An Enhancement Method Based on Modifying CFB Mode for Key Generation in AES Algorithm

Dr. Hasanen S. Abdulah
Computer Sciences Department, University of Technology/ Baghdad

Dr. Maha A. Hamood Al-Rawi
Computer Sciences Department, University of Technology / Baghdad

Dalal N. Hammood
Science College, University of Al-Nahrain / Baghdad
Email: dal_scin81@yahoo.com

Received on: 4/11/2015 & Accepted on: 24/11/2016

ABSTRACT

There are two very important characteristics in the block cipher, the amount of time for encryption process and key complexity which caused increasing the complexity of encryption process. This research aims to enhance the key generation of Advanced Encryption Standard (AES) algorithm with high efficiency. The proposed enhancement method architecture based on modifying cipher feedback (MCFB) mode which produce key block from each key generation step in addition to represent current output that is repeated lyre used as input to produce next key block. In the block cipher encryption step, two processes are implemented: Substitution bytes process and Shift rows process. This proposed method improves the performance, efficiency, and speed of the encryption algorithm.

Keywords: Advanced Encryption Standard; Key Generation; Mode Operation; Cipher Feedback.