Egyptian Informatics Journal xxx (2016) xxx–xxx

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Full length article

Parametric comparison of EMDS algorithm with some symmetric cryptosystems

Mani Arora [a,*], Sandeep Sharma [b], Derick Engles [b]

[a] Khalsa College, Amritsar, Punjab, India
[b] Guru Nanak Dev University, Amritsar, Punjab, India

ARTICLE INFO

Article history:
Received 22 April 2016
Revised 20 October 2016
Accepted 10 November 2016
Available online xxxx

Keywords:
EMDS
Algorithm
Data security
Encryption
Decryption
Reduce cipher
Throughput

ABSTRACT

Over the last decades owing to the incredible boost in the electronics industry and wireless technology, there has been an extraordinary outburst in the extent of digital data transmitted via the internet by means of handheld chic devices. The hefty amount of transmitted data requires data to be safe and sound in addition to transmission speed should be swift. In this document we have prepared qualitatively crypt-analysis of our proposed technique 'EMDS' and evaluated against it with further preferred symmetric algorithms. We have analyzed the diverse variety of symmetric algorithms by following the tangible approach and examined dissimilar parameters implicated. This document endows with estimation of ten of the majority of frequent algorithms. A contrast has been carried out connecting those algorithms and EMDS based on diverse parameters.

1. Introduction

Cryptography is considered necessary to solve tribulations concerning secrecy, authentication, integrity and fraudulent community. Owing to incredible boost in transmission of data over the networks by the side of security there is requirement to ensure on dimension of transmitted data so as to condense the utilization of bandwidth and memory space required to store data. If these factors will be restricted it will automatically enhance the pace of transmission [1]. There have been a number of suggestions to cut down the size of cipher text while providing security for asymmetric encryption however there have been extremely inadequate proposals of symmetric encryption cipher technique. EMDS algorithm anticipated by us gratifies the problem of huge storage space, amplified bandwidth, energy consumption, transmission speed and security. In this document preferred block cipher algorithms DES, triple DES, IDEA, Blowfish, CAST 128 as well as stream cipher algorithm RC2 and RC5 are examined simultaneously with EMDS algorithm. The performance of various symmetric algorithms is usually determined by using simulation or mathematical methods. In this paper we present the simulation results of various metrics used to measure the performance of proposed and existing symmetric cryptography algorithms. The performance of EMDS is evaluated by implementing the algorithm in Java

The purpose of this analysis is to

1. Compare EMDS with other symmetric algorithms.
2. Calculate the average cutback in cipher text size as compared to plain text size with reverence to EMDS algorithm

2. Various techniques for cryptography

In the present time, most symmetric encryption schemes are based on Fiestel network. It consist of number of rounds where each round includes bit shuffling, non linear substitutions (S-boxes) and exclusive OR operations. A short description of diverse Fiestel Network symmetric cryptographic algorithms is as follows.

2.1. Simplified Data Encryption Standard (SDES)

Simplified DES (S-DES) is an educational but not a secure block cipher algorithm. It was simplified version of DES formulated by Professor Edward Schaefer of Santa Clara University. Encryption algorithm acquires an 8-bit block of plaintext along with a 10-bit

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

* Corresponding author.

E-mail addresses: mani_mcain@yahoo.com (M. Arora), Sandeep_gndu@yahoo.com (S. Sharma), derickengeles@yahoo.com (D. Engles).

http://dx.doi.org/10.1016/j.eij.2016.11.004
1110-8665/© 2016 Production and hosting by Elsevier B.V. on behalf of Faculty of Computers and Information, Cairo University.

key as input and generates an 8-bit block of cipher text as output vice versa decryption algorithm acquires 8 bit cipher text and a 10 bit key as input to create 8 bit original plain text [2].

Major operations of encryption algorithm

1. An initial permutation (IP).
2. An intricate function marked as fK, which engages both permutation as well as substitution operations furthermore it depends on a key input.
3. An effortless permutation function that switches (SW) the two halves of the data
4. The function fK yet again.
5. To end with a permutation function that is the contrary to the initial permutation (IP^{-1}).

S-boxes

S-boxes offer non linearity to algorithm. It makes use of fixed type (Non Key dependent) of S-boxes.

Number of S-boxes used: 02 (S0 and S1).

Number of operators

It employs merely a particular operator i.e. exclusive OR while computing function fK.

Number of Keys.

It employs merely 01 key of size 10 bits.

2.2. Data Encryption Standard (DES)

Frequently and extensively used of all encryption algorithms is data encryption standard. It was designed by IBM in the 1970s and implemented by the National Bureau of standards (NBS) [now the National Institute for Standards and Technology] in 1977 for commercial and unspecified government applications .It encrypts and decrypts 64 bit data at a time. The 56 bit cipher key is utilized for both encryption and decryption.[3] It is most generally used for conservative algorithm.

Major operations of encryption algorithm

1. An initial permutation IP.
2. Permutations and substitution functions are applied using XOR operator and S-boxes in 16 rounds.
3. An uncomplicated permutation function is implemented that substitute two halves i.e.32 bit data.
4. Contrary to initial permutation (IP^{-1})

S-boxes

Number of S-boxes used: 08(S0, S1–S8).

Number of operators

It uses only single operator i.e. exclusive OR.

Number of keys

It makes use of merely 01 key of size 56 bits.

2.3. Triple DES (3DES)

Formulated by Tuchman to preserve privacy and amalgamation of information illustrated by data during transmission or while in storage. Triple data encryption algorithm was chosen for applying in financial applications in ANSI standard X9.17.It is a three level put up using DES at each level to defend in opposition to savage drive attacks, exclusive of devising an utterly latest block cipher algorithm. In addition to it, Triple DES is put into operation with diverse number of keys i.e.

1. 3DES (2):-DES used thrice with two different keys.
2. 3DES (3): DES used thrice with three different keys.

2.3.1. 3DES(2)

It acquires 64 bit block of plain text and key of 112 bits as input and generates cipher text of 64 bits. Permutation and substitution functions are applied in 48 rounds.

Major operations of encryption algorithm

1. Encrypt using key K1.
2. Decrypt using key K2.
3. Resulted data is again encrypted using key K1.

S-boxes

Number of S-boxes used: 24.

Number of operators

It employs merely particular operator i.e. exclusive OR.

Number of keys

It exercises 02 keys.

2.3.2. 3DES(3)

Triple DES with two keys undergo meet in the middle attack so triple DES with three keys move towards subsistence. Despite the fact that it is more safe and sound but time-consuming than DES. It is applied by Federal organizations to protect receptive data. It captures 64 bit plaintext in addition to 168 bit key to produce cipher text of 64 bits in 48 rounds. Encryption course is an effort of Encryption and decryption process of single DES cipher.

Major operations of encryption algorithm

1. Encrypt data using DES with key K1 characterized as E_{K1}
2. Decrypt E_{K1} with key K2 by means of DES symbolized as D_{K2}
3. Yet again DES encryption is executing of D_{K2} with key K3.

Where K1, K2, K3 are independent keys.

S-boxes

Number of S-boxes used: 24.

Number of operators

It utilizes only single operator i.e. exclusive OR.

Number of keys

It uses 03 keys.

2.4. International Data Encryption Algorithm (IDEA)

The global Data Encryption Algorithm (IDEA) is a symmetric block cipher projected by Xuejia Lai and James Massey of ETH Zurich in 1991. It was anticipated to be a substitution for the Data Encryption Standard. Encryption algorithm acquires a 64-bits block of plaintext in addition to a 128-bit key as input along with it brings into being a 64-bits block of cipher text as output [4]. The strength of IDEA lies with utilization of XOR, binary addition and binary multiplication of 16-bit integers.

Major operations of encryption algorithm

1. Key Scheduling: Sub key generation algorithm is used to create 52 16bit sub keys as output.
2. Plaintext is disintegrated into four 16 bit sub blocks.
3. Three dissimilar categories of operations are executed on splitted data in 8 rounds.
   (i) Addition (+):-Addition of integers modulo 2^{16} with inputs and outputs treated as unsigned 16 bit integers.
   (ii) Multiplication Θ:-Multiplication of integers modulo $2^{16}+1$, with inputs and outputs taken care of as unsigned 16-bit integers excluding a block of all zeros is considered as representing 2^{16}.
   (iii) Bitwise exclusive OR ($\oplus$).
4. Output transformation: Again operators are used on interchanged data and sub keys to produce final output.

Please cite this article in press as: Arora M et al. Parametric comparison of EMDS algorithm with some symmetric cryptosystems. Egyptian Informatics J (2016), http://dx.doi.org/10.1016/j.eij.2016.11.004