Abstract

The protection of information authentication is based on cryptographically secure hash function. A function that compresses an arbitrarily large message into a fixed small size message digest is known as a hash function. The most currently used hash functions are based on block ciphers and the dedicated hash functions e.g. MD5, SHA-0 and SHA-1 etc. A hash function is said to be broken if an attacker is able to show that the design of the hash function
violates at least one of its claimed security property. In present paper we are planning to design and develop an efficient and effective hashing scheme for information authentication. We will try to design a hashing method which has certain features like speed and more security.

Referenc

ences


Index Terms

Computer Science

Emerging Trends in Technology

Keywords

Cryptography