Title: The knapsack and its applications

Author: Romana Linkeová

Department: Department of Algebra

Supervisor: doc. Mgr. Pavel Příhoda, Ph.D., Department of Algebra

Abstract: This thesis is focused on various aspects of cryptosystems based on $\mathcal{NP}$ (non-deterministic polynomial) complete knapsack problem. From the theory of complexity point of view, the less known parts of the proof of knapsack problem $\mathcal{NP}$ completeness are shown in detail. From the cryptographical point of view, a demonstration of breaking of the Merkle-Hellman cryptosystem (the basic design of knapsack-type cryptosystems) is provided, showing that poor parameters choice can lead to easy obtaining of the whole private key. Another contribution of this thesis consists in a presented proposal of a new cryptosystem concept based on the matrix 0-1 knapsack problem. This concept was developed in order to prevent known attacks, however, in the thesis we provide a proof analogous to J. C. Lagarias and A. M. Odlyzko, 1985, which shows that an attack based on the LLL algorithm will be successful on the majority of the matrix 0-1 knapsack problem cryptosystems. Finally, a list of modern cryptosystems based on the knapsack problem is provided and a cryptanalysis thereof is given.

Keywords: knapsack problem, $\mathcal{NP}$ complete problems, LLL algorithm