Abstract

In today's world every person relies on internet for various purposes. There is always a need to take appropriate measures for getting secure communication all the way throughout this unsecure internet. Integrity is one of the most significant factors in the communication scenario. There are various algorithms that ensure the integrity but almost all are either not secure or not efficient. This paper highlights some of such algorithms and also introduces an integrity algorithm and also proves its efficiency with its implementation result.

References

- A new Hash Function Based on Combination of Existing Digest Algorithms pub 2007.
- The Collision Rate Tests of Two Known Message Digest Algorithms 2009.
- Marc Stevens hash clash - Framework for MD5 & SHA-1 Differential Path Construction and Chosen-Prefix Collisions for MD5
- X. Wang, H. Yu and Y. L. Yin, &quot;Efficient Collision Search Attacks on SHA-0&quot;,(Pub 2005)
- Florent Chabaud, Antoine Joux, &quot;Differential collisions in SHA-0,&quot; Advances in Cryptology-CRYPTO'98, LNCS 1462, Springer-Verlag, 1998.
- Ricardo Chaves, Georgi Kuzmanov, Leonel Sousa, and Stamatis Vassiliadis &quot;Cost-Efficient SHA Hardware Accelerators&quot; IEEE transactions on very large scale integration (VLSI) Systems, VOL. 16, NO. 8, AUGUST 2008

Index Terms

Computer Science Security

Keywords

Computer Security SHA Hash Message Digest