European Journal of Scientific Research
ISSN 1450-216X / 1450-202X Vol. 126 No 4 November, 2014, pp.465 – 480
http://www.europeanjournalofscientificresearch.com

A Modified Flexible Data Encryption Standard Algorithm

Essam M. Ramzy Hamed
Management Information System Department
Arab Academy for Science Technology and Maritime Transport
Heliopolis, Cairo, Egypt
E-mail: dodessammisr@gmail.com
Tel: +201141099922

Mohammad Hosam Sedky
Computer Science Department
Arab Academy for Science Technology and Maritime Transport
Heliopolis, Cairo, Egypt
E-mail: m.hosamsedky@hotmail.com
Tel: +201151122592

Abstract

This paper proposed flexible, advanced DES algorithms that solve many drawbacks in the DES algorithm. First, they increase the key size to 224 bits instead of 56 bits (the main weakness of DES) that make the Brute-Force attack effect impossible or takes very large number of years for exhaustive key search. Second, they increase the block size of the plain text messages from 64 bits to be 256 bits without increasing the simulation time. Last, the most important contributions of the proposed algorithms are: 1) they change the number of rounds from fixed number in DES (16 rounds) to dynamic number (N) that will be selected as a variable input number by the user according to the data sensitivity level he wants. Therefore, N sets the sub-keys numbers to be dynamic too. This makes the brute force attack on the proposed algorithms has no effect. 2) The algorithms codes accept any language as the plain text input messages and the secret key too. They accept the plain text message and the key to be written with any language, like English, Russian, Arabic, .etc. The importance of this modification is encouraged using any language in the applications that deal with information needed to be in certain language; like the secured e-voting application.

Keywords: Cryptography, Feistel cipher, Symmetric key, Data Encryption Standard (DES), Symmetric block Cipher, Advanced Encryption standard (AES), Key length, block size, and Advanced Data Encryption Standard (ADES)