World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:14, No:12, 2020

Modification Encryption Time and Permutation in Advanced Encryption Standard Algorithm

Authors : Dalal N. Hammod, Ekhlas K. Gbashi

Abstract : Today, cryptography is used in many applications to achieve high security in data transmission and in real-time communications. AES has long gained global acceptance and is used for securing sensitive data in various industries but has suffered from slow processing and take a large time to transfer data. This paper suggests a method to enhance Advance Encryption Standard (AES) Algorithm based on time and permutation. The suggested method (MAES) is based on modifying the SubByte and ShiftRrows in the encryption part and modification the InvSubByte and InvShiftRows in the decryption part. After the implementation of the proposal and testing the results, the Modified AES achieved good results in accomplishing the communication with high performance criteria in terms of randomness, encryption time, storage space, and avalanche effects. The proposed method has good randomness to ciphertext because this method passed NIST statistical tests against attacks; also, (MAES) reduced the encryption time by (10 %) than the time of the original AES; therefore, the modified AES is faster than the original AES. Also, the proposed method showed good results in memory utilization where the value is (54.36) for the MAES, but the value for the original AES is (66.23). Also, the avalanche effects used for calculating diffusion property are (52.08%) for the modified AES and (51.82%) percentage for the original AES.

Keywords : modified AES, randomness test, encryption time, avalanche effects
Conference Title : ICSRD 2020 : International Conference on Scientific Research and Development
Conference Location : Chicago, United States
Conference Dates : December 12-13, 2020