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

3. Ashish Vijay, Priyanka Trikha, Kapil Madhur, “A New Variant of RSA Digital Signature”
   https://www.ijarcsse.com/docs/papers/10_October2012/Volume_2_issue_10_Octobe
   r2012

   Signature Algorithm (MERDSA)”
   https://www.ijarcsse.com/docs/papers/8_August2012/Volume_2_issue_8

5. Kamal kumar Agrawal, Ruchi Patira, Kapil Madhur, “A Digital Signature Algorithm based
   on xthRootProblem”
   https://www.ijarcsse.com/docs/papers/11_November2012/Volume_2_issue_11
   _November2012

6. Bernstein, Daniel J.; Duif, Niels; Lange, Tanja; Schwabe, Peter; Bo-Yin Yang (2012).

7. T. ElGamal. A public key cryptosystem and a signature scheme based on discrete

Index Terms

Computer Science Algorithms

Keywords

Digital signature, Authentication, Non-repudiation, Integrity