Abstract

This work uses enhanced symmetric key encryption algorithm, in which same structure of encryption and decryption procedure algorithm is used. In conventional encryption methods the key for encryption and decryption is same and remain secret. The algorithm uses key generation method by random number in algorithm for increasing efficiency of algorithm. The algorithm use key size of 512 bits for providing better security and it also provide the concept of internal key generation at receiver end on the basis of 512 bits key which will entered by the sender. This internal key will store in the sender end database and send to the receiver end by other path for preventing brute force attack and other harmful attacks on security. This algorithm is more efficient for large data where existing algorithms provides efficient encryption and decryption only for 2MB data. This work provides better speed in comparison to existing algorithms for large size of files with less overhead.
An Enhanced Symmetric Key Cryptography Algorithm to Improve Data Security

Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath


Yan Wang and Ming Hu

Timing evaluation of the known cryptographic algorithms; 2009 International Conference on Computational Intelligence and Security 978-0-7695-3931-7/09 $26.00 © 2009 IEEE DOI 10. 1109/CIS.2009.81.


Neal Koblitz

A Course in Number Theory and Cryptography; Second Edition Published by Springer-Verlag.

By Klaus Felten

An Algorithm for Symmetric Cryptography with a wide range of scalability; published by 2nd International Workshop on Embedded Systems, Internet Programming and Industrial IT.

Majdi Al-qdah & Lin Yi Hui


T Morkel, JHP Eloff


Md. Nazrul Islam, Md. Monir Hossain Mia, Muhammad F. I. Chowdhury, M. A. Matin


Index Terms

Computer Science

Security

Keywords

Information security Encryption Decryption Cryptography Brute force attack