Abstract

In the past few years, there have been significant research advances in the analysis of hash functions and it was shown that none of the hash algorithm is secure enough for critical purposes whether it is MD5 or SHA-1. Nowadays scientists have found weaknesses in a number of hash functions, including MD5, SHA and RIPEMD so the purpose of this paper is combination of some function to reinforce these functions and also increasing hash code length upto 256 that makes stronger algorithm against collision attests.

References

- R. Rivest. The MD5 Message-Digest Algorithm [rfc1321]
- . NIST, &quot;Secure Hash Standard,&quot; FIPS PUB 180, May. 1993.
- F. Chabaud, A. Joux. &quot;Differential Collisions in SHA-0&quot;. In Advances in Cryptology CRYPTO'98, Santa Barbara, CA, Lecture Notes in Computer Science 1462.
New modified 256-bit MD5 Algorithm with SHA

Index Terms

Computer Science Communications

Keywords
Md Algorithm; Hash Function; Compressed Function And Hash Code Length