Abstract

In this paper, the authors propose a new combined symmetric key cryptographic method, SJA-I, which basically has four steps: Firstly, each byte is broken into its equivalent binary format and then single bit manipulation is executed on that; secondly Modified Caesar Cipher technique (SD-REE) and TTJSA cipher algorithm are applied on the data (message) randomly, which depends on the key provided during the time for encryption; thirdly DJSA method applied and in the final stage, Bit Reversal technique is applied to reach the final encrypted form of the original data. The method applied here is being tested on different plain text files and the results were analyzed very carefully. It was found that there was no pattern in the encrypted text and this combined cipher technique can not be broken by usual cryptanalysis attack like, differential attack, plain text attack, spectral analysis (frequency analysis), etc. The authors proposes that SJA-I can be applied for encryption of short message, password, secret key or any type confidential message.
An Advanced Combined Symmetric Key Cryptographic Method using Bit Manipulation, Bit Reversal, Modified Caesar Cipher (SD-REE), DJSA and TTJSA methods: SJA-I Algorithm


- Ultra Encryption Standard (UES) Version-I: Symmetric Key Cryptosystem using generalized modified Vernam Cipher method, Permutation method and Columnar Transposition method,


- Somdip Dey, &quot;SD-REE: A Cryptographic Method To Exclude Repetition From a Message&quot;, Proceedings of The International Conference on Informatics & Applications
An Advanced Combined Symmetric Key Cryptographic Method using Bit Manipulation, Bit Reversal, Modified Caesar Cipher (SD-REE), DJSA method, TTJSA method: SJA-I Algorithm (ICIA 2012), Malaysia, p. 182 – 189.


Index Terms

Computer Science Security

Keywords

Caesar Cipher Ttjsa Msa Nijsa Ues Djmna Sd-ree Sd-aree Djsa Cryptography