Název práce: Statistické testy hašovacích (=žvýkacích) funkcí
Autor: Adam Christov
Katedra: Katedra algebry
Vedoucí bakalářské práce: Doc. RNDr. Jiří Tůma, DrSc.
e-mail vedoucího: tuma@karlin.mff.cuni.cz

Abstrakt: V předložené práci popisujeme obecnou konstrukci hašovacích funkcí a podrobněji hašovací funkce MD5. Ukazujeme metodu Wangové a kol. na hledání kolizí hašovací funkce MD5 a popisujeme algoritmy Vlastimila Klímy a Marca Stevense, které jsou na této metodě založené. Dále pak provádíme jednoduché statistické testy, kterými se snažíme ověřit náhodnost výstupu MD5 a naplnění postačujících podmínek, které se využívají v obou zmíněných algoritmech na hledání kolizí.
Klíčová slova: MD5, hašovací funkce, kolize, statistické testy

Title: Statistical testing of hash functions
Author: Adam Christov
Department: Department of Algebra
Supervisor: Doc. RNDr. Jiří Tůma, DrSc.
Supervisor's e-mail address: tuma@karlin.mff.cuni.cz

Abstract: In this paper we describe the general workings of hash functions and deal with MD5 hash function in more detail. We present Wang et al. method for finding collisions in MD5 hash function and we describe Vlastimil Klíma's and Marc Stevens's algorithms that are based on this method. We also perform simple statistical tests to verify randomness of MD5 output and fulfilment sufficient conditions which are used in both mentioned algorithms for finding collisions.

Keywords: MD5, hash functions, collision, statistical testing