In this research, we have invented a method to generate the secure block cipher using modern transposition and substitution with 128bit key, modular and integral functions. This method supports an input in the form of ASCII, extended ASCII characters, images and diagrams etc. Initially, the algorithm converts the given input into ANSI characters using rich text format, then it performs 16 rounds of permutations with internal functions and finally it carries out color substitution. The functions used in this algorithm alter the plain text in various ways before it takes the shape of cipher text. A brief introduction about the tree data structures and its traversal methods has explained. The process of encryption, decryption and the sub key generation algorithms are explained with example. The avalanche effect and the cryptanalysis inspected in this investigation evidently indicate that the cipher is potential one.

References

An Impregnable Block Cipher Generation using Modern Transposition and Substitution Algorithms with a large Key, Modular Arithmetic and Integral Functions

- Ravindra, Udaya and Vinaya babu, An Improved Playfair Cipher Cryptographic Substitution Algorithm, JARCS, (0976-5697), Volume 2, No-1, Jan-Feb 2011.
- Ravindra Babu, Udaya Kumar and Vinaya babu, An Enhanced Poly alphabetic Cipher using Extended Vigenere Table, IJARCS, (0976-5697), Volume 2, No. 2, Mar-April 2011.
- Ravindra, Udaya Kumar and Vinaya babu, A Contemporary Poly alphabetic Cipher using Comprehensive Vigenere Table, WCSIT,(2221-0741), Vol. 1, No 4, 167-171,2011
- Alaa, Bilal, A fast approach for braking RSA cryptosystem, WCSIT,2221-0741, Vol 1, No 6, 260-263, 2011.
- Ravindra Babu, Udaya Kumar and Vinaya babu, A More secure block cipher generation involving multiple transposition and substitution with a large key, IJARCS, (0976-5697), Vol 2, No 2, Mar-April 2011.
- Ravindra Babu, Udaya Kumar and Vinaya babu, A Modern Play color cipher involving dynamic permuted key with iterative and modular arithmetic functions, IJARCS, (0976-5697), Vol 2, No 3, May-June 2011.
- Ravindra Babu, Udaya Kumar and Vinaya babu, An Unassailable Block Cipher generation with an extended play color cipher, concerning a large alphanumeric key, modular arithmetic and integral functions, (0975-8887), IJCA, Volume 28-no. 9, August 2011.
- Ravindra Babu, Udaya Kumar and Vinaya Babu, A Block Cipher Generation Using an Innovative Permutation Algorithm, Communicated to International Journal of Mathematical Archive, ISSN-2229-5046.
- Ashok N. Kamthane, C and Data Structures, Pearson Education, ISBN 81-297-0261-4,
Index Terms

Computer Science  Pattern Recognition

Keywords

Symmetric Block Cipher  Play Color Cipher (pcc)  Substitution  Permutation  Rsa Algorithm
Rich Text Format (rtf)
Pub: Public Key Of User B
Pra: Private Key Of User A
Pua: Public Key Of User A
Prb: Private Key Of User B