Abstract

Most of the sensitive information in the data communication has latent security problems. The algorithm method of AES, DES, 3DES and RC2 which were widely used are not suitable for the coding of advanced language tools. Therefore, we proposed the mixed encryption algorithm based on bit shifting and matrix calculation to solve the problem. Our method is easy to adopt the coding of advanced language and is safe enough. The security mechanism uses some algorithms to scramble data into unreadable text which can be only being decoded or decrypted by party those know the secret key. The proposed algorithms consume very less amount of computing resources such as CPU time, memory and battery power [18]. Our implementations also showed the highest throughputs for all type of files and file size and comparison has been conducted with AES, DES, 3DES,RC2 [1] and result shows the effectiveness and speed of our algorithm.
A New Method in Symmetric Encryption for block cipher module: A Bit Shifting Approach

Reference

- Introduction to cryptography, Part 2: Symmetric cryptography
- PrakashKuppuswamy et al./ Indian Journal of Computer Science and Engineering (IJCSE) “Enrichment of security through cryptographic public key algorithm based on block cipher”
- An introduction to information security
  http://openlearn.open.ac.uk/mod/oucontent/view.php?id=397613&section=1
- IJCST Vol. 2, Issue 2, June 2011 I S N : 2 2 2 9 - 4 3 3 3 ( P r i n t ) | I S S N : 0 9 7 6 - 8 4 9 1 (O n l i n e ) "Comparative Analysis Of Encryption Algorithms For Data Communication"Shashi Mehrotra Seth, Rajan Mishra"
- "A Performance Comparison of Data Encryption Algorithms," IEEE [Information and
A New Method in Symmetric Encryption for block cipher module: A Bit Shifting Approach


Index Terms

Computer Science
Security

Key words

AES
DES
3DES
RC2
Computer Security
Encryption Techniques
Cryptography