{tag} {/tag}
International Journal of Computer Applications

Volume 67 - Number 12

Year of Publication: 2013

Authors:

Paul A. J.

Saju A.

Lekshmi R. Nair

10.5120/11445-7039

{bibtex}pxc3887039.bib{/bibtex}

Abstract

In symmetric block ciphers, substitution and transposition operations are performed in multiple rounds to transform plaintext blocks into ciphertext blocks. In advanced Encryption Standard (AES) the transposition of data is facilitated by shift row and mix column operations. In Matrix Array Symmetric Key (MASK) Encryption, a block cipher proposed by the author, the data transposition is achieved by data based rotations. The data based transposition procedure offers two advantages. First, it is simple to implement and secondly, the procedure produces a strong data avalanche effect and differential data propagation. In this paper the possibility of improvising the performance of AES using data based transposition in its diffusion rounds is examined. As a case study, the data based transposition procedure has been introduced in AES. The data avalanche and differential data propagation produced in AES have been observed. The paper describes the data based transposition procedure and the enhanced data avalanche and differential data propagation produced in AES. It has been shown that, the data avalanche effect and differential data propagation characteristics of AES have been improved.

Refer

ences

- William Stallings, "Network Security Essentials (Applications and Standards)," Pearson Education, pp. 2-80, (2004).
- Charles P. Pfleeger, Shari Lawrence Pfleeger, "Security in computing," Pearson Education, pp. 66-120, (2004).
- Jose J. Amador, Robert W. Green. "Symmetric-Key Block Ciphers for Image and Text Cryptography," International Journal of Imaging System Technology, Vol. 15 – pp. 178- 188, (2005).
- Dragos Trinca, "Sequential and Parallel Cascaded Convolution Encryption with Local Propagation: Toward future Directions in Cryptography," Proceedings of The third International Conference on Information Technology-New Generations. (ITNG'06), 0-695-2497- 4/2006, IEEE Computer Society, (2006).
- Data Encryption Standard : http://csrc. nist. gov/publications/fips/fips46-3/fips-46-3. pdf
- Advanced Encryption Standard: http://csrc. nist. gov/publications/fips/fips197/ fips- 97. pdf
- Escrowed Encryption Standard: http://csrc. nist. gov/publications/fips/fips1185/ fips-185. txt
- Krishnamurthy G. N, Ramaswamy V. , Leela G. H, Ashalatha M. E, "Performance enhancement of Blowfish and CAST-128 algorithms and Security analysis of improved Blowfish algorithm using Avalanche effect," International Journal of Computer Science and Network Security, Vol. 8, No. 3, March 2008, pp. 244-250.
- Paul A. J. , Varghese Paul, P. Mythili, " Matrix Array Symmetric Key Encryption," Journal of Computer Society of India, Vol. 37, Issue No. 1, January – March 2007, pp. 48-53.
- Paul A. J. , Varghese Paul, P. Mythili, "A Fast and Secure Encryption Algorithm for Message Communication," IETECH International Journal of Communication Techniques, Vol. 2, No. 3, 2008, pp 104-109.
- Paul A. J. , Varghese Paul, P. Mythili, "Fast Symmetric Cryptography using Key and Data based Masking operations," International- Journal of Computational Intelligence - Research & applications, Vol 3, Number 1, January – June 2009, pp. 5-10.
- Paul A. J. , P. Mythili, Poulose Jacob "Matrix based Key Generation to Enhance Key Avalanche in Advanced Encryption Standard", International Journal of Computer Applications, No. 2, article 1, pp. 31–34, 2011. Published by Foundation of Computer Science (USA).

Index Terms

Computer Science Security

Keywords

Ciphertext Data based transposition Data avalanche Differential data propagation

Plaintext

Secret key