Abstract

In this paper, we have developed a novel block cipher, which involves a key bunch matrix in the process of encryption. In order to carry out the decryption process, we have obtained the multiplicative inverse of each key in the encryption key bunch matrix by using the concept of multiplicative inverse, and constructed the decryption matrix. In this analysis, the cryptanalysis clearly shows that the strength of the cipher is remarkable, and this cipher can be used for the transmission of information, like any other well-known cipher, through internet.

References

A Novel Block Cipher Involving a Key Bunch Matrix

- VUK Sastry, Ch. Samson, Generalized Hill Cipher Involving Multiple Keys, Mixing and Key Dependent Substitution, International Journal of Computational Intelligence and Information.

Index Terms

Computer Science
Security

Keywords
Key bunch matrix encryption decryption avalanche effect cryptanalysis