**Title:** *Security and usability of standard hash functions, in particular MD-5, SHA-1 and SHA-2*
**Author:** *Galaczová Barbora*
**Department:** *Department of Algebra*
**Supervisor:** *Doc. RNDr. Tůma Jiří, DrSc., Department of Algebra*
**Consultant:** *Ing. Budiš Petr, Ph.D.*

**Abstract:** *In the present work we try to digestedly describe standard hash functions, in particular MD-5, SHA-1 and SHA-2. We describe resume of existing attacks on these hash functions. We closely focused on MD-5 collision attacks, because the other hash function collision attacks result from these. Next we describe posibilities of practical usage of hash function collisions, in particular into the qualified certificates area and possible threats. At the end to the present work we describe new hash functions, which could replace current hash functions. This work also contains software to calculate MD-5 hash and search it`s collisions. The software is based on method invented by Czech cryptoanalytist Vlastimil Klíma.*

**Keywords:** *hash function, collision, qualified certificate, security.*