Journal of Engineering and Applied Sciences 12 (Special Issue 10): 9035-9040, 2017
ISSN: 1816-949X
© Medwell Journals, 2017

AES Cryptography Algorithm Based on Intelligent Blum-Blum-Shub PRNGs

[1]Estabraq Abdul Redaa Kadhim, [2]Zaid Khudhur Hussein and [3]Hadi Jameel Hadi
[1]Department of Computer Engineering Techniques,
[2]Department of Medical Instrumentation Engineering,
Al-Esraa University College, Baghdad, Iraq
[3]Department of Computer Engineering Techniques, Al-Mustafa University College, Qom, Iraq

Abstract: One of the relative common encryption algorithm in the literature is Advanced Encryption Standard (AES) procedural steps. It is public key algorithm which has a number of drawbacks to its security. This study presents new combining advanced encryption standard with intelligent BBS-PRNGs (i.e., hybrid of Blum-Blum-Shub (BBS) and Iterated Local Search (ILS) metaheuristic technique) for generating strong crypto key using some of non-parametric statistic tests. The simulation tool has been conducted using MATLAB simulator for enhanced AES cryptography model.

Key words: AES encryption algorithm, Blum-Blum-Shub (BBS), Iterated Local Search (ILS), PRNGs, artificial intelligence, simulator, conducted

INTRODUCTION

Encryption algorithm can be classified into data flow encryption algorithm and grouping encryption algorithm. Data flow encryption algorithm is that plaintext performs a bitwise exclusive or on secret key to generate cryptograph. Secret key is usually a pseudorandom sequence. Same pseudorandom sequence is generated throughout decryption and pseudorandom sequence performs a bitwise exclusive or on cryptograph to restore plaintext. Grouping encryption algorithm is related to plaintext that is divided into some data block of fixed bit number. Secret key is also a data block which has a fixed bit number (Zhang and Zhang, 2005). Plaintexts of each group perform complex mathematical operation on secret key of each group to get cryptograph.

AES stands for a division of the Rijndael cipher created by dual Belgian cryptographers (Daemen and Rijmen, 2001). Rijndael is a relation group of ciphers with dissimilar block sizes and key. National Institute of Standards and Technology (NIST) had chosen three constituents of the Rijndael family for AES. Every one of them with a block size of 128 bits of three dissimilar key lengths: 128, 192 and 256 bits (Daemen and Rijmen, 2001).

Intelligent Blum-Blum-Shub (BBS) is an eminent cryptographically protected pseudo arbitrary number generator that combine between BBS PRNGs and ILS metaheuristic search technique. BBS is fully irregular even if a lengthy bit's sequence is produced. The principal hypothesis is derived from quadratic residues and cracking is comparable with integer factorization. Iterated Local Search (ILS) is a straightforward and influential metaheuristic procedure. It employs local search to a preliminary solution until it locates a neighboring the best possible one (Bishop, 2003).

Traditional Blum-Blum-Shub (BBS) has been classified as one of the best and strong method for random bit sequence but the Improved Blum-Blum-Shub (Improved-BBS) proved to be generating strong integer numbers and bit sequence for cryptokey purpose.

The existence of some nonparametric statistic test as a means for evaluate the frequency, magnitude and randomness of improved BBS-cryptokey had given sober BBS-cryptokey.

Enhancement of cryptokey basically dependent on seed number (i.e., size, randomness and distribution of BBS-cryptokey are different from one sequence to another that have same nBlum) (Kadhim, 2015).

The AES algorithm idea was first suggested by Daemen and Rijmen (2001) and later many studies and techniques have been developed to improve the AES initial key.

Paul a speedy and protected encrypted procedure using substitution mapping, translation and transposing methods has been presented. The process of the symmetric encrypted system has dual benefits over customary schemes. Firstly, the encrypting and

Corresponding Author: Estabraq Abdul Redaa Kadhim, Department of Computer Engineering Techniques, Al-Esraa University College, Baghdad, Iraq

decrypting techniques are very simple and therefore to a large extent quicker. Secondly, the security level is superior because of the inherent poly-alphabetic performance of used replacement plotting system.

By Jianyong Huang, analysis of the key arrangement of the AES algorithm and extant some recurrent differential characteristic for AES-128 and AES-256 key arranges has been reported.

Pitchaiah *et al.* in 2012 produced a 128 bit AES encrypting and decrypting into a synthesizable using Verilog code implemented on to FPGA. The process is combined from three parts, cipher, inverse cipher and key expansion.

Yang *et al.* (2015) for solving the safety problems of existed AES encryption algorithm an enhanced AES encryption procedure in accordance with chaos hypothesis is proposed. Simulation is conducted to verify the feasibly and correctness of the proposed improved AES encryption algorithm by MATLAB (Yang *et al.*, 2015).

In this approach, AES will be combined by using intelligent Blum-Blum Shub (BBS) to generate initial key for AES algorithm as tricky enhanced AES cryptography technique useful for modern secure wireless communication systems.

AES algorithm: The AES method is a symmetric-key secret message that is in cooperation with the transmitter and the receiver to employ a solitary key for encrypting and decrypting. The data block length is unchanging to be 128 bits, although, the length is possible to be 128, 192 or 256 bits. Additionally, the AES method is an iterative procedure, every iteration is known as a round and the overall number of rounds is 10, 12 or 14 if key length is 128, 192 or 256 in that order. The 128 bit data block is split into 16 bytes. These bytes are configured to a 4×4 array called the state and the entire inner processes of the AES algorithm are carried out on the state (Karthigaikumar and Rasheed, 2011).

Encryption has procedures of transforming the text words into a layout that is uneasily decipherable which is known as cipher. The cipher is acquired by performing a sequential arithmetical operation based on iteration levels. There are four main steps of the algorithm sub-bytes, shift rows, mix columns and add round key (Thulasimani and Madheswaran, 2010).

Sub bytes: In this step as depicted in Fig. 1, the data in the plain text is replaced with by a number of pre-arranged magnitudes from a substitution box. The generally used box is Rinjdale substitution box which can be inverted.

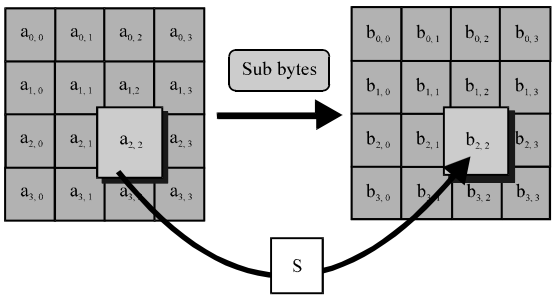

Fig. 1: Sub-bytes

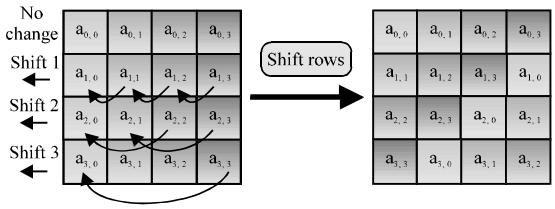

Fig. 2: Shift rows

Shift rows: In this step, the rows in the 4×4 matrix is moved to left r bits and r is variable with the rows of the matrix (r = 0 for row 1, r = 1 for row 2, r = 2 for row 3, r = 3 for row 4). This procedure is shown in Fig. 2.

This has the consequence of transferring the lower positions in the row whereas the minimum byte's wrap around to the peak of the row (Thulasimani and Madheswaran, 2010).

Mix columns: It can have determined based on the following equation:

$$\begin{bmatrix} R0 \\ R1 \\ R2 \\ R3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 3 & 3 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} a0 \\ a1 \\ a2 \\ a3 \end{bmatrix} \quad (1)$$

where, a0, a1, a2 and a3 are determined using the polynomials as follows:

$$a(x) = \{2\}x^3 + \{3\}x^2 + \{1\}x + \{1\} \quad (2)$$

The transformation of mix column research on the state column by column, each column represents a four term polynomial. The columns are defined as polynomials over Gaussian Field GF (28) and multiplied modulo (x^4+1) with a fixed polynomial a (x) that can be obtained from the previous equation. This can as well be arranged as a matrix multiplication (Fig. 3):

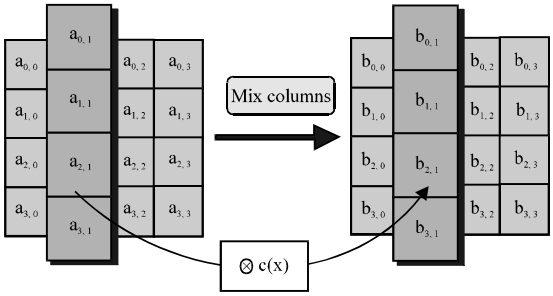

Fig. 3: Mix columns

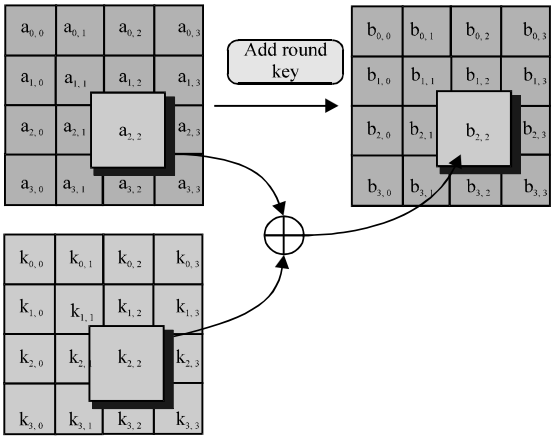

Fig. 4: Add round key

$$s'(x) = a(x) \otimes s(x) \quad (3)$$

Add round key: In the add round key step as shown in Fig. 4, the 128 bit data is manipulated by XOR logical function with the sub key of the present round using the key expanding process. The add round key can be employed in dual dissimilar positions, one throughout the beginning as round r = 0 and then through the other rounds as 1≤round≤Nr. Nr represents the highest rounds number. The method to carry out the add round key is:

$$S'(x) = S(x) \oplus R(x) \quad (4)$$

Where:
S′(x) = State after adding round key
S(x) = State before adding round key
R(x) = Round key

Every bite of the state is joint with a round key that is not similar to key per round based on the Rinjdale key schedule (Thulasimani and Madheswaran, 2010). Figure 5 illustrates the flowchart of the AES algorithm.

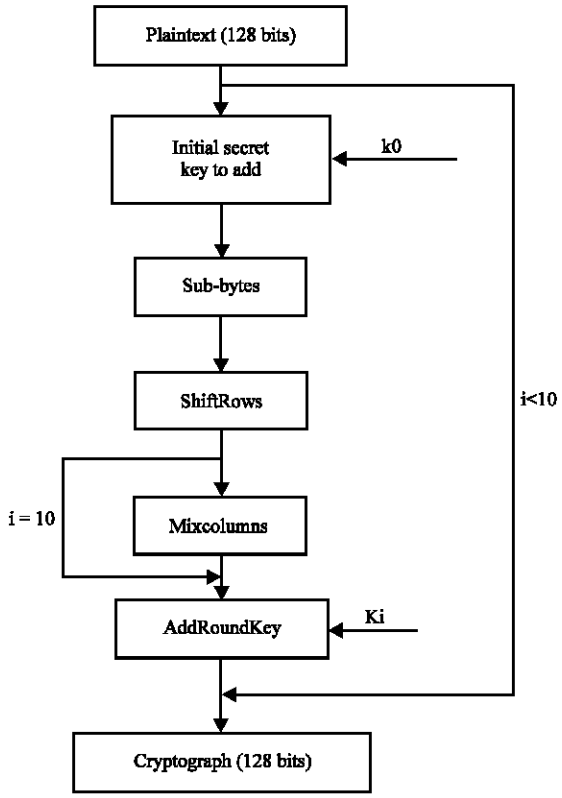

Fig. 5: Flow chart of AES encryption algorithm

MATERIALS AND METHODS

Blum-Blum-Shub (BBS): A pseudorandom generator has deterministic procedural steps that, given an accurately arbitrary binary sequence of length n, outputs a binary sequence of length m>n that "looks random". The generator input is known as the seed and the output is known as the pseudorandom bit sequence. Security of a pseudorandom generator is a feature that explains how difficult it is to notify the dissimilarity among the pseudorandom sequences and accurately random sequences. For the Blum-Blum-Shub pseudorandom generator recognizing these dual sequences is as hard as factoring a huge complex integer. The Blum-Blum-Shub pseudo random number generator is based on the following steps:

Step 1: Generate p and q, two big blum prime numbers
Step 2: n: = p×q
Step 3: Select s∈R [1, n-1], the arbitrary seed
Step 4: x: = s2 (mod n) 0
Step 5: The series is identified as x: = x2 (mod n) and z: = parity (x). Where parity (x) is define as R (x)

Iterated Local Search (ILS): ILS intends to look for the space of local optima. A random solution S is produced

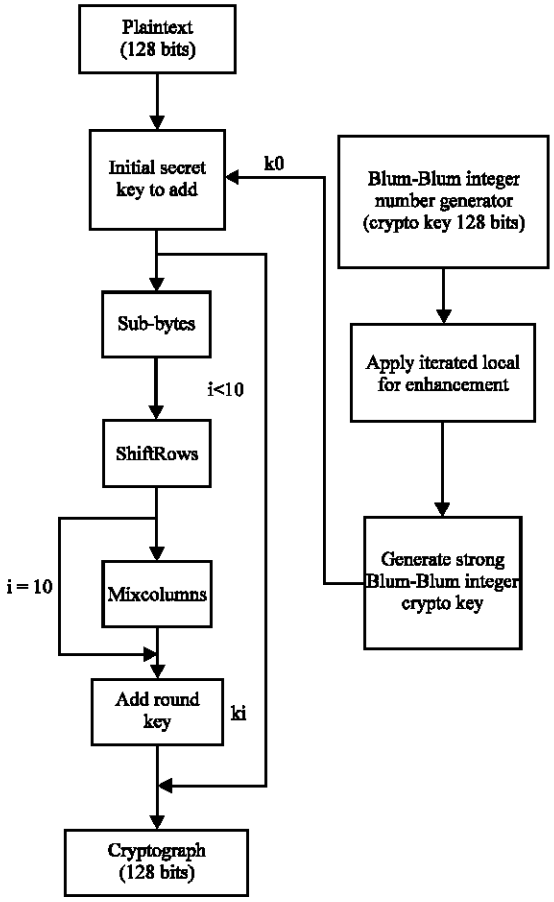

Fig. 6: Flow chart of improving AES using intelligent Blum-Blum-Shub (BBS)

and then local search is S0 functional to reach a local optimum S*. This local optimum is then mapped in some manner to acquire S' and local search is then adopted to accomplish another local optimum S*′. A number of decisive factor is applied to find out whether the "move" from S* to S*' is acknowledged. Accordingly, the high level moves are clearly to be amid local optima.

The perturbation strength is a criterion of how much it varies the solution. This may be unchanging or may vary with dynamism. A diversity of acceptance criterion can be applied (always accept, accept only improving moves, accept probabilistically in an annealing-like manner, etc.) (Kadhim, 2015).

Proposed approach: AES security key is public. Computer hackers can get the security key according to the security key expansion algorithm if they get one round secrete key. The original text will be determined according to decryption algorithm by computer hackers after they know the security key. Therefore, the traditional public AES encryption algorithm has safety problems.

In this study, there is enhanced, strong approach has been used for improving and increasing the safety and secrecy of AES encryption algorithm. Pseudorandom sequences which have enough length generated by intelligent Blum-Blum-Shub Pseudorandom Generator (PRNGs) used to generate initial key for AES rounds. Figure 6 illustrates in details the main steps of AES enhancement.

RESULTS AND DISCUSSION

This study describes full examples about the proposal. Let the sentence to be sent is "MY NAME IS HADI", this massage is represented in ASCII as shown in Fig. 6, p = 23, q = 11, n_{blum} = 253 and s = 157, after applying traditional BBS the initial cryptokey = (190 174 169 225 25 119 246 49 124 196 213 82 146 64 48 27) and for intelligent Blum-Blum-Shub the cryptokey equal to (47 47 47 169 59 223 179 31 71 36 108 192 12 174 48 144) more than one cryptokey is generated from different seed number to ensure security for AES algorithm.

In Fig. 7, the original massage (plaintext) is shown as the example to send the message "MY NAME IS HADI". The massage has 16 bit length in form numerical value as ASCII code presented in (4×4) matrix. If the original massage length more than 16 bit, 16 bit window (4×4) matrix is taken.

In Fig. 8, intelligent Blum Blum Shub cryptokey is shown come from combined Iterated Local Search (ILS) with Blum Blum Shub (BBS) to reach a local optimum random solution S, intelligent Blum Blum Shub (BBS) cryptokey does not affected by n blum or length of key number, it only affected by how numbers are distributed within key sequence.

Traditional BBS classified as one of best and strong method for random bit sequence but Improved-BBS proved to be generating strong integer numbers and bit sequence for cryptokey purpose.

Enhancement of cryptokey basically dependent on seed number (i.e., size, randomness and distribution of BBS cryptokey are different from one sequence to another that have same n Blum).

The cipher text after encryption with AES intelligent Blum-Blum Shub is become unreadable text as shown in Fig. 9. The cipher text 16 bit key can be converted to binary system and send it to receiver. When some systems using 32 bit or larger words, the execution of cipher possible to speed up by combining the first and second steps of AES algorithm (Sub-bytes and

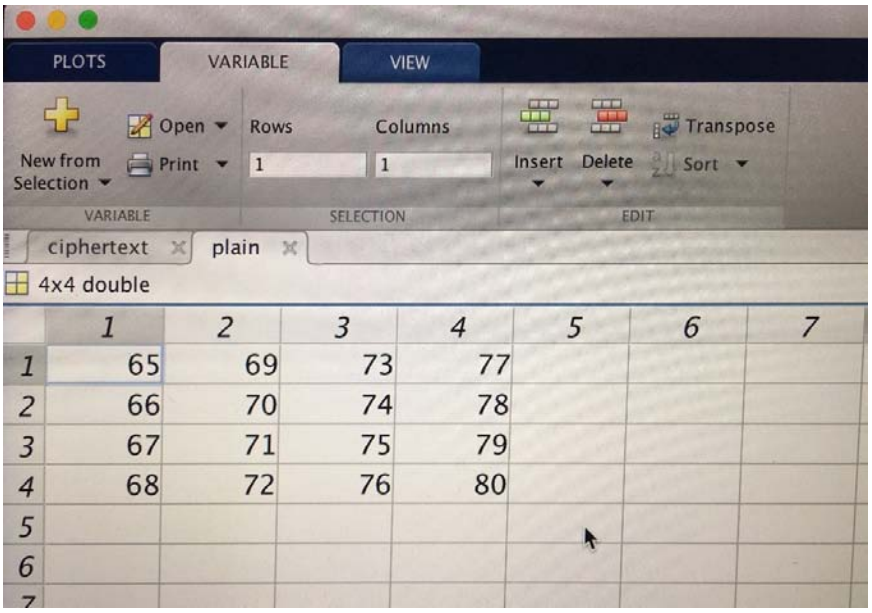

Fig. 7: Workspace of massage ASCII code

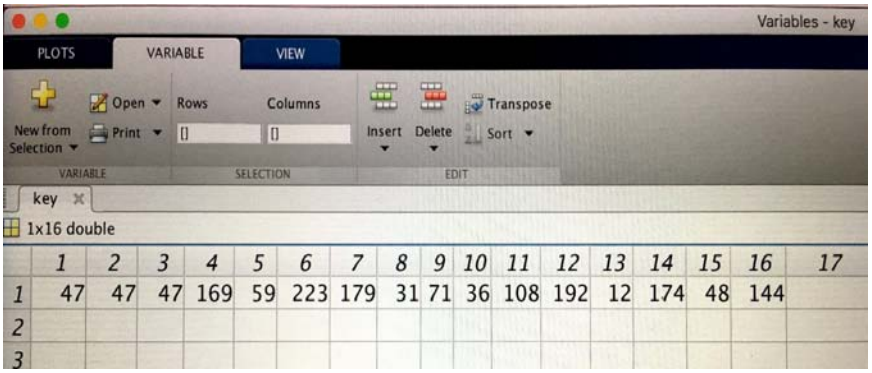

Fig. 8: Workspace of intelligent Blum Blum Shub cryptokey

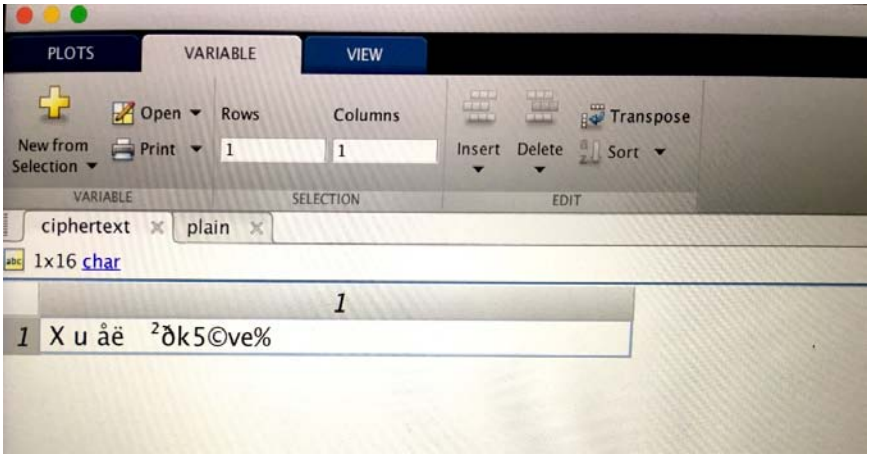

Fig. 9: Workspace of AES ciphertext with intelligent Blum Blum Shub

ShiftRows) steps with the third step mix columns by converting them into a series of table look ups. This requires four 256 entry 32 bit tables (together occupying 4096 bytes).

CONCLUSION

This study was introducing combining method for AES encryption algorithm with intelligent BBS that research as initial key generator. This method has increased the efficiency of the encryption process. Intelligent BBS provide hard mathematical relation among of numbers, so, it is difficult to hack and analyze preliminary key. So, the generated crypto-key can be considered as high randomly and secrecy. Additional future research can be conducted to carry out deciphering for the proposed enhanced cryptography method using genetic algorithm techniques (Yaqeen and Seevan, 2017; Toemeh and Arumugam, 2008). Also, LiFi technique can be used to enhance the security levels of adopted cryptography system in this study.

ACKNOWLEDGEMENTS

This research was supported by Research Dr. Eng. Waail Mahmod Lafta PhD, MSc., BSc. ASME member, IEEE member, UoIE member, IIE member, NSECP member, AASCIT Member, Brisbane-QLD 4113-Australia.

REFERENCES

Bishop, D., 2003. Introduction to Cryptography with Java Applets. In: A History of Cryptography, Bishop, D., (Ed.). Jones & Bartlett Learning, Burlington, Massachusetts, USA., ISBN:9780763722074, Pages: 229-377.

Daemen, J. and V. Rijmen, 2001. Announcing the Advanced Encryption Standard (AES). Federal Information Processing Standards, USA.

Kadhim, E.A.R., 2015. Number generator improvement based on artificial intelligent and nonparametric statistic methods. Intl. Educ. Res. J., 1: 28-33.

Karthigaikumar, P. and S. Rasheed, 2011. Simulation of image encryption using AES algorithm. IJCA. Comput. Sci New Dimensions Perspect., 2011: 166-172.

Thulasimani, L. and M. Madheswaran, 2010. Design and implementation of reconfigurable rijndael encryption algorithms for reconfigurable mobile terminals. Intl. J. Comput. Sci. Eng., 2: 1003-1011.

Toemeh, R. and S. Arumugam, 2008. Applying genetic algorithms for searching key-space of polyalphabetic substitution ciphers. Intl. Arab J. Inf. Technol., 5: 87-91.

Yang, Z.H., A.H. Li, L.L. Yu, S.J. Kang and M.J. Han *et al*., 2015. An Improved AES encryption algorithm based on chaos theory in wireless communication networks. Proceedings of the 2015 3rd International Conference on Robot, Vision and Signal Processing (RVSP), November 18-20, 2015, IEEE, Kaohsiung, Taiwan, ISBN:978-1-4673-9647-9, pp: 159-162.

Yaqeen, S.M. and F.A. Seevan, 2017. Affine cipher cryptanalysis using genetic algorithms. J. Algebra Number Theory Appl., 39: 785-802.

Zhang, L. and Y. Zhang, 2005. Research on Lorenz chaotic stream cipher. Proceedings of the 2005 IEEE International Workshop on VLSI Design and Video Technology, May 28-30, 2005, IEEE, Suzhou, China, pp: 431-434.