A Review of Comparative Study of MD5 and SHA Security Algorithm

Volume 104 - Number 14
Year of Publication: 2014

Authors:
Surbhi Aggarwal
Neha Goyal
Kirti Aggarwal

Abstract

Security algorithms or cryptography enables secure communication between two parties in the presence of a third-party or an eavesdropper. It assures the recipient of the message of the authenticity of the claimed source, protects the message against the unauthorized release of the message content by the adversaries, limits the access to authorized users, protects against sender/receiver denying sending/receiving a message. MD5 and Security Hash algorithms (SHA), cryptographic hash algorithms are one-way hashing functions which are easier to compute but are much harder to reverse and would take around millions of years to compute the authentic or verifiable message content. This research paper aims to analyze and juxtapose the two hash algorithms, MD5 and SHA, using various key features and performance metrics. Their features have also been highlighted in order to provide the researchers a better comparison picture so that they can reach to the final upshot, which algorithm has superseded the other.
A Review of Comparative Study of MD5 and SHA Security Algorithm

- Wikipedia, the free encyclopedia.
- Jerry Li, MD5 Message Digest Algorithm. San Jose University, Computer Science department
- Ruth Betcher, Secure Hashing Algorithm.
- MD5 is faster than SHA-1. Journal Of Omnifarious-Myth.
- http://stackoverflow.com/questions/2948156/algorithm-complexity-security-md5-or-sha1
- http://idrbtca.org.in/inf_crypto.htm
- Addam Schroll, ITNS and CERIAS CISSP Luncheon Series: Cryptography.
- http://science.opposingviews.com/advantages-disadvantages-symmetric-key-encryption-2609.html

Index Terms

Computer Science    Security

Keywords

MD5    SHA    hash