DOI: http://dx.doi.org/10.30684/etj.37.3B.4

Abdul Monem S. Rahma
Computer Science Dept.,
University of Technology
Baghdad, Iraq.

Atheer M. Abbas
Computer Science Dept.,
University of Technology
Baghdad, Iraq.
cs_uot@uotechnolog.edu.iq

Received on: 08/05/2018
Accepted on: 11/02/2019
Published online: 25/10/2019

A modified Matrices Approach in Advanced Encryption Standard Algorithm

Abstract-*The cryptographic algorithms became the main proceeding for protection of very important data from unauthorized access. There are several cryptographic algorithms to ensure the data, but algorithms must be selected according to speed, strength and the implementation. Thus, choosing the advance encryption standard (AES) for encryption and decryption data because its speed and strength of encryption, flexible, complex processing and its resistance to Brute-force attack. This paper presents enhancement of the AES algorithm to increase the security of the encrypted documents by using different sizes data matrices based on multiple irreducible polynomials with order 2, 4, and 8. The proposed modifications results tested and provide a high randomness.*

Keywords-: *AES, irreducible polynomial, randomness*.

How to cite this article: A.S. Rahma and A.M. Abbas, "A modified Matrices Approach in Advanced Encryption Standard Algorithm," *Engineering and Technology Journal*, Vol. 37, Part B, No. 3, pp. 86-91, 2019.

1. Introduction

The work aims to enhance the AES-128 algorithm by using different sizes data matrices. To find out the efficiency of the modified method will be rely on random tests of the results by using the approved tests by researchers in the same subject [1]. The AES includes three -128, AES-192, and AES-with block size of 128, 192, or 256 bits. The block-size has a maximum of 256 bits. The cipher uses number of encryption rounds, which converts plain text to cipher text. The output of each round is the input to the next round. The output of the final round is the encrypted plaintext known as cipher text. The plaintext given by the user is entered in a matrix (4*4 byte) called State Matrix. The total number of rounds that consist of different numbers (10, 12, or 14 rounds), depending on Rijndael round function stages (addroundkey, subbytes, shift row, mixcolumn) [2].

2. Previous Modifications of AES Algorithm

There are many modifications in AES to increase security, improve the efficiency and performance and keeping the same complexity on algorithm steps. The AES modifications applied on software and hardware according to the specific proposes.

In [3] present to modified AES algorithm by producing a modified algorithm to generate a dynamic S-Box stage. The performance of this algorithm is verified by varying only selected two bits of encryption key to produce novel S-Boxes to increase the complexity of algorithm. In [4] present to modify the AES algorithm by enlarge encryption keys sizes and data matrix. The data matrix extended to 8 row and variable number of columns (6, 8, 12, and 16), the input data block is (48, 64, 96, and 128) and enlarged the key length to (384, 512, 768, and 1024). In this paper the first and second stages of AES algorithm not change, while third stage (shift row) change from shift 3 row to 7 row and fourth stage (mix column) change the state matrix 3*3 to new matrix 8*8. In [5], this work modified the AES algorithm to generate large number of S-boxes by using dual keys to solve the problem of the fixed structure S-boxes, this lead to increase the complexity, robustness and security level of the AES algorithm.

In [6] present to modify the AES algorithm by reduce the calculation and computation overhead. To overcome the problem of high calculation it replace the mixcolumn step by a permutation step. The mixcolumn stage gives high security but it takes long time calculation that makes the encryption algorithm very slow. The other transformations in AES remain with no change.

3. Advance Encryption Standard (AES) Algorithm

AES is a symmetric algorithm and considered one of types of block cipher. It is widely used in several industry standards and is used in many security institutions. AES is defined as AES-128, AES-192, or AES-256 that name depended on key length that used in the encryption process. The size of data matrix is same key length and having 10, 12, & 14 iterations. AES based on special mathematical rules called the *Galois field GF* (256) with the irreducible polynomial m(x) =

$x^8 + x^4 + x^3 + x + 1$. This mathematical use in s-box, mix columns and used in creation of the key. It consists of four different stages (add round key, substitution, shift row, and mixcolumn) [**7**], as shown in the Figure 1.

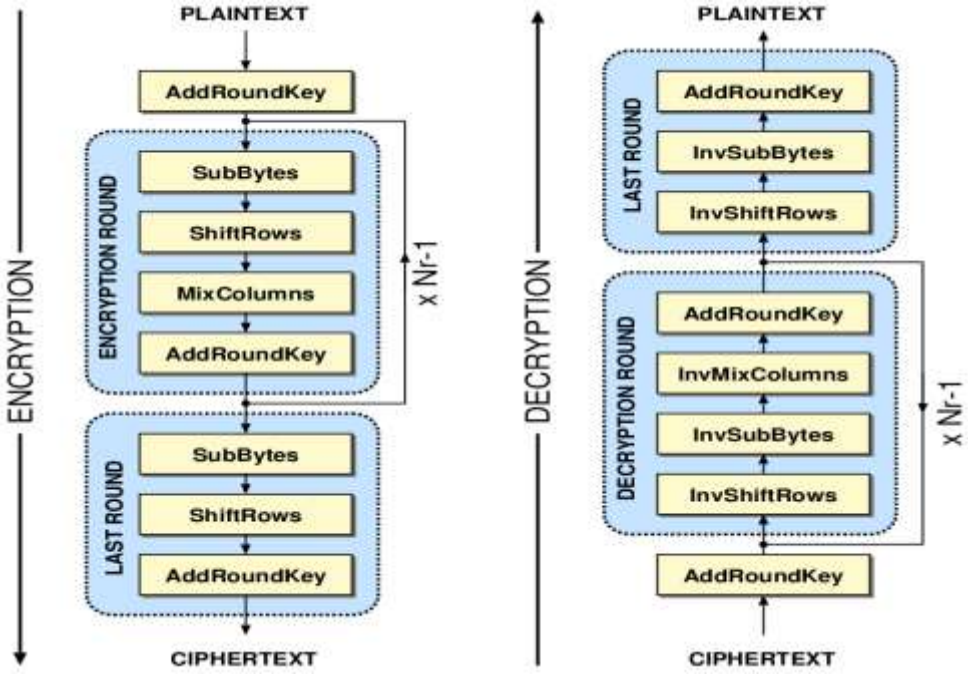

Figure 1: AES structure

I. Description of AES Algorithm Stages

It used block size of 128 bits, which mean the data-matrix is 16 bytes; the algorithm consists of two parts. The first part is key expansion that convert the key sequence length of at most 16 bytes (128 bits) into several subkeys array totaling 176 bytes (1408 bits) and the second part is data encryption by using 10 rounds.

II. Substitution Byte Stage

In this stage, each byte replace with another byte by using s-box. The AES s-box operation provides the non-linearity in the cipher and used the multiplicative inverse over GF(256) that know as good non –linearity properties to avoid attack. As shown in Figure 2.

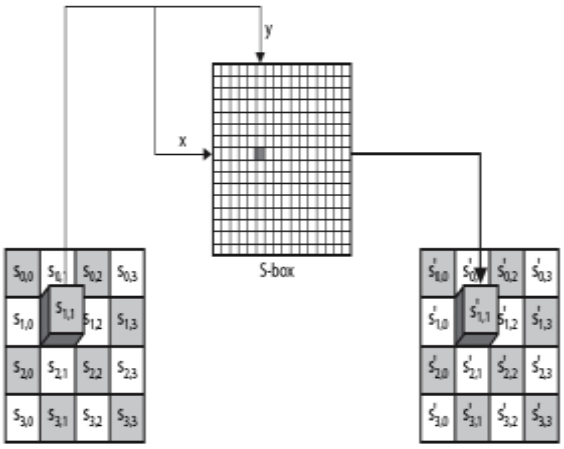

Figure 2: subbytes stages. [7]

III. Shift Row Stage

In this stage, shift the row of data matrix to cyclically left shifts. The first row in data matrix is unchanged, the second row shift one byte to left, the third row shift 2-byte to left and the fourth row shift 3-byte to left. as shown in Figure 3.

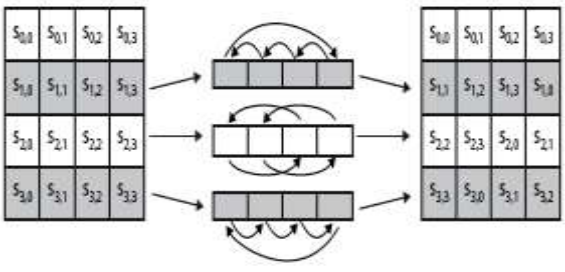

Figure 3: ShiftRow stage. [7]

IV. Mix Column Stage

In this stage, transfers map of each column of input state to a new column in output state. Every one input column considered as a polynomial above GF (256) and that multiplied with constant matrix the multiplied operator used polynomial mathematical, as shown in Figure 4.

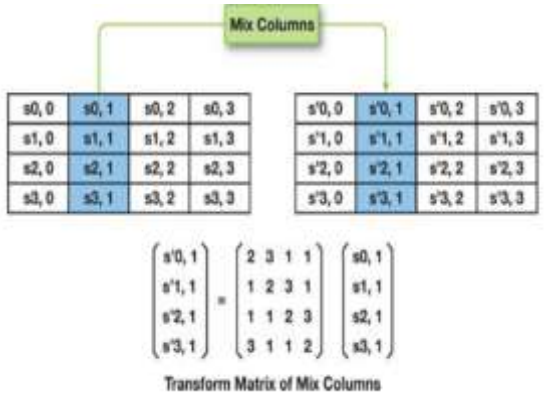

Figure 4: Mixcolumns stage.

V. Add Round Key Stage

In this stage, combined between data matrix 16 bytes and sub key matrix derived from original key matrix by key expansion. The combinatiom process by xoring each byte from data and sub key, as shown in Figure 5.

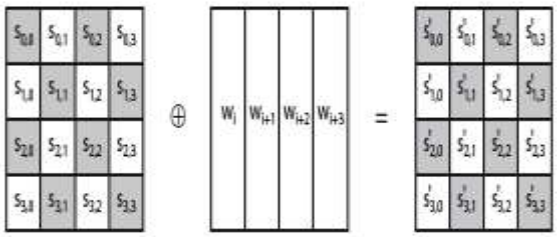

Figure 5: AddRoundKey stage. [7]

4. The Proposed Modification of AES Algorithm

The aim of the modification to increase the security of the encrypted documents by changing the size of the element in the data block and key size, thus the randomness of cipher text will increase.

The proposed system mix the polynomial concept and only use the size of one element inside one round and only one block and it was used GF(2^8) for the first level with high complexity, GF(2^4) used for the second level with medium complexity. It used GF(2^2) for the third level with less complexity. The order of GF(2,4 and 8) is represented by using key control which responsible of encryption/decryption process.

I. The Modified Algorithm Keys Provider

In this modification, the key provider generates (10) different keys randomly with order (2, 4, and 8) for each round of AES algorithm, that means, the size of each key matrix in the algorithm will be variable to increase the robustness and randomness of the AES.

For example, the randomly series of key are:

2 4 4 2 8 8 8 2 4 2

The following stages shows the changes that take place on four stages of AES algorithm as shown in Figure 6.

1. Add round key

At this stage, we changed the size of the element within the data block with order (2, 4, and 8) and also the key matrix is different in each round, while in the standard AES the size of element is fixed, as well as, the key matrix is constant in all (10) rounds.

2. Substitution

In the proposed algorithm, it built three s-boxes depending on the three cases GF(2,4,8), while in the standard AES there is only one s-box.

3. Shift row

At this stage, creating a master key used to choose the number of shifts to right for each row in the matrix depending on the three cases GF(2,4,8), while in the standard AES there is fixed shifts for each row.

4. Mix column

In the standard AES the key size is fixed (4*4), while in modified AES , the key is generated for each round randomly and the size of the key matrix is different according to the GF(2,4,8), as show in figure (6) below.

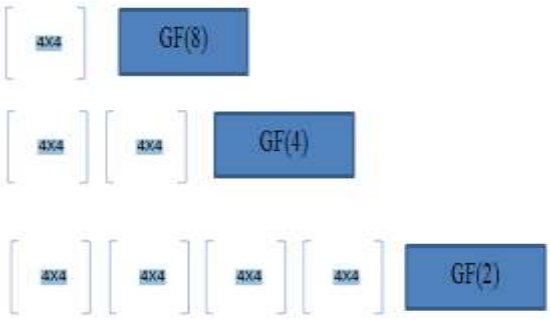

Figure 6: Size of key matrix

For illustrating the work of the proposed system with example showing the processes of the system for one block and one round, the plaintext (128-bits) size is:

E1

1. Write c++

It can be represented in c-sharp as a vector:

E	l	\r	\n	l	.	\t	W	r	i	t	e		c	+	+

The control key is 4822448824 and the keys are provided for one round. Since the first element in control key is 4 then the first round will be provided with keys of GF(4) for all stages (from Add Round key, Substitution, Shift Rows and Mix column). First, each letter in the plaintext is converted to ASCII code then it is converted to binary digit then it is split into two cells (each cell of 4-bits), at last the letter is converted to decimal. For example, the first letter in the above plaintext is (E) and in ASCII code it is (69) then it is converted to binary (01000101) then it is split into two cells with 4-bits (0100 0101) and this is represented in decimal by (4 and 5) and so on for the rest of letters of plaintext as shown in Figure 7.

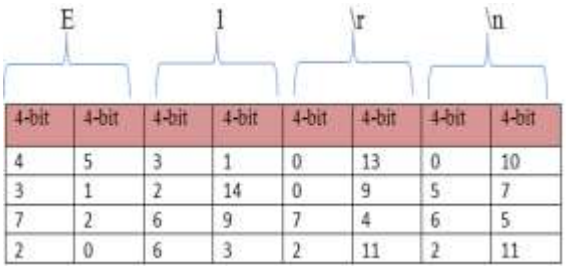

Figure 7: The presentation process of plaintext in decimal in GF(2^4)

Then the above block is added with the key matrix of GF(2^4) that is shown in table (1)

Table 1: The key matrix in GF(2^4)

6	8	13	9	3	3	2	8
6	9	6	14	13	15	14	4
1	14	5	15	15	11	14	13
11	6	3	15	3	10	15	1

Based on the addition in Table 1 in GF(4), the result is shown in the Table 2.

Table 2: The result of adding plaintext with key in GF(2^4)

2	13	14	8	3	14	2	2
5	8	4	0	13	6	11	3
6	12	3	6	8	15	8	8
9	6	11	12	1	1	13	10

Based on the S-box stage in GF(4) the result is shown in Table 3.

Table 3: The result of S-box in GF(2^4)

6	11	13	1	4	13	6	6
8	1	10	2	11	14	7	4
14	9	4	14	1	5	1	1
3	14	7	9	0	0	11	5

When the key vector is (0 1 3 0) the result of shift Rows stage of GF(4) will be as follows:

Table 4: The result of shiftRows in GF(2^4)

6	11	13	1	4	13	6	6
1	10	2	11	14	7	4	8
14	1	15	1	1	14	9	4
3	14	7	9	0	0	11	5

In mixcolumn stage with GF(4), any element is the total of products of items of one row in the key matrix with elements of one column in the block matrix as follows in Figure 8.

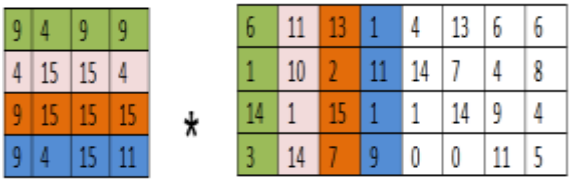

Figure 7: The multiplication of key matrix with block in GF(2^4)

Table 5 represent the ciphertext for one block and one round.

Table 5: The ciphertext of one block and one round in GF(2^4)

8	12	3	7	6	7	1	12
13	4	9	10	9	15	6	4
11	10	3	11	8	1	7	13
12	5	9	0	0	5	7	13

This steps continue for (9) rounds with different keys based on the degree of GF(8,4 and 2) based on control key.

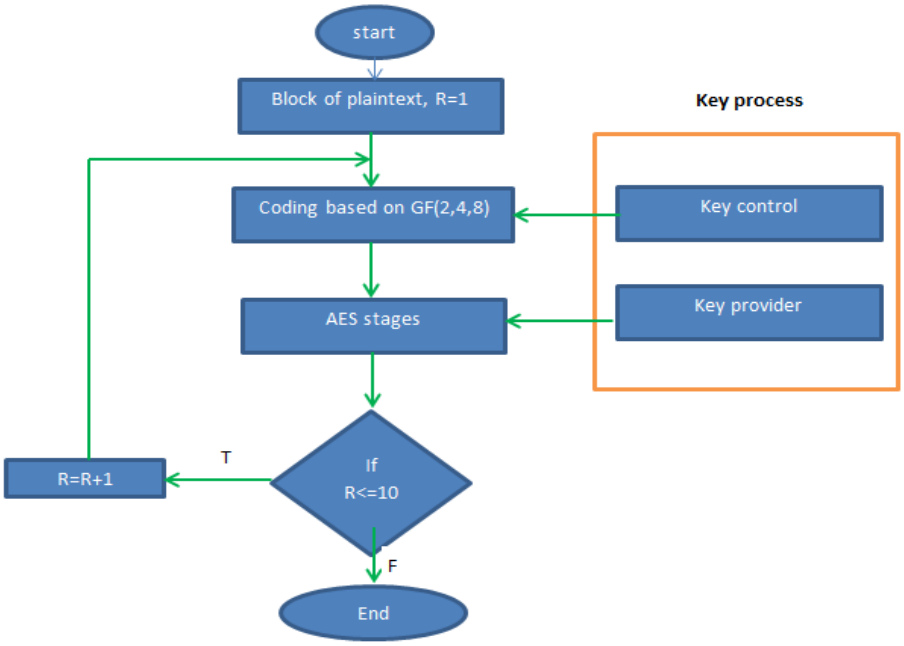

Figure 8: Illustrates modified AES flow chart

5. Experimental Results

To test the performance of modified AES algorithm, take three different size text file and used the usable tests that are (Frequency test, Serial test, Poker test, Runs test, Autocorrelation test) as test1, test2, test3, test4, and test5, respectively to measure the efficiency of the output for the modified method.

Table 6 shows the results of testing of modified AES, which pass the threshold of usable text criteria (standards). Table 7 shows the results of testing of standard AES.

Table 6: Testing of modified AES.

File size	Test 1	Test 2	Test 3	Test 4	Test 5
1k	0.258	10.535, 10.271	6.341	0.381	0.485,1.758 ,1.334 ,0.000 , 0.270,0.258 ,0.724 ,1.373 , 0.651,0.040
2k	0.009	8.162, 10.529	4.010	7.418	0.005,0.793 ,0.343 ,4.855 , 0.059,0.055 ,2.875 ,2.642 , 0.362,3.756
3k	0.001	20.234, 20.335	1.307	5.115	1.677,0.047 ,0.044 ,1.571 , 0.022,0.023 ,1.190 ,1.275 , 2.443,1.695

Table 7: Testing of standard AES.

File size	Test 1	Test 2	Test 3	Test 4	Test 5
1k	0.360	12.035, 12.001	6.756	1.377	1.477,2.558 ,2.774 ,0.338 , 1.270,1.778 ,1.720 ,2.373 , 1.677,0.648
2k	0.20	9.162, 11.349	6.011	8.418	2.005,1.279 ,1.355 ,4.997 , 1.088,2.011 ,3.343 ,3.232 , 1.772,4.785
3k	0.240	22.434, 22.215	3.307	6.335	2.547,2.097 ,1.114 ,2.881 , 0.889,0.979 ,2.160 ,2.445 , 3.773,2.775

Table 8: Measured time of modified AES

File size	Time (h,m,s)/high GF(8,4 and 2) Key:8842484428	Time (h,m,s)/medium GF(4 and 2) Key:4442422422	Time (h,m,s)/low GF(2) Key:2222222222
1 K	00.01.09	00.00.05	00.00.04
3 K	00.02.42	00.00.07	00.00.05
5 K	00.03.37	00.00.08	00.00.06
10 K	00.05.60	00.00.10	00.00.08

Table 9: Measured time of original AES

File size	Time (h,m,s) GF(8) Key:8888888888
1 K	00.02.31
3 K	00.03.60
5 K	00.04.56
10 K	00.06.30

In the above tables, notice that the randomness results of modified AES less than standard AES, which mean the randomness of modified AES better than the standard AES and the time factor has been counted for three levels of complexity (high, medium and low) and provided results are faster than the standard AES Algorithm.

7. Conclusion

The proposed modification shows that this development by using multiple irreducible polynomials degrees with order 2,4 and 8 can increase the efficiency of randomness and it can provide a greater efficiency and speed.

References

[1] A. Rukhin, et al. "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications (revised)," Natl. Inst. Stand. Technol.(US) Spec. Publ, 2008.

[2] F.Y. Mohammad, A.E. Rohiem and A.D. Elbayoumy, "A Novel S-box of AES Algorithm Using Variable Mapping Technique," International Conference on Aerospace Sciences & Aviation Technology, ASAT- 13, May 26 – 28, 2009.

[3] H. Razi, and H.H. Seyyed. "Using cipher key to generate dynamic S-box in AES cipher system," International Journal of Computer Science and Security (IJCSS), 2012.

[4] L. Scripcariu, and M.D. Frunza. "Modified Advanced Encryption Standard," 11th International Conference on Development and Application Systems, Romania, 2012.

[5] N.H. Ali, S.R. Abdul Monem, and A. Jaber. "Encryption using Dual Key Transformation based on Creation of Multi S-Boxes in AES Algorithm," International Journal of Computer Applications, 2013.

[6] K. Pravin, et al. "Modified Advanced Encryption Standard," International Journal of Soft Computing and Engineering (IJSCE), 2014.

[7] W. Stallings, "'Cryptography and Network Security," 4th Edition, Prentice-Hall, 2005.