Název práce: Problém batohu a jeho aplikace

Autor: Romana Linkeová

Katedra: Katedra algebry

Vedoucí diplomové práce: doc. Mgr. Pavel Příhoda, Ph.D., Katedra algebry

Abstrakt: V této práci se zabýváme kryptosystémy postavenými na $\mathcal{NP}$ (nedeterministický polynomiální) úplném problému batohu z mnoha aspektů. Z pohledu teorie složitosti podrobně uvedeme méně známé části důkazu $\mathcal{NP}$ úplnosti problému batohu. Z hlediska kryptografie ukážeme, že u Merkleova-Hellmanova kryptosystému, který vystihuje základní schéma kryptosystémů postavených na problému batohu, je pro velice nevhodně zvolené parametry tohoto kryptosystému možné odhalit celý soukromý klíč. Dalším přínosem práce je představení nového navrženého konceptu kryptosystému postaveném na problému maticového 0-1 batohu. Ač bylo toho schéma vytvořeno ve snaze předejít známým útokům, dokážeme analogií důkazu J. C. Lagariase a A. M. Odlyzka z roku 1985, že útok založený na LLL algoritmu bude úspěšný pro většinu kryptosystémů tohoto typu. Práci uzavírá souhrn moderních kryptosystémů postavených na problému batohu společně s jejich kryptoanalýzou.

Klíčová slova: problém batohu, $\mathcal{NP}$ úplné problémy, LLL algoritmus