Kryptologie pro praxi

Jak jsme uvedli už minule [1], označujeme přívlastkem asymetrická taková schémata, která jsou založena na filozofii veřejných a privátních klíčů. Někdy se též používá označení schémata s veřejným klíčem. U asymetrických systémů dále zavádíme pojem instance. Instance je tvořena konkrétní sadou hodnot veřejných parametrů, veřejného klíče V a privátního klíče P. Odpovídající si dvojici (V,P) označujeme také jako klíčový pár. Účelem veřejného klíče V je například umožnit prakticky komukoliv zašifrovat zprávu určenou pro majitele privátního klíče P, případně ověřit platnost jím vytvořeného digitálního podpisu. To vše samozřejmě bez toho, aby s pouhou znalostí V bylo možné zprávy také dešifrovat či podepisovat.

Bezpečnost současných asymetrických systémů je založena na složitosti určitých vybraných algebraických problémů. V teorii složitosti přitom rozlišujeme mezi pojmy problém a instance problému. Prvním z nich označujeme obecně určitý druh úlohy, například rozklad celého čísla na jeho prvočíselné faktory (takzvaný problém faktorizace). Druhým výrazem pak nazýváme zadání dotčené úlohy pro konkrétní čísla, například: faktorizujme číslo 15. Výsledkem je 15=5×3. Z uvedeného také vyplývá, že zatímco nějaký problém může být obecně považován za neschůdný (jako tomu u faktorizace je), mohou existovat i takové jeho instance, které jsou triviálně řešitelné. Tento postřeh je pro asymetrickou kryptografii zcela zásadní, neboť nás varuje před tím, abychom bezpečnost konstruovaných systémů zakládali na zcela libovolných instancích jinak složitých problémů. Přitom rozhodně nejde jen o délku zadání dané úlohy. Jistě, faktorizace čísla 15 vypadá na první pohled mnohem nadějněji, než pokud bychom v zadání viděli například číslo o 155 dekadických řádech. Nicméně existují i takto dlouhá čísla, která lze díky jejich struktuře velmi snadno faktorizovat. Proto je nutné volbě konkrétní instance „zabezpečovacího“ problému věnovat patřičnou péči. Jedním z důsledků je explicitní zavedení zmíněných veřejných parametrů, které slouží právě ke konkrétnímu určení matematické úlohy, jejíž náročnost bude garantovat bezpečnost dané instance kryptografického schématu. Dalším důsledkem je mnohem větší péče věnovaná otázkám generování klíčů pro asymetrické systémy, neboť, narozdíl od běžných symetrických šifer, zde rozhodně nelze postupovat tak, že každý binární řetězec příslušné délky je automaticky vhodným kandidátem.

Situaci kolem veřejných parametrů ještě poněkud komplikuje to, zda je lze u daného schématu sdílet mezi více uživateli (kde každý uživatel má svůj pár (V_i,P_i)), či nikoliv. Příkladem prvního typu je podpisové schéma DSA a jeho rozšíření ECDSA [2], [3], [4]. Zástupcem druhého typu je pak RSA [2], [3], [4], [5], kde sice můžeme jako veřejný parametr z definice označit takzvaný modul N, avšak jedno konkrétní N není možné sdílet mezi více uživateli, neboť by to vedlo k zásadnímu oslabení bezpečnosti. Z tohoto důvodu se modul N často spíše považuje za inherentní součást veřejného a privátního klíče. Z praktického hlediska se nemožnost sdílení modulu u RSA nepovažuje za nějakou zásadní nevýhodu.

Základní druhy asymetrických schémat

Mezi základní druhy asymetrických kryptoschémat patří kromě šifer ještě protokoly pro dohodu na klíči a podpisová schémata. Instance asymetrické šifry určuje takzvanou šifrovací (E_V) a odšifrovací (D_P) transformaci, splňující $D_P(E_V(x))=x$ pro všechna x z definičního oboru funkce E_V. Zároveň požadujeme, aby pro náhodně volené $y\in \mathrm{Im}(E_V)$ bylo při pouhé znalosti E_V neschůdné najít x takové, že $y=E_V(x)$. Tento požadavek se často nesprávně nahrazuje požadavkem neschůdnosti výpočtu P ze znalosti V, což je v tomto případě slabší důsledková forma. S ohledem na současné způsoby konstrukce E_V a D_P je nutné zdůraznit, že tyto transformace většinou samy o sobě ještě nedokáží vytvořit odolné šifrovací schéma. Velmi důležitou roli hrají ještě kódovací a dekódovací transformace, jejichž použití se často souhrnně označuje jako formátování. Smyslem těchto transformací není bezprostřední utajení, nýbrž úprava algebraických vlastností zpráv před šifrováním. Označíme-li si kódovací, respektive dekódovací funkci jako ψ, respektive ψ^{-1}, vypadá výpočet šifrového textu C pro zprávu M následovně: $C=E_V(\psi(M))$. Odšifrování pak probíhá jako $M=\psi^{-1}(D_P(C))$. Vzhledem k důležitosti této problematiky se otázkám správného formátování ještě budeme věnovat.

Schémata pro dohodu na klíči je možné chápat jako jistý druh optimalizace asymetrických šifer s ohledem na způsob, jakým jsou tyto běžně používány. Víme [1], že asymetrická šifra v praxi většinou šifruje pouze náhodně vygenerovaný symetrický klíč, kterým se pak již s pomocí řádově rychlejších symetrických šifer zabezpečí vlastní data přenášené zprávy. Úlohou asymetrické kryptografie je tak ve skutečnosti jen to, aby si odesilatel s příjemcem bezpečným způsobem ustanovili dočasný symetrický klíč, nemusí tedy nutně jít o to, aby odesilatel klíč vygeneroval a pak přenesl příjemci. Protokoly dohody na klíči tuto skutečnost reflektují tím, že v sobě de facto atomicky kombinují proces náhodného generování symetrického klíče s jeho asymetricky chráněným přenosem. Díky tomu jsou v jistém smyslu robustnější a efektivnější nežli klasické asymetrické šifry. Konkrétně se jedná například o Diffieho-Hellmanův protokol [2], [3], [4], [5].

Podpisové schéma lze elegantním způsobem vytvořit například z asymetrické šifry splňující rovnici $E_V(D_P(x))=x$ pro všechna x z definičního oboru funkce D_P. Příkladem takové (reverzibilní) šifry je třeba RSA. Označme h nějakou jednocestnou bezkolizní hašovací funkci [1], splňující $\mathrm{Im}(h)\subseteq\mathrm{Def}(D_P)$. Zprávu M pak můžeme podepsat jako $S=D_P(h(M))$. Ten, kdo bude chtít podpis S ověřit, spočítá $y=E_V(S)$ a ověří, zda $y=h(M)$. Pokud ano, uzná podpis jako platný, v opačném případě jej odmítne. Podmínka na nepadělatelnost podpisu zde říká, že pro libovolnou zprávu M musí být při pouhé znalosti E_V neschůdné najít S takové, že $h(M)=E_V(S)$. To přesně konvenuje s výše uvedenou podmínkou kladenou na bezpečnost asymetrických šifer. Čili, neprolomitelnost použité šifry zároveň garantuje nepadělatelnost našeho podpisu. Pro praxi je důležité poznamenat, že zatímco zde jsme pracovali s ideálními transformacemi E a D, aktuálně používané funkce (třeba RSA) rozhodně takto ideální nejsou, a tak i v případě podpisových schémat tohoto typu hraje důležitou roli správné formátování. Takže místo podepisování haše zprávy M ve skutečnosti podepisujeme $\psi(h(M))$, tedy tuto haš dále zformátovanou pomocí formátování ψ. Dále si všimněme, že podpis S zprávy M jsme získali tak, že hodnotu $h(M)$ jsme pomocí D_P odšifrovali, nikoliv zašifrovali, jak se často mylně uvádí. Abychom si však ušetřili častá nedorozumění, je nanejvýš taktické označovat transformaci D_P, respektive E_V v kontextu podpisového schématu jako podepisovací, respektive ověřovací. Uvedená obecnější terminologie navíc usnadňuje pochopení takových schémat, která nejsou takto jednoduše založena na bázi nějaké asymetrické šifry. Jedná se například o standardy DSA a ECDSA, které popisuje norma FIPS PUB 186-2 vydaná americkou autoritou NIST.

Vlastimil Klíma, Tomáš Rosa,
v.klima@volny.cz, t_rosa@volny.cz

LITERATURA

[1] Kryptologie pro praxi (2), Sdělovací technika č. 7, str. 16, 2003.

[2] Menezes, A.-J., van Oorschot, P.-C. and Vanstone, S.-A.: Handbook of Applied Cryptography, CRC Press, 1996

[3] http://adela.karlin.mff.cuni.cz/tuma/ciphers.html

[4] http://decros.cz/bezpecnost/kryptografie.html

[5] http://www.rsasecurity.com/rsalabs/pkcs/index.html