Názov práce: Experimentálne overenie a rozšírenie Coppersmithovho útoku na RSA

Autor: Ria Ruppeldtová

Katedra: Katedra algebry

Vedúci bakalárskej práce: Mgr. Martin Hlaváč

e-mail vedúceho: hlavm1am@artax.karlin.mff.cuni.cz

Abstrakt: Práca sa zaoberá Coppersmithovým útokom na RSA s verejným kľúčom 3 a krátkym paddingom. Jadro útoku spočíva v probléme hľadania malých koreňov modulárnych polynomiálnych rovníc s jednou neznámou. V teoretickej časti práce sme popísali a podrobne dokázali Howgrave-Grahamovu metódu riešenia tohto problému, ktorá je založená na teórii mriežok a algoritme LLL. V experimentálnej časti sme skúmali maximálnu dĺžku napadnuteľného paddingu a prezentovali naše výsledky. Tie ukazujú, že teoreticky dokázaná maximálna dĺžka paddingu sa líši od v praxi zistenej dĺžky len o niekoľko bitov.

Kľúčová slová: Coppersmithov útok na RSA, malé korene modulárnych polynomiálnych rovníc, mriežka, algoritmus LLL

Title: Experimental verification and extension of Coppersmith's attack on RSA

Author: Ria Ruppeldtová

Department: Department of Algebra

Supervisor: Mgr. Martin Hlaváč

Supervisor's e-mail address: hlavm1am@artax.karlin.mff.cuni.cz

Abstract: The work deals with Coppersmith's attack on RSA with the public key equal to 3 and short padding. The heart of this attack lies in the problem of looking for small roots of univariate modular equations. In the theoretical part we have described and proved in detail Howgrave-Graham's method of solving the problem which is based on the theory of lattices and the LLL algorithm. In the experimental part we investigated the maximal length of attackable padding and we presented our results. They show that the theoretically proved maximal length of padding differs from practically observed length only by a few bits.

Keywords: Coppersmith's attack on RSA, small roots of univariate modular equations, lattice, LLL algorithm