Název práce: *Bezpečnost a použitelnost základních hashovacích funkcí, zejména MD-5, SHA-1 a SHA-2*
Autor: *Galaczová Barbora*
Katedra: *Katedra algebry*
Vedoucí diplomové práce: *Doc. RNDr. Tůma Jiří, DrSc., Katedra algebry*
Konzultant: *Ing. Budiš Petr, Ph.D.*

Abstrakt: *V této práci se snažíme přehledně popsat základní hashovací funkce, zejména MD-5, SHA-1 a SHA-2. Uvádíme souhrn dosavadních útoků na tyto hashovací funkce, přičemž podrobně jsme se zaměřili především na postupy hledání kolizí funkce MD-5, neboť z těchto vycházejí útoky také na ostatní hashovací funkce. Dále popisujeme možnosti praktického využití kolizí hashovacích funkcí zejména v oblasti kvalifikovaných certifikátů a možné hrozby při jejich zneužití. V závěru uvádíme přehled nových hashovacích funkcí, jež mohou v budoucnu nahradit stávající. Součástí práce je také software na výpočet MD-5 hashe a hledání kolizí této hashovací funkce, založený na postupu českého kryptoanalytika Vlastimila Klímy.*

Klíčová slova: *hashovací funkce, kolize, kvalifikovaný certifikát, bezpečnost.*