Modifying Advanced Encryption Standard (AES) Algorithm

Assist. Prof. Dr. Abeer T. Maolood
abeer282003@yahoo.com
University of Technology - Department of Computer Sciences
Assist. Lect. Yasser A. Yasser
yasserkabashi@gmail.com
University of Technology - Department of Computer Sciences

Abstract: *This paper presents modifications on AES algorithm to improve the security of Standard AES, the improving has been done by three modifications. The first modification use key-dependent dynamic S-box (10 S-box) instead of static S-box (1 S-box), that used by Standard AES in order to improve "confusion" properties represented by Byte Substitution layer. The second modification use key-dependent variable values for shifting "state-matrix" rows process instead of fixed values that used by Standard AES in order to improve "diffusion" properties represented by ShiftRows layer. The third modification is by using two keys instead of one key that used by Standard AES, both of them used for encryption and decryption process instead of one key that used by Standard AES in order to improve the general structure and key generation algorithm of AES. The Modified AES tested and evaluated by five scales (Basic Five Statistical Tests, NIST Tests Suite, Encryption*

Run Time, Brute-Force Attack and Cryptanalytic Attack) to prove the functionality of modifying.

Keywords: Cryptography, Symmetric cipher, Block cipher, Advanced Encryption Standard (AES), National Institute of Standards and Technology (NIST).

1. Introduction

Currently is the age of information, the flow of information becoming lifeline for humanity. So it becomes very important to provide security for this information transmission from tapping. One of the most important forms for information security technologies is cryptography [1].

Cryptology is the science that combines cryptography: coded plaintext to ciphertext is (encryption), restoring the plaintext from the ciphertext is (decryption), and cryptanalysis: breaking the code [2]. Symmetric cipher: One key use for encryption and decryption process. Asymmetric cipher: The key used for encryption process differ from the key that used for decryption process, (privet key and public key) [3].

Stream cipher: Plaintext digits are combined with a pseudorandom cipher digit stream (keystream), each plaintext digit is encrypted one at a time with the corresponding digit of the keystream. Block cipher: Fixed-sized blocks of plaintext and key, process by iterating function for some rounds to generate fixed-sized ciphertext [4].

2. Standard Advanced Encryption Standard

In January 1997 the NIST announced the development of an advanced encryption Standard (AES) from five candidate algorithms, the block cipher rijndael designed by cryptographers Joan Daemen and Vincent Rijmn was chosen as the Advanced Encryption Standard (AES). Finally, AES published as the *Federal Information Processing standard* FIPS in November 2001 [5, 6, 7].

The AES algorithm is iterated symmetric block cipher, each iteration represents a round, 128-bit length input treated as 4×4 bytes matrix called state matrix (plaintext) after passes all the rounds the output is 128 bits length (ciphertext) [2, 3].

The block size of the AES is 128 bits while the key length is variable of 128, 192, or 256 bits, the number of rounds depends on the key length (10, 12 or 14 rounds) as shown in Table (1), [8,9].

Table (1) Key lengths and number of rounds for AES [3].

Key lengths	No. of Rounds ($n_{r)}$
128 bit	10
192 bit	12
256 bit	14

The round functions are consisting of four layers [2, 3, 8]:

1- Byte Substitution Layer: the bytes of state matrix are substitute by another bytes form given substitution table (S-Box), this layer provide *confusion* to the data.

2- ShiftRows layer: the rows of state matrix are shift (byte oriented) to left, each of rows by fixed value.

3- MixColumn layer: the state matrix mix with constant matrix use GF (2^8) and modular reduction p(x)= $x^8+x^4+x^3+x+1$. Layer tow and layer three provide *diffusion* for the data.

4- Key Addition layer: the state matrix XORed with round key bit by bit.

The AES 128-bit ***encryption process*** is beginning with Initial Round (Round 0) that include one layer (Key Addition layer) followed by nine rounds each round include the four layers ends by the tenth round that include the four layers exclude the MixColumn layer, as shown in Figure (1), [2,3].

For The AES 128-bit ***decryption process*** the layers must be inverted and becomes Inv Byte Substitution layer, Inv ShiftRows layer, and Inv MixColumn layer. the Key Addition layer still the same as encryption process but subkeys order must be reversed, to get back the plaintext, the order of rounds must be reversed as shown in Figure (2), [2, 3].

Inv MixColumn layer: the constant matrix used in encryption must be replaced with its inverse. Inv ShiftRows layer: shifting in opposite direction to the direct use in encryption process. Inv Byte Substitution layer: The S-Box replaced with its inverse.

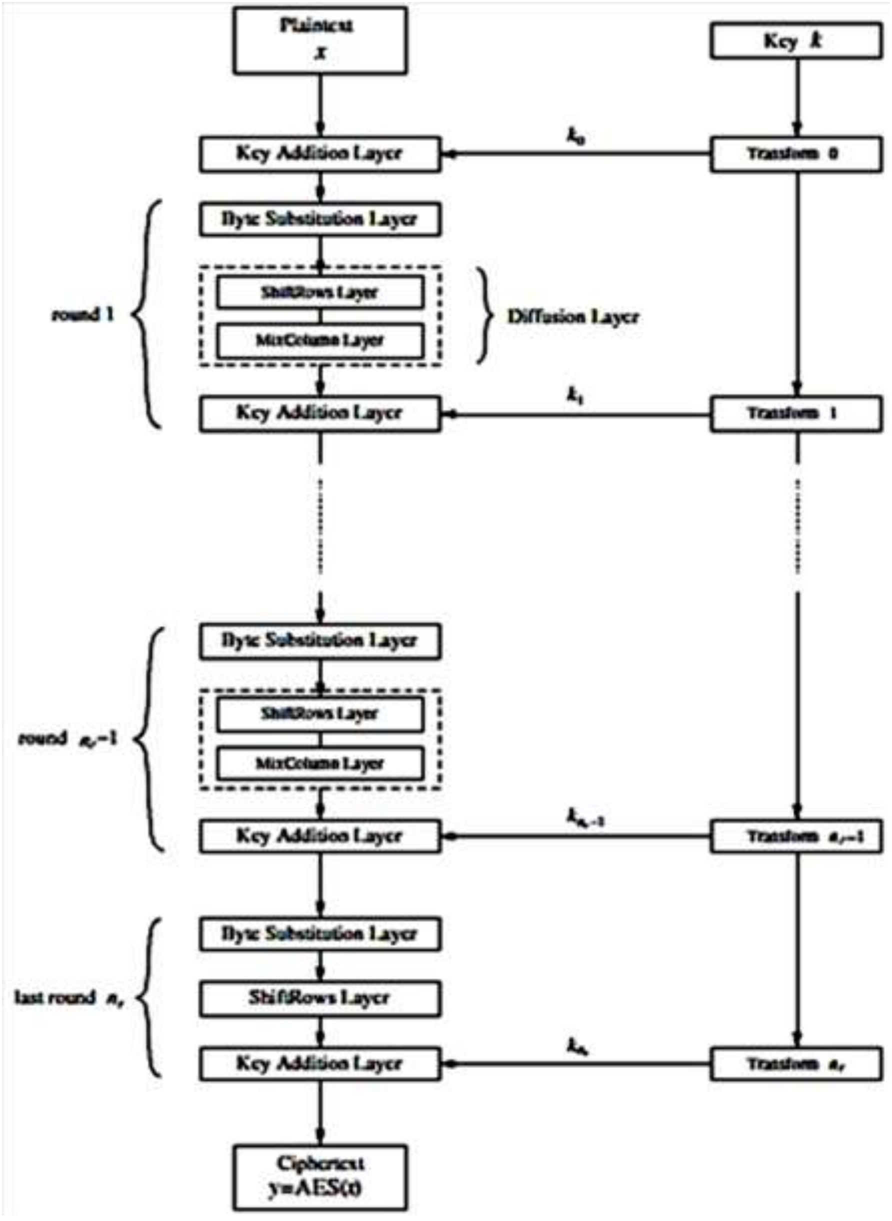


Figure (1): AES Encryption Block Diagram [3].

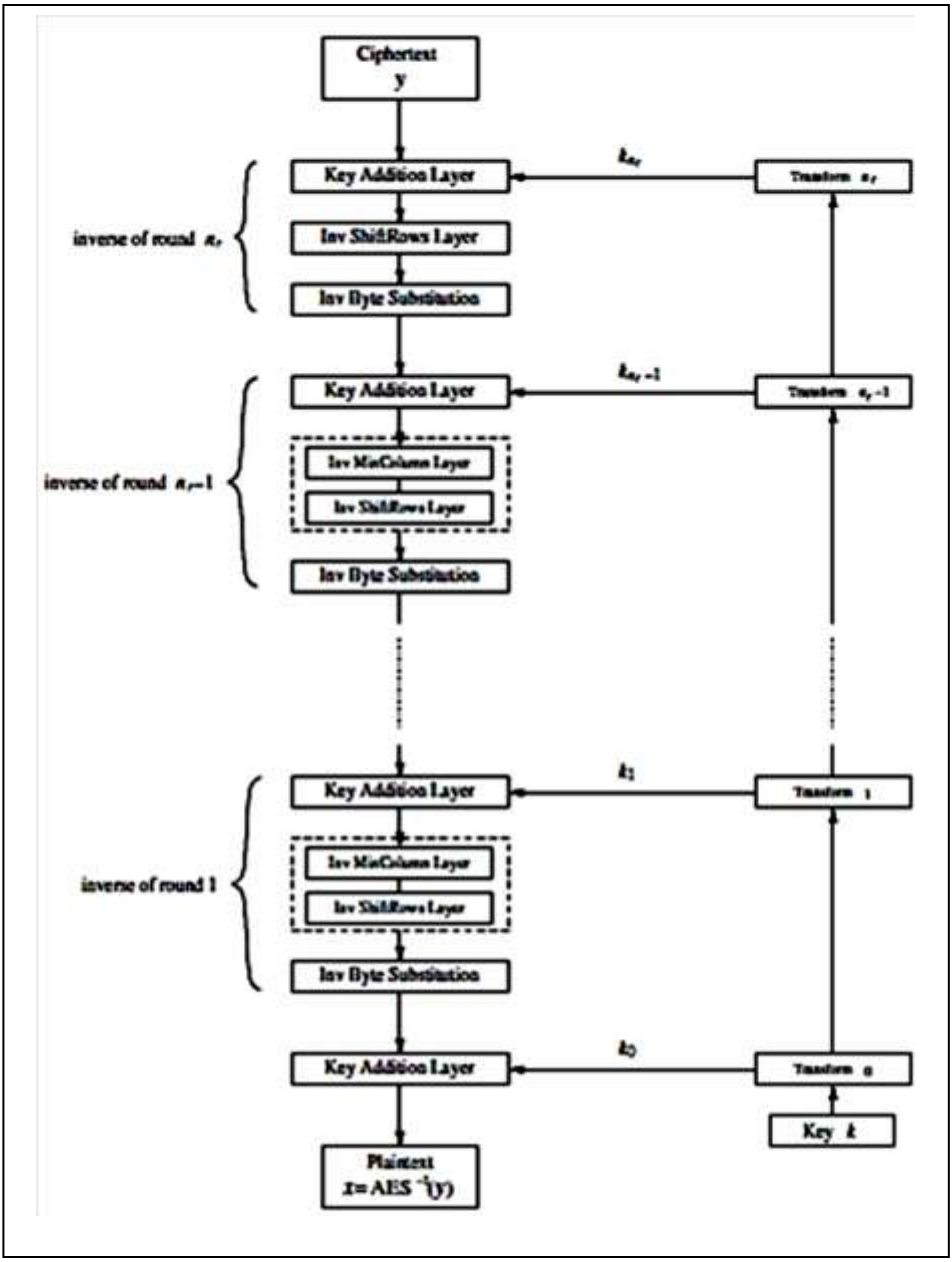


Figure (2): AES Decryption Block Diagram [3].

AES key expansion algorithm: It takes the original key of length (128, 192 or 256 bit) as input and derived the subkeys from it. The algorithm treat keys as words oriented each word consist of 4 bytes.

Every round need to a round key for the key addition layer that’s mean the number of subkeys equal to number of rounds plus one because of initial round. AES-128 bit has 11 subkeys with 44 words [2, 3].

3. Related work

In the last years there are many papers appeared try to modify the Standard AES to obtain more secured AES. In October, 2011, Pimpale P., Rayarikar R. and Upadhyay S. [10], proposed modifications on Standard AES algorithm try to enhance the complexity of the encryption process through modifications on the rounds of the algorithm in several layers Bytes Substitution layer, ShiftRows layer and MixColumns layer. These modifications provide stronger diffusion and confusion properties, they also increase the complexity of the algorithm multiple times.

In January, 2013, Sahmoud S., Elmasry W. and Adudalaf S. [11], proposed a new AES design to improve the security of Standard AES algorithm against modern attacks through modify the key generation algorithm, first modify is the use of AES with feedback pseudorandom key generator and the second modify is the use of AES with counters pseudorandom key generator. The proposed AES algorithm is more complex and secure against the modern attacks (such as impossible differential and met-in-the-middle) and because of use AES twice it is also secure against brute force attack, differential attack and linear attack, the proposed algorithm takes twice as much time compared to classical AES algorithm.

In July, 2013, Arrag S., Hamdoun A., Tragha A., and Khamlich S. [12], Modified the AES algorithm by modifying of the S-box depending on the key. Selecting one byte from the master key and following XORed with the original S-box, the result from XOR operation is a new S-box, it is used for encryption process, and the inverse of the new S-box is used in the decryption process. Even if the original AES algorithm is very secure, these proposed changes in the treatment of the algorithm will encrypt the information by performing high diffusion and confusion. It also increases the complexity of the AES algorithm several times.

4. Proposals to Modifying AES Algorithm

This section explains the design of the proposed encryption and decryption methods. The Modified AES contains three modifications on Standard AES as shown in the Figure (3):

1. Proposed Dynamic S-box Modification: Aims to add more complexity to "Byte Substitution layer ", targeting confusion properties.
2. ShiftRows Operation Modification: Aims to add more complexity to "ShiftRows layer" targeting diffusion properties.
3. Dual Key Modification: aims to add more complexity to "Key Expansion Algorithm" and "Key Addition layer".

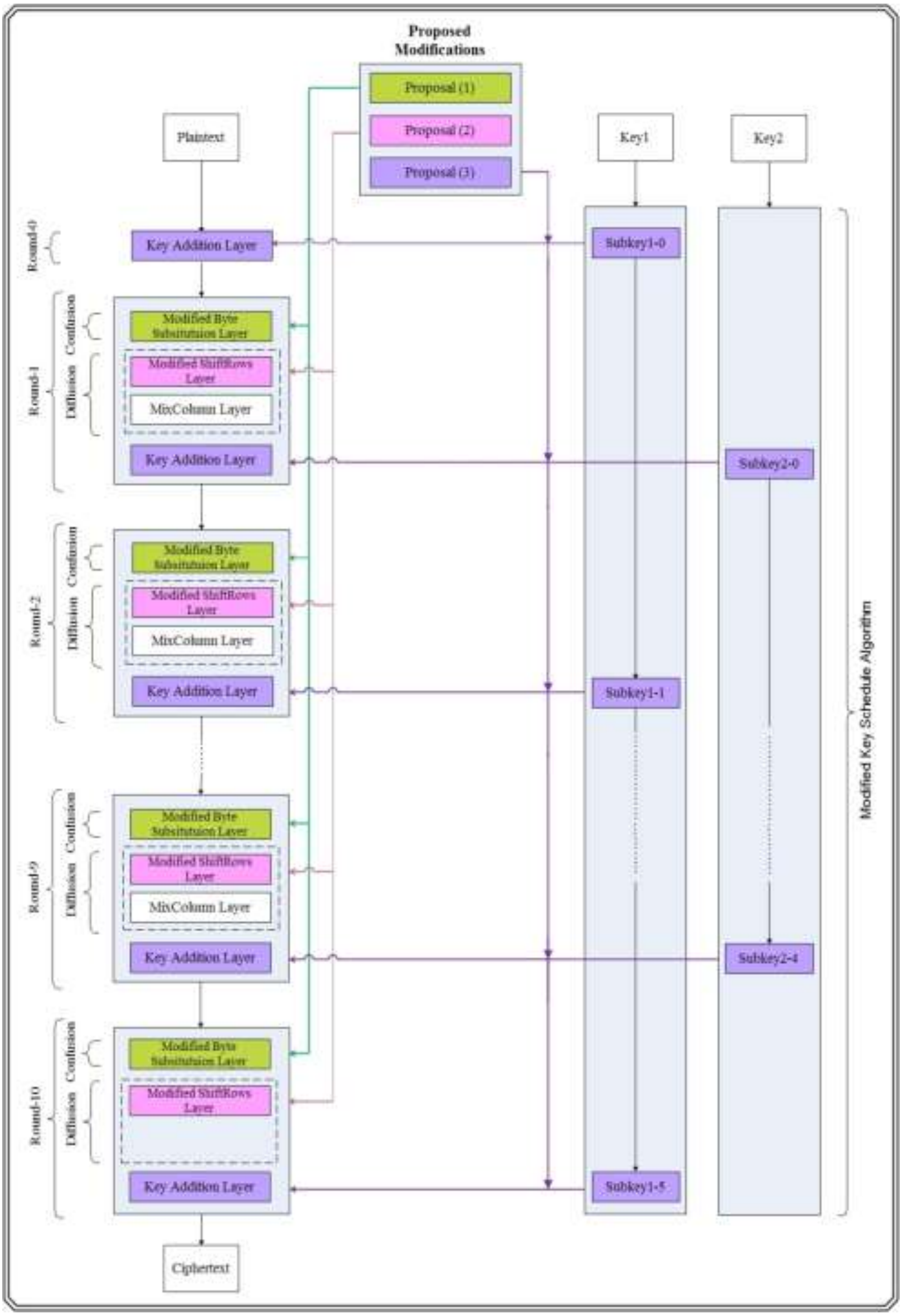
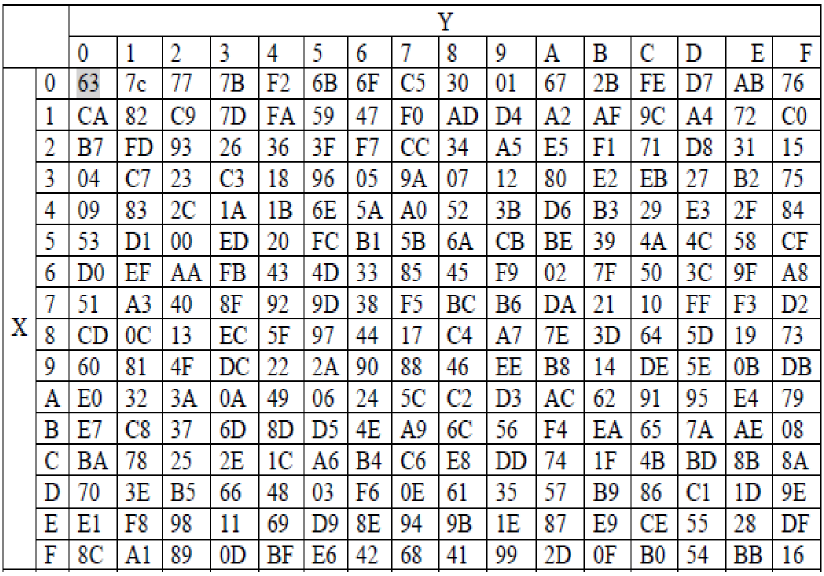


Figure (3): Modified AES Diagram.

First Modification: Proposed Dynamic S-box Modification

The Byte Substitutions layer is the major source of confusion properties, (Confusion: Obscured the relationship between key and ciphertext through substitution process). These properties are introduced by substituting state matrix bytes with other bytes provided by lookup table which has special mathematical properties called Substitution-Box [3]. The S-box of Standard AES shown in Table (2).

Table (2 S-box of Standard AES [3].



		Y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
X	0	63	7c	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Static or fixed S-box that is used by Standard AES uses the same S-box in each round (1 S-box for 10 rounds), while the proposed dynamic S-box that is used by Modified AES uses different S-box in each round, depending on the round key (10 new S-box for 10 rounds). The proposed byte substitution technique rotates or cycle shifts S-box bytes on each round by variable value, this variable value depends on the round key (subkey), this technique will improve the complexity of Byte Substitution operation with more randomness results as shown in tests and results later, the round key value will be used to find a value that is used to rotating S-box bytes, the proposed idea takes the value of the first and the last bytes of the round key and combines them by applying XOR operation, the resulted value will represents the rotating value that will be used for cycle shifting the S-box bytes to right, this value will differ from round to round depending on round key value and holds for all possible 256 shifting values (0 to 255). To illustrate the proposed idea of the first modification, follow Algorithm (1) and Example (1).

Algorithm (1): Proposed Dynamic S-Box Modification.

```
Input: S_box1 [256], Round_Key [4,4].
Output: S_box2 [256].
Process:
Shifting_Value = 0.
Step1:  Find shifting value for the bytes of s-box by taking the first and
the last bytes of the round key and combining them by XOR operation.
            (Shifting_Value= Round_Key [0,0] XOR Round_Key [3,3] ).
Step2:  Shift s-box bytes by the value found in Step1.
         (For i= 0 to 255 do
                  S_box2 [i]= S_box1 [(i+Shifting_value) mod 256] ).
End.
```

Example (1): The example supposes for round keys (round-key1 and round-key10), then shows only the proposed dynamic S-box of the round1 and round10 for shortcut:

Round-key1

0	A2	31	BC	6F
1	65	5D	64	D0
2	C3	23	F0	11
3	33	4D	A3	63

For *the round1*, the first and the last bytes of round-key1 are combined by XOR operation.

	$A2_{hexa}$	10100010_{binary}
XOR		
	63_{hexa}	01100011_{binary}
	$C1_{hexa}$	11000001_{binary}

The result is $C1_{hexa}$ which is equal to $193_{decimal}$ that means the S-box bytes will cycle shifting 193 byte positions to right (The process of rotation includes all elements of the matrix as if the matrix is a single row with 265 positions).

Round-key10

0	11	AC	2B	74
1	26	B9	A3	4E
2	59	6A	FF	4C
3	E1	5A	32	3C

For *the round10*, the first and the last bytes of round-key10 are combines by XOR operation.

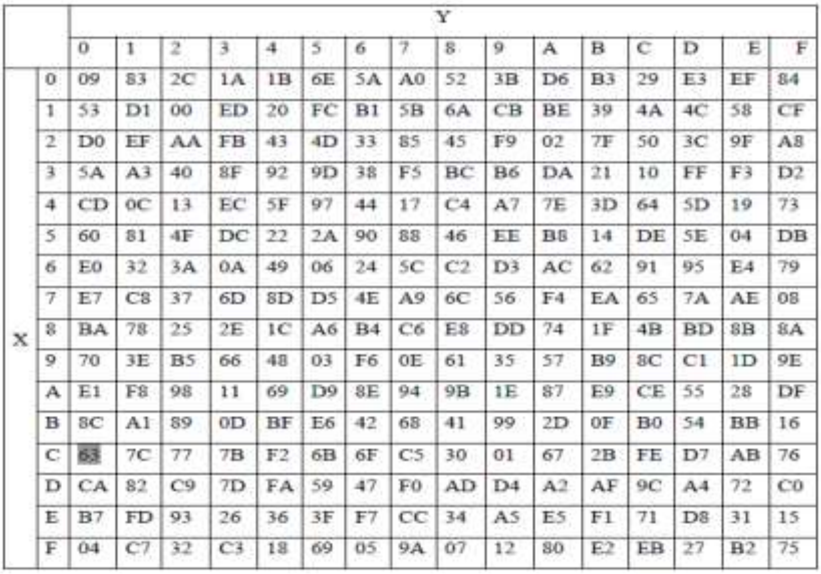
	11_{hexa}	00010001_{binary}
XOR		
	$3C_{hexa}$	00111100_{binary}
	$2D_{hexa}$	00101101_{binary}

The result is $2D_{hexa}$ which is equal to $45_{decimal}$ that means the S-box bytes will cycle shifting 45 byte positions to right (The process of rotation includes all elements of the matrix as if the matrix is a single row with 265 positions).

The proposed dynamic S-box for the Example (1) of round1 and round10 are shown consecutively on Table (3) and Table (4).

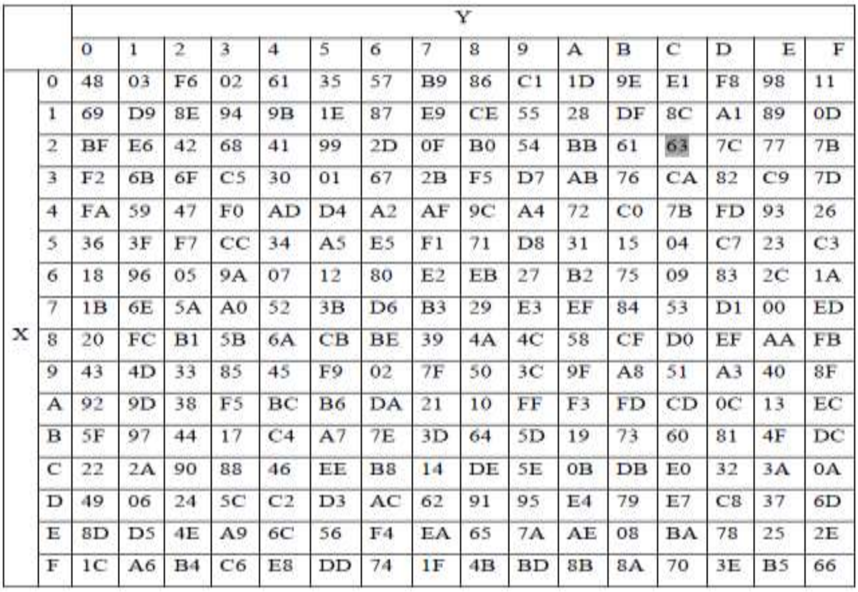
During the decryption process, the Inverse Bytes Substitution operation performs the proposed bytes substitution technique but with the Inverse S-box to get back to the plaintext.

Table (3) Proposed Dynamic S-box for Round1, Example (1).



		Y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
X	0	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	EF	84
	1	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	2	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	3	5A	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	4	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	5	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	04	DB
	6	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	7	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	8	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	9	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	8C	C1	1D	9E
	A	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	B	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16
	C	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	D	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	E	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	F	04	C7	32	C3	18	69	05	9A	07	12	80	E2	EB	27	B2	75

Table (4) Proposed Dynamic S-box for Round10, Example (1).



		Y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
X	0	48	03	F6	02	61	35	57	B9	86	C1	1D	9E	E1	F8	98	11
	1	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF	8C	A1	89	0D
	2	BF	E6	42	68	41	99	2D	0F	B0	54	BB	61	63	7C	77	7B
	3	F2	6B	6F	C5	30	01	67	2B	F5	D7	AB	76	CA	82	C9	7D
	4	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0	7B	FD	93	26
	5	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15	04	C7	23	C3
	6	18	96	05	9A	07	12	80	E2	EB	27	B2	75	09	83	2C	1A
	7	1B	6E	5A	A0	52	3B	D6	B3	29	E3	EF	84	53	D1	00	ED
	8	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF	D0	EF	AA	FB
	9	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8	51	A3	40	8F
	A	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	FD	CD	0C	13	EC
	B	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73	60	81	4F	DC
	C	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB	E0	32	3A	0A
	D	49	06	24	5C	C2	D3	AC	62	91	95	E4	79	E7	C8	37	6D
	E	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08	BA	78	25	2E
	F	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A	70	3E	B5	66

Second Modification: ShiftRows Operation Modification

The ShiftRows operation is a source of diffusion properties along as with the MixColumn operation, (Diffusion: Hiding statistical properties of the plaintext through permutation process). The Standard AES ShiftRows transformations cyclic shifts the bytes in each row of the state matrix to the left by fixed values, these fixed values represent a motivation for modification to get more complex AES algorithm [3]. The Modified AES presents a proposed ShiftRows transformation technique that uses variable key-dependent shifting values instead of static values that are used by Standard AES.

The proposed ShiftRows technique cyclically shifts the bytes in each row by variable values depend on round key (subkey). This proposed ShiftRows technique will improve the complexity of ShiftRows operation with more randomness results as shown in tests and results later, the round key value will be used to find the values that is used to shift the bytes in each row of the state matrix. The proposed idea takes the value for each diagonal byte of round key and mod by 4, the resulted value will present the shifting value that will be used for cycle shifting the bytes of the equivalent row in state matrix to left, these values will differ from round to round depending on round key value and holds for all possible 4 shifting values (0 to 3). To illustrate the proposed idea, follow Algorithm (2) and Example (2).

Algorithm (2): ShiftRows Operation Modification Algorithm.

```
Input: State1 [4,4], Round_Key [4,4].
Output: State2 [4,4].
          Process:
Shifting_Value = 0
Step1:  Find shifting values for the rows of state matrix by taking the
diagonal values of the rows of key, then modulate these values by four
        (For i= 0 to 3 do
                Shifting_Value [i]= Round_Key [i,i] mod 4 ).
Step2:  Shift state matrix rows by the values found in Step1.
(For i= 0 to 3 do
      For j=0 to 3 do
                State2 [i,j]= State1 [i, ((j+Shifting_value[i]) mod 4)] ).
End.
```

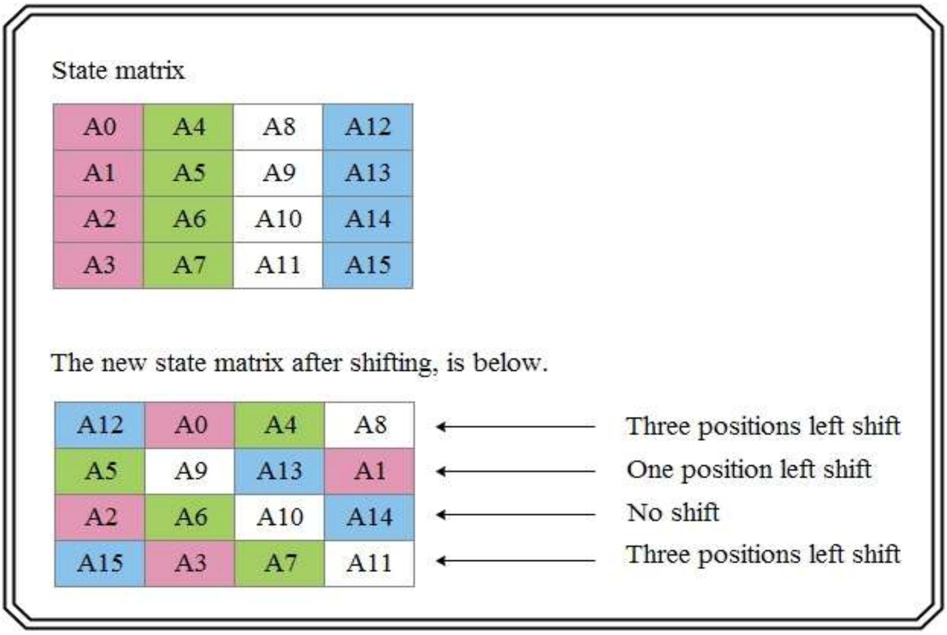
Example (2): Suppose for a particular round n, the round key is the key below**:**

Round key

0	1B	31	BC	6F
1	65	5D	64	D0
2	C3	23	F0	11
3	33	4D	A3	AB

Shifting for the bytes in (row-0) of the State matrix is computed as follow: The value of the diagonal byte in row-0 of the round key is $1B_{hexa}$ which is in decimal equal to ($27_{decimal}$ mod 4), the shifting of bytes in row-0 is 3 positions cyclically to the left.

Shifting for the bytes in (row-1) of the State matrix is computed as follow: The value of the diagonal byte in row-1 of the round key is $5D_{hexa}$ which is in decimal equal to ($93_{decimal}$ mod 4), the shifting of bytes in row-1 is 1 position cyclically to the left. And so on for row-2 and row-3.



State matrix

A0	A4	A8	A12
A1	A5	A9	A13
A2	A6	A10	A14
A3	A7	A11	A15

The new state matrix after shifting, is below.

A12	A0	A4	A8	← Three positions left shift
A5	A9	A13	A1	← One position left shift
A2	A6	A10	A14	← No shift
A15	A3	A7	A11	← Three positions left shift

Figure (4) ShiftRows Transformation of Modified AES, Example(2).

For a particular round key that is supposed previously, the state matrix will shift as shown in Figure (4).

Note: The shifting values by Example (2) are dedicated for the particular round key that was previously supposed, and these values will change from round to round and by round key changes.

Third Modification: Dual Key Modification

The Modified AES presents a modified AES design which targets the general structure and Key Addition layer, by presenting a design use dual key instead of single key that is used by Standard AES.

The Modified AES adds more complexity and randomness results for: (1) the general structure, (2) the key expansion algorithm, and (3) the Key Addition layer, as shown in tests and results later. This implementation is made by using "two keys" instead of "one key" and non-sequential allocation of the subkeys to the AES round.

The (key1) will generate subkeys that are allocated to (even rounds) and the (key2) will generate subkeys that are allocated to (odd rounds) as shown in Figure (5) and Figure (6).

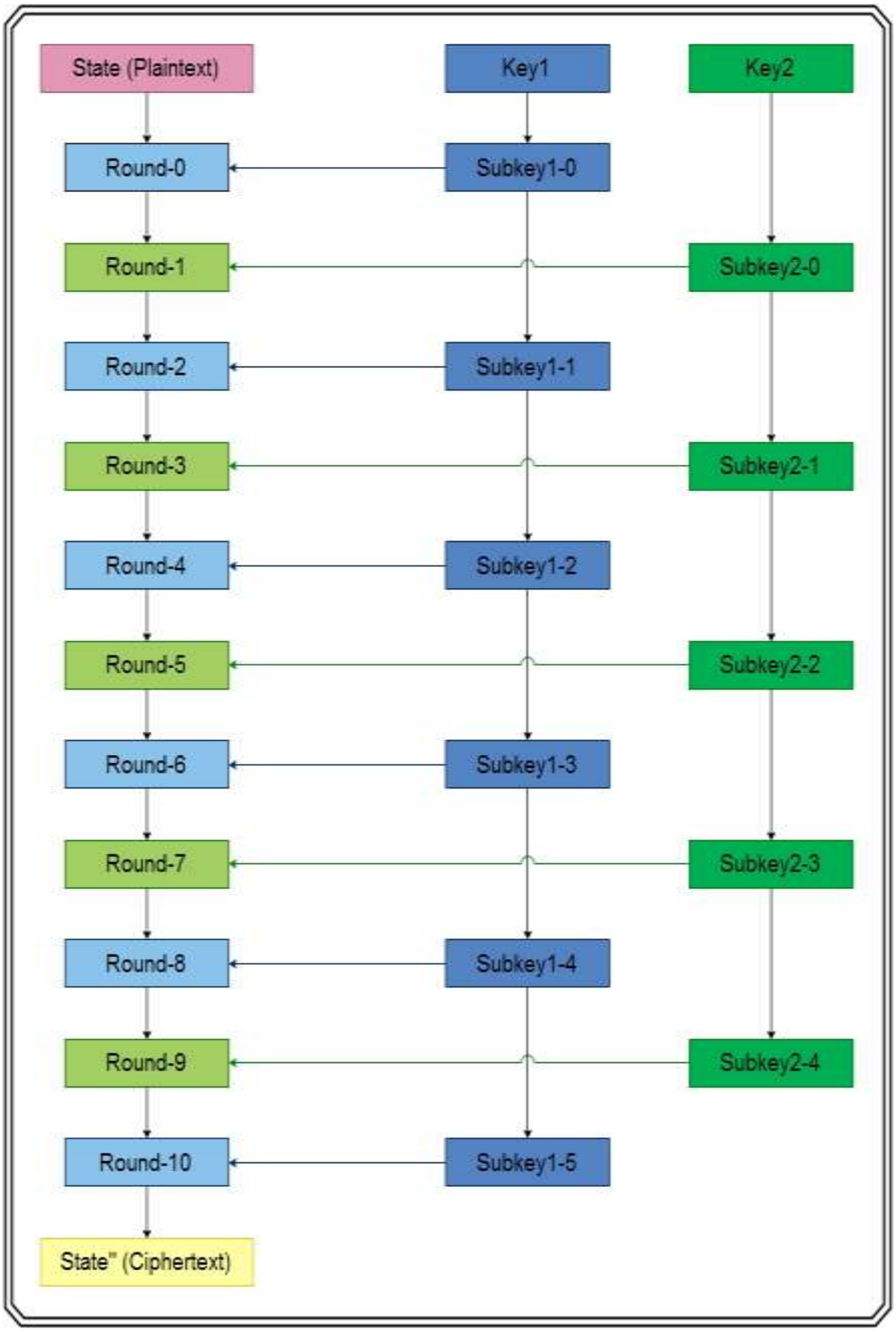


Figure (5): Applying The Subkeys in Each Round (encryption process).

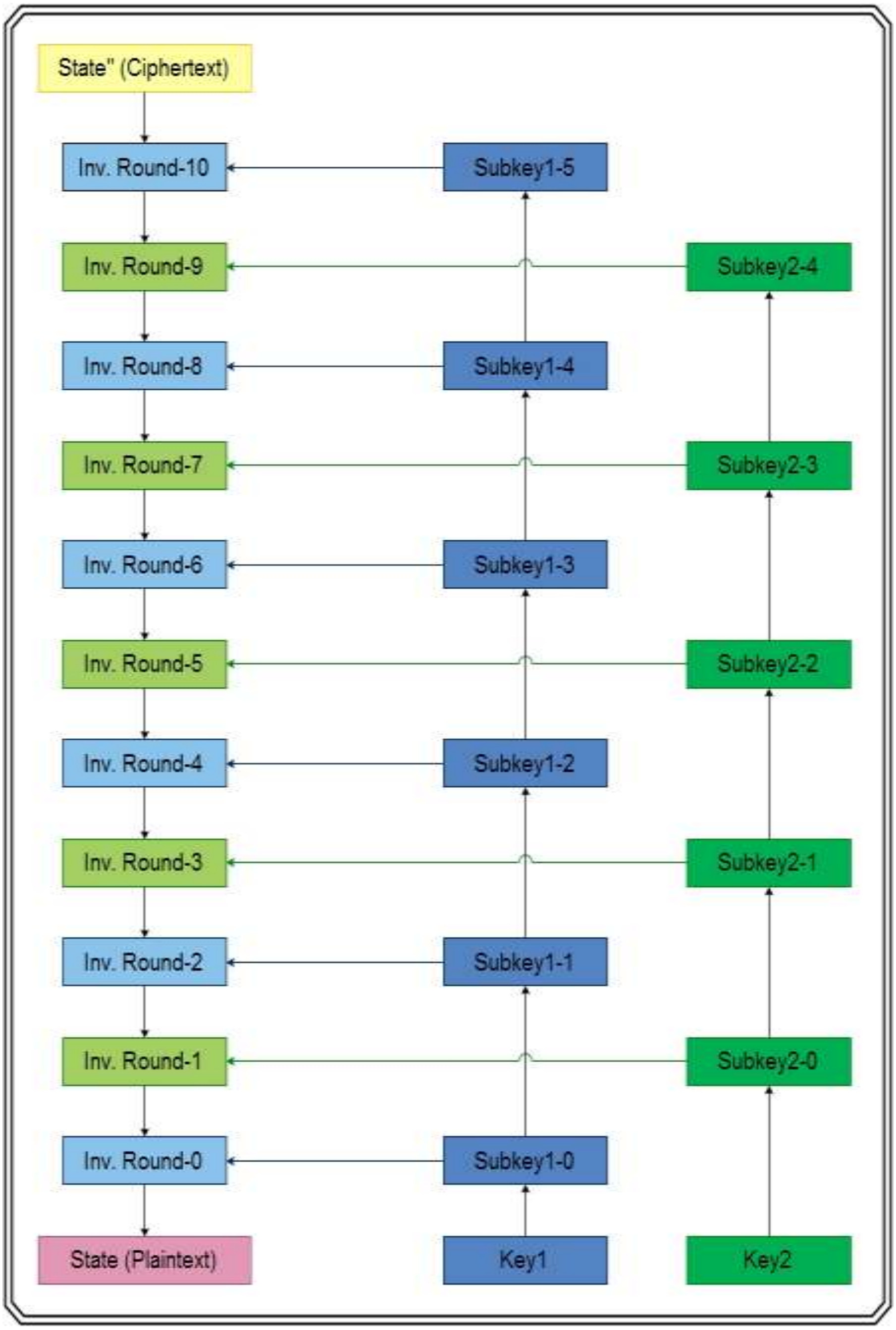


Figure (6): Applying The Subkeys in Each Round (decryption process).

The modified AES uses the same technique that used by Standard AES for the subkeys generation.

Algorithm (3): Dual key Modification.

```
Input: Key1 [6], Key2 [5].
Output: Key [11].
Process:
K = 0
Step1: Initiate the key that is used by the algorithm for the key addition operation from the Key1 and Key2, subkeys of Key1 will be used with even rounds and subkeys of Key2 with odd rounds.
    (For i= 0 to 6 do
        Key [k] = Key1 [i]
        Key [k+1] = Key2 [i]
            K = K+2).
End.
```

5. Tests and Results

As evaluation of the Modified AES algorithm there are five tests (Basic Five Statistical Tests, NIST Tests Suite, Encryption Run Time, Brute-Force Attack and Cryptanalytic Attack), selected to examine the output ciphertext of (Standard AES algorithm and Modified AES algorithm) and comparison of the results, to evaluate performance of the modified algorithm and prove the effectiveness of modifications on increasing complexity properties.

This paper will use the same inputs for Standard AES and Modified AES algorithm, (same 128-bit input block size (plaintext) and same 128-bit key length (key)), then test the 128-bit output block size (ciphertext) by the five selected tests. Example (3) will shows the progression of State matrix through the modified AES encryption process.

Example (3): An example of the modified AES, used input plaintext and keys are:

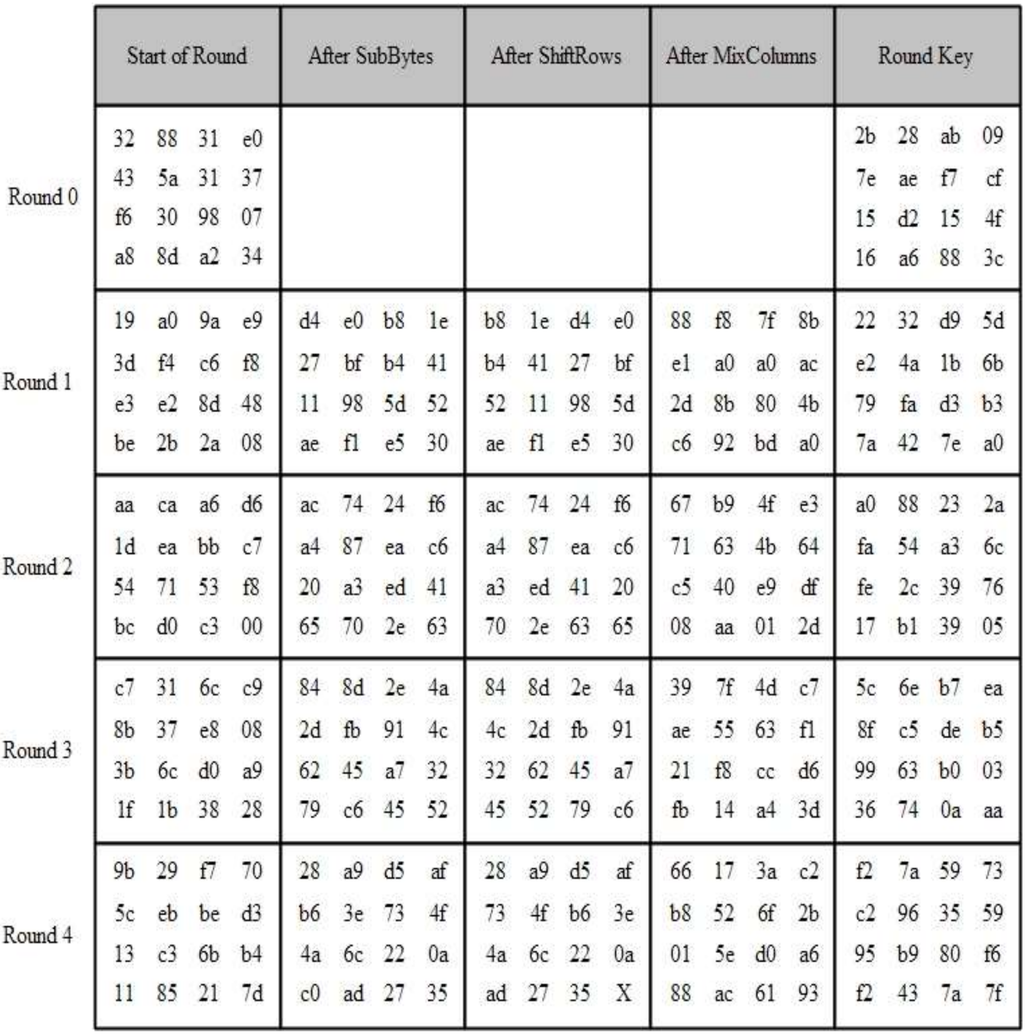
Plaintext:	32881e0435a3137f6309807a88da234
Key1:	2b28ab097eaef7cf15d2154f16a6883c
Key2:	2232d95de24a1b6b79fad3b37a427ea0

The example resulting ciphertext is:

Ciphertext:	8040fa18f1908598656982223fa2dd8d

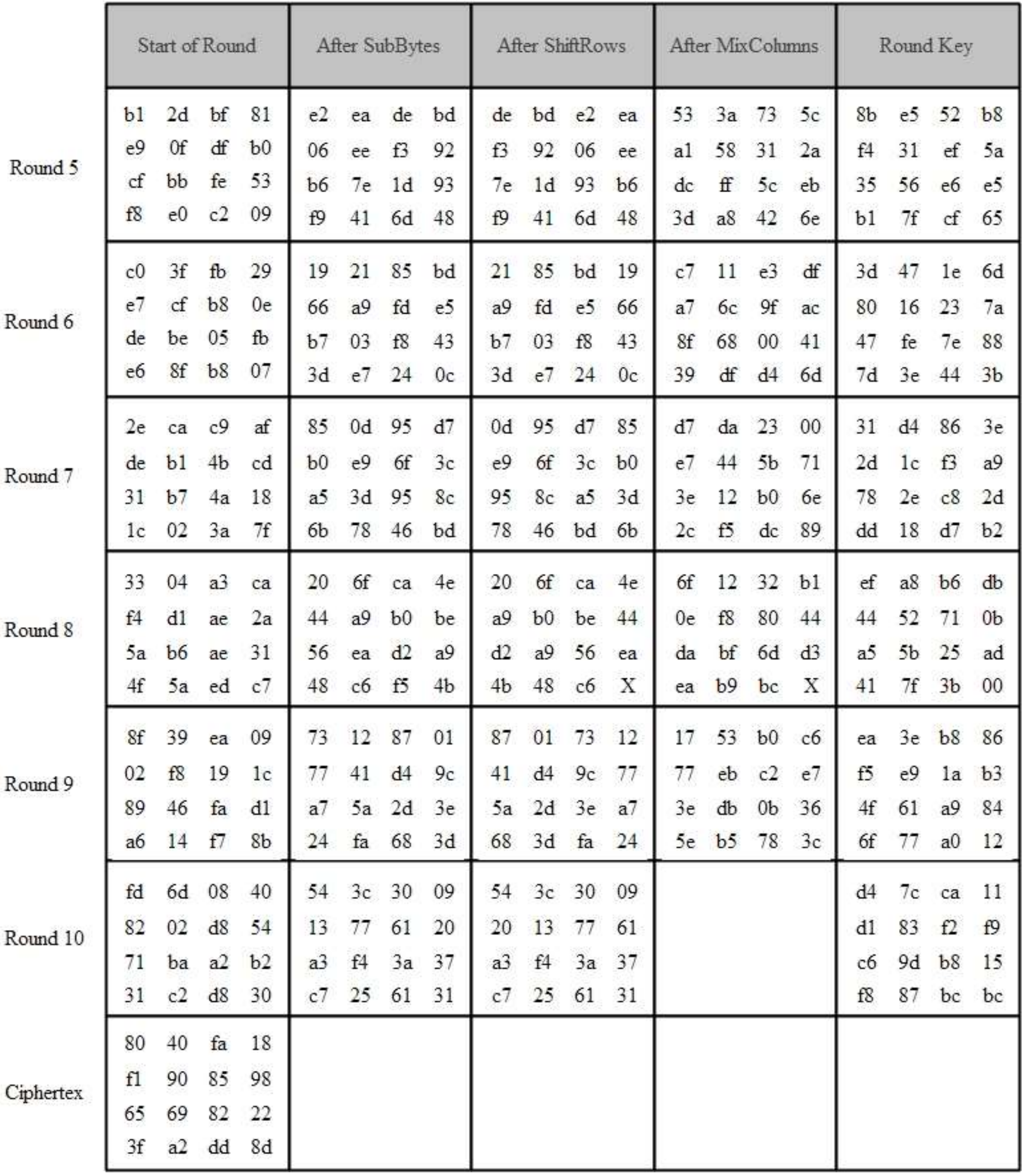
The proceed of the state matrix through the modified AES encryption process is shown in Table (5).

Table (5): Modified AES State Matrix Progression Example (3).



	Start of Round	After SubBytes	After ShiftRows	After MixColumns	Round Key
Round 0	32 88 31 e0 43 5a 31 37 f6 30 98 07 a8 8d a2 34				2b 28 ab 09 7e ae f7 cf 15 d2 15 4f 16 a6 88 3c
Round 1	19 a0 9a e9 3d f4 c6 f8 e3 e2 8d 48 be 2b 2a 08	d4 e0 b8 1e 27 bf b4 41 11 98 5d 52 ae f1 e5 30	b8 1e d4 e0 b4 41 27 bf 52 11 98 5d ae f1 e5 30	88 f8 7f 8b e1 a0 a0 ac 2d 8b 80 4b c6 92 bd a0	22 32 d9 5d e2 4a 1b 6b 79 fa d3 b3 7a 42 7e a0
Round 2	aa ca a6 d6 1d ea bb c7 54 71 53 f8 bc d0 c3 00	ac 74 24 f6 a4 87 ea c6 20 a3 ed 41 65 70 2e 63	ac 74 24 f6 a4 87 ea c6 a3 ed 41 20 70 2e 63 65	67 b9 4f e3 71 63 4b 64 c5 40 e9 df 08 aa 01 2d	a0 88 23 2a fa 54 a3 6c fe 2c 39 76 17 b1 39 05
Round 3	c7 31 6c c9 8b 37 e8 08 3b 6c d0 a9 1f 1b 38 28	84 8d 2e 4a 2d fb 91 4c 62 45 a7 32 79 c6 45 52	84 8d 2e 4a 4c 2d fb 91 32 62 45 a7 45 52 79 c6	39 7f 4d c7 ae 55 63 f1 21 f8 cc d6 fb 14 a4 3d	5c 6e b7 ea 8f c5 de b5 99 63 b0 03 36 74 0a aa
Round 4	9b 29 f7 70 5c eb be d3 13 c3 6b b4 11 85 21 7d	28 a9 d5 af b6 3e 73 4f 4a 6c 22 0a c0 ad 27 35	28 a9 d5 af 73 4f b6 3e 4a 6c 22 0a ad 27 35 X	66 17 3a c2 b8 52 6f 2b 01 5e d0 a6 88 ac 61 93	f2 7a 59 73 c2 96 35 59 95 b9 80 f6 f2 43 7a 7f

Table (5): Continued.



	Start of Round	After SubBytes	After ShiftRows	After MixColumns	Round Key
Round 5	b1 2d bf 81 e9 0f df b0 cf bb fe 53 f8 e0 c2 09	e2 ea de bd 06 ee f3 92 b6 7e 1d 93 f9 41 6d 48	de bd e2 ea f3 92 06 ee 7e 1d 93 b6 f9 41 6d 48	53 3a 73 5c a1 58 31 2a dc ff 5c eb 3d a8 42 6e	8b e5 52 b8 f4 31 ef 5a 35 56 e6 e5 b1 7f cf 65
Round 6	c0 3f fb 29 e7 cf b8 0e de be 05 fb e6 8f b8 07	19 21 85 bd 66 a9 fd e5 b7 03 f8 43 3d e7 24 0c	21 85 bd 19 a9 fd e5 66 b7 03 f8 43 3d e7 24 0c	c7 11 e3 df a7 6c 9f ac 8f 68 00 41 39 df d4 6d	3d 47 1e 6d 80 16 23 7a 47 fe 7e 88 7d 3e 44 3b
Round 7	2e ca c9 af de b1 4b cd 31 b7 4a 18 1c 02 3a 7f	85 0d 95 d7 b0 e9 6f 3c a5 3d 95 8c 6b 78 46 bd	0d 95 d7 85 e9 6f 3c b0 95 8c a5 3d 78 46 bd 6b	d7 da 23 00 e7 44 5b 71 3e 12 b0 6e 2c f5 dc 89	31 d4 86 3e 2d 1c f3 a9 78 2e c8 2d dd 18 d7 b2
Round 8	33 04 a3 ca f4 d1 ae 2a 5a b6 ae 31 4f 5a ed c7	20 6f ca 4e 44 a9 b0 be 56 ea d2 a9 48 c6 f5 4b	20 6f ca 4e a9 b0 be 44 d2 a9 56 ea 4b 48 c6 X	6f 12 32 b1 0e f8 80 44 da bf 6d d3 ea b9 bc X	ef a8 b6 db 44 52 71 0b a5 5b 25 ad 41 7f 3b 00
Round 9	8f 39 ea 09 02 f8 19 1c 89 46 fa d1 a6 14 f7 8b	73 12 87 01 77 41 d4 9c a7 5a 2d 3e 24 fa 68 3d	87 01 73 12 41 d4 9c 77 5a 2d 3e a7 68 3d fa 24	17 53 b0 c6 77 eb c2 e7 3e db 0b 36 5e b5 78 3c	ea 3e b8 86 f5 e9 1a b3 4f 61 a9 84 6f 77 a0 12
Round 10	fd 6d 08 40 82 02 d8 54 71 ba a2 b2 31 c2 d8 30	54 3c 30 09 13 77 61 20 a3 f4 3a 37 c7 25 61 31	54 3c 30 09 20 13 77 61 a3 f4 3a 37 c7 25 61 31		d4 7c ca 11 d1 83 f2 f9 c6 9d b8 15 f8 87 bc bc
Ciphertex	80 40 fa 18 f1 90 85 98 65 69 82 22 3f a2 dd 8d				

5.1 Basic Five Statistical Tests

The basic five statistical tests (frequency, run, poker, serial, and correlation), use to measure the randomness of ciphertext, the test results are evaluated by reference to the " Chi-squared distribution" with *k* degrees of freedom of that statistic [13], Results show in Table (6) and Figure (7). *K* degrees in used tests are: Frequency=1, Serial=2, Poker=5, Run=7 and Correlation=1. Significance level (α) for the results of the test is 0.050.

Table (6): Results of the Five Tests Applied to Standard and Modified AES Algorithms.

N O.	Tested AES	Frequency Test <= 3.84	Serial Test <= 7.81	Poker Test <= 11.1	Run Test <= 13.784	Correlation Test <= 3.84
1	Standard AES	pass=2.000	Pass=4.633	Pass=1.845	Pass=7.962	Pass= 0.871
2	Modified AES	pass=0.847	Pass=1.000	Pass=7.431	Pass=5.235	Pass= 0.009

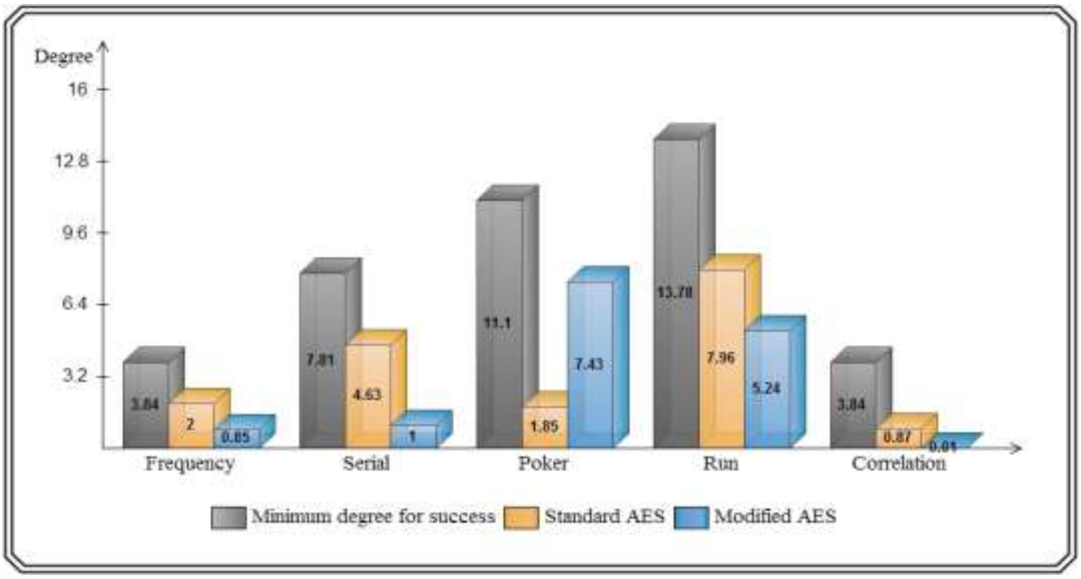


Figure (7): Results of the Five Tests Applied to Standard and Modified AES Algorithms.

According to results of the basic five statistical tests, the Modified algorithm shows better results against Standard AES. The results show more randomness degree on the output (ciphertext) of the Modified AES algorithm. That proves that the proposed modifications add more randomness to the Standard AES (ciphertext), and effectiveness to complexity properties.

5.2 National Institute of Standards and Technology (NIST) Test Suite

The NIST Test Suite is a statistical package consisting of 16 tests, developed to test the randomness of binary sequences, the output (ciphertext) of cryptography algorithms can be tested by using the “National Institute of Standards and Technology (NIST)” test suite.

Table (7): Results of the NIST16 Tests Applied to Standard and Modified AES Algorithms.

NO.	Test	Standard AES	Modified AES
1	Frequency	True	True
2	Block Frequency	True	True
3	Cumulative Sums	True	True
4	Runs	True	True
5	Longest Run	True	True
6	Rank	True	True
7	Discrete Fourier Transform	True	True
8	Non-periodic Templates	True	True
9	Overlapping	True	True
10	Universal	True	True
11	Approximate Entropy	True	True
12	Random Excursions	True	True
13	Random Excursions Variant	True	True
14	Serial	True	True
15	Lempel-Ziv Compression	True	True
16	Linear Complexity	True	True

These tests focus on a variety of different types of non-randomness that could exist in a sequence such as (Linear

Complexity, Overlapping, and Lempel - Ziv Compression…etc.) [14]. Results show in Table (7). According to results of the NIST 16 tests, the modified algorithm succeeded in all randomness and non-randomness NIST 16 tests.

5.3 Encryption Run Time

One another evaluation scale is the encryption run time, this paper measures the encryption run time for the Modified AES algorithm and Standard AES, of encrypt the same 128-bit data block, 0.5MB file, 1MB file, 1.5MB file and 2MB file, then comparison of the results. The results show a slight increase in encryption run time of the Modified AES algorithm. Results shown in table (8).

Table (8): Results of the Encryption Run Times to *Standard and Modified AES Algorithms.*

Algorithm	(16byte) \ Second	(0.5MB) \ Second	(1MB) \ Second	(1.5MB) \ Second	(2MB) \ Second
Standard AES	00.0017	01.697	03.236	4.714	06.362
Modified AES	00.0018	01.699	03.239	4.718	06.367

The results show a slight increase in encryption run time of Modified AES algorithm compared with Standard AES.

<u>**NOTE**</u>: The encryption run time for the tested algorithms measured by personal computer with hardware specifications: (Processor: Intel(R) Core(TM) i7 CPU @ 2.20GHz & Installed Memory (RAM): 4.00 GB & Hard Disk: 500 GB).

5.4 Brute-Force Attack

This attack tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained [2].

The standard AES 128-bit used 128-bit key size, that means the brute force attack required (2^{128}) possible keys, and number of possible to decrypt the cipher text with key size 128-bit is $(2^{128})^{11}$ possible where the number 11 is the number of used “Key Addition” stage, the number $(2^{128})^{11}$ will considered as the complexity for brute force attack of algorithm because it is represent the effort required to cryptanalysis ciphertext of algorithm [15].

The Modified AES will have more complexity for brute force attack than standard AES because of used for dual-key (two 128-bit key), the complexity degree will be [$2*(2^{128})^{11}$].

5.5 Cryptanalytic Attack

These attacks relay on nature and behavior of algorithm, trying exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used [2].

The standard AES have complex nature because of its complex substitution and permutation process which is effect on confusion and diffusion properties, AES have complex key expansion algorithm also. That gives AES algorithm high complexity for cryptanalytic attacks because of high effort required to cryptanalysis ciphertext of algorithm [15].

The Modified AES will have more complexity for cryptanalytic attacks because of more complex nature and behavior than standard AES through the modifications which will use for, key-dependent dynamic S-box (10 S-box) in Byte Substitution layer instead of static S-box (1 S-box), use variable key-dependent shifting values in ShiftRows layer instead of static shifting values and use for dual key (two keys) instead of one key that used in standard AES.

6. Conclusions

This paper introduces a view on cryptology science and the importance of information security. A brief overview for Standard AES algorithm followed by explain the Modified AES algorithm which is improve the security through three changes, first by use for key-dependent dynamic S-box (10 S-box) instead of static S-box (1 S-box) in Byte Substitution layer, the second by use key-dependent variable shifting values in ShiftRows layer instead of fixed values and the third by use for dual key (two keys) instead of one key that used in standard AES. Next, this paper presents many related work modifying the Standard AES. Then the Modified AES evaluate and testing by five scales (Basic Five Statistical Tests, NIST Tests Suite, Encryption Run Time, Brute-Force Attack and Cryptanalytic Attack).

References

[1] Loepp S. and Wootters W. K., "Protecting Information - From Standard Error Correction to Quantum Cryptography", ©Susan Loepp and William K.Wootters, Cambridge University Press, New York, 2006.

[2] Stalling W., "Cryptography and Network Security Principles and Practice – Fifth Edition", © Pearson Education, Inc., Prentice Hall, USA, 2011.

[3] Paar C. and Pelzl J., "Understanding Cryptography", ©Springer-Verlag Berlin Heidelberg, 2010.

[4] Stamp M., "Information Security-Principles and Practice – Second Edition", ©John Wiley & Sons, Inc., New Jersey, USA, 2011.

[5] Cid C., Murphy S. and Robshaw M., "Algebraic Aspects of the Advanced Encryption Standard", ©Springer Science + Business Media, LLC., NY, USA, 2006.

[6] Konheim A. G., "Computer Security and Cryptography", ©John Wiley & Sons, Inc., New Jersey, USA, 2007.

[7] Daernen J. and Rijrnen V., "The Design of Rijndael AES - The Advanced Encryption Standard", ©Springer-Verlag Berlin Heidelberg, 2002.

[8] Oppliger R., "Contemporary Cryptography", ©Artech House, Inc., 2005.

[9] Talbot J. and Welsh D., "Complexity and Cryptography - An

Introduction", ©Cambridge University Press, 2006.

[10] Pimpale P., Rayarikar R. and Upadhyay S., "Modifications to AES Algorithm for Complex Encryption", IJCSNS International Journal of Computer Science and Network Security, Vol. 11, No 10, 2011.

[11] Sahmoud S., Elmasry W. and Adudalaf S., "Enhancement The Security of AES Against Modern Attack by Using Variable Key Block Cipher", International Arab Journal of E-Technology, vol. 3, No. 1, January 2013.

[12] Arrag S., Hamdoun A., Tragha A., and Khamlich S., "Implementation of Stronger AES by Using Dynamic S-Box Dependent of Master Key", Journal of Theoretical and Applied Information Technology, Vol 35, No.2, 2013.

[13] Menezes A., Van Oorschot P. C. and Vanstone S. A., "Applied Cryptography", © Electrical Engineering Journal, 1996.

[14] Rukhin A., Soto J. and Nechvatal J., "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", National Institute of Standards and Technology (NIST), USA, 2010.

[15] Yacob Z. B., "An Improved Algorithm for Partial Cryptography of Digital Video", PhD Thesis Computer Science, University of Zakho, 2012.

تعديل خوارزمية معيار التشفير المتقدم

أ.م.د عبير طارق مولود
abeer282003@yahoo.com
الجامعة التكنولوجية – قسم علوم الحاسوب
م.م ياسر علي ياسر
yasserkabashi@gmail.com
الجامعة التكنولوجية – قسم علوم الحاسوب

المستخلص

تعرض هذه الورقة البحثية تصميم جديد لخوارزمية التشفير المتقدم القياسية (AES) لتحسين أمن خوارزمية معيار التشفير المتقدم (AES) سوف يتم هذا التحسين بواسطة ثلاث تعديلات. التعديل الاول يتم باستخدام "dynamic S-box (10 S-box)" معتمدة على المفتاح بدلا من "static S-box (1 S-box)" المستخدمة في (AES) القياسية، وذلك لتحسين خاصية ال"confusion" المتمثلة بطبقة "Byte Substitution". التعديل االثاني يتم باستخدام قيم متغيرة معتمدة على المفتاح لعملية تحريك الصفوف لمصفوفة الحالة "state-matrix" بدلاً عن القيم الثابتة المستخدمة في (AES) القياسية، وذلك لتحسين خاصية ال"diffusion" المتمثلة بطبقة "ShiftRows". التعديل الثالث يتم باستخدام مفتاحين كلاهما يستخدم لعملية التشفير وفك التشفير بدلا من المفتاح الواحد المستخدم في (AES) القياسية وذلك لتحسين الهيكل العام و خوارزمية توليد المفاتيح لخوارزمية (AES). خوارزمية (AES) المحسنة تم اختبارها وتقييمها بواسطة خمسة مقاييس لاثبات فعالية التعديلات.

الكلمات الرئيسية: التشفير، التشفير المتماثل، تشفير الكتلة، معيار التشفير المتقدم، المعهد الوطني للمعايير والتكنولوجيا.