Abstract

Digital signature methodology provides cryptographic services like entity authentication, authenticated key transmission and authenticated key agreement. A Digital Signature is used to provide authentication, non-repudiation & integrity over the digital data in data exchanged and to validate the recipient for the authorized identity over open network. The goal of a Digital signature algorithm is to provide security for message or data. The present paper focuses on a comparative study of some existing algorithms of digital signature on the basis of many hard problems.

References


Index Terms
Computer Science Algorithms

Keywords
Digital signature, Authentication, Non-repudiation, Integrity