Performance Evaluation of Selected Encryption Algorithms

Ahmida ABIODUN[1], Olanrewaju LAWAL[1], Oyediran OYEBIYI[1], Odiete JOSEPH[2], Adeyemi ADETORO[2]
[1] Department of Computer Engineering, Moshood Abiola Polytechnic, Abeokuta, Nigeria
Lawaloo.mapoly@gmail.com, Oyediran.george@mapoly.edu.ng
[2] Department of Computer Engineering, Ladoke Akintola University of Technology, Ogbomoso, Oyo State, Nigeria
odietej@yahoo.com

Abstract

Data security is a key aspect of today's communication trend and growth. Various mechanisms have been developed to achieve this security. One is cryptography, which represents a most effective method of enhancing security and confidentiality of data. In this work, a hybrid based 136bit key algorithm involving a sequential combination of XOR (Exclusive –Or) encryption and AES (Advanced Encryption Standard) algorithm to enhance the security strength is developed. The hybrid algorithm performance is matched with XOR encryption and AES algorithm using encryption and decryption time, throughput of encryption, space complexity and CPU process time.

Index terms: AES, Cryptographic algorithm, Hybrid Encryption, XOR

References

[1]. Bello Alhaji Buhari, Afolayan Ayodele Obiniyi, Kissinger Sunday, Sirajo Shehu (2019). Performance Evaluation of Symmetric Data Encryption Algorithms: AES and Blowfish. Saudi J Eng Technol. ISSN 2415-6272 (Print) | ISSN 2415-6264 (Online). DOI: 10.36348/SJEAT.2019.v04i10.002.

[2]. Ruziq F, Sihombing P, Sawaluddin. Combination analysis of data encryption standard (DES) algorithm and LUC algorithm on file security. International Journal of Research and Review. 2020; 7(2): 140-144.

[3]. R. K. K. Ramesh Yegireddi, "A survey on Conventional Encryption Algorithms," IEEE, pp. 5090 - 5515, 2016.

[4]. F. Ruziq, "Combination Analysis of Data Encryption Standard (DES) Algorithm and LUC Algorithm on File Security," International Journal of Research and Review, vol. 7, no. 2, 2020.

[5]. Alireza Arab, Mohammad Javad Rostami, Behnam Ghavami. An image encryption method based on chaos system and AES algorithm. The Journal of Supercomputing (2019) 75:6663–6682. https://doi.org/10.1007/s11227-019-02878-7.

[6]. R. Enayatifar, A.H. Abdullah, M. Lee, A weighted discrete imperialist competitive algorithm (WDICA) combined with chaotic map for image encryption, Opt. Lasers Eng. 51 (2013) 1066–1077.

[7]. S. Vikendra and D. Sanjay. "Analysing Space Complexity of Various Encryption Algorithms". International Journal of Computer Engineering and Technology (IJCET), ISSN 0976-6367(Print), ISSN 0976 – 6375(Online) 4(1), pp. 414-419, April 2013.

[8]. R. H. Rajdeep Bhanot, "A Review and Comparative Analysis of Various Encryption Algorithms," International Journal of Security and Its Applications, vol. 9, no. 4, pp. 289 - 306, 2015.

[9]. R. S. A. M. R. Amorado, "Enhanced Data Encryption Standard (DES) Algorithm based on Filtering and Striding Techniques," in Proceedings of International Conference on Information Science and Systems, Tokyo, 2019.

[10]. M. A. A. Jain, "Implementation of Hybrid Cryptography," International Journal of Core Engineering & Management, vol. 1, no. 3, pp. 126-142., 2014.

[11]. S. Pavithra and E. Ramadevi. "Performance Evaluation of Symmetric Algorithms", Journal of Global Research in Computer Science, 3(8), pp. 43-45, 2012.

[12]. Hossein Movafegh Ghadirli, Ali Nodehi, Rasul Enayatifar. An overview of encryption algorithms in color images. Journal of signal processing (164). Elsevier. (2019).

[13]. Priyadarshini Patil, Prashant Narayankar, Narayan D G, Meena S. M., A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, India.