A New Key Generation to Greate Enhanced Security Version of AES Encryption Method

Hassan Rahmah Zagi
Asst. Prof. Dr. Abeer Tariq Maolood

University of Technology / Computer Science Department

hassanzajee55@gmail.com
110032@uotechnology.edu.iq

Abstract

Encryption by AES algorithm plays a significant role in concurrent encryption algorithms because of its high performance. The AES algorithm cryptography and Cryptanalysis technology are always wrestling. The more the strength of the algorithm and the complexity of key generation, the more difficult it will be to break it by the various attackers.

This paper provides changes to the AES algorithm to improve standard AES security. Optimization is effected by two modifications. The first modification, by generating keys to its algorithm (AES) by relying on (DES-key, Substitutions layer, and one-way function (MD5)) The keys are used for encryption and decryption, to boost layer-represented 'confusion' (Substitutions) characteristics And Layer-represented 'diffusion' properties (MD5). The second modification produces the variable values of the key to transfer the "state matrix" rows instead of the static keys (AES). The proposed revised algorithm reveals the high performance and encryption security. The experimental results showed that the proposed algorithm was efficient and powerful comparing the original algorithm with the improved algorithm using the Basic Five Statistical Tests, producing good and more complex results against different attackers on a freshly.

Keywords: Cryptography, Encryption, Advanced Encryption Standard (AES), Hash function, statistical analysis.

1-Introduction

The present era of digital information has become, and the flow of information has become the lifeline of humanity. Therefore, it is very important to be safe to click on the form to send information via the Internet that has become part of everything we do in our daily lives and the way we live and work is changing now [1]. The global transformation online helps promote the creation and implementation of government businesses. The information age has become very important in terms of individual life, as we share information online. As a result, it has become important to draw attention to the protection and protection of information for all of us, because it is vulnerable to cyber-attacks if sensitive and confidential information is provided over an insecure network and stored as archived data. When exchanging sensitive data and information, it is necessary to meet the basic requirements. Over the network. Among the most important requirements (confidentiality, security, reliability, and non-eavesdropping), digital information security can be implemented through several widely known encryption algorithms [2].

One of the most important highly efficient encryption AES algorithm, which is designed by Belgian encoders Joan Damon and Vincent Regimen, the encryption standard starting in 2002 [3]. The algorithm consists of a 128-bit block with 128-bit (AES-128), 192-bit (AES-192), and 256-bit (AES-

245), variable keys. The number of rounds for encryption is based on the size of the key: 10 for AES-128; 12 for AES-192, 14 for AES-256 [14]. AES has different advantages, including safety, high performance, versatility and fast implementation [4].

The AES algorithm powerful and highly successful, enhancement is still possible, particularly in the features of "diffusion" and "confusion"[4]. This paper introduced two amendments to the AES standard to improve propagation property and confusion property. The first amendment is the generation of algorithm keys based on (DES-key, Substitutions, and MD5) and the second in the AES encryption round where variable keys(ShiftRows) have been generated, both of which achieve faster and faster randomization and randomization rates for encrypted data.

2-Related work

In this section, the most relevant previous works will be clarified of the AES algorithm

1-Junjie Yan* and Feng Chen.,(2016). In this proposal for the AES algorithm the dual model (S-Box) is used based on nonlinear equations. To increase the spread and randomness of the data. The results of the experiments conducted on the proposed model show efficient results that can improve the security of the cryptographic key of the algorithm [5].

2- Meltem . K. P, Nevcihan . D and Fatma . B .S ,.(2017). This paper considers block ciphers and key schedule algorithm that is one of the crucial components of a block cipher. It computes round keys/subkeys for relevant round from a short key. The presented experiments show that proposed key schedule algorithm which inspired by Advanced Encryption Standard's (AES) key schedule has desirable properties: Avalanche Effect and Strict Avalanche Criterion (SAC). It satisfies good bit confusion and diffusion. The average success rate of the proposed key schedule algorithm for the SAC test is 95%. As a side result it was found that while testing SAC effect computed values that lie between confidence lower and upper bounds, greater than upper bounds and less than lower bound all of them reach normal distribution. Also based on example given experimental result, proposed structure exhibits a very strong Avalanche Effect because almost at the first round approximately half the bits are changed in the key [6].

2-Abeer.T.M and Yasser A.Y.,(2017). Enhancement the AES algorithm by using the dynamically reactive S-box (10 S-box) to improve the "confusion" features of the Computing Memory Unit Substitution Layer rather than the static S-box (1 S-box) used by standard AES. The second improvement uses key-based values to change the "state-matrix" row system instead of elevated values used by traditional AES to boost the "diffusion" functionality of the ShiftRows layer. The third improvement is by using 2 keys instead of 1 key used with commonly used AES, one used for cryptography and encryption rather than one used by commonly used AES to boost overall efficiency and power of the proposed algorithm and this key generator is used in the process of encryption and decryption the algorithm (AES) [10].

4- Aye. A. T and Mie. M. S. T.(2019). Enhancement AES algorithm by adding a second key and another modification Adding the transport function to the original SubBytes function would allow another adaptation in the sub bytes stage[2].

5- Edjie .M. D ; Ariel.M.S and Ruji .P.M.,(2019).AES has been modified in the early-round to resolve the weak diffusion rate by introducing additional basic operations in the cipher round including

exclusive OR and modulo arithmetic. Also, the central plan algorithm has been introduced byte substitution and round constant extension [4].

3- Theoretical background

3.1- MD5 Algorithm

The MD5 is designed to operate at 32-bit machines very easily. Moreover, the MD5 no large replacement tables are required; the algorithm is very compact. The MD5 algorithm is a somewhat lighter extension of the MD4 message digester algorithm MD5 that is more "Preventive" in nature. The MD5 algorithm takes an arbitrary-length message as input and generates a 128-bit data digest. A digest of the entire message data used for Authentication is determined using the authentication algorithm. The message digest is usually registered with a trusted third party or otherwise encrypted. One of the most important features of hash function (MD5) is that it produces a unique output in every execution [7].To verify a message, the digester is used by the recipient. It can also be used to encrypt the contents of a message through another algorithm via a second pass over the data. MD5 requires that the sender and recipient measure the digest of a message throughout the body.

The general structure of its MD5 algorithms shown in Figure (1)[8].

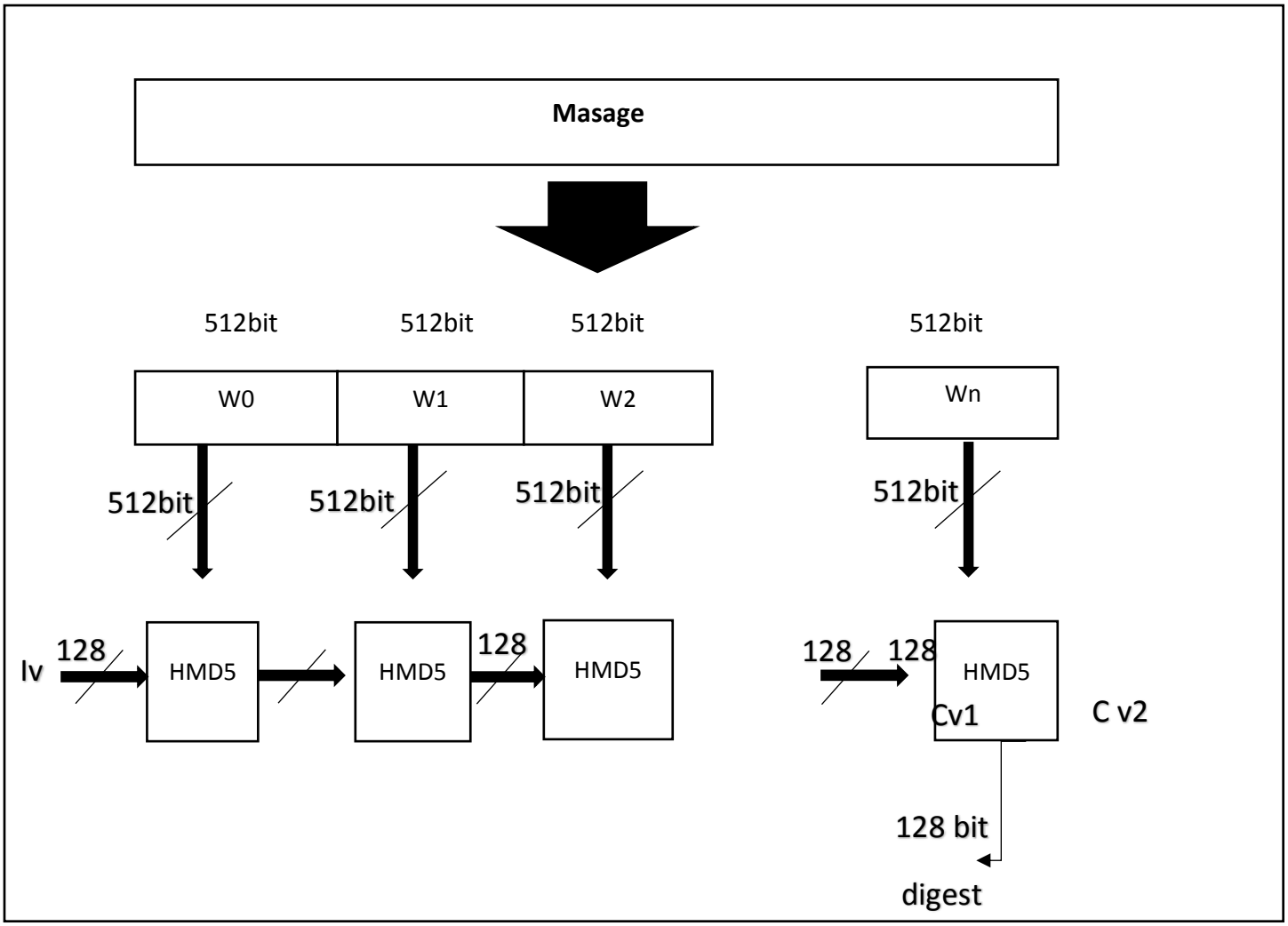

Figure 1: The general structure of the MD5 algorithm [7]

Steps for working a cipher (Md5) algorithm: -

1- Insert a set of bits called (the fill bits), which in turn match the bits to be encrypted with the length of the block used by the algorithm adding the first bit (1) followed by many (0).
2- The last block is reserved to insert the length of the original message.
3- 3-Provide the algorithm (MD5) 128-bit Buffer, divided by four with bit length 32(A, B, C, D): A= 0x01234567; B = 0 x89abcdef; C = 0 xfedcba98; D = 0x76543210.
4- The process of transforming the input data (with a length of 32 bits) is the basis for the work of the algorithm by compressing a "cycle" by logical functions and through which 32 bits are generated, as will be illustrated in Figure 3. The logical functions used for each session: F (X, Y, Z) = (XY v not(X) Z), G (X, Y, Z) = (XZ v Y not (Z). H (X, Y, Z) = (X xor Y xor Z), I (X, Y, Z) = (Y xor (X v not(Z))) bit (X, Y, Z), G (X, Y), H (X, Y, Z), and I (X, Y, Z) is neutral and objective if the bits of X, Y and Z are objective and unbiased Steps [9].
5- The output is generated at a fixed length.

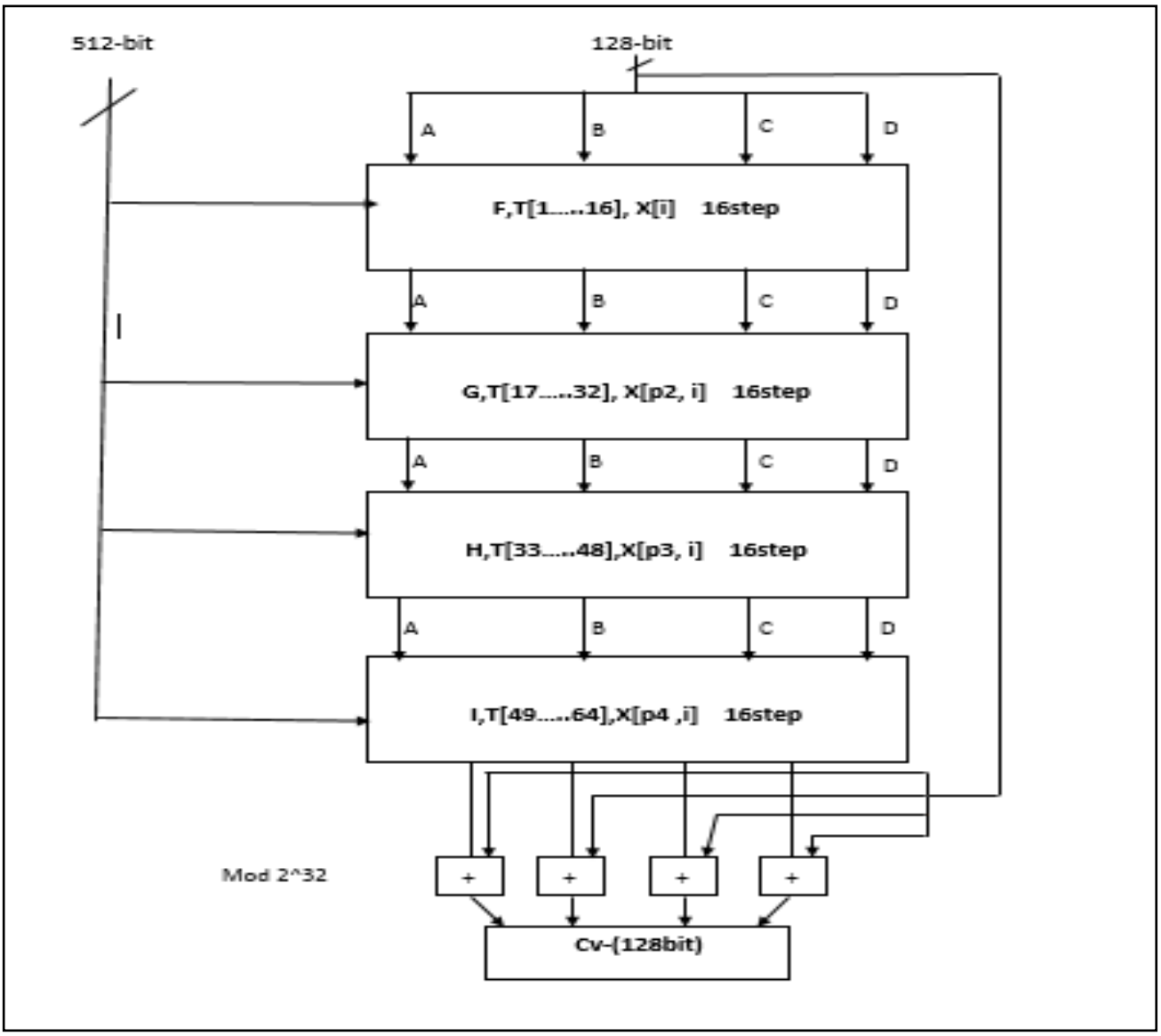

Figure 2: Rounds algorithms MD5 [9].

3.2- Advanced Encryption Standard (AES) Algorithm

Advertised Encryption Standard (AES), also known as Rijndael, is used to protect information. AES has been extensively researched and is now used as a symmetric block cipher. The symmetrical encryption algorithm AES, therefore, is used for 128-bit encryption. The length of input, after going through every loop, is known to be a 4 to 4 bytes matrix called the status matrix [1,3]. The AES block is 128 bit long, While the key has different lengths (128 bits the number of turns is 10, the length of 192 bits is the number of round 12 or 256 bits the round number 14). It will also be shown in table (1) [10].

Table (1): Round Key for AES [10]

AES Key length	128	192	256
Round	10	12	14

AES Algorithms' characteristics include resistance to any known attack, fast encoding speed, free royalty around the world, hardware, and software adaptability. Mathematical efficiency and high reliability. Algorithm of AES. Figure (3) shows the AES process for Encryption and Decryption [10].

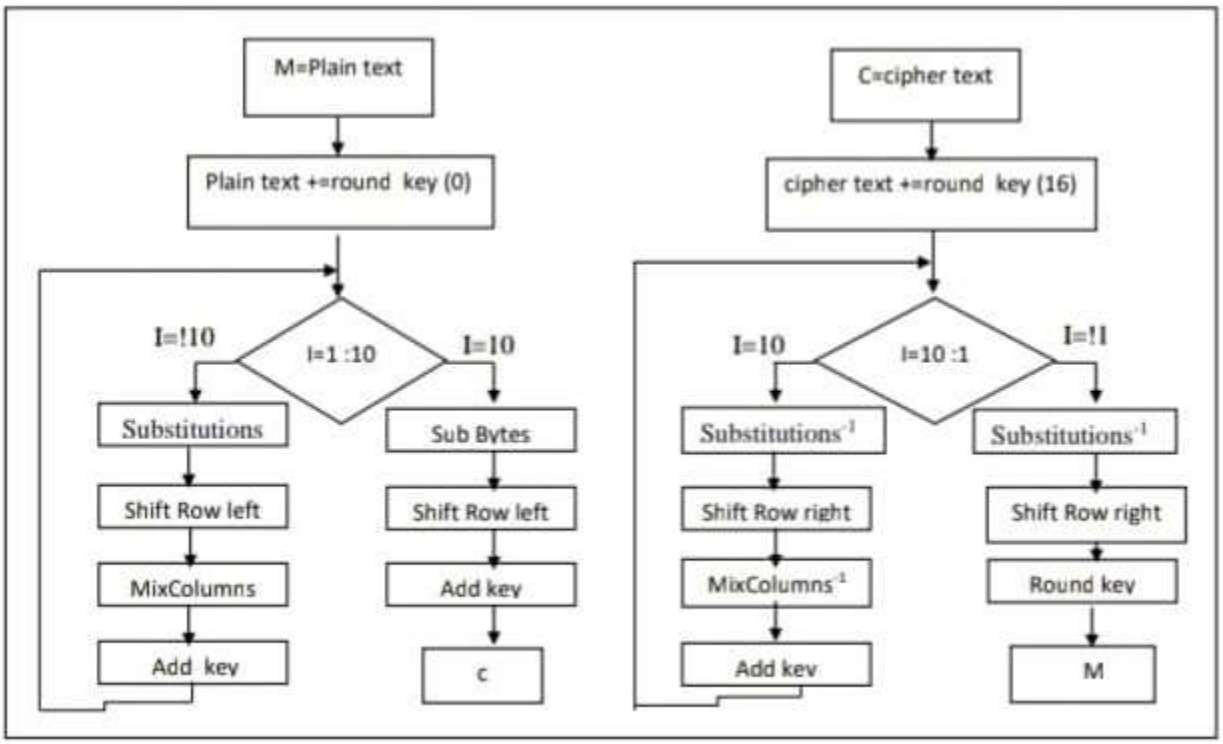

Figure 3: The AES algorithm structure [10].

A-Functions Used Inside The AES Algorithm (Encryption and Decryption) [4, 10, 11]:

1-**Function Substitution (s-box):** The resulting matrix bytes are replaced by process (message Matrix Xor Add key) another byte presented as the substitution table (SBox). This layer helps by increasing the propagation property together maintaining the number of bits.

2- **Function Shift Rows**: State matrix rows are shift (byte-orientated) towards the left, with fixed rows each.

3 – **Function MixColumn**: state matrix mix using GF (2^8) and modular p(x) = x8+x4+x3+x+1. The data diffusion is given by the layer tow and layer 3.

4- **Function Add round key**: the Process (MixColumn xor key).

Encyption the AES 128-bits Consists of ten ronds in the round 0 (the main addition layer) and through these Rounds data is processed, begins with 128-bits, by four-functions (Substitution, ShiftRows, MixColumn,and add round key).

Decryption the AES 128-bits The inverse of each function (Substitution, ShiftRows, and MixColumn).

B-AES Key Expansion Algorithm

Different ranges of key can be used: 128, 192, or 256-bit, ten cycles for 128-bit keys, 12 cycles for 192 bit keys and 14 cycles for 256-bit keys. AES supports three different key ranges. The AES key has a 4-byte, 32-bit, word notion. The crypt key column is thus a title, just as each row is [12].

The length of the key is assumed to be 128 bit per part. The first four terms of a main column matrix are distributed as shown in Figure (4) [13].

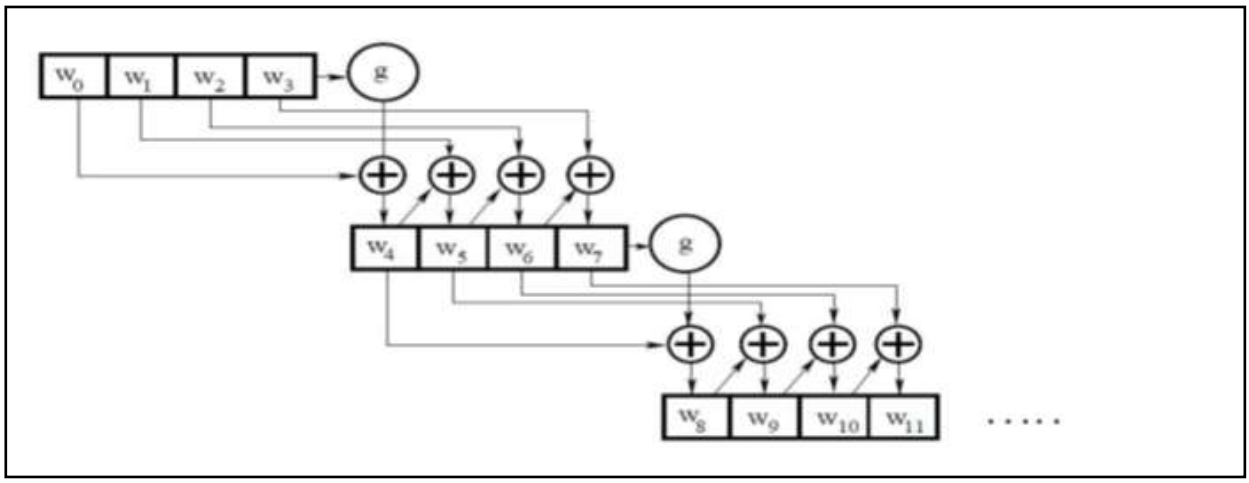

Figure 4: Key generation AES algorithm [13].

4-Proposals to Modifying AES Algorithm

The AES algorithm was improved by two amendments, the first was in Add Round Key by a new approach to generate keys used for encryption and decryption, and the second modification to ShiftRow was by dynamically generating keys.

A-The First Proposed Improvement of AES Algorithm.

The increased protection of sensitive data requires modifications to the encryption of AES algorithm.The first amendment to the algorithm includes a new method for creating the keys used for encryption and decryption. This approach is enhanced with many functions that create 10 keys with high efficiency, strict confidentiality, and increased randomness and complexity. It will also be explained in detail through the following steps:-

Step 1:- This proposal depends on the external structure of the DES algorithm with a slight change in this structure used for encryption and decryption by adding a function (shift<<<) which in turn enhances randomness by circularly changing one bit. For this, the data that is entered must be processed by means. The entry is 128 bits, and as the entry is passed in 10 rounds and in each round a key is produced that is used within the modified algorithm. In this approach, 128 bits of plain text are

divided into two halves, L and R of sixty-four (64) bits each. R_{i+1} will be calculated as(L_i(shift<<<)),and L_{i+1} will be calculated as(R_i (shift<<<) .

Step2:- Within the external structure of the proposed algorithm,(F-Function) was used, which in turn contains many functions:-

1-In the modified algorithm, a layer (SubBytes(S-Box)) is used by two of ((S-Box-L),(S-Box-R)) by which the (confusion) property is strengthened, which contributes to maintaining the quantity and quality (statistical characteristics) of the data, and it was adopted on the map of even and odd numbers arranged in the form of a matrix (8x8) from (S-box- left), where the input for this layer is 64 bits to produce 64 new bits and a matrix (8X8) from (S-box- Right), where the input for this layer is 64 bits to produce 64 new bits , as was shown in table (2) S-box-left, and in table (3) S-box- Right, where x_ indicates the bits to be rearranged, and the numbers indicate the location of the bits.

Table (2):-The S-box-left Using in AES

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Table 3:-The S-box-Right Using in AES

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

2-After completing a layer of SubBytes, the output is passed to a function (Concat), which in turn merges the output from (s-box-left) and the output from (s-box-right) along (128-bit), and the output from this function becomes an entry to the function that they useafterward.

3-After completing a layer of (function-Concat), the output is passed to a function (MD5) and it is based on the reduction of the entered message with a length of 128 bits to a fixed length of 128 bits, regardless of its original length, where the message is converted into blocks of length of 512 bits each for the purpose of reducing it in later steps. Any change of any size in the original text produces a completely different reduction value compared with the previous value, and the advantage that this function provides from others is that it provides a different outlet for each entry no matter how small the difference between them, which is called fingerprint in addition to that it is impossible to return from the value of the shorthand to the original message. That is, the key resulting from this function is strong and efficient, in addition to the advantages of other functions that were used in the proposal in order to enhance "confusion" and "diffusion ". These are important characteristics of the operation of safe encryption. In figure (5), the general scheme for generating keys is shown.

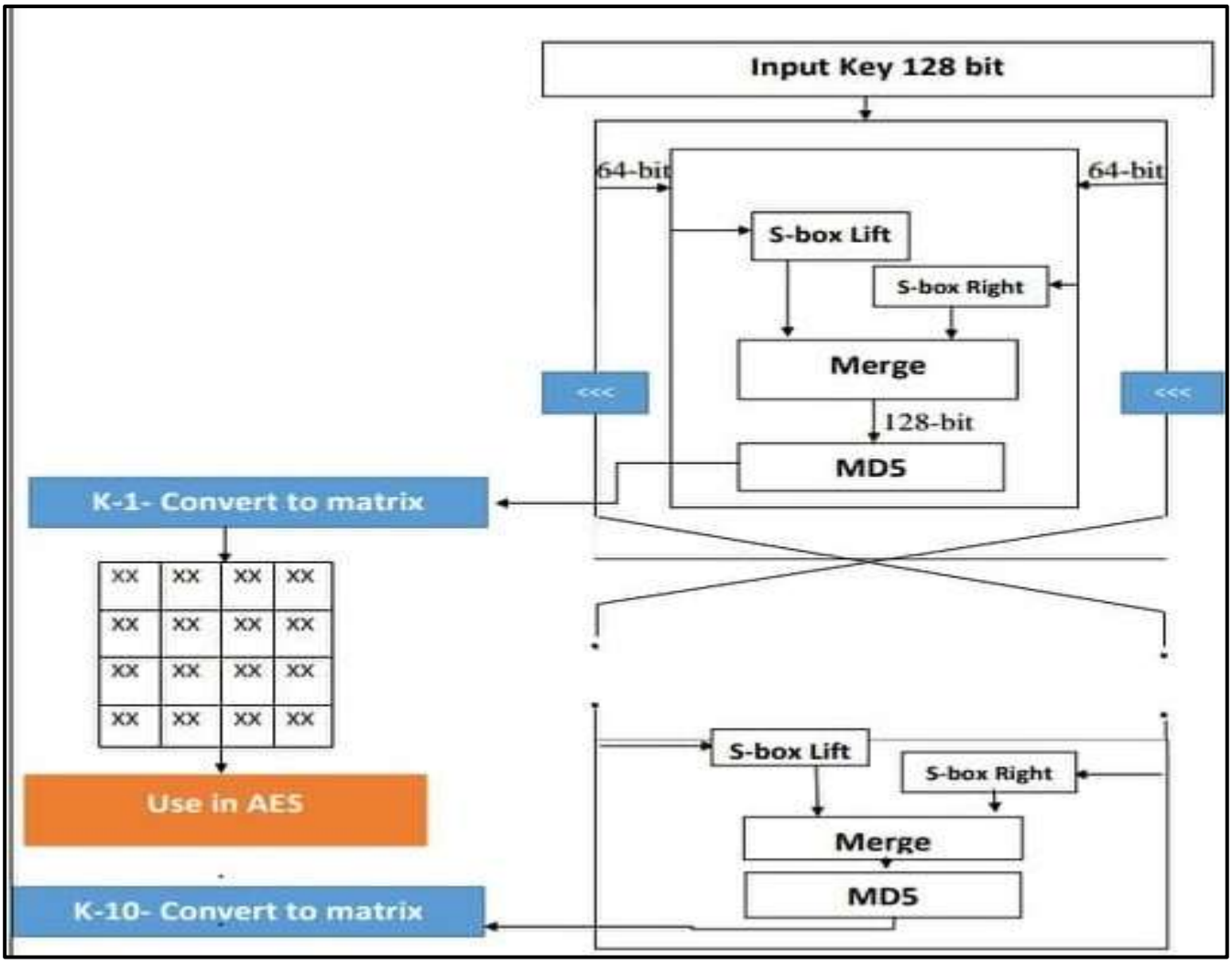

Figure 5: AES Round key Modified Block Diagram

B- The Second Proposed Improvement of AES Algorithm

The modified method way it depends on entering a main key by a user who is shared between the sender and the receiver after the 128-bit key length is entered and passed to the (hash function) that produces 128 bits as well, and after the status matrix is built (4 * 4), the byte in each cell is taken from the secondary diameter and converted to decimal a mathematical equation is applied depending on the common denominator 4 [I mod 4]. After the equation which is applied, the special keys ShiftRows are produced and are ready in all cycles. Thus, strong and more complex keys were produced as will be illustrated when comparing the results of the modified algorithm with the original one. The algorithm is highly efficient and reliable against various attacks. The idea of producing keys for ShiftRows will be clarified through algorithm (1) that explains the second modification of the algorithm. Figure (6) shows the general proposal of the algorithm

Algorithm 1: ShiftRows Operation Modification

Input: Key by the user 128 bit .
Output: key-shift [4], State-Matrix shift rows [4,4].
Process:
Shift Value = 0
Begin
Step1: 128 bit input in hash function (MD5).The output from (MD5) is converted to state-matrix[4x4].
Step2: Modulate these values by taking secondary diameter values for the rows of the state matrix in the rows of the primary input by the user .

```
For i=0 to 3
        begin
 Shift value [i]= State-Matrix( [i],[4-i] mod 4).
        key-shift  [i]= Shift value [i].
         i=i+1
          End
```

Step 3 : Shift Matrix produced from S-box by the values found in Step2.
For i= 0 to 3 do
For j=0 to 3 do
State-Matrix shift rows = state-matrix [i, ((j+Shift value[i]) mod 4)]).
End
End
End Algorithm

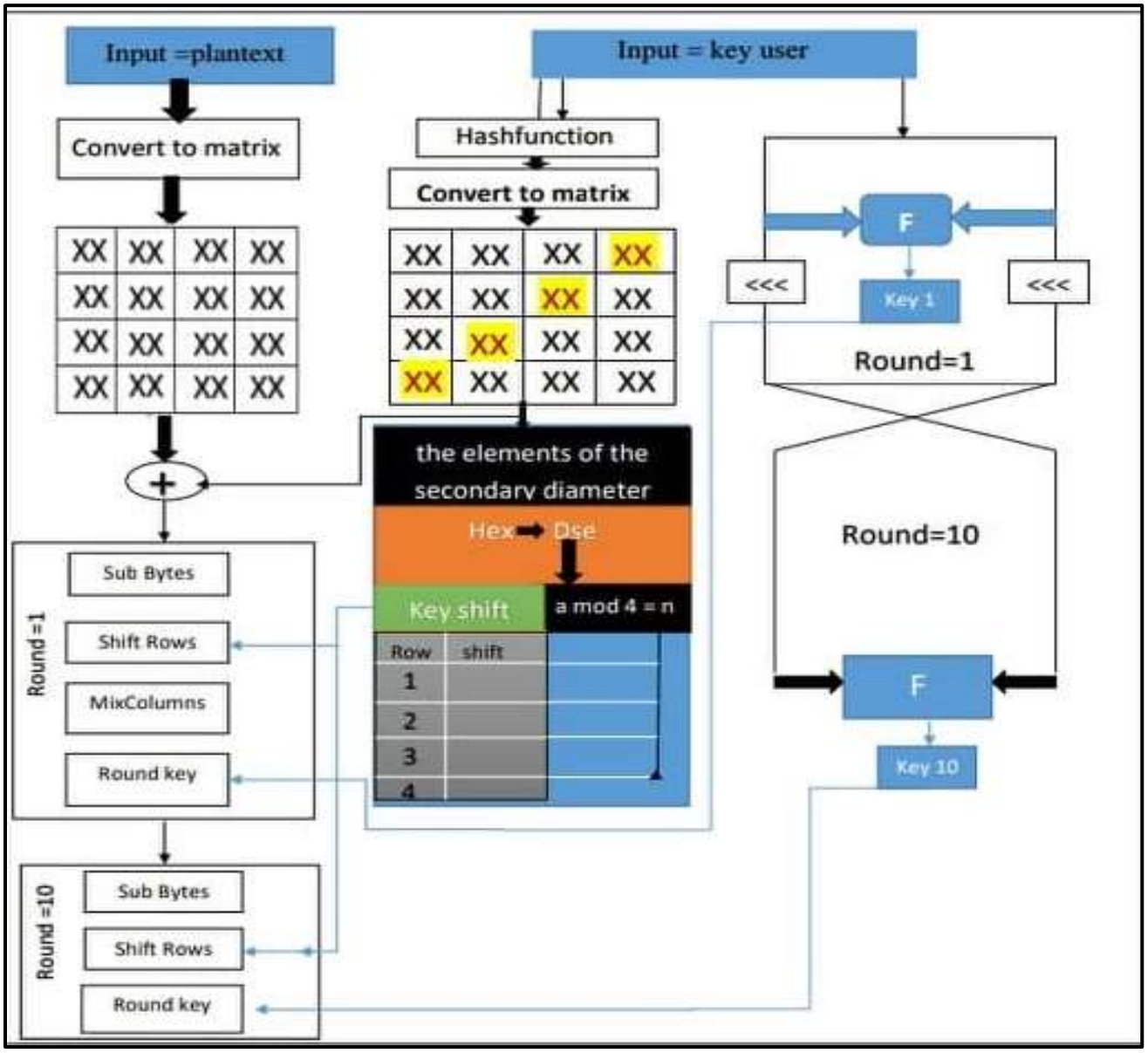

Figure 6: Proposed modified AES encryption Block Diagram

5-Tests and Results

Evaluate the success of the algorithm and describe the benefit of the modification to the algorithm, the algorithm is compared before the AES modification and the modified AES algorithm by the following tests (Frequency Test, RunTest, Poker Test, Serial Test, Auto Correlation Test)

In this paper, same thing basic AES and Modified AES inputs (the same plaintext and 128 bits of key lengths) are used. The 128-bit output block size (ciphertext) is evaluated using 5 selected tests. The following tests are used. The following inputs are given. The state matrix progression increasing the modified AES encryption method is seen in example (1).

Ex (1): The modified AES example, the input plaintext is used and the keys are:

Plaintext M:	63 6F 6D 70 75 74 65 72 73 63 69 65 6E 63 68 68
Input key K0:	6E 75 6C 6C 6E 75 6C 6C 31 32 33 34 38 37 36 35

The ex (2): resulting ciphertext is:

C=96 EA B0 6E DA AD 6F D9 8B A5 18 B8 C1 8A AB CD

" Key genterter by Figure(5) AES Key Modified Block Diagram"	
Round 1	68 61 73 73 61 6E 68 61 73 73 61 6E 31 32 33 34
Round 2	6E 6F 72 68 61 73 73 61 6E 31 32 33 34 35 36 37
Round 3	61 6C 69 73 61 6D 65 72 39 38 37 36 35 34 33 32
Round 4	31 32 33 34 35 36 37 38 39 30 68 61 73 73 61 6E
Round 5	61 68 61 6D 61 64 68 61 73 73 61 6E 34 34 35 35
Round 6	6F 6D 70 75 74 65 72 73 63 69 65 6E 68 68 31 32
Round 7	71 61 7A 78 73 77 65 64 63 76 66 72 74 67 62 6E
Round 8	33 6A 75 79 68 6E 6F 6C 39 38 37 36 35 34 33 32
Round 9	71 77 65 72 74 79 75 69 6F 70 6C 6B 6A 68 67 66
Round 10	6C 6B 6A 68 67 66 64 73 61 71 7A 72 63 76 79 62

Table 4: **Shows an integrated example of the modified algorithm encryption process**

R	Start Round	SubByte	ShiftRows	MixColumns	Add-key
0	63 6F 6D 70 75 74 65 72 73 63 69 65 6E 63 68 68				6E 75 6C 6C 6E 75 6C 6C 31 32 33 34 38 37 36 35
1	D1 E4 D9 Dc E3 E9 D1 DE A4 95 9C99 A6 9A 9E9D	3E F8 35 86 BA 15 DC 4F 62 04 79 E8 B7 1F F1 3A	86 3E F8 35 4F BA 15 DC 79 E8 62 04 F1 B7 4A 1F	3E 3C 3F 21 40 23 24 25 5E 26 2A 28 29 6F 79 74	68 61 73 73 61 6E 68 61 73 73 61 6E 31 32 33 34
. .	. .	. .	. .	. .	. .
9	2B 5F 29 28 2A 26 5E 25 24 23 40 21 22 3F 3E 3A	F1 CF A5 34 E5 F7 58 3F 36 26 09 B7 93 75 B2 80	34 F1 CF A5 3F E5 F7 58 09 B7 36 26 B2 80 93 75	7E 21 40 23 24 25 5E 26 2A 28 29 39 37 37 36 35	71 77 65 72 74 79 75 69 6F 70 6C 6B 6A 68 67 66
10	EF 98 A5 95 98 9E D3 8F 99 98 95 A4 A1 9F 9D 9B	DF 46 06 2A A7 0B 66 73 EE 46 2A 49 32 DB 5E 14	2A DF 46 06 73 A7 0B 66 2A 49 EE 46 5E 14 32 DB		6C 6B 6A 68 67 66 64 73 61 71 7A 72 63 76 79 62

5.1- Basic Five Statistical Tests

In order to determine the randomness of the ciphered text, five statistic tests are applied for the randomness of the text test (frequency, race, poker, series, and correlation) and through the scale test, efficient and sharp scores are shown compared to the original algorithm as will be shown in the table (5) .They are: Freq-T_1 = 1, Ser-T_1 = 3, Book-T_1 = 5, RunT_0 = 5, RunT_1 = 2 ,Correl-T_1= 1, respectively.

Table 5 : Results of 5 tests used for standard and algorithms of modified AES.

Statistical Test					
Tests		**Freedom Degree**	Standard AES	**Freedom Degree**	ModifiedAES
Frequency Test		MUST BE <= 3.84	PASS = 0.000	MUST BE <= 3.84	PASS = 2.314
RunTest	**T0**	MUST BE <=10.788	PASS = 3.874	MUST BE <= 7.531	PASS = 3.418
	T1	MUST BE <= 7.531	PASS = 3.418	MUST BE <=5.702	PASS = 3.656
Poker Test		MUST BE <= 11.1	PASS = 2.708	MUST BE <= 11.1	PASS = 4.429
Serial Test		MUST BE <= 7.81	PASS = 0.154	MUST BE <= 7.81	PASS = 3.386
Auto Correlation Test	Shift-1	MU- BE <= 3.84	PASS =0.020	MU- BE <= 3.84	PASS =0.471
	Shift-2		PASS = 1.280		PASS = 0.030
	Shift-3		PASS = 0.020		Pass =2.408
	Shift-4		PASS = 0.333		PASS = 0.290
	Shift-5		PASS = 0.021		PASS = 3.333
	Shift-6		PASS= 0.087		Pass =1.190
	Shift-7		PASS =2.689		PASS = 0.571
	Shift-8		PASS =0.364		PASS = 0.333
	Shift-9		PASS = 0.023		PASS =0.615
	Shift-10		PASS =0.000		PASS =1.000

The modified algorithm produces greater results than Normal the AES depending on the performance of the five simple statistical measures. The results suggest a more altered degree of randomness in the AES algorithm Modified output (ciphertext). It shows that the changes introduced bring randomness and usefulness to the difficult properties of the regular AES (ciphertext).

5.2-Running Time Modified and Standard (AES) algorithm (Encryption and Decryption).

The actual running time of the text is computed by the modified and standard AES algorithm using the personal computer, but using different data blocks of sizes (10,20,30) kb. The results show a slight difference in both algorithms,as shown in table (6) and the Curve (1).

Table 6: Running Time comparison between modified and standard AES. .algorithm

File size	operation	Standard AES in Sec	Modified AES in Sec
10kb	Encryption	8.666	9.000
	Decryption	10.996	11.444
20kb	Encryption	15.666	16.564
	Decryption	18.999	19.111
30kb	Encryption	23.963	25.999
	Decryption	26.060	28.101

6- Measuring the complexity of the proposed AES algorithm

Many characteristics of the algorithm are relied upon to illustrate the degree of complexity between the Standard AES algorithm and the improved AES algorithm, as shown in Table (7). The extent of the algorithm's constraint is measured based on the parameters and characteristics (external structure, number of rounds, inputs, outputs, key sizes, key generation function (number and length of the key), and implicit functions used

Table 7: Complexity between the Standard AES algorithm and the improved AES algorithm.

Caption	Standard AES algorithm	Modified AES algorithm
number of rounds	10,12,14	10
Input block length	128,192,256 bit	128 bit
Output block length	128,192,256 bit	128 bit
Key block length	128,192,256 bit	128 bit
key Scheduling	Standard method of generating keys	Suggested method for generating(10) keys which includes: 1-Input:128 –bits 2-Use the exoskeleton (DES)algorithm 3-Use -Function S-Box right -Function S-Box left 4-Use the combination function of the result from both sides

		5-Use Hash Function (MD5) 6-The generated key is in one direction only 6-It is extremely difficult to break the generated key due to the properties of the used methods
Internal used functions	1- Substitution (s-box) 2-ShiftRows 3-MixColumn 4-Add round key	1- Substitution (s-box) 2-ProposalShiftRows (Depending on the generation of keys (ShiftRows) bypassing the key entered by the user to the hash function (MD5), the output is transformed into an array and taking the secondary diameter and performing a mathematical operation (Shift value [i]= State-Matrix([i],[4-i] mod 4) so that the product of each cell of the secondary diameter is the user's key) 3-MixColumn 4- Add round key(The proposed algorithm is provided with the key used from each round by the proposed key generation approach)

7-Conclusions

By evaluating the experiments that were conducted on the proposal:

Several functions have been used to increase the complexity of key generation through the use of an extended key generator algorithm (S-Box right and S-Box left) to achieve the Property "confusion". In conjunction with the product(S-Box right and S-Box left) that enters the hash function (MD5) to achieve the generation of key unique involved in the encryption and decryption process.

2-Taking into consideration. The work of the cryptanalyst to obtain the key used in encryption and decryption takes time and effort because the hash functions work in one direction.

3-The AES algorithm is further complicated by the use of several new functions

4-The new proposal is used to encrypt all types of data. Then this paper presents several works related to amending the standard AES. Then the modified AES measure the (difusion) and (confusion) property of the bits, which were tested by five metrics (five basic statistical tests, , encryption runtime, brute force attack and analytical attack) the result subkeys passed the test and achieved a full spread For bits

8-References

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

[2] Aye. A. T and Mie. M. S. T. (2019). Modification of AES Algorithm by Using Second Key andModified SubBytes Operation for Text Encryption, Springer Nature Singapore Pte Ltd.

[3]-William .S.(2012).Cryptography and Network Security Principles and Practice .5th edn ,. USA: Prentice Hall: 900 -pp.

[4]-Edjie .M. D ; Ariel.M.S and Ruji .P.M.,(2019).Modified AES cipher round and key schedule, Indonesian Journal of Electrical Engineering and Informatics (IJEEI).7(1) :29-36 -pp.

[5]- Junjie Yan and Feng Chen., (2016). An Improved AES Key Expansion Algorithm, International Conference on Electrical, Mechanical and Industrial Engineering,:113-116 -pp.

[6]- Meltem . K. P, Nevcihan . D and Fatma . B .S ,.(2017). The New Approach of AES Key Schedule for Lightweight Block Ciphers,. IOSR Journal of Computer Engineering (IOSR-JCE).,19 (3) : 21-26-pp.

[7]- Aso, A.M.(2017). Cluster forming based on spatial information using HMAC in WSN.Tikrit Journal of Pure Science,22 (6) :131-139-pp.

[8]- Shweta.M.S and Nilesh .K,.(2013).Hashing Algorithm: MD5, IJSRD - International Journal for Scientific Research & Development,. 1(9) :2321-0613- pp.

[9]-Ye .Ta, Kun .Z, Pu .W, Yuming .Z.and Jun .Y.(2018). Add "Salt" MD5 Algorithm's FPGA Implementation. Procedia computer science,131 : 255-260 -pp.

[10]- Abeer.T.M and Yasser A.Y.,(2017) Modifying Advanced Encryption Standard (AES) Algorithm, Journal of Al Rafidain University College, 1681-6870 :pp.

[11]- Zahraa . K .T.,(2016).Text Encryption using Modified AES-2 Keys , International Journal of Computer Applications , 149(4): 116 –120 -pp.

[12]- Felicisimo .V. W, Jr.,(2015).Performance Efficiency of Modified AES Algorithm Using Multiple S-Boxes , International Journal of New Computer Architectures and their Applications (IJCAA), : 1-9-pp.

[13]- Kak A.,(2016).AES Advanced Encryption Standard., Avinash Kak, Purdue University, West Lafayette, Indiana, USA.