REVIEW OF THE JOURNEY FROM DES TO AES

NEETA WADHWA, SYED ZEESHAN HUSSAIN & S. A. M RIZVI

Department of Computer Science, Jamia Millia Islamia, New Delhi, India

ABSTRACT

DES [Data Encryption Standard] was born in mid 70's and died in late 90's. A new secure and fast algorithm was required to replace it. And it was replaced by AES [Advanced Encryption Algorithm] in 2001. This paper reviews the whole process of replacing the DES and finding the AES. It presents the critical analysis of all the 15 finalists of first round of AES process. All the participant algorithms are analyzed from the Speed versus Security perspective.

KEYWORDS: AES, DES, Symmetric Ciphers, Symmetric Cryptography