Abstract

This paper introduces a new approach of MD Algorithm for security design. This approach comprises of the 160-bit hash algorithm for secure message digest. The results show that the 160-bit Message Digest Algorithm code is more secured than 128-bit Message Digest Algorithm code. This effort can alternate efficiently the accessible Message Digest Algorithm and hash function implementations for security design, so this approach proves a high security step towards design.

References

- R.Rivest. The MD5 Message-Digest Algorithm [rfc1321]
- Janaka Deepakumara, Howard M. Heys and R. Venkatesan, FPGA IMPLEMENTATION OF MD5 HASH ALGORITHM, Faculq of Engineering and Applied Science Memorial University of Newfoundland St. John S, NF, Canada.
A New Approach 160-bit Message Digest Algorithm

- Danyang Cao, Bingru Yang, Design and implementation for MD5-based data integrity checking system, College of Information Engineering, North China University of Technology, NCUT Beijing 100144, China
- Kimmo Järvinen, Matti Tommiska and Jorma Skyttä, Hardware Implementation Analysis of the MD5 Hash Algorithm, Helsinki University of Technology Signal Processing Laboratory, Shenyang, China Otakaari 5 A, FIN-02150, Finland
- Janaka Deepakumara, Howard M. Heys and R. Venkatesan, FPGA IMPLEMENTATION OF MD5 HASH ALGORITHM, Faculty of Engineering and Applied Science Memorial University of Newfoundland St. John’s, NF, Canada A1B 3X.

Index Terms
Computer Science
Security

Keywords
MD Algorithm; Hash Function; Data Integrity