Abstract

In ancient times we did not have technology to transfer messages (data) electronically and hence only the receivers receives it. No third could intercept it. Nowadays web apps have become popular and widely used in fields that require high level of security such as finance, military systems, E-mails, medicals, etc. With increase in this, increase in malicious activities and attacks have been observed. Hosts have become botnets[1], number of host scam phishing sites have increased. Actions without a prior thought and thinking without acting can now not be given any place. It's high time to secure our data. This paper comprises of an overview of security algorithms that are a shield to our electronic data.

References
- Dmitry Khovratovich, Ivica Nikoli´c, and Ralf-Philipp Weinmann, 2009, Meet-in-the-Middle Attacks on SHA-3 Candidates, International Association for Cryptologic Research.
- Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.
Overview of Security Algorithms

Index Terms

Computer Science

Security

Keywords

Secret Key Cryptography
Public Key Cryptography
RSA
Cryptographic Algorithms
AES
ECC