Comparative Study of Cryptographic Algorithms

Mohanad Abdulhamid[1], **Nyagathu Gichuki**[2]
[1] Al-Hikma University, Iraq, e-mail: moh1hamid@yahoo.com
[2] University of Nairobi, Kenya, e-mail: researcher12018@yahoo.com

Abstract

This paper presents a comparative study of two cryptosystems, Data Encryption Standard (DES) and the Rivest-Shamir-Adleman (RSA) schemes. DES is a symmetric (or private) key cipher. This means that the same key is used for encryption and decryption. RSA, on the other hand, is an asymmetric (or public) key cipher, meaning that two keys are used, one for encryption and the other for decryption. The objective of this paper is to implement these two schemes in software. The program is written in the Java™ language. It generates a key from a passphrase given by the user, encrypts and decrypts a message using the same key, for the case of DES. In RSA, decryption is done by computing the decryption key from the encryption key. Finally, the program returns the time taken to encrypt and decrypt a message.

Index terms: Cryptographic algorithms, RSA, DES

References:

[1]. N. Gichuki, "Comparative DES/RSA performance evaluation", Graduation Project, University of Nairobi, Kenya, 2009.

[2]. G. Chhabra, "Computer trend with security by RSA, DES and Blowfish algorithm", International Journal of Computer Science and Technology, Vol. 4, Issue 2, PP.618-620, 2013.

[3]. P. Patil, "A Comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish", Procedia Computer Science, Vol. 78, pp. 617-624, 2016.

[4]. A. Rao, "Survey paper comparing ECC with RSA, AES and Blowfish Algorithms", International Journal on Recent and Innovation Trends in Computing and Communication, Vol. 5, Issue 1, PP.44-47, 2017.

[5]. S. Kaur, "Study of multi-level cryptography algorithm: Multi-Prime RSA and DES", International Journal Computer Network and Information Security, Vol. 9, PP. 22-29, 2017.