A STUDY OF MARS, RC6 AND SERPENT

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

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

ABSTRACT

After DES [Data Encryption Standard] was cracked, the new symmetric encryption standard hunt was started in 1999 and finished in 2001. The process was comprised of two rounds.This paper presents the study of 3 out of 5 finalists of second round of AES [Advanced Encryption Standard] process: MARS, RC6 and SERPENT. It analyzes the structure and working of these algorithms. It also analyzes the three algorithms on the basis of their encryption and decryption time.

KEYWORDS: AES, DES, MARS, RC6, SERPENT, Symmetric Cryptography