Oponentní posudek na bakalářskou práci: „*Ria Ruppeldtová: Experimentálne overenie a rozšírenie Coppersmithovho útoku na RSA, 2008*"

Bakalářská práce byla předložena ve slovenském jazyce. Následuje popis jednotlivých kapitol s případným jejich hodnocením.

První kapitola sumarizuje hlavní teoretické nástroje, které budou v práci použity. Jedná se hlavně o celočíselné mřížky. Výběr témat je výstižný a podaný popis přehledný.

V kapitole 2 je popsána metoda hledání malých kořenů polynomů $p(x)$ mod N. K tomuto účelu jsou použity celočíselné mřížky a s nimi úzce související algoritmus LLL (Lenstra-Lenstra-Lovász). Popsaný algoritmus vychází z článku Nicka Howgrave-Grahama uvedeného v citaci [5] předložené práce. Zatímco je ovšem autor originálního článku [5] při svém popisu od začátku do konce fixován na myšlenku převedení problému hledání kořene „polynomu modulo N" na hledání kořene polynomu na celých číslech, soustředí se autorka předložené práce více na vlastnosti bázové matice jistého typu mřížky a převod na hledání kořene na celých číslech nechává teprve postupně vyplynout jako důsledek použité konstrukce. Vznikl tak de facto alternativní teoretický popis původního algoritmu, který lze považovat za samostatný výsledek prezentované práce. Jeho podání mohou ocenit ti, kterým se původní popis v [5] zdál poněkud účelový a nepřehledný.

V kapitole 3 je připomenut kryptografický algoritmus RSA. Jeho popis víceméně vychází ze standardu PKCS#1 (citace [9] v práci).

Kapitola 4 ukazuje využití metody popsané v kapitole 2 k útoku na určité implementace algoritmu RSA. Konkrétně se jedná o dodnes intenzivně využívané šifrování zpráv s nízkým veřejným exponentem a náhodným doplňkem, viz například již zmíněný standard PKCS#1. Oproti standardu PKCS#1 autorka rozebírá drobně odlišné formátovací schéma (jde o pořadí zprávy a doplňku ve zformátovaném řetězci), avšak úprava předvedeného postupu pro schéma skutečně používané dle citovaného standardu je věcí ryze kosmetickou, která nijak nesnižuje hodnotu předložené práce.

Pátá, poslední kapitola prezentuje výsledky experimentálního ověření útoku popsaného v kapitole 4. Samotná funkční implementace útoku v jazyku C++ s podporou knihoven NTL a GMP dokládá, že autorka studovanému tématu dobře porozuměla. Výsledky experimentů pak ukazují, že teoreticky odvozené mezní podmínky úspěšnosti útoku jsou velmi těsné, což dokládá kvalitu odhadů prezentovaných v předchozích kapitolách.

Pro svůj alternativní popis metody [5] je práce přínosná teoreticky, díky připomenutí jednoho stále aktuálního druhu útoků na RSA s nízkým veřejným exponentem a jeho zevrubnému experimentálnímu ověření úspěšnosti je oponovaný materiál významný prakticky. Úroveň zpracování je jistě nadprůměrná, elaborát připomíná spíše práci diplomovou Jednoznačně doporučuji předloženou práci přijmout k obhajobě.

Tomáš Rosa
Praha, 1. září 2008

Známka: výborně!