DIFFUSION AND TIME ANALYSIS FOR AES CANDIDATES

MOHAN .H .S[1] & SNEHA .M[2]

[1]Professor and Head of the Department, Department of Information Science and Engineering,

S J B Institute of Technology, Bangalore, Karnataka, India

[2]4th Semester M.Tech, Department of Information Science and Engineering,

SJB Institute of Technology, Bangalore, Karnataka, India

ABSTRACT

In this modern world, internet is the main means of communication. So there is a threat to the data always flowing through this network. That's why the security of data came into picture. There are different ways in which the data can be secured; one of the ways is by using different cryptographic algorithms. The strongest algorithm in symmetric key cryptography till now is AES. This paper provides the performance comparison between MARS, Serpent and Rijndael different candidate algorithms of AES interms of encryption, decryption, and key setup time and also through diffusion analysis. AES is a block cipher and are based on substitution, transposition to encrypt a plain-text message and to produce a cipher-message. Those transformations are based on well understood Mathematical problems using non-linear functions and linear modular algebra.

KEYWORDS: AES Algorithm, Cryptography, MARS, Serpent, Rijndael