Analysis of AES Algorithm Effects on the Diffusion Property

Hasanen S. Abdulah* Ph.D,(Asst Prof.), Maha A.Hamood Al-Rawi* Ph.D,(Asst Prof),
Dalal N. Hammod**Msc.(Lecturer)

Abstract

In cryptography, confusion and diffusion are two very important characteristics, which must be achieved these characteristics in the ciphertext to obtain a strong cipher and avoid any attacker for attacked. This research aims to propose three methods based on a different sequence of operations of Advanced Encryption Standard (AES) algorithm. In this research is used hamming distance ,which it is a number of different symbols between two strings of equal length, for calculating diffusion. The proposed methods obtained approximately (63 bits) change in each round corresponding to the total number of bits (128 bits), but the standard AES obtains approximately (65 bits). The proposed methods use hamming distance for calculated diffusion property the (49.5%) percentage value of the proposed methods and the (50.9%) percentage value of the standard AES. After testing and verifying, it was concluded the AES algorithm is the best sequence of operations to achieve the best confusion and diffusion of data.

Keywords: Advanced Encryption Standard (AES); Confusion; Diffusion; Hamming Distance.

* University of Technology
** University of Al-Nahrain

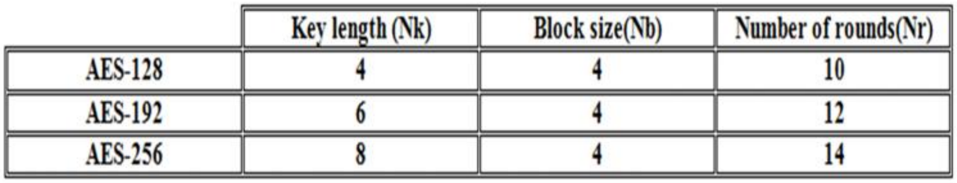
1. Introduction

In 1945, Claude Shannon identified two very important properties in a secure cipher for cryptography and in the design of robust pseudorandom number generators and hash functions. These properties are: confusion and diffusion [1].

Both confusion and diffusion are excellent in the Advanced Encryption Standard (AES) and for increasing the amount of scrambling that repeated several times for each input. In AES, the confusion look-up tables are very good at destroying non-linear patterns. The diffusion changes one bit of input changes half the output bits on average. Because the secret key is mixed in at each stage, that an attacker cannot pre-calculate what happen in the cipher for one-stage scramble based on a key [2].

AES algorithm supports block size fixed for 128 bits (16 bytes) and supports key sizes of 128 bits (16 bytes), 192 bits(24 bytes), and 256 bits (32 bytes). The block sizes can mirror those of the keys, see Table (1), which represents the variable number of rounds (number of rounds depending on key length and block size) [3] .

Table (1): Number of Rounds depending on Key length and Block size.



	Key length (Nk)	Block size(Nb)	Number of rounds(Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

AES operates on which called *state* that is represented by a 4x4 matrix of bytes. The main functions that comprise the AES are substitute bytes, shiftRows, mixColumns, and addRoundKey [4] .

2. Related Work

There are many achievements that occurred in the field of encryption by AES; each suggests improving AES algorithm for enhancement the diffusion. The most useful ones are mentioned in the following:

Shize Guo, et.al., "Exploiting the Incomplete Diffusion Feature: A Specialized Analytical Side-Channel Attack against the AES and its Application to Microcontroller Implementations ", 2013[5] .

The researchers proposed a new technique called incomplete diffusion analytical side-channel analysis (IDASCA). The IDASCA exploited the incomplete diffusion feature in one AES for analytical side-channel attack on AES. The attack types are performed against the software implementation of AES on an 8-bit microcontroller. Testing the proposed method show that IDASCA can exploit the side-channel leaks in all AES rounds using a single power trace, It has more robustness and less time complexity than previous ASCAs, especially when considering the error-tolerant attack scenarios, and it can calculate the reduced key search space of AES for the given amount of side-channel leaks.

R.Elumalai and A.R.Reddy," Improving Diffusion Power of AES Rijndael with 8x8 MDS Matrix", 2011 [6] .

The researchers focused on enhancing the diffusion power AES Rijndael in MixColumn operation the branch number of MDS matrix is raised from 5 to 9 using a new 8X8 MDS matrix with trade off of speed and implemented on R8C microcontroller. After testing the proposed method the result shows the code area consumed is 11.19% more and number of cycle required is 20.08% more and in the case of revised AES with 8x8 MixColumn compared to AES Rijndael. The increase in code memory and cycle is the tradeoff for the increase in diffusion strength which increases the security of the algorithm.

Mohan H.S., et. Al.," Improving the Diffusion power of AES Rijndael with key multiplication", 2011 [7] .

The researchers proposed a method of improving the diffusion power in AES by replace the conventional key addition with key multiplication. Key multiplication, as a diffusion element, is a better solution in the design of encryption algorithms. The proposed method indicate more diffusion when compared with the existing method. After testing the proposed method result shows the desired diffusion level when attractive to design an encryption algorithm using key multiplication apart from the key addition in order. the key multiplication runs more CPU cycles, therefore it finds applications on platforms with high-speed processors.

3.Cryptography Principles

Confusion and diffusion are two cryptography principles. Shannon’s definitions for these principles as: *confusion* is an involved and complex relationship between the ciphertext and the symmetric key; *diffusion* is a dissipating the statistical structure of plaintext over the bulk of ciphertext. This complexity is generally implemented through repeatable series of *substitutions* and *permutations* where the replacement of certain bits with other bits, following certain rules called "Substitution" and the manipulation of the bits order according to some algorithm called "permutation" [8] .

In other words, the process of data changes from input form to the output is called confusion and the process of change of many characters of the output when changing a single character of the input is called diffusion [9] .

4.The Structure of the AES [10]

AES is based on a substitution-permutation network, which combination of both substitution process and permutation process , therefore it is fast in both software and hardware. An AES encryption runs through r rounds. The structure of the AES algorithm is explained in the figure (1).

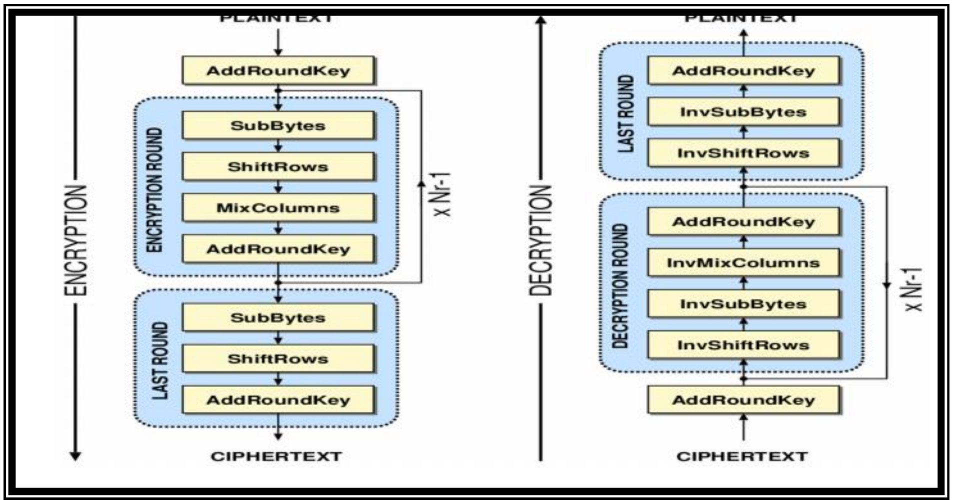


Figure (1) The Structure of AES

Each round of AES (or Rijndael) consists of four operations:

1. **SubBytes Operation,** In the SubBytes operation Rijndeal used S-box for replacing each byte *a*$_{i,j}$ in the *state* matrix with a SubByte S(*a*$_{i,j}$). This operation represents the non-linearity in the cipher. This operation is illustrated in figure (2).

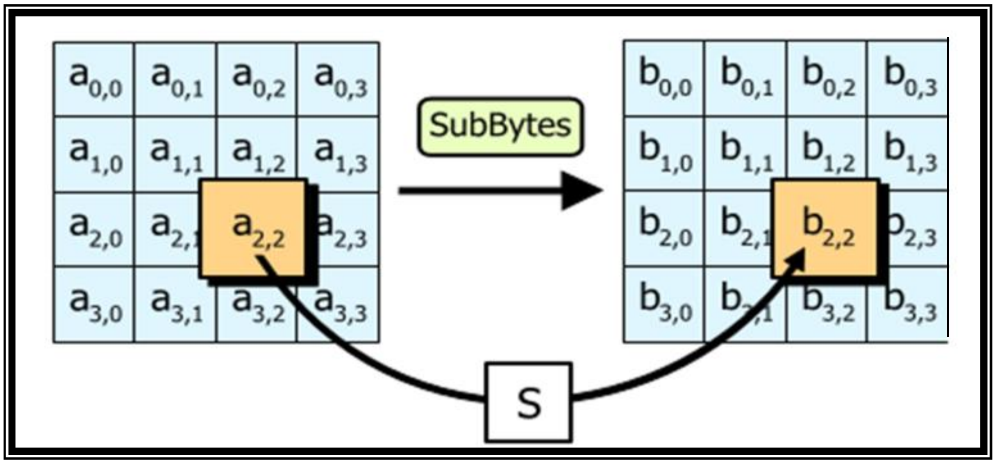

$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
SubBytes
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
S

Figure (2) The SubByte Operation

2. **ShiftRows Operation,** The ShiftRows operation cyclically shifts the bytes in each row by a certain offset. For AES, the first row of the state is shifted by offset zero, the second row shifted by offset one, the third row shifted by offset two, and the fourth row shifted by offsets three. This operation illustrated in figure (3)**.**

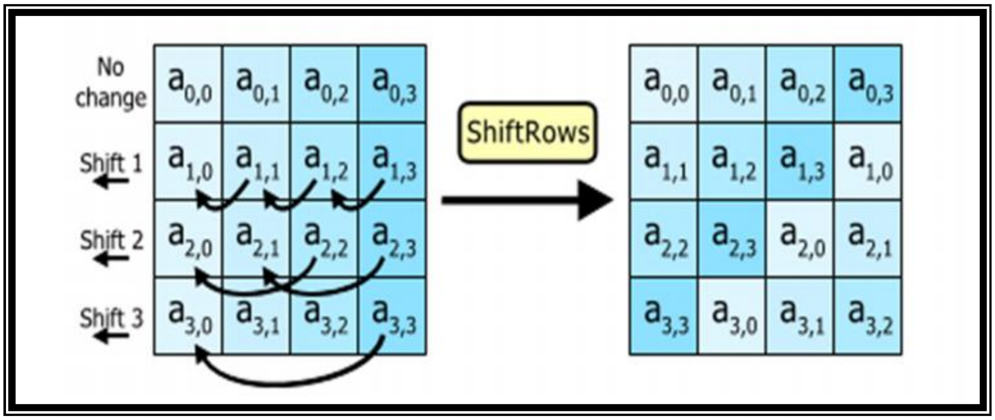
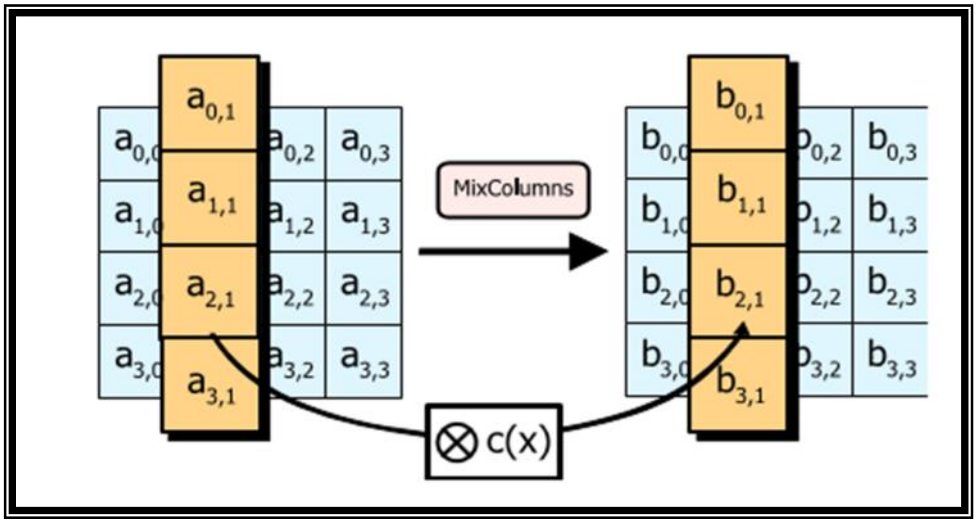

No change
Shift 1
Shift 2
Shift 3
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
ShiftRows
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,1}$ $a_{1,2}$ $a_{1,3}$ $a_{1,0}$
$a_{2,2}$ $a_{2,3}$ $a_{2,0}$ $a_{2,1}$
$a_{3,3}$ $a_{3,0}$ $a_{3,1}$ $a_{3,2}$

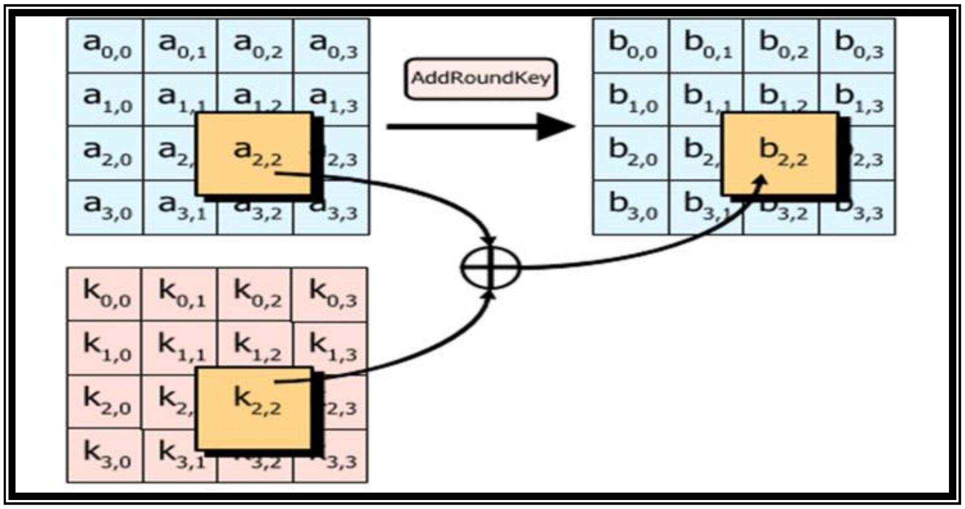
Figure (3) The ShiftRows Operation

3. **MixColumns Operation,** In the MixColumns operation, an invertable linear transformation is used for combining columns (the four bytes) bytes. The Shiftrows and Mixcolumns represents diffusion in the cipher. The inputs for the mixColumns function are four bytes and outputs four bytes too, where each byte of input affects all four bytes of output. This operation is illustrated in figure (4).



Figure(4) The MixColums Operation

4. AddRoundKey Operation, In the AddRoundKey operation bitwise XOR is used between subkey and state for combining each byte of the subkey with the corresponding byte of the state. Key schedule used for driven subkey from main key for each round. This operation is illustrated in the figure (5).


AddRoundKey
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
$k_{0,0}$ $k_{0,1}$ $k_{0,2}$ $k_{0,3}$
$k_{1,0}$ $k_{1,1}$ $k_{1,2}$ $k_{1,3}$
$k_{2,0}$ $k_{2,2}$ $k_{2,3}$
$k_{3,0}$ $k_{3,1}$ $k_{3,2}$ $k_{3,3}$

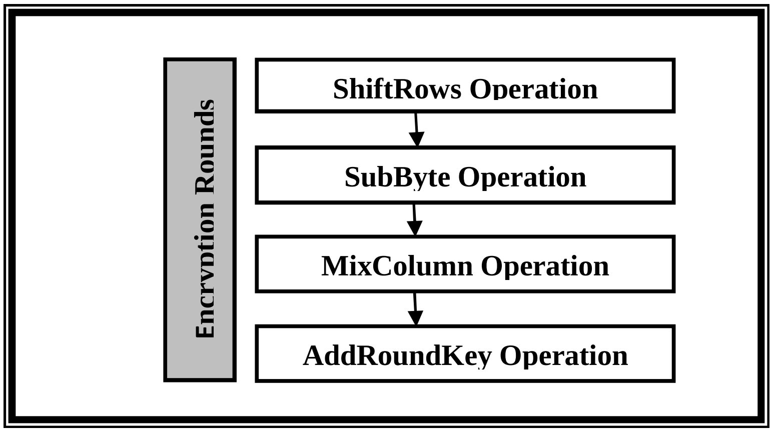
Figure(5) The AddRoundKey Operation

5.Description of Proposed Methods

In this paper, three different methods are proposed based on the different sequence of four operations in AES and the effect on the diffusion property with respect to the standard AES. The proposed methods are: the first method, the change of shiftrows operation, the second method, the change mixcolumns operation, and finally the third method, the change of shiftrows and mixcolumns operations.

5.1 The First Method: The Change Shiftrows Operation

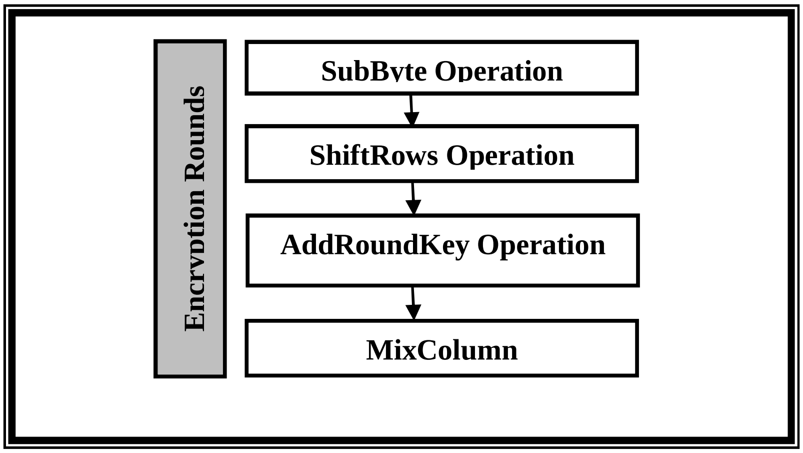
In this method, it is proposed to change the position of the shiftRows operation by exchange with SubByte operation in the sequence of AES operations. In this method, each block (16-byte) of plaintext is treated in the following sequence: the first, shiftRows operation, the second, subByte operation, the third, mixColumn operation, and finally, the four, addRoundKey operation. The figure (6) illustrates the structure of the change ShiftRows operation.



Figure(6) The Structure of The Change Shiftrows Operation.

5.2 The Second Method: The Change Mixcolumn Operation

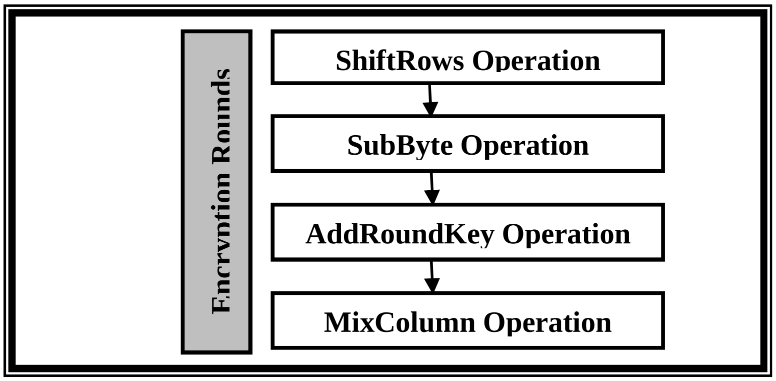
In this method, it is proposed to change the position of the mixColumn operation by exchange with AddRoundKey operation in the sequence of AES operations. In this method, each block (16-byte) of plaintext treated in the following sequence: the first, subbyte operation, the second, shiftrows operation, the third, addRoundkey operation, and finally, the four, mixcolumn operation. The figure (7) illustrates the structure of the change MixColumn operation.



Figure(7) The Structure of The Change Mixcolumn Operation

5.3 The Third Method: The Change Of Shiftrows And Mixcolumns Operations.

In this method, it is proposed to change the position of shiftrows operation and to change the position of mixcolumns operation. The change involves the position of shiftrows operation by exchange between the subByte and ShiftRows operations and the change the position of mixcolumns operation by exchange between addRoundKey and mixColumn operations. In this method, each block (16-byte) of plaintext treated in the following sequence: the first, shiftrows operation, the second, subbyte operation, the third, addRoundkey operation, and finally, the four, mixcolumn operation. The figure (8) illustrates the structure of the change shiftRows and MixColumn operations.



Figure(8) The Structure of The Change Shiftrows And Mixcolumn Operations.

6. Discussion and Experimental Results

This section containes an evaluation of diffusion property in the three proposed methods compared with diffusion of the standard AES. Diffusion property calculated by using hamming distance (HD), where the **HD** is a number of different symbols between two strings of equal length. In the run time of four previous methods for testing the change in the cipher value and measured hamming distance between input and output (current output) for each round. We suggested the message "firstmessagetoo!" as input for all methods that consist of 16 char which represent a one block and notice the changing. The following Table (2) shows a change in the cipher value and hamming distance for each round in the standard AES. Table (3) shows a change in the cipher value and hamming distance for each round in the first proposed method: the change ShiftRows operation.

Table (2): Change In The Cipher Value And Hamming Distance for Standard AES.

No. of Round	standard Method	
	Ciphertext (Hex)	Hamming Distance (bits)
1	3E255675EF266A0CC21B1E51C781D374	67
2	24EB9D7BF913E25FB653C646014F1027	58
3	C78C383894858F0701B1BDF078384986	74
4	49FFB7E0217CDA1D6D3FE0FC092F98AD	68
5	9753362C6E67712555CE6E0791DC7721	65
6	C879925FE44A172E93173CA8331BB606	66
7	5A0B6B2CA8429935B421E5123DDBA1E7	58
8	962F00B7E2FA68B8A8B778D973CDF261	61
9	708EB7A7DB1F1ED613C5791055391803	70

Table (3): Change In The Cipher Value And Hamming Distance for the Change ShiftRows Operation.

No. of Round	The Change ShiftRows Operation	
	Ciphertext (Hex)	Hamming Distance (bits)
1	ED929F833CE4E477AC6E592A7A3694F9	59
2	FA9EE9B1E2F55052BB04CFAF02B80338	64
3	D58EC022FA8FF6BA9A45E04432CEFD0B	54
4	9914046C9D8E6B42BC65B30CE7472B68	64
5	B0C1717882B857183AE1F141BE37CCC9	68
6	53B1B87096A87A5EFCD89EE631A67850	61
7	6133EF24F69C7F36E132CBA7CBA43A07	58
8	B23DBE5C2B84557CBBC342EE7DFB29C1	68
9	361DE10DD7C35412337D96766B47E69E	74

From the results explained in table(2) and table(3), we notice the hamming distance values in table(2) range from 58 bits to 74 bits, but the hamming distance values in table(3) are ranged from 54 bits to 74 bits. When shiftrows operation changed the position by exchange with subbyte operation, it caused less diffusion property. Therefore the sequence of operations in the AES standard obtained the best diffusion.

Table (4) shows a change in the cipher value and hamming distance for each round in the second proposed method: the change MixColumn operation.

Table (4): Change In The Cipher Value And Hamming Distance for the Change MixColumn Operation.

No. of Round	**The Change MixColumn Operation**	
	Ciphertext (Hex)	**Hamming Distance (bits)**
1	**ED929F833CE4E477AC6E592A7A3694F9**	**59**
2	**53B1B87096A87A5EFCD89EE631A67850**	**61**
3	**B23DBE5C2B84557CBBC342EE7DFB29C1**	**68**
4	**361DE10DD7C35412337D96766B47E69E**	**74**
5	**6133EF24F69C7F36E132CBA7CBA43A07**	**58**
6	**FA9EE9B1E2F55052BB04CFAF02B80338**	**64**
7	**B0C1717882B857183AE1F141BE37CCC9**	**68**
8	**D58EC022FA8FF6BA9A45E04432CEFD0B**	**54**
9	**9914046C9D8E6B42BC65B30CE7472B68**	**64**

From the results shown in table(2) and table(4), we notice the hamming distance in table(2) ranged from 58 bits to 74 bits but the hamming distance in table(4) ranged from 54 bits to 74 bits. When mixcolumn operation changed its the position by exchange with Addroundkey operation it caused less diffusion property. Therefore the sequence of operations in the AES standard obtained the best diffusion.

Table (5) shows a change in the cipher value and hamming distance for each round in the third proposed method: the change ShiftRows and MixColumn operations.

Table (5): Change In The Cipher Value And Hamming Distance for the change ShiftRows and MixColumn Operations.

No. of Round	The Change ShiftRows and MixColumn Operations	
	Ciphertext (Hex)	Hamming Distance (bits)
1	ED929F833CE4E477AC6E592A7A3694F9	59
2	FA9EE9B1E2F55052BB04CFAF02B80338	64
3	B23DBE5C2B84557CBBC342EE7DFB29C1	68
4	9914046C9D8E6B42BC65B30CE7472B68	64
5	6133EF24F69C7F36E132CBA7CBA43A07	58
6	53B1B87096A87A5EFCD89EE631A67850	61
7	B0C1717882B857183AE1F141BE37CCC9	68
8	D58EC022FA8FF6BA9A45E04432CEFD0B	57
9	361DE10DD7C35412337D96766B47E69E	74

From the result explained in table(2) and table(5), we notice the hamming distance in table(2) ranged from 58 bits to 74 bits but the hamming distance in table(5) ranged from 57 bits to 74 bits. When mixcolumn operation changed its the position by exchange with Addroundkey operation it caused less diffusion property. Therefore the sequence of operations in the AES standard obtained the best diffusion.

Table (6) illustrates the comparison of hamming distance for the different proposed methods.

Table (6) The Comparison of Hamming Distance for the Different Methods.

No of Round	Hamming Distance (bits)			
	Standard AES	The Change Shiftrows Operation	The Change Mixcolumns Operation	The Change Shiftrows& mixcolumn Operations
1	67	59	59	59
2	58	64	61	64
3	74	54	68	68
4	68	64	74	64
5	65	68	58	58
6	66	61	64	61
7	58	58	68	68
8	61	68	54	57
9	70	74	64	74

when hamming distance value is increased, the diffusion of bits in ciphertext is increased and become a more secure for encryption algorithm. For example, see round 3 in table (5) hamming distance for standard AES is 74 bits (total number of differ bits between original message and ciphertext of round three) from 128 total number of bits (message length is equal to 16-byte), hamming distance for shiftrows first method is 54 bits from 128 total number of bits, hamming distance for Mixcolumns first method is 68 bits from 128 total number of bits, and hamming distance for Mixcolumns and shiftrows first method is 68 bits from 128 total number of bits.

From the results above, we notice the hamming distance values differ for the three proposed methods but we have the same percentage value (49.5%) of the diffusion property which means (49.5 %) of input bits exchange in the output for obtain a secret message and cannot be attacked by any attacker. In the standard AES, percentage value is (50.9%) of the diffusion property. From the testing it may be concluded that AES algorithm is the best sequence of operations to achieve the best confusion and diffusion of data.

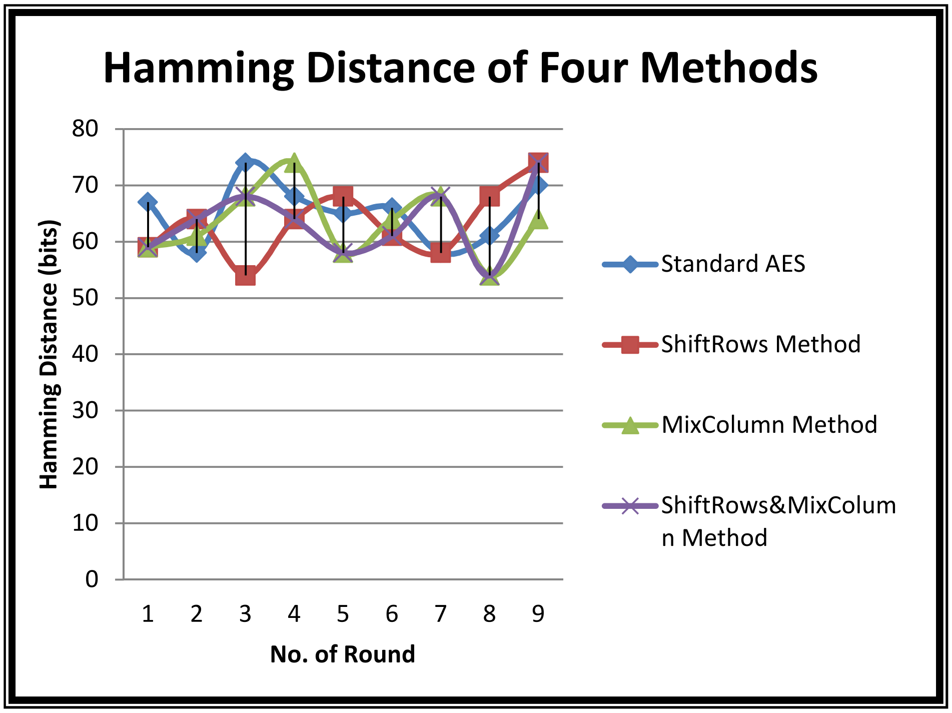


Figure (9) Hamming Distance of Standard Method and Proposed Methods (bits per Round).

7. Conclusions

This paper shows the efficiency of Advanced Encryption Standard (AES) algorithm by comparison with AES algorithm in three proposed methods. The proposed methods are based on a different sequence of operations of Advanced Encryption Standard (AES) algorithm. In the first method, the position of shift rows operation changed, in the second method, the position of mix columns operation changed, and finally in the third method, the position of shift rows operation changed and also the position of the mix columns operation changed. Diffusion property was calculated by using hamming distance (HD) which the HD is a number of different symbols between two strings of equal length. The obtained results from using these proposed methods have the same result for the three proposed method. We obtained approximately (63 bits) change in each round corresponding to the total number of bits (128 bits). The standard AES obtains approximately (65 bits) change in each round corresponding to the total number of bits (128 bits). We used hamming distance for calculating diffusion property of the (49.5%) percentage value of the proposed methods and the (50.9%) percentage value of the standard AES.

REFERENCES

[1] Douglas Selent," **Advanced Encryption Standard**", InSight: Rivier Academic Journal, Volume 6, Number 2, Fall 2010.

[2] Shay Gueron," **Intel Advanced Encryption Standard (AES) New Instructions Set**", Intel Corporation, 2012.

[3] Stallings W., "**Cryptography and Network Security: Principles and Practice**", Prentice Hall, 2011.

[4] Federal information processing standards publication 197,"**Advanced Encryption Standard**", Available at http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, 2001.

[5] Shize Guo, Xinjie Zhao, Fan Zhang, Tao Wang, Zhijie Shi, Francois-Xavier Standaert, Chujiao Ma. ,"**Exploiting the Incomplete Diffusion Feature: A Specialized Analytical Side-Channel Attack against the AES and its Application to Microcontroller Implementations** ", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 2013.

[6] R.Elumalai, Dr.A.R.Reddy**," Improving Diffusion Power of AES Rijndael with 8x8 MDS Matrix",** International Journal of Scientific & Engineering Research Volume 2, Issue 3, 2011.

[7] Mohan H.S., A. Raji Reddy, and Manjunath T.N**," Improving the Diffusion power of AES Rijndael with key multiplication",**International Journal of Computer Applications (0975 – 8887) Volume 30– No.5, 2011.

[8] Raj Jain," **Block Ciphers and DES**",2011, available at:

http://www.cse.wustl.edu/~jain/cse571-11/

[9] David Basin and Ueli Maurer, "**The Block Cipher Companion**", Springer, 2011.

[10] Kaderali I. F., "**Foundations and Applications of Cryptology Symmetric and Asymmetric Encryption, Digital Signatures, Hash Functions, Key Management and PKI**", 2007, available at https://www.kaderali.de/fileadmin/vorlesungsskripte/Buch_Crypto_A4.pdf

تحليل تأثير خوارزمية التشفير المتقدم القياسية على خاصية الانتشار

أ.م.د. حسنين سمير عبدالله*, أ.م.د. مها عبدالكريم حمود*, م.دلال نعيم حمود**

المستخلص

في التشفير, التشويش والانتشار تعتبران خاصيتان مهمتان, لذلك يجب ان تتحقق هذه الخاصيتان في النص المشفر للحصول على نص مشفر قوي وبنفس الوقت نمنع اي مهاجم من محاولة هجوم النص المشفر ومحاولة كشف النص الصريح. يهدف هذا البحث الى اقتراح ثلاثةطرق تعتمد على تغيير ترتيب العمليات في خوارزمية التشفير المتقدم القياسي. كذلك تم استخدام المسافة المبالغة حيث هو مقياس يعتمد على ايجاد العدد الكلي للبتات ذات القيم المختلفة في نصبين متساويين بالطول. الطرق المقترحة حصلت تقريبا على (63 بت) تغيير في كل دورة من دورات الخوارزمية بالنسبة للعدد الكلي (128 بت). لكن خوارزمية التشفير المتقدم القياسية كانت النتيجة (65 بت). في هذا البحث تم استخدام مقياس المسافة المبالغة في حساب خاصية الانتشار والنتيجة لكل الطرق المقترحة هي (49,5 %) والنتيجة بالنسبة الى خوارزمية التشفير المتقدم القياسية (50,9%). بعد الاختبار والتحقق نستنتج بان خوارزمية التشفير المتقدم القياسية هي افضل ترتيب للعمليات مما يحقق افضل تشويش وانتشار للبيانات.

*قسم علوم الحاسوب - الجامعة التكنولوجية.

**قسم علوم الحاسوب – جامعة النهرين.