Abstract

In this paper, we have developed a block cipher which includes a pair of key matrices. The first key matrix E is a key bunch matrix which is containing several odd integers as keys lying in [1-255], and the second key matrix F is an additional matrix, linked with xor operation, containing the integers in [0-255]. The corresponding key bunch D, used in the decryption process, is obtained by using the concept of multiplicative inverse. From the cryptanalysis carried out in this investigation we have found that this cipher is a very strong one and it cannot be broken by any attack.

References

- National Bureau of Standards NBS FIPS PUB 46 "Data Encryption Standard
- V. U. K. Sastry, K. Shirisha, "A Novel Block Cipher Involving a Key Bunch Matrix"; sent for publication.

**Index Terms**

Computer Science Security

**Keywords**

Encryption key bunch matrix Decryption key bunch matrix avalanche effect cryptanalysis