Abstract

Information security is more important for data communication in physical or network environment. Sending and receiving data over the internet is easy, fast and cost efficient due to development of information technology. Protected communication is more imperative for data move in the network. That put forward a new technique for hybrid cryptography with message digest and symmetric Algorithm, asymmetric algorithm. This research study proposes hybrid cryptography is a permutation of Message digest and Symmetric Key cryptography algorithm in the form of Digital Envelope. Message Digest is a fingerprint or the summary of a memo or data. Now the proposed system will try to improve the existing problem for integrity, proposed system use the MD5 algorithm. Due to this basis proposed system is capable then existing system. The message is initially encrypted with AES and the symmetric keys of AES are encrypted with RSA then the hybrid of both AES-RSA is embedded with message digest of data. The new results based on grouping of symmetric algorithm and Message digest will approve the effectiveness of the planned concept, and show the huge difference in key space and provide high-level security. This algorithm provides additional security as well as authentication comparing to other
existing hybrid algorithm. It guarantees all cryptographic primitives, integrity, confidentiality and authentication. The implementation of the proposed technique is made with the help of JAVA technology and their performance is description with the help of space and time complexity. According to the trial results the proposed technique offers more secure environment and with less computational overheads.

References

15. Mouza Bani Shemaili, Chan Yeob Yeun, Khalid Mubarak, Mohamed Jamal Zemerly "A


Index Terms

Computer Science                   Algorithms

Keywords

Message Digest, Symmetric key Encryption Algorithm, Cipher text, Plain text, Asymmetric key Encryption, Hybrid Algorithm