Studentská konference Fakulty mechatroniky, informatiky a mezioborových studií 2017
Technická univerzita v Liberci

Rozšířený abstrakt

Distribuovaná aplikace pro kryptoanalýzu asymetrických kryptosystémů

Bc. David Salač, doc. RNDr. Miroslav Koucký, CSc.

Abstrakt

V rámci práce jsou představeny problémy faktorizace celých čísel a řešení diskrétního logaritmu v souvislosti se šiframi a protokoly s veřejným klíčem. Důležitou součástí práce je představení důležitých numerických metod pro řešení těchto tříd problémů. Jako praktická část následuje vytvoření distribuované aplikace, která předmětné šifry implementuje v rámci distribuovaného systému. Aplikace je rozdělena na část webové aplikace a terminálové aplikace. Webová aplikace slouží především pro vkládání problémů a jejich správu a představuje hlavní uzel v síti. Terminálová aplikace implementuje numerické metody pro výpočet problémů a představuje podružný uzel v rámci sítě. V závěru následuje analýza použitelnosti aplikace v reálných situacích.

Úvod

Kryptografie s veřejným klíčem (synonymem též asymetrická kryptografie) je v drtivé většině případů postavena na problému řešení diskrétního logaritmu či faktorizace přirozených čísel. Řešení obou zmíněných problémů je časově náročný proces – dosud nebyl objeven algoritmus, který by zvládal tyto úlohy vyřešit v polynomiálním čase. Existují však algoritmy řešící ten či onen problém v podstatně efektivnějším způsobem, nežli při použití hrubé síly. Některé tyto algoritmy jsou v rámci práce implementovány v terminálové aplikaci. Ta tvoří součást distribuované aplikace představující hlavní předmět praktické části práce. Další součást distribuované aplikace je webová aplikace představující řídící uzel v rámci distribuovaného systému. Vytvořená distribuovaná aplikace byla také analyzována s ohledem na použitelnost výstupů v reálných situacích.

Faktorizace přirozených čísel, diskrétní logaritmus a příslušné numerické metody

Problém faktorizace celých čísel lze formulovat takto: mějme složené přirozené číslo n, hledáme rozklad čísla n ve tvaru:

$$n = \prod_{i=1}^{r} p_i^{\alpha_i} \tag{1}$$

kde p_i je nějaké prvočíslo a α_i je nějaké (nenulové) přirozené číslo – oboje pro všechny platné hodnoty i. Pokud navíc platí, že $p_i < p_{i+1}$ pro všechny platné hodnoty i, je takový rozklad definován jednoznačně (základní věta aritmetiky).

Tohoto problému se využívá například v rámci šifry RSA, jenž využívá veřejný klíč n ve tvaru $n = p \cdot q$ pro nějaká velká prvočísla p a q (která jsou naopak tajná). Bezpečnost této šifry je postavena právě na skutečnosti, že neexistuje algoritmus, který by prvočísla p a q dokázal rychle nalézt (míněno například v nejvýše řádu několika let).

V rámci práce jsou posány některé metody používané pro řešení tohoto problému v současnosti. Mezi hlavní patří (názvy jsou ponechány v angličtině): General Number Field Sieve, Quadratic Sieve, Pollard's Rho method.

Diskrétní logaritmus je hledání přirozeného čísla k takového, že platí následující kongruence:

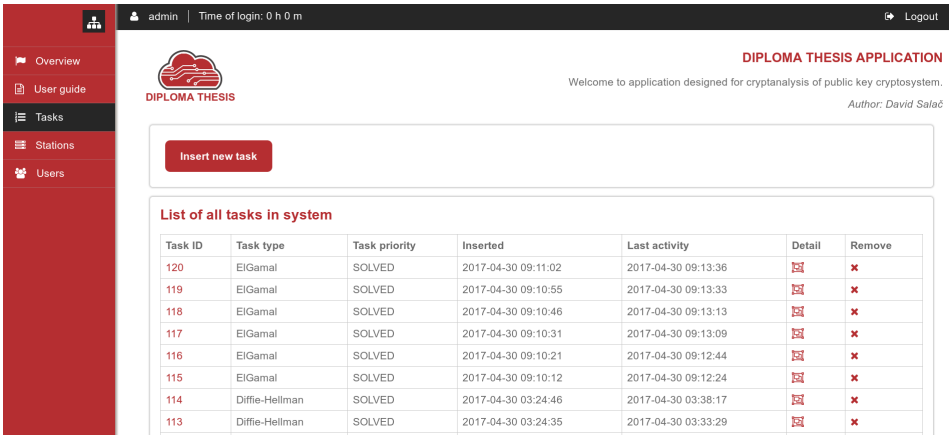
$$g^k \equiv a \pmod{p} \tag{2}$$

pro vhodně zvolená čísla g, a a p.

Mezi používané metody pro řešení diskrétního logaritmu se řadí (názvy ponechány v angličtině): Shanks' baby–step giant–step algorithm, Silver–Pohlig–Hellman method, Index Calculus. Diskrétní logaritmus se na přímo využívá v rámci šifry ElGamal, dále v rámci Diffie-Hellmanovy výměny klíčů, ale i v řadě dalších kryptosystémů.

Distribuovaná aplikace

V rámci práce byla vytvořena distribuovaná aplikace. Ta se skládá z webové aplikace představující řídící uzel distribuovaného systému a dále z terminálové (desktopové) aplikace představující podružný uzel v rámci systému. Webová aplikace slouží primárně ke správě vložených kryptografických úloh do systému. Terminálová aplikace naopak implementuje numerické metody pro řešení popsaných problémů.



Ilustrace 1: Ukázka webové aplikace (součást distribuovaného systému)

Jednotlivé kryptografické úlohy jsou nejdříve přeneseny z webové aplikace do terminálové aplikace. Zde jsou převedeny na popsané problémy, vyřešeny a výsledek je vrácen zpět na server. V systému lze vstupovat následující kryptosystémy: šifru ElGamal, Diffie–Hellmanovu výměnu klíčů a šifru RSA.

Závěr

V rámci práce byla vytvořena distribuovaná aplikace sloužící ke kryptoanalýze asymetrických kryptosystémů. Bezpečnost těchto systémů je odvislá od časové náročnosti řešení problému faktorizace přirozených čísel či diskrétního logaritmu. Aplikace se skládá z webové a terminálové aplikace. Webová aplikace (řídící uzel) slouží jako rozhraní pro vkládání úloh, terminálová (podružný uzel) pak k jejich vyřešení. V poslední kapitole proběhlo měření v reálných situacích prokazující, že pokud neudělá vývojář v rámci implementace kryptosystémů chybu, jsou v současnosti prakticky nenapadnutelné.

Reference

[1] DELFS, Hans a Helmut KNEBL, 2015. *Introduction to Cryptography: Principles and Applications*. Third edition. Berlin: Springer.

[2] Y. YAN, Song, Moti YUNG a John RIEF, 2013. *COMPUTATIONAL NUMBER THEORY AND MODERN CRYPTOGRAPHY*. Higher Education Press: Singapore. ISBN 9781118188583.

[3] YAN, Song Y. *Number theory for computing*. 2nd ed. New York: Springer, 2002. ISBN 35-404-3072-5.