Kryptologie pro praxi – metoda RSA

Když roku 1978 vyšel článek pánů Rivesta, Shamira a Adlemana (zkráceně R-S-A) o nové asymetrické metodě vhodné pro šifrování a podepisování zpráv, patrně nikoho z autorů nenapadlo, že jejich systém bude o nějakých 26 let později nejrozšířenějším standardem asymetrické kryptografie. Autoři RSA měli štěstí a použili pro jištění bezpečnosti RSA solidní matematický problém, který dodnes nebyl prakticky přemožen a navíc vhodně použili parametr (délku modulu), jehož zvyšováním lze snadno a efektivně zvyšovat bezpečnost RSA. To vše ovšem neznamená, že RSA jako kryptografická metoda by byla bez jakýchkoliv vad na kráse. Naopak, prakticky každý rok se na RSA něco většího či menšího „záplatuje". Základní definice RSA se totiž zabývá pouze zavedením šifrovacích/odšifrovacích, respektive ověřovacích/podepisovacích transformací [1], zatímco nejvíce problémů vznikalo ve formátování (kódování) zpráv pro RSA [2]. Další „záplatování" konkrétních aplikací RSA přinesl objev postranních kanálů [3], které ukázaly, že RSA je extrémně bezpečnostně citlivá na každý detail konkrétní implementace. RSA se však zatím dokázala ze všech problémů vždy nějak „oklepat" a žije dál.

Klíče a transformace

Veřejný klíč RSA V je tvořen dvojicí celých čísel (N, e), kde N nazýváme modul a e veřejný exponent (viz též [1], [2]), přičemž $N=pq$, kde p a q jsou přibližně stejně velká prvočísla. Optimální a zároveň obvyklá délka N dnes činí 1024 bitů, přičemž pro velmi citlivé aplikace se volí 2048 a pro mimořádně zásadní účely (ovlivňující bezpečnost států, atp.) někdy i 3072 či rovnou 4096 bitů. Délka čísla N se v případě RSA nazývá a chápe jako délka klíče. Privátní klíč RSA je v základním případě definován jako $P=(N, d)$, kde d je privátní exponent, pro který platí, že e.d mod λ=1, kde λ=lcm (p–1, q–1) je nejmenší společný násobek čísel p–1 a q–1. O výpočtech, souvisejících s RSA jsme se již v našem miniseriálu zmínili, o dalších se lze dočíst více v dostupné literatuře ([4], [5]). S využitím výše zavedeného veřejného a privátního klíče můžeme definovat šifrovací transformaci RSA jako $E_V(x)=x^e \bmod N$, kde $V=(N, e)$. Jak vidíme, máme před sebou opravdu „přátelsky" a nezáludně vyhlížející funkční předpis. Odšifrovací transformace RSA je přitom definována velmi podobně: $D_P(y)=y^d \bmod N$, kde $P=(N, d)$. Platí přitom, že $D_P(E_V(x))= E_V(D_P(x))=x$, čili RSA je reverzibilní šifra [1].

Šifrování a podpis

Budeme-li chtít RSA použít k šifrování zpráv, musíme ještě výše uvedené transformace doplnit o definici toho, jak zpracovat vstupní informaci (symetrické klíče v případě šifrování nebo haše v případě digitálního podpisu), tj. jak definovat vhodné kódovací a dekódovací schéma ψ a ψ^{-1}. Konkrétní možné metody byly představeny v [2] a podrobně popsány v [4]. I když je dnes bezesporu nejrozšířenější kódovací schéma EME-PKCS1-v1_5, je s ohledem na jeho slabiny nanejvýš vhodné maximálně preferovat jeho nástupce EME-OAEP. V případě, že budeme chtít použít metodu RSA pro podepisování, je situace v zásadě obdobná s tím, že příslušné kódovací předpisy i způsob jejich začlenění do celého výpočtu najdeme v [2] a [4].

Novinka: multiprvočíselný modul

V souvislosti s implementací RSA (včetně [4]) se často setkáme se zkratkou RSA-CRT, což znamená, že se při realizaci transformací RSA použila tzv. Čínská věta o zbytku (Chinese Remainder Theorem). Ta umožňuje urychlit odšifrovací/podepisovací transformaci za předpokladu, že k výpočtu kromě privátní hodnoty d máme ještě k dispozici další privátní hodnoty, mezi nimiž nechybí například i původní faktory p, q nebo jejich deriváty, které se jinak s hodnotou d nemusí ukládat. Právě podle této rozšířené struktury obvykle poznáme, že se jedná o implementaci RSA-CRT [4]. Hlavním parametrem určujícím zrychlení výpočtu realizovaného podle RSA-CRT je počet prvočíselných faktorů modulu N. Označíme-li tento počet b (dosud se obvykle používá b=2), potom činitel zrychlení pomocí RSA-CRT oproti klasickému RSA lze odhadnout jako b^2, takže už při klasickém b=2 dostáváme zhruba 4násobné zrychlení. To je dosti podstatné například u čipových karet provádějících autonomně digitální podpis apod. „Novinkou" je tzv. multiprvočíselná varianta RSA, kde modul N se skládá z více (b>2) faktorů, čímž lze výpočet RSA pomocí CRT ještě více urychlit. Počet faktorů modulu N nelze ale příliš zvyšovat, neboť jednotlivé faktory nesmí být příliš malé, aby to zase neumožnilo luštění celého schématu. Konzervativci proto obvykle nejdou nad b=3. Poznamenejme rovněž, že zatímco patent na klasické RSA (b=2) už vypršel, multiprvočíselná verianta pro b>2 podléhá (na území USA) patentové ochraně (US Patent #5,848,159).

Bezpečnost RSA

Základní elegance a jednoduchost RSA spolu se základní neznalostí některých „bezpečnostních expertů" vedou často k mylným závěrům, že na RSA už není co řešit, a že je to vše jen otázka nějaké běžné freewarové knihovny. Další zase šmahem odepisují celé RSA s poukazem na existenci lušticích metod a zařízení typu kvantových počítačů, TWINKLE, TWIRL, masivní paralelní NFS, atp. (o většině z těchto fenoménů viz [5]). Pravda je přitom tradičně někde mezi se zřetelným příklonem k tomu, že RSA jako taková se v blízké době padnout zjevně nechystá. Například současný rekord v délce celých čísel, která se podařilo faktorizovat, činí 576 bitů a je ze 3. prosince 2003. Když uvážíme, že složitost této úlohy roste zhruba exponenciálně s délkou N, vyjde nám, že délka 1024 bitů je daleko za horizontem současných metod. Obávané kvantové počítače jsou na tom v porovnání s klasickými faktorizačními metodami co do prakticky demonstrovaných výsledků ještě daleko hůř, jsou ale cenné v tom smyslu, že jistým způsobem potvrzují pravdivost teorie, na které jsou postaveny. U optoelektronických akcelerátorů typu TWIRL (dříve TWINKLE) jsou prognózy rozvoje součástkové základny podstatně uvěřitelnější, avšak opět zde chybí pro praxi zásadní výsledky. Za nejnebezpečnější druh útoků lze dnes považovat ty, které se na rozdíl od předchozích metod soustřeďují na zcela konkrétní implementace a jejich konkrétní slabiny, kam patří zmíněné postranní kanály [3], které pravidelně plní sborníky světových konferencí úspěšnými útoky. Zatímco u faktorizačních metod (s výjimkou vyzrálých kvantových počítačů) se může RSA snadno bránit prodlužováním modulu N, což se v podstatě kontinuálně děje, problematice související s konkrétním způsobem implementace již bohužel často taková pozornost věnována není. Praxe ukazuje, že i u poměrně velkých vývojářských a integračních firem je dnes v tomto směru kultura někde hluboko pod bodem mrazu. Přitom i zde existuje velká naděje, že při zodpovědném přístupu bude případná slabina včas odhalena a odstraněna. Znamená to ovšem nepodceňovat a včas uplatňovat nové výsledky, které se na první pohled zdají být jen další zbytečnou teorií. Zejména v případě „triviálního eresáčka" se totiž takový přístup opravdu velmi vyplácí.

Vlastimil Klíma, Tomáš Rosa,
klima@lec.cz, trosa@ebanka.cz

LITERATURA

[1] Kryptologie pro praxi (3) , ST č. 8/2003

[2] Kryptologie pro praxi (5), ST č. 10/2003

[3] Klíma, V., Rosa, T.: Vybrané aspekty moderní kryptoanalýzy, ST č. 3/2003

[4] PKCS#1: RSA Cryptography Standard, http://www.rsasecurity.com/rsalabs/pkcs/index.html

[5] Archivy článků přístupné přes: http://cryptography.hyperlink.cz a http://crypto.hyperlink.cz