Abstract

In this paper, we have developed a block cipher, by using a key bunch matrix and an additional key matrix. In order to carry out the decryption process, the decryption key bunch matrix is obtained, basing upon the encryption key bunch matrix, on using the concept of multiplicative inverse. In the cryptanalysis, we have found that, this cipher is a very strong one as it includes the additional key matrix and supported with modular arithmetic addition. From the viewpoint of efficiency and strength, this cipher is quite comparable with any other cipher available in the literature of cryptography.

References

- V. U. K. Sastry, K. Shirisha, "A Novel Block Cipher Involving a Key Bunch Matrix"; sent for publication.
- V. U. K. Sastry, K. Shirisha, "A Block Cipher Involving a Key Bunch Matrix and Including another Key Matrix Supplemented with Xor Operation"; sent for publication.
A Block Cipher Involving a Key Bunch Matrix and Including another Key Matrix Supported With Modular Arithmetic Addition

Index Terms
Computer Science
Security

Keywords
encryption key bunch matrix decryption key bunch matrix additional key matrix cryptanalysis
avalanche effect