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]
New modified 256-bit MD5 Algorithm with SHA


"Collisions in SHA-0 and Reduced SHA-1- In Advances in Cryptology" –
Eurocrypt’05, Springer-Verlag, 2005.
- S. Chang, M. Dworkin, Workshop Report, The First Cryptographic Hash Workshop,
- E. Biham, R. Chen, "New results on SHA-0 and SHA-1"; Crypto 2004 Rump
- K. Matusiewicz and J. Pieprzyk; Finding good differential patterns for attacks on
- F. Chabaud, A. Joux; Differential Collisions in SHA-0; In Advances in
Cryptology CRYPTO’04, Santa Barbara, CA, Lecture Notes in Computer Science 1462.
- Rivest R L; The MD5 message digest algorithm [EB/OL].
- Xiaoyun Wang, Dengguo; HAVAL-128 and RIPEMD; Cryptology ePrint
Archive Report 2004/199, 16 August 2004,
- J. Black, M. Cochran, T. Highland: A Study of the MD5 Attacks: Insights and
Improvements, March 3, 2006
- Tao Xie and Dengguo Feng (30 May 2009). How to Find Weak Input Differences for MD5
Collision Attacks.
- X. Wang, X. Feng, X. Lai and H. Yu; "Collisions for Hash Functions MD4,
MD5, HAVAL-128 and RIPEMD; Cryptology ePrint Archive: Report 2004/199, Aug. 2004
http://eprint.iacr.org/2004/199/

Index Terms

Computer Science Communications

Keywords

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