The work summarizes author's research during the doctoral studies in the field of hash functions. The first part of the thesis presents a generalised theory of equations built from two basic building blocks of cryptographic primitives: modular addition and eXclusive OR. In particular we study AX-equations of depth 1. The second and third sections were written after Wang's publication of collisions in MD5 and show that minor modifications of the hash function does not work. We present collisions in the 3C and 3C+ constructions of hash function suggested by Gauravaram and feedback ring-iterative structure by Su et al. The results were published at the conferences ICISC 2006 and SPI 2007. The last part presents a newly constructed type of collisions in MD5 with a newly proposed message differences. The result was published and presented at the conference Indocrypt 2008.