Abstract

Block ciphers are very important in communication systems as they provide confidentiality through encryption. The popular block cipher is an Advanced Encryption Standard (AES). Each cipher uses several rounds of fixed operations to achieve desired security level. The number of rounds in a block cipher is decided based upon the resistivity levels against the known attacks.
The very first level of attack on an encryption algorithm is to search for repetitive cipher values and relate them to plaintext. The diffusion enables to spread out the repetitive plain text patterns in the cipher values. The diffusion is achieved using linear operations such as key addition, rotate byte, MDS matrix multiplication, etc. In this paper we propose a method of enhancing the diffusion power by key multiplication rather than conventional key addition used in the Advanced encryption standard algorithm. The paper discusses the problems associated with the key multiplication and provides the possible solutions. The measured results indicate more diffusion when compared with the existing method. Key multiplication, as a diffusion element, is a better solution in the design of encryption algorithms.

Reference

  - 1.

Index Terms

Computer Science

Security
Key words

Advanced Encryption Standard        Diffusion        Strict
Avalanche Criteria
Improving the Diffusion power of AES Rijndael with key multiplication