Abstract

At the end of 70th of last century the concept began to emerge, now is referred as a cryptographic hash function. Currently, these functions are associated especially with a digital signature. In 2005, the worldwide most used function SHA-1 was broken. This fact led in 2007 NIST announced a public competition to create a new secure hash algorithm. This Thesis deals with issues of cryptographic hash functions from the beginning of their theoretical formulation to current events in this area.

Key words: Cryptographic hash functions, SHA-1, MD5, NIST competition