Malaysian Journal of Mathematical Sciences

Journal homepage: https://einspem.upm.edu.my/journal

An Efficient 2048-bit Block Cipher

Abu, N. A.*

Information Security Forensics and Computer Networking, Faculty of ICT, Universiti Teknikal Malaysia Melaka, Malaysia

E-mail: nura@utem.edu.my
**Corresponding author*

Received: 29 October 2020
Accepted: 5 July 2021

Abstract

An Advanced Encryption Standard (AES) has been the most popular block cipher in the last two decades. It has been extensively analyzed and efficiently implemented. Since 2000, an AES has been preset to be upgradable from the current 128-bit key to 192-bit key and finally 256-bit key on the same 128-bit plain text-cipher text block. A new call for 256-bit standard symmetric cipher is expected by 2030. Currently, an input file runs in kilobytes. It is apparent that a more practical cipher is much needed in handling daily task of protecting an important document from a user stand point of view without having to go through technical knowledge of encryption. A symmetric cipher has been traditionally operated on a small block. In this paper, however, a new proposal on a large 2048-bit block cipher using 256-bit key is presented.

Keywords: mega cipher, AES, symmetric cipher, block cipher.