémů mohou být ukryta zadní vrátka vedoucí například k hodnotě soukromého klíče. Taková vrátka by mohl vytvářet třeba kryptografický modul v podobě čipové karty, kterou uživatel používá k vytváření svých podpisových klíčů a následně k podepisování elektronických dokumentů. Autor firmware čipové karty by si tímto trikem kupříkladu mohl zjednat přístup k soukromým klíčům milionů uživatelů, a to pouze na základě znalosti veřejných hodnot získaných z jimi podepsaných zpráv nebo certifikátů. Šance na obranu před takovým útokem se u schémat RSA a Diffie-Hellman radikálně liší. V prvním případě není nutné o veřejných parametrech nic tajit, takže je možné zveřejnit kompletně celý postup jejich generování včetně inicializačních hodnot, které slouží jako certifikát korektnosti generovaných klíčů. V případě RSA však něco takového není možné, neboť bychom prozradili exponent λ, který musí zůstat utajen. Diffie ovšem tuto vlastnost nikdy nevyužil v konkurenčním boji proti RSA a dnes toho, zdá se, poněkud lituje.

Certifikáty veřejných parametrů DSA

Podpisové schéma DSA (ST 4/2004) můžeme také považovat za člena rodiny Diffie-Hellman, i když od prvotní myšlenky [1] už tento potomek urazil pěkný kus cesty. Schopnost nezávislé ověřitelnosti korektního generování veřejných parametrů mu však zůstala. Celý princip, je jednoduchý. Procedura generování veřejných parametrů je deterministický algoritmus, který je inicializován náhodným vektorem vytvářejícím požadovanou diverzitu jeho výsledků. Výpočet parametrů schématu DSA z náhodného vstupního vektoru je však jednosměrný proces, takže útočník nemá šanci nejprve vytvořit veřejné parametry se zadními vrátky a potom k nim dohledat správný startovní vektor. Inicializační hodnota, která je veřejná, potom společně s popisem použitého algoritmu tvoří průkaz korektnosti příslušných parametrů. Každý může opětovným výpočtem ověřit, že připojená inicializační hodnota skutečně vede k předloženým parametrům instance DSA. Něco takového je pro RSA nedosažitelným snem.

Závěr

Problematika nezávislé ověřitelnosti instancí kryptografických schémat s ohledem na existenci zadních vrátek je téma, které je aktuální, zejména díky stále intenzivnějšímu využívání nejrůznějších „černých skříněk“, tedy zařízení a implementací kryptografických algoritmů, o jejichž vnitřním uspořádání máme jen velmi málo informací. Aspekty diskutované v tomto článku by tak měly být známé všem bezpečnostním architektům.

Zajímavé je i komerční pozadí celé věci. Podle Whitfielda Diffieho by rozdělení sil mezi RSA a ostatní algoritmy vypadalo dnes poněkud jinak, jen kdyby si včas povšiml zjevného handicapu na straně RSA a jednal. Těžko samozřejmě už tvrdit, nakolik by jeho tah uspěl, ale mohl to alespoň zkusit.

Vlastimil Klíma, Tomáš Rosa,
v.klima@volny.cz, trosa@ebanka.cz

LITERATURA

[1] Diffie, W., Hellman, M. E.: New directions in cryptography, IEEE Transactions on Information Theory, Vol. 22, pp. 644-654, 1976.

[2] FIPS PUB 186-2: Digital Signature Standard,NIST, 20.1.2000, change 5.10.2001

[3] Rivest, R. L., Shamir, A., Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, 21, pp. 120-126, 1978.

[4] E-archivy http://cryptography.hyperlink.cz, http://crypto.hyperlink.cz