An Enhancement Method Based on Modifying CFB Mode for Key Generation in AES Algorithm

Dr.Hasanen S. Abdulah
Computer Sciences Department, University of Technology/ Baghdad
Dr.MahaA.Hamood Al-Rawi
Computer Sciences Department, University of Technology /Baghdad
Dalal N.Hammod
Science College, University of Al-Nahrain /Baghdad
Email:dal_scin81@yahoo.com

Received on:4/11/2015 & Accepted on:24/11/2016

ABSTRACT

There are two very important characteristics in the block cipher, the amount of time for encryption process and key complexity which caused increasing the complexity of encryption process. This research aims to enhance the key generation of Advanced Encryption Standard (AES) algorithm with high efficiency. The proposed enhancement method architecture based on modifying cipher feedback (MCFB) mode which produce key block from each key generation step in addition to represent current output that is repeated lyre used as input to produce next key block. In the block cipher encryption step, two processes are implemented: Substitution bytes process and Shift rows process. This proposed method improves the performance, efficiency, and speed of the encryption algorithm.

Keywords: Advanced Encryption Standard; Key Generation; Mode Operation; Cipher Feedback.

INTRODUCTION

The AES algorithm is an advanced model of DES. 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), presents the variable number of rounds (number of rounds depending on key length and block size)[1].

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, Shift Rows, Mix Columns, and Add Round Key [2].
In ciphering algorithms, schedule key is very important phase. A strong cipher dependent on the strong schedule key that would be more resistant to different types of attacks, such as linear and differential cryptanalysis [3].

https://doi.org/10.30684/etj.34.6B.5
2412-0758/University of Technology-Iraq, Baghdad, Iraq

Related Work

There are many achievements occurred in the field of encryption by AES, each suggests new method for developed AES. The most useful ones are mentioned in the following:

Deguang Le. et. al., "Parallel AES Algorithm for Fast Data Encryption on GPU", 2010 [4]

The researchers proposed a new algorithm for AES parallel encryption based on technologies of GPU parallel computing that designed and implemented a fast data encryption system. The test proves that proposed approach can accelerate the speed of AES encryption significantly**.**

P Penchala Reddy, et. al., "Implementation of Multi-Mode AES Algorithm Using Verilog", 2014 [5]

The researchers present implementation of three modes ECB, CBC, and CTR modes AES algorithm that implemented with 128-bit plaintext, 192, and 256 bits key lengths. Each program results are verified with Model Sim PE and are synthesized in Xilinx ISE 9.2i. These results are useful for important hardware.

ShathaHabeeb,"Proposal for Complex AES Security using key Generator and text Permutation", Eng. & Tech. Journal Vol.3 No.12, 2012[6]

The researcher proposed a technique intended to make AES safer and secure which the generation of random key and permutation key sites in each round. Also, the researcher proposed permutation the plaintext before entering the encryption and inverse permutation for resulting cipher text.

Confusion and Diffusion [7]

The encryption process of block cipher depends on integrated confusion and diffusion. Confusion is a measure of the statistical properties of the input with relation to the output. While diffusion attempts to extend the influence of the input symbols in order to disguise the tendencies of the input. A successful diffusion can be applied using a shift rows which exchanges individual bytes locations. A well diffused cipher will satisfy the strict avalanche criteria. Confusion can be achieved by substitution to each value in the block by a new value from S-box table. Figure (1) explained S-box table.

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure (1) S-box table

Modes of Operation [8]

A mode of operation explains the application of cipher's single-block operation repeatedly (fixed-length group of bits called *a block*) to transform amounts of data securely larger than a block to achieve important services such as confidentiality or authenticity. In different modes of operations, to randomize encryption and produce distinct cipher text, we can use starting variable (SV) or initialization vector (IV) that is represented as a block of bits even if multiple times encrypted the same plaintext, without needing to the re-keying process. Messages come in a variety of lengths then block cipher applies on block that has a fixed size. Padded process is required for ECB and CBC modes before encryption by several padding schemes. The simplest way is adding null bytes to the plaintext to obtain its length up to a multiple of the block size. There are many types of operation modes that explain in the following:

ECB mode

Electronic Codebook (ECB) mode is the most simple of the encryption modes. The message is divided into blocks and each block is encrypted separately.

CBC mode

Cipher Block Chaining (CBC) mode in vented by IBM in 1976.In this mode, each block of plaintext is treated by XORed process with the previous block of cipher text before being encrypted. Each cipher text block depends on all plaintext blocks processed up to that point. When using an initialization vector in the first block to make each message unique.

OFB mode

The Output Feedback (OFB) mode makes a block cipher into a synchronous stream cipher. It generates key stream blocks, and cipher text obtained by XORed process between plain text blocks and key stream blocks. Flipping a bit in the cipher text produces a flipped bit in the plaintext at the same location such as other stream ciphers,. This property allows many error correcting codes to function normally even when applied before encryption.

CFB mode

The Cipher Feedback (CFB) is a mode of operation for a block cipher. Block cipher means encrypts a set of bits of plaintext at a time, it is at times desirable to encrypt and transfer some plaintext values instantly one at a time, for which cipher text feedback is a method. In this mode used an initialization vector (IV) like cipher block chaining (CBC).

$C_i=E_k(C_i \oplus P_i$ ….(1)

$P_i=D_k(C_{i-1} \oplus C_i$ ….(2)

Where, C_0=IV (initialization vector)

CFB uses a block cipher as a component of a random number generator. In CFB mode, the previous block of cipher text is encrypted and the output is XORed process with current plain text block to create the current cipher text block. The XORed operation conceals plaintext patterns, the diagram of CFB mode shown in Figure (2).

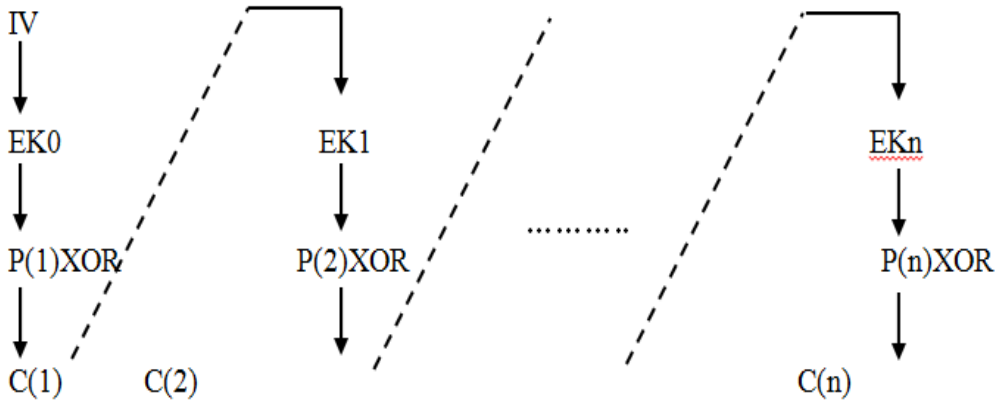


Figure (2) Diagram of CFB Mode

Where, IV represents initialization vector, EK0 represents encryption process by key 0, P(1)XOR implemented XOR operation between plaintext 1 and the result from EK0, and C(1) represented cipher text.

In common cryptographic applications, feedback modes are much interest and much faster since dedicated stream ciphers, Cipher Feedback (CFB) mode encryption process and decryption process shown in Figure (3).

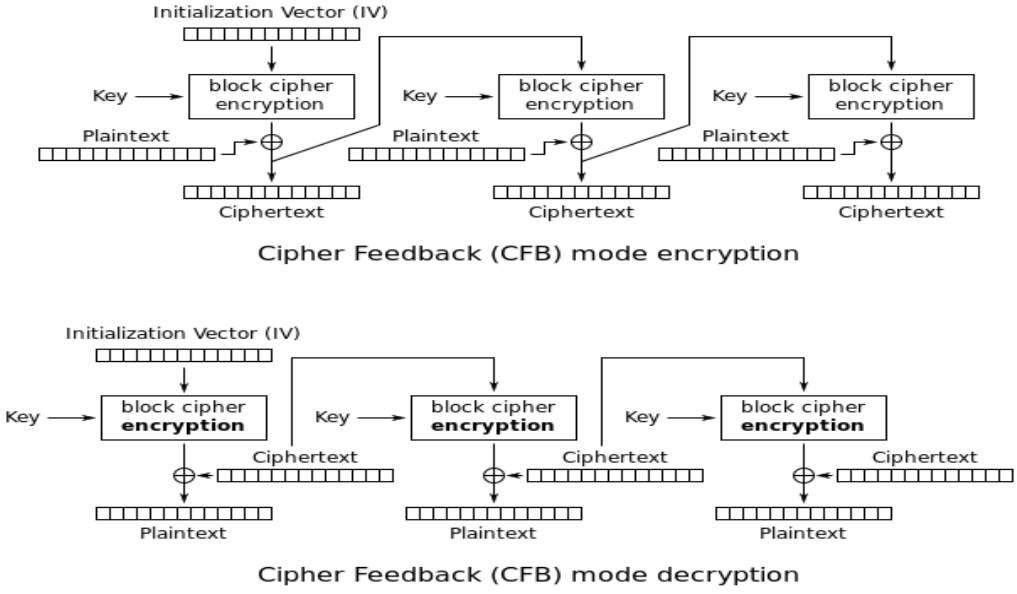


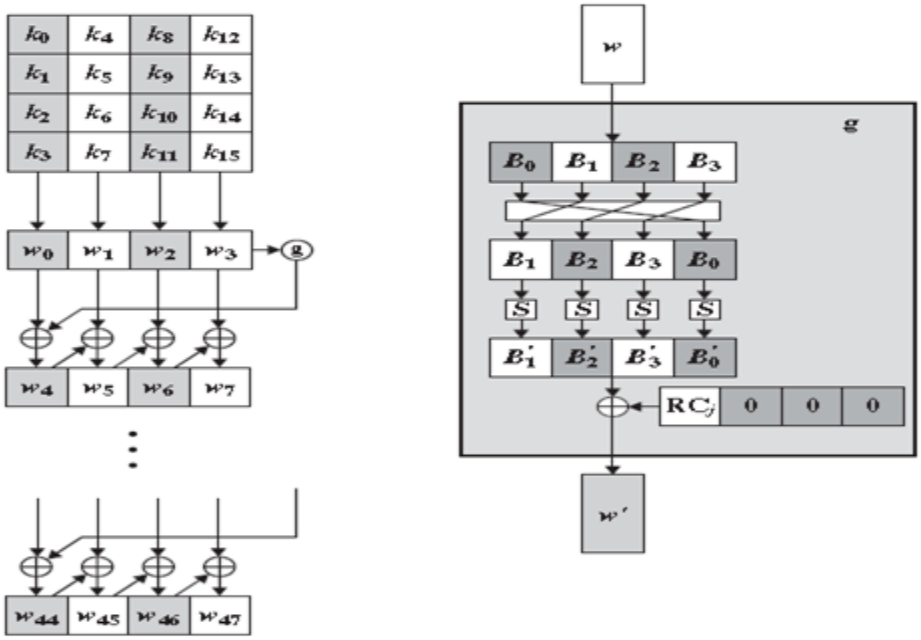
Figure (3) CFB Mode Encryption Process and Decryption Process [9]

Description of Key Scheduling Algorithm [1]

In AES algorithm a critical process is called *key expansion process* that uses a Cipher Key K to generate a key schedule. Where key scheduling generates (Nr+1) round keys based on original single key, see Figure (4). Key generated steps explain in below:

1. Taken the last column of master key (16-byte represented original key) and move the top byte to the bottom.
2. A substitution runs for each byte.
3. Apply the XOR to the column with a "round constant"(RCj, 0, 0, 0) that is different for each round.
4. Apply the XOR between results of step 3 with the first column of the previous round key.

In this work the enhancement method will be performed to assist in scheduling process of the key ciphering.



(a)Overall algorithm **(b) Function g**

Figure (4) Expansion Key in AES

Description of an Enhancement Method of Key Generation

This section explains enhancement method of key generation in AES and describes each stage of it in details. Enhancement method of key generation is generated a block of encryption key and the same method used to generate decryption key by keeping only master key (16-byte represented original key that used for expansion). This method is based on modified CFB mode where master key represented as the initialization vector (IV). The initialization vector (IV) forwarded to a block cipher encryption (BCE). BCE consist of two processes: substitution process and shift rows process. Then, the output of the BCE treated as XORed with IV (input key block) to produce the one key block, as shown in Figure (5). This process was repeated to (Nr+1) times to produce a complete key blocks, as shown in Figure (6). The following algorithm describes An Enhancement Method of Key Generation.

Algorithm: An enhancement method of key generation
Input: master key (16-byte original key)
Output: encryption key (complete key blocks)
Begin
Step1: for i=1 to 11 do
Begin

Step1.1: copy master key to key1.
Step1.2: substitution process for each byte in the key1.
Step1.2: shift rows process for each row in the key1.
Step1.3: XOR process between key1 and master key and save result at key2.
Step1.4: save key2 as a one block of encryption key.
Step1.5: set key2 as master key.
End
Step2: return blocks of encryption key.
End.

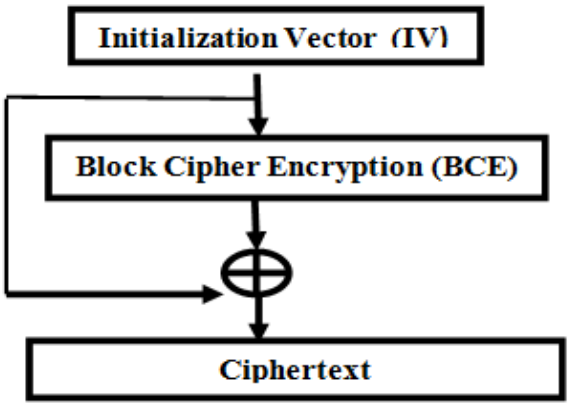


Figure (5) MCFB Mode to Produce One Block Key

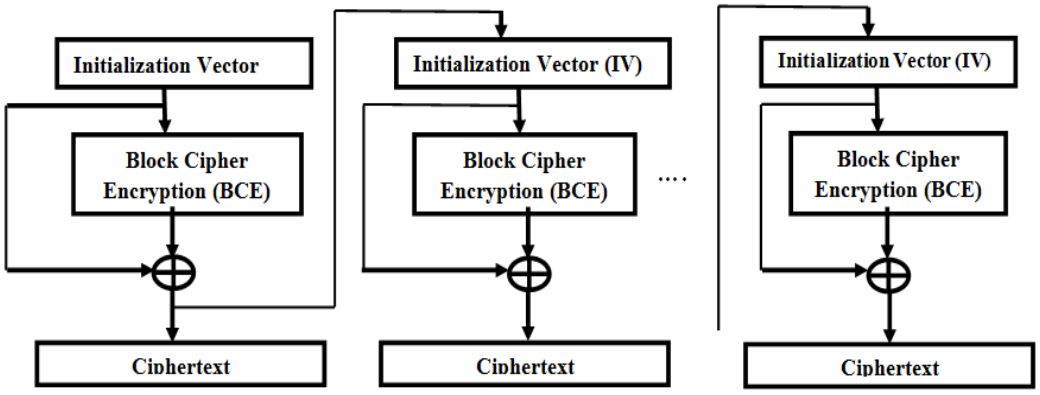


Figure (6) MCFB Mode to Produce a Complete Key Blocks

Block cipher encryption (BCE) consist of two operations: Substitution bytes process and Shift rows process, as shown in Figure (7), the following sections describes each process in details.

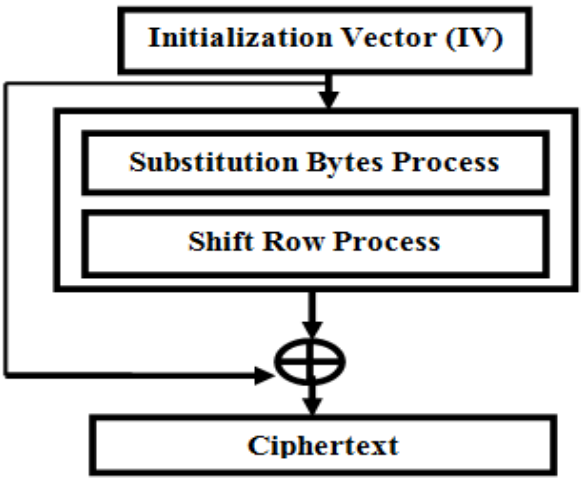


Figure (7) Block Diagram of the BCE

Substitution Bytes Process

In this process used S-box matrix that defined by AES algorithm which contains a permutation of all possible 256 8-bit values. Each byte in the key block is mapped into a new byte in the following way: by division byte in to two parts each part consists of four bits: The left part (4 bits of a byte) is represented as a row value and the right part (4 bits of a byte) is represented as a column value. Row value and column value represent as indexes into the S-box to select a unique 8-bitoutput value, as shown in Figure (8).

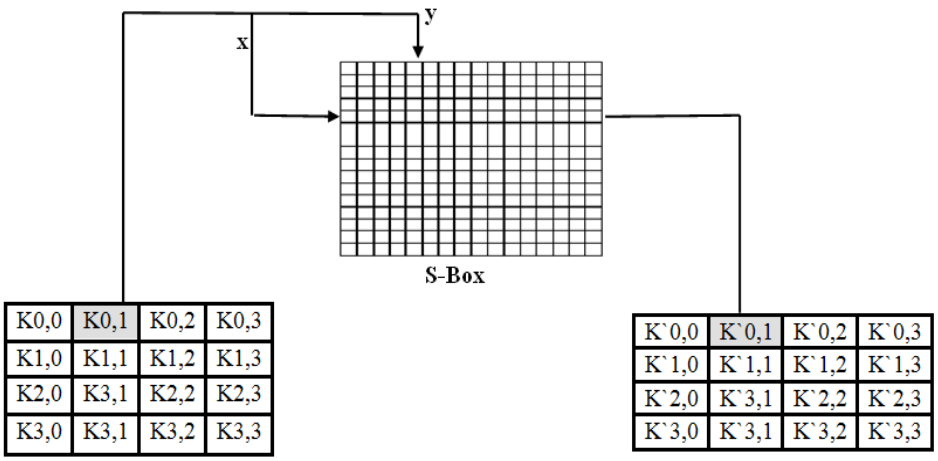


Figure (8).Substitue BytesTransform.

Shift Rows Process

In this process used a matrix of 4x4 byte represented key block and circular left shift for each row by different times. The first row of key block is circular left shift by zero times, second row is circular left shift by one times, the third row is circular left shift by two times, and the fourth row is circular left shift by three times, as shown in Figure (9).

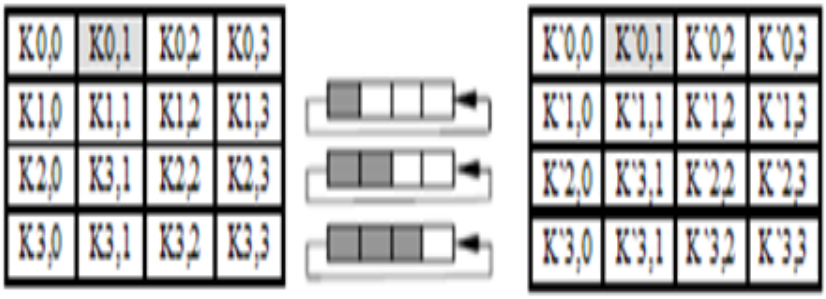


Figure (9) Shift Rows Process

Discussion and Experimental Results

This section displayed an evaluation speed and complexity in both key expansion (standard method) and enhancement method for key generation. Complexity calculated the run time of two previous methods for testing the running time measure by counting the number of "basic operations". The XOR operation is considered as a runtime complexity measurement that used between two methods and founded the number of operations in enhancement method equal to **(160)** operations and in the standard method equal to **(200)** operations and a primitive operation executed in the class O (n^3)time as the same class for the standard method thus the consuming run time is reduced in acceptable amount, the following Table (2) shows a comparison of encryption time between the standard method and enhanced method.

Table (2): Comparison between Standard Method and Enhancement Method.

Plaintext Length (char)	Plaintext Length (Block)	Time Encryption (ms)	
		Standard method	Enhancement method
20	2B	250	115
40	3B	266	131
60	4B	296	145
80	5B	388	162
100	7B	452	176
200	13B	592	223

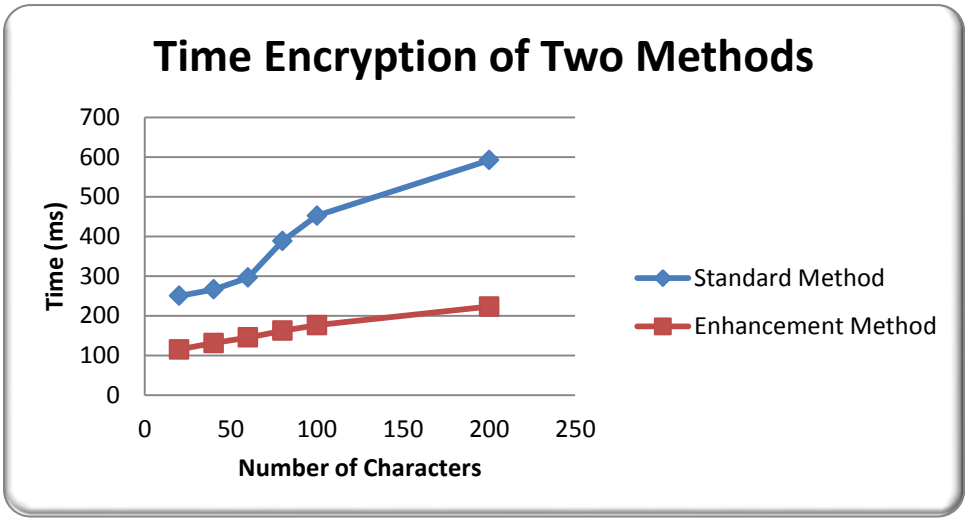


Figure (10) Time Encryption of Standard Method and Enhancement Method (char per ms).

From the results above, the run time is reduced in an enhancement method than in the standard method. When using plaintext of length 20 characters that is represented as two blocks, the time of encryption in enhancement method is (115 ms) and in the standard method is (250 ms).When using plaintext of length 40 characters that represented as three blocks the time of encryption in enhancement method is (131 ms) and in the standard method is (266 ms), and when usingplaintext of length 200 characters that represented as thirteen blocks the time of encryption is (223 ms) and in the standard method is (592ms).The average run time of the encryption process through the above assumption examples in the enhancement method is equal to 28 bpms (block per millisecond) and the average of standard method is equal to 66 bpms. Enhancement method reduced time consuming to %57.6.

An enhancement method has less complexity than the standard method, and a short time for key generation, therefore this method can be used in many applications that require higher speed and enough complexity such as real time communication which can perform the required security for sending received in formation through secret plat form.

In the decryption process the same steps of the AES algorithm will be done but with the suggested enhanced key generation method in an inverse manner so to reproduce the plaintext again from the obtained cipher text without needing any further descriptions.

The proposed method focus on the key generation process not on the AES internal functions, thus we are not mentioned about the deciphering processes because the enhancement method deals with the key generation steps only.

CONCLUSIONS

This paper showed an enhancement method for key generation of Advanced Encryption Standard (AES) algorithm with high efficiency. The proposed enhancement method architecture is based on modifying cipher feedback (MCFB) mode. In the block cipher encryption step, two processes are implemented: Substitution bytes process and Shift rows process. The obtained results from using this method has explained more efficient algorithm and a highly secured. Also, it decreased the complexity of the original AES algorithm by more than 20%because data structure related to schedule key are changed (also many operations are changed). Data structure for data input is changed from vector to block 4x4 bytes. The enhancement method can be used in different AES

key length (128, 196 and 256). The reduced key generation time lead to decrease the encryption time in the enhancement method than the original method. This method is tested with different sizes of samples which lead to efficient results when comparing with other previous approaches in term of secrecy and privacy.

REFERENCES

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

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

[3].El-Sheikh A. N. A. and Rashed A.A., "New Approach in Key Generation and Expansion in Rijndael Algorithm", International Arab Journal of Information Technology, Vol. 3, No. 1,2006.

[4]. Deguang L., Chang J., Gou X., Zhang A., andLu C., "Parallel AES Algorithm for Fast Data Encryption on GPU",IEEE Conference (Computer Engineering and Technology (ICCET), 2nd International Conference on, Vol. 6), 2010.

[5]. Reddy P. P., ThrimurthuluV., and Kumar K. J., "Implementation of Multi-Mode AES Algorithm Using Verilog", Dept. of ECE, CREC, Tirupathi, A.P, India,2014.

[6].Habeeb S., "Proposal for Complex AES Security using Key Generator and Text Permutation", Eng. & Tech. Journal, Vol.3, No.12, 2012.

[7].SalihH.H., SadiqA.T., and FarhanA. K., "Proposal of New Block Cipher Algorithm", Eng. & Tech. Journal Vol.28,No.10,2010.

[8].KaderaliI. 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

[9].Wikipedia website, "Block Cipher Mode", available at https://en.m.wikipedia.org/wiki/Block_Cipher_Modes_of_Operation.html.