Design for Scientific RENAISSANCE

Modification AES algorithm based on Extended Key and Plain Text

Ahmed Tariq Sadiq, Faisal Hadi Faisal
Computer Sciences Department
University of Technology
drahmaed_tark@yahoo.com, myemail_welcome@yahoo.com

ISSN: 2231-8852

ABSTRACT

Encryption is important for keep to confidential data. There are many of encryption algorithms to ensure the data, but should be the select the algorithm depended on the fast, strong and implementation. For that choose the advance encryption standard (AES) algorithm for encryption data because speed and easy implementation on small devices and some the feature for it. In this paper, a modification AES algorithm is presented within five proposals, the first modification is an extended plain text 4x4 for AES from 16 bytes to 64 bytes (8x8 array) this modified increase speed encryption, more security and increase complexity, second modification is an extended keys by change the key length that used from 176 bytes to 704 bytes for encryption and decryption process because change input state this involves key length, change key length is give more robust to encryption and more complexity, third modification is shift row stage by increment number of shift in each row and number of shift based on part of key, this modification because increase number of row and column in state input, fourth modification in mix column stage by change the static matrix to four separated matrix used for multiple input state this modified to increase the diffusion in data, and five modification in add round key stage by make it based on part of key to determent the number of sub key used with input state in XOR operation. Modifications process focused on the way increment the random sequence process inside algorithm by used some parts of key in development process.

Keywords: **AES, Block Cipher, Extended Key, Extended Plain Text, Cascaded Keys**.

1- Introduction

Information security very important for protect the confidential data form unauthorized access. The data contents (image, audio, text, video,), are considered the very important parts in the computer and protect this data based on encryption. Encryption data facilitate to convert the clear data to unintelligible data. There are many of algorithms encryptions used to encryption data, but the large size of data will be encryption are consider main challenges for this algorithms therefore should be choice one of them based on fast computation and more complexity because the large size of data and non-ability to broken, So the better algorithm is the advance encryption standard (AES) (Pravin Kawle, et al., 2014). The AES algorithm is block cipher that can be encrypts data of block size 128 bits. It uses symmetric private key for encryption and decryption, and the key size are 128 bits,192 bits or 256 bits, this key length is determent type AES is used, thus determent number of rounds used inside AES (10,12,or 14) rounds(Luminiţa Scripcariu, et al., 2012). Implementation cost of AES is very a few so, can be used for small devices with emphases high security.

In this paper, modified AES for increases speed computation process for encryption and decryption, and efficiency of security of file encryption (Saurabh Kumar, 2013).

2- Related work

There are several modified in AES to improve speed the performance, increase the security and addition same complexity on algorithm steps. The reason development is appeared many different the implementation on software and hardware. Each implementation has need to modified AES according to the specific proposes.

In (Luminiţa Scripcariu, et al., 2012) a modified AES by used longer key length and data matrix. That extended the data matrix to 8 row and variable number of column (6, 8, 12 and 16) the input data block (48, 64, 96 and 128), and extended the key length to (384,512, 768 and 1024). This paper not change the first and fourth stages (substitution byte, Add Round Key) , third stage shift row change from shift third row to seventh row shifted left and four stage (mix column) change the static matrix 3x3 to new matrix 8x8, should be calculate inverse static matrix used in Mix column on GF(2^8). This modification is increase robustness and use a few time for encryption and decryption processing.

In (Pravin Kawle, et al., 2014) modified the AES algorithm by reduce the calculation, computation overhead, and reduce the time encryption process. It replaces the mix column stage in AES algorithm into permutation stage (like the permutation table (IP) that used in DES algorithm) because the mix column is take large calculation time and that makes the encryption process are slow. The other stages in AES algorithm don't change.

In salim M.wadi, et al. (2013) modified AES by used three modification . first change the shift row stage only, The change depended on the first byte in state matrix if the byte is even the second and third row are shifted left one and two times respectively, else the second and fourth row are shifted left, second decreasing the number of round from 10 to one round only, this modification is enhance performance of AES and reduce time processing, and finally modification used simple S-box for encryption and decryption to reduce the computation amount, the new S-box has some properties , simple generation and same S-box used for encryption and decryption.

3- The advance encryption standard (AES):

AES is symmetric algorithm and consider one of type the block cipher. It widely used in several industry standards and is used in many commercial systems like (IPsec, the internet Skype, the IEEE 802.11i and TLS …). AES is defined as AES-128, AES-192 or AES-256 that name depended on key length is used in the encryption. The size of data matrix is 128 bits and having 10, 12 & 14 rounds depended on key length. AES operator on special math-ematical called the Galois filed (256) with the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$, this mathematical use in s-box, mix columns and also used in create the key. It consists four different stages (Add round key, substitution, shift row and mix column) (Christof Paar, et al., 2010). Figure (1) illustrates AES block diagram process (Vishal Pachori, et al.,2012).

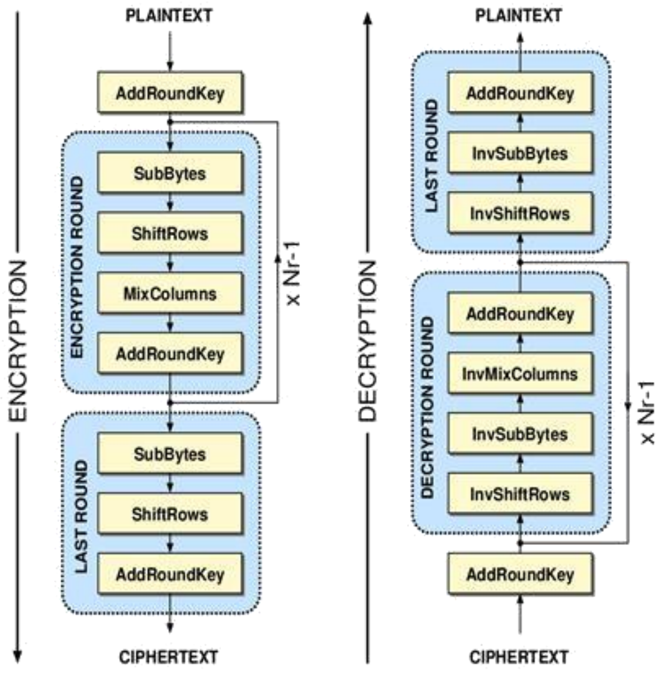


Fig.1 AES block cipher

3.1 Substitution byte:

In this stage, each byte replace with another byte by using s-box. The s-box operation provides the non-linearity to encryption data, its used the multiplicative inverse over GF(2^8) to contract S-box. The GF(2^8) know as good non –linearity properties for to avoid attack (Christof Paar, et al., 2010). See the figure (2) illustrate substitution byte process (Stallings W.2011).

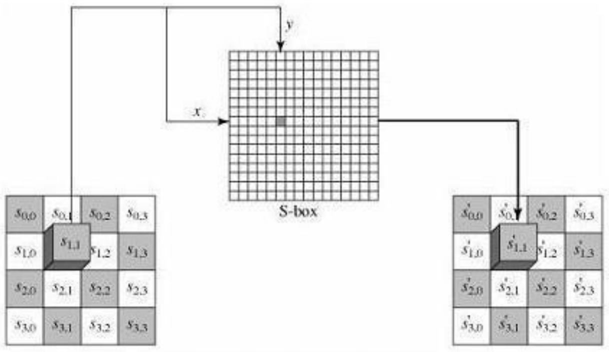
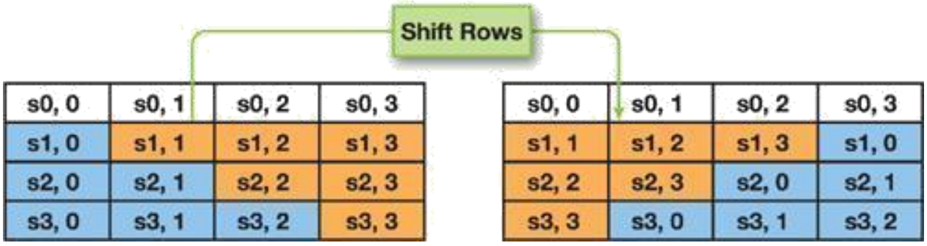

y
x
S-box
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{1,1}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

Fig. 2. Substitution byte

3.2 Shift row:

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 two bytes to left and the fourth row shift three bytes to left see the figure (3) (Arrag S. et al.,2013).



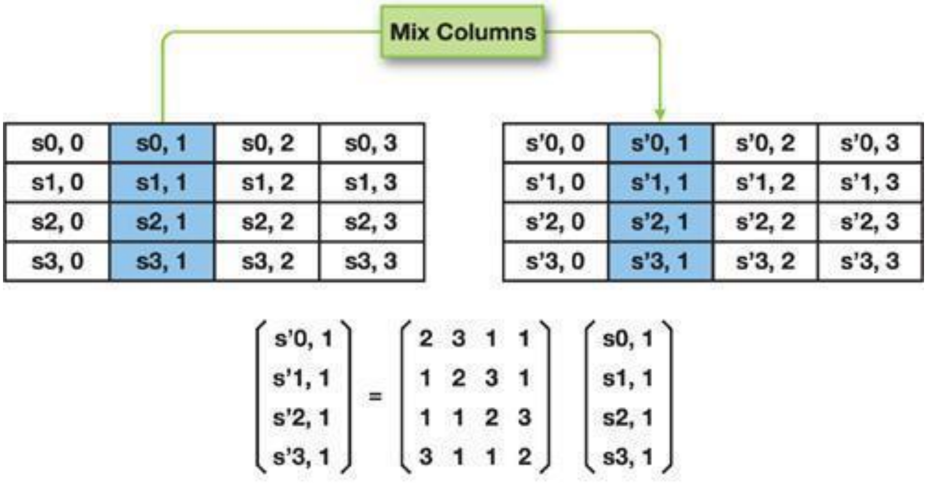
s0, 0	s0, 1	s0, 2	s0, 3
s1, 0	s1, 1	s1, 2	s1, 3
s2, 0	s2, 1	s2, 2	s2, 3
s3, 0	s3, 1	s3, 2	s3, 3

s0, 0	s0, 1	s0, 2	s0, 3
s1, 1	s1, 2	s1, 3	s1, 0
s2, 2	s2, 3	s2, 0	s2, 1
s3, 3	s3, 0	s3, 1	s3, 2

Fig. 3. Shift Row

3.3 Mix column:

In this stage, transfers map of each column of input data matrix to a new column in output data matrix. Every one input column considered as a polynomial vector above GF (28) and that multiplied with constant matrix .the multiplied operator used polynomial mathematical see the figure(4) (Arrag S. et al.,2013)..



s0, 0	s0, 1	s0, 2	s0, 3
s1, 0	s1, 1	s1, 2	s1, 3
s2, 0	s2, 1	s2, 2	s2, 3
s3, 0	s3, 1	s3, 2	s3, 3

s'0, 0	s'0, 1	s'0, 2	s'0, 3
s'1, 0	s'1, 1	s'1, 2	s'1, 3
s'2, 0	s'2, 1	s'2, 2	s'2, 3
s'3, 0	s'3, 1	s'3, 2	s'3, 3

$$\begin{pmatrix} s'0,1 \\ s'1,1 \\ s'2,1 \\ s'3,1 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} s0,1 \\ s1,1 \\ s2,1 \\ s3,1 \end{pmatrix}$$

Transform Matrix of Mix Columns

Fig. 4. Mix Column.

3.4 Add round key

In this stage, combined between data matrix 16 byte and sub key matrix derived from original key matrix by key expansion. The combine process by XOR operation each byte from data and sub key.

4- key Expansion

Convert the initial matrix 16 byte to 4 words and take as input, Each word generation new word until 44 words and used every 16 bytes with 16 bytes data matrix in Add Round Key stage) (Christof Paar, et al., 2010)..

To execute key expansion there are three functions:

1. rotate word: only rotate the word.

2. Substitution: replace the byte by using s-box.
3. Rcon :XOR the result from step 2 with constant matrix.

The figure (5) below describe the process) (Christof Paar, et al., 2010).

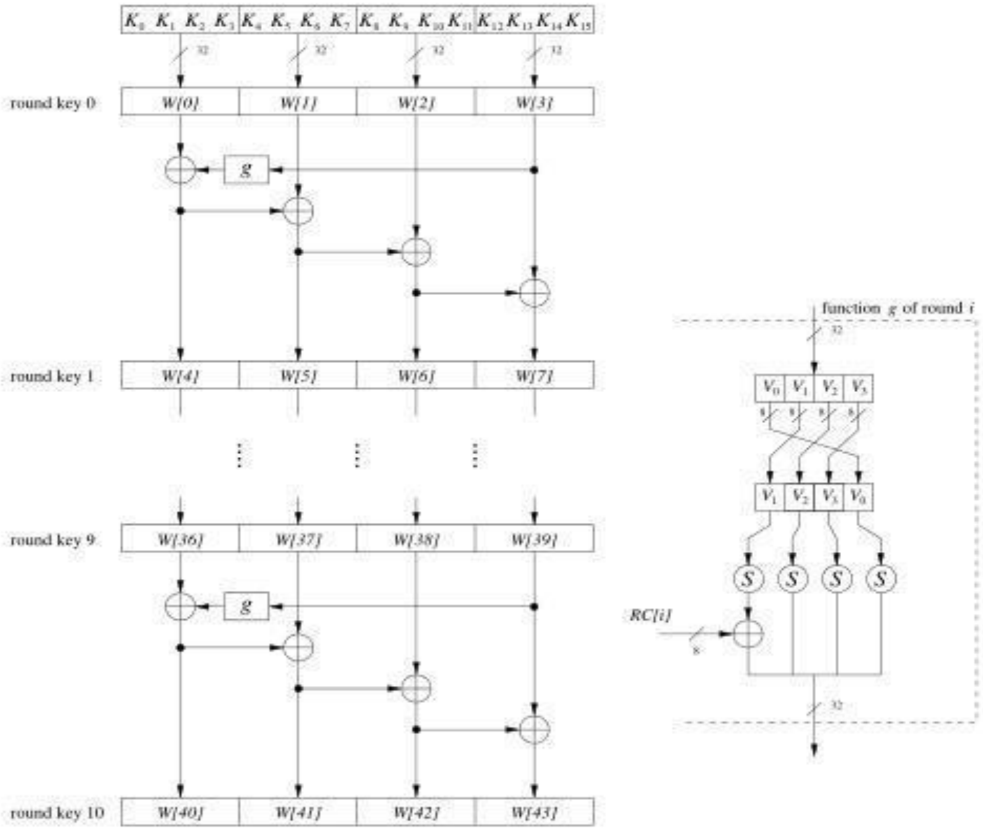


Fig. 5. Key Expansion

5- The proposed AES modification

The proposed enhance the AES algorithm to increase the robustness and speed of encryption and decryption data. For that, take several changes in AES by used longer key encryption and longer data matrix encryption for increase the speed encryption process with algorithm complexity.

The modified AES by extended the data matrix from 4x4 (16 bytes) to 8x8 (64 bytes) and change the key length from (176) bytes to (704) bytes for encryption data. In AES classic the key used only with one stage (add round key), in modified AES also used the part of key in second stage (shift row), also use part of key to mapping the XOR process between key and data matrix (add round key) and update the (max column) stage by using four separated matrixes to multiple with data matrix. Discuss the modification details in this paper, for that, the modified in three stages are (Add Round Key, Shift Row, and Mix Column) and modified key expansion. The key Expansion update by using extended key, repeated generation process key fourth times with replace the initial value in every generation. The initial value depended on the old key.

5.1 The modification AES and Key Expansion:

5.1.1 Extended input size:

To increase the robustness of the AES, extended the data matrix and key matrix. The data matrix is extended to 8x8 matrix instead of 4x4 matrix and key matrix is extended to same size. This extended is also increase the speed of encryption process. See figure (6).

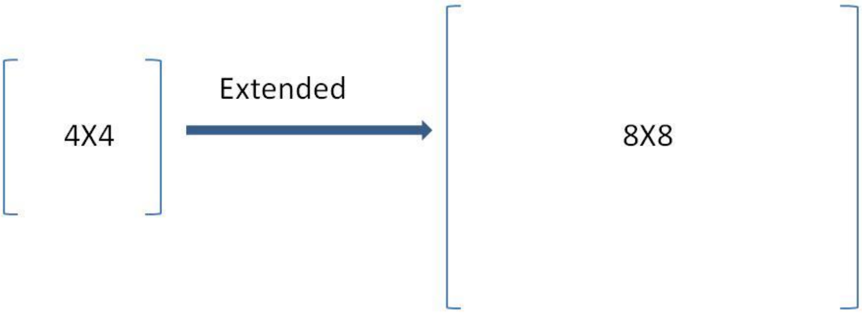


Fig. 6. Data matrix

5.1.2 Key to key mapping:

In this stage modified Add round key stage by using part of key to determent the sequence key matrix well used in XOR operation. The parts of key matrix most to be 11 matrixes. Each matrix contains values less than 12 because the number of key matrixes is 11 matrixes see figure (7), to achieve this by using mod operation.

Key sequence [I] = key[i] mod 12.(ex: parts of keys sequence are 3,7,1..etc, this determent the first key matrix is used in XOR operation between key matrix and data matrix is third key matrix , second matrix is seventh key matrix , third matrix is first key matrix and so on).

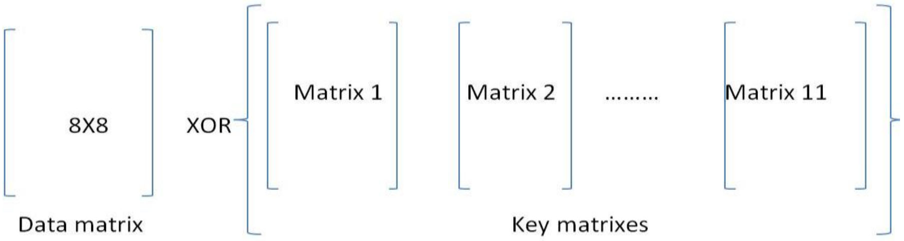
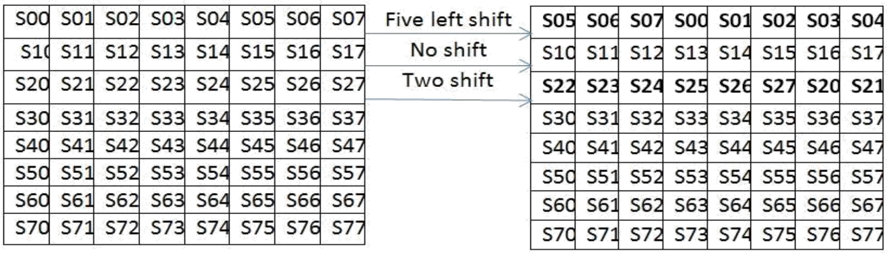


Fig. 7. Key to key mapping

5.1.3 Key based shift row:

In this stage modified the shift row, After extended data matrix from 4x4 to 8x8 matrix, shifted 8 row instead of 4 row. Also the number of shift depended on parts of keys. The parts keys array are 80 bytes and most be values less than 8 because the number of column is 8 and number of shift equal 8 bytes only. To calculate this by using (shift array [i]=key[i] mod 8).Ex: the parts key sequence are 5,0,2 ..etc., the first row in data matrix is shift left are 5 times ,the second row no shifted because the value is zero and third row is shift left two see figure (8) .



S00	S01	S02	S03	S04	S05	S06	S07
S10	S11	S12	S13	S14	S15	S16	S17
S20	S21	S22	S23	S24	S25	S26	S27
S30	S31	S32	S33	S34	S35	S36	S37
S40	S41	S42	S43	S44	S45	S46	S47
S50	S51	S52	S53	S54	S55	S56	S57
S60	S61	S62	S63	S64	S65	S66	S67
S70	S71	S72	S73	S74	S75	S76	S77

S05	**S06**	**S07**	**S00**	**S01**	**S02**	**S03**	**S04**
S10	S11	S12	S13	S14	S15	S16	S17
S22	**S23**	**S24**	**S25**	**S26**	**S27**	**S20**	**S21**
S30	S31	S32	S33	S34	S35	S36	S37
S40	S41	S42	S43	S44	S45	S46	S47
S50	S51	S52	S53	S54	S55	S56	S57
S60	S61	S62	S63	S64	S65	S66	S67
S70	S71	S72	S73	S74	S75	S76	S77

Fig. 8. Example shift row

5.1.4 4x4 separated mix column:

Mix column in AES classical algorithm is multiple the data matrix 4x4 with static matrix 4x4. In AES modified have four different static matrixes, each one of them is multiple with parts of extended data matrix 4x4 figure (9) illustrate separated mix column.

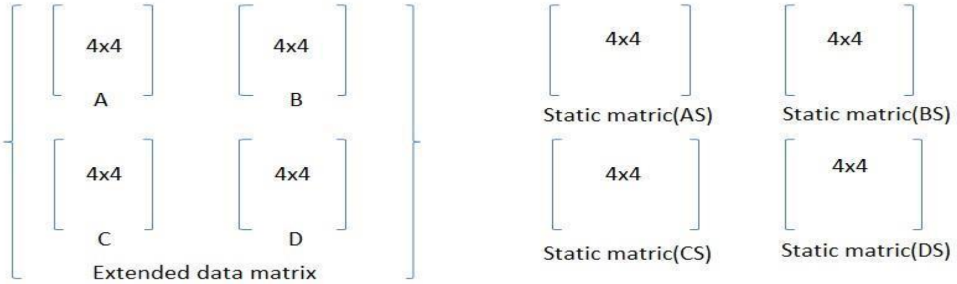


Fig. 9. Separated mix column

In this figure the matrix A is multiple with matrix AS, the matrix B is multiple with matrix BS, the matrix C is multiple with matrix CS and the matrix D is multiple with matrix DS.

5.1.5 Cascaded Key extended:

Key extended from 176 bytes to 704 bytes because extended data matrix from 16 bytes to 64 bytes. The extended process by repeated four times same algorithm for generation key, with used different initial for every time. The initial that used result XOR operation between last previous key matrix and any key matrix (in this modified used five matrix) see this figure (10).

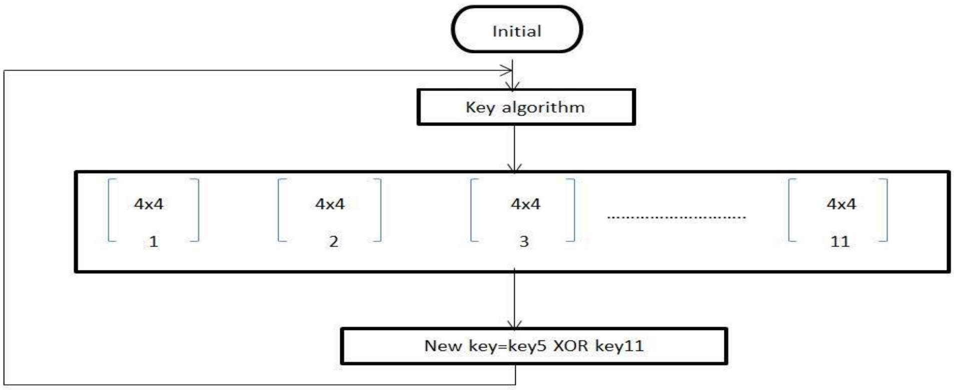


Fig. 10. Cascaded Key extended

6- Experiment Result:

To test the performance modified AES algorithm. The performance of the modified AES algorithm is done by taking three different size text file for compare the speed encryption process between AES algorithm and modified AES.

Table1 show compare between both.

Note: the result is different according to mobile device.

Table 1: Comparison of AES and modified AES algorithms

File size	*AES*	*Modified AES*
128k	00:00:00:233	00:00:00:84
256k	00:00:00:607	00:00:00:156
512k	00:00:00:887	00:00:00:204

7- Conclusion:

The modification AES algorithm has more robustness, more security, more complexity and increase the speed encryption process. The modification focus on convert the sequence steps in AES classic algorithm to random steps inside modified AES algorithm by depended on some parts of keys. Step sequence in Shift Row is shift left second, third and fourth row by constant value, in modified the Shift Row the number of left shift is unknown because the number of shift depended on part of key value. Also step sequence in Add Round Key is XOR between data matrix and sequence sub key is constant (11 sub key), in modified the sequence sub key is random because sub key depended on part of key value. This random steps increase the confusion and diffusion in data encryption. The Mix Column modification is used four constant matrix instead of one matrix in multiplication, thus, increase the diffusion in data encryption. And finally extended the key length and data matrix to increase the strong encryption process, and whenever key length and data matrix are longer, the difficult analysis cipher text by attacker because the data encryption be complexity.

References

Kawle P., Hiwase A., Bagde G., Tekam E., and Kalbande R. (2014), Modified Advanced Encryption Standard, research paper, International Journal of Soft Computing and Engineering (IJSCE) vol. 4 Issue-1.

Scripcariu L., and Frunza D. Mircea (2012), Modified Advanced Encryption Standard, research paper, 11th International Conference on DEVELOPMENT AND APPLICATION SYSTEMS Vol. 2, Issue 3.

Saurabh Kumar. (2013). VLSI IMPLEMENTATION OF AES ALGORITHM. Department of Electronics and communication Engineering. National Institute of Technology. Rourkela .

Salim M. Wadi and Nasharuddin Zainala. (2013). Rapid Encryption Method Based on AES Algorithm for Grey Scale HD Image Encryption. The 4th International Conference on Electrical Engineering and Informatics (ICEEI).

Christof Paar and Jan Pelzl.(2010). Understanding Cryptography A Textbook for Students and Practitioners. Springer-Verlag Berlin Heidelberg .

Vishal Pachori, Gunjan Ansari, Neha Chaudhary (2012), Improved Performance of Advance Encryption Standard using Parallel Computing, International Journal of Engineering Research and Applications (IJERA) ,Vol. 2, Issue 1.

Stallings W.2011, Cryptography and Network Security Principles and Practice, 5th Edition.

Arrag S., Hamdoun A., Tragha A., and Khamlich E. Salah (2013), Implementation Of Stronger AES By Using Dynamic S-box Depended Of Master Key , Journal of Theoretical and Applied Information Technology Vol. 53 No.2 .