Abstract

The aim of our research is to develop a new framework for secure block cipher generation using color substitution and permutations on alphanumeric letters, symbols, images, diagrams or any kind of text. To transfer the keys from source to destination we have used RSA public key algorithm and for encryption / decryption of the information, we have used our invented
‘play color substitution’ algorithm. Importance of RTF will be explained, Cryptanalysis attacks were discussed and shown that the cipher cannot be broken by any cryptanalysis attacks.

Reference

- Ravindra Babu K, Dr. S. Udaya Kumar, A Survey on Cryptography and Steganography Methods for Information Security, IJCA, Volume-12, No-2, November 2010
- Ravindra Babu K, Dr. Udaya Kumar, Dr. A. Vinaya Babu, An Improved Playfair Cipher Cryptographic Substitution Algorithm, IJARCS, Volume 2, No-1, Jan-Feb 2011.
- Ravindra Babu K, Dr. S. Udaya Kumar, Dr. A. Vinaya Babu, An enhanced and efficient cryptographic substitution method for information security, IJNS, (Paper in a journal)
- Lt. Ravindra Babu Kallam, Dr. S.Udaya Kumar, A Block Cipher generation using Color Substitution, IJCA, 2010 Vol 1, No-28.

Index Terms

Computer Science

Security
**Key words**

RSA

PUB: Public key of user B

PRA: Private Key of user A

PUA: Public key of user A

PRB: Private key of user B

PCC: Play color cipher

RTF: Rich text format

LHS: Left hand side

RHS: Right hand side.

ETF: Electronic Frontier Foundation