Abstract

In the age of Information Technology Information Security is very important. To provide the security to the communication data, we are using different encryption algorithms. Encryption algorithms can be categorized into Symmetric key cryptography and Asymmetric key cryptography. Many of the Symmetric encryption algorithms (DES, 3DES, Blowfish, RC6 etc…) following the feistel structure, some algorithms (AES etc…) are following substitutions, permutations structure. These all are block ciphers. Symmetric Encryption Algorithms encrypting the plain text by using the secret key and producing cipher text. Decryption algorithms takes the cipher text and secret key and produces the original plain text, this is basically the encryption algorithm run in reverse. This paper specifies a new method for Symmetric key cryptography that can be used to protect data which is transferred through internet. This algorithm is not following the feistel structure, substitutions and permutations. This algorithm can be used for stream ciphers and block ciphers.

References


3. Introduction to Modern Cryptography by Jonathan Katz and Yehuda Lindell.


Index Terms

Computer Science Networks

Keywords

Symmetric key cryptography, Plain text, Cipher text, Secret key, Encryption algorithm
Decryption algorithm, Rasilabdacheda misravibhaga sutram, Divisor, Dividend, Quotient.