Abstract

In this paper, Advanced Feedback Encryption Standard Version 1 (AFES-1), Nath et al have combined both bit-level and byte level operations on the plain text. Nath et al had recently published Multi Way Feedback Encryption Standard Ver-3 MWFES-3[5]. MWFES-3 is a byte level encryption algorithm. The authors have capitalized on the strength of MWFES-3[5] by introducing a bit-shuffling operation at the beginning of each iteration. At the beginning of each iteration, the plain text bits of that iteration are shuffled by using 24 different shuffling functions. Now, the order in which the 24 different functions are called, changes at each iteration, and that order is taken as a function of the key. After the initial shuffling of the bits, the bits are
converted back to bytes and MWFES-3 is applied on the bytes. This process goes on Encryption Number (EN) times, where EN is also taken as a function of the key. So, at the beginning of each iteration, the bits obtained from the last iteration are shuffled in a different way. This method has been tested on standard plain texts such as ASCII ‘0’, ASCII ‘1’ and the results are quite satisfactory. This method is immune to any classical form of attacks.

References

- Neeraj Khanna, Joel James, Joyshree Nath, Sayantan Chakraborty, Amlan Chakrabarti, Asoke Nath, "New Symmetric key Cryptographic algorithm using combined bit..."


Index Terms

Computer Science

Security

Keywords

MWFES-I  MWFES-2  MWFES-3  Encryption Number.