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

Distribuovaná aplikace pro kryptoanalýzu asymetrických kryptosystémů

Autor diplomové práce: Bc. David SALAČ
Vedoucí: doc. RNDr. Miroslav Koucký, CSc.

Abstract

Thesis analyze potential of distributed application in cryptanalysis of public–key systems. The theoretical part of thesis refers about relation among public–key cryptosystems and the problem of discrete logarithm or integer factorization. There is also the description of some numerical methods for solving of these problems. Practical part of thesis is represented by the distributed application for cryptanalysis of public–key cryptosystems. It is composition of web and terminal application. The web application provide interface for submitting of cryptographics tasks. The terminal application implements numerical methods for solving of mentioned problems. The measurement and estimation of application's usability in real situation is also included.

Asymetrické systémy

V rámci práce jsou posané pouze vybrané kryptosystémy s veřejným klíčem.

RSA: bezpečnost šifry je založena na složitosti problému faktorizace celých čísel

ElGamal: bezpečnost šifry je založena na složitosti řešení problému diskrétního logaritmu

Diffie-Hellman: bezpečnost výměny klíčů je založena na složitosti řešení problému diskrétního logaritmu

Co je to faktorizace čísel

Problém faktorizace celých čísel je možné přeformulovat jako hledání rozkladu čísla n následujícího tvaru:

$$n = \prod_{\forall i} p_i^{k_i} \qquad (1)$$

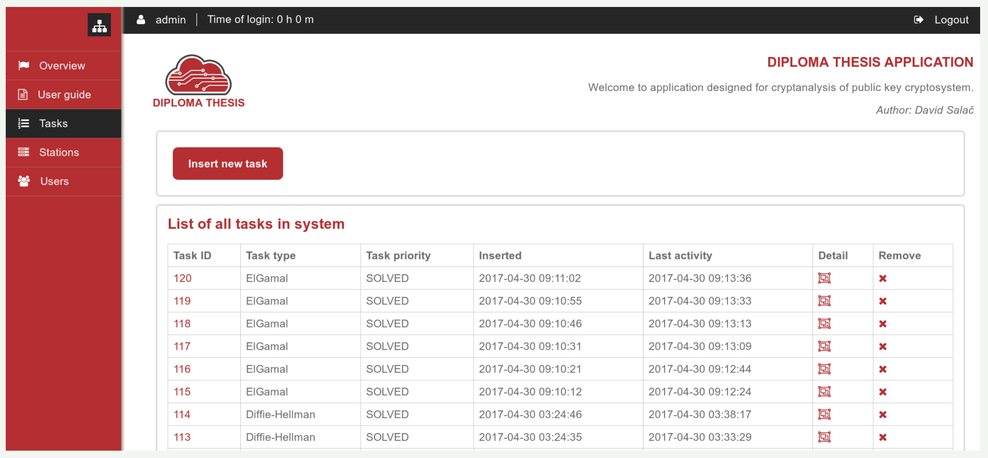
kde p představuje prvočíslo a k představuje nenulové přirozené číslo. Takový rozklad je dán jednoznačně až na pořadí činitelů.

K řešení daného problému jsou v rámci práce implementovány zejména metody: Pollardova Rho metoda, Dixonova metoda náhodných čtverců, Kvadratické síto a některé další.

Aplikace

Aplikace je rozdělena na webovou aplikaci a dále na terminálovou aplikaci. Účelem webové aplikace je především poskytnou rozhraní pro správu úloh použitých pro následnou kryptoanalýzu.

Účelem terminálové aplikace je naopak vyřešení konkrétních úloh, které byly zadány v rámci webové aplikace.



Ilustrace 1: ukázka rozhraní webové aplikace

V rámci terminálové aplikace jsou používány numerické metody pro řešení daných úloh.

Závěr

V rámci práce se podařilo vytvořit distribuovanou aplikaci pro kryptoanalýzu asymetrických kryptosystémů. Ačkoli jsou použité numerické metody pro reálné kryptografické úlohy nedostačující, jedná se o shůdný koncept pro tvorbu podobných kryptoanalytických problémů.

Reference

DELFS, Hans a Helmut KNEBL, 2015. *Introduction to Cryptography: Principles and Applications*. Third edition. Berlin: Springer.
Y. YAN, Song, Moti YUNG and John RIEF, 2013. *COMPUTATIONAL NUMBER THEORY AND MODERN CRYPTOGRAPHY*. Higher Education Press: Singapore. ISBN 9781118188583.
Y. YAN, Song, Moti YUNG a John RIEF, 2013. *COMPUTATIONAL NUMBER THEORY AND MODERN CRYPTOGRAPHY*. Higher Education Press: Singapore. ISBN 9781118188583.

Kontaktní informace: Bc. David Salač, email: david.salac@tul.cz

Tato práce byla podpořena z projektu Studentské grantové soutěže (SGS) na Technické univerzitě v Liberci v roce 2017.