A Byte-Oriented Multi Keys Shift Rows Encryption and Decryption Cipher Processes in Modified AES

Nada Hussein M. Ali, Abdul Monem S. Rahma, Abdul Mohsen Jaber, Sufian Yousef
nada.husn@gmail.com

Abstract— Implementing AES for security over data provides benefits of less memory consumption and less computation time as compared to other algorithms. The security of AES relies only on keeping the key secret, whereas the algorithm itself is fully public. The cipher process uses the Shift Rows transformation where the bytes in the last three rows of the state array are cyclically shifted while the bytes in the first row are not shifted. The AES shift-row transformation is a byte oriented, while the proposed algorithm is bit oriented .The present work is aimed to achieve higher complexity compared to original AES without incurring additional time for encryption and decryption processes. Such complexity was justified by applying the Modified Shift-Row transformation. The proposed algorithm has been applied to the variable length sizes of audio files. A comparison between standard AES, and the modified AES Shift-Row transformation in time delay, has shown marginal change. In the standard AES, the Shift-Row transformation uses a single key for encryption and decryption process, while the modified AES uses five different keys in each round for both operations.

Index Terms— AES algorthim, Encryption, Decryption, SHIFT ROWS , Plaintext, Ciphertext , Symmetric key, Audio files

1 Introduction

Implementing AES for security over data provides benefits of less memory consumption and less computation time as compared to other algorithms. The security of AES relies only on keeping the key secret, whereas the algorithm itself is fully public. The cipher process uses the Shift Rows transformation where the bytes in the last three rows of the state array are cyclically shifted while the bytes in the first row are not shifted. The AES shift-row transformation is a byte oriented, while the proposed algorithm is bit oriented .The present work is aimed to achieve higher complexity compared to original AES without incurring additional time for encryption and decryption processes. Such complexity was justified by applying the Modified Shift-Row transformation. The proposed algorithm has been applied to the variable length sizes of audio files. A comparison between standard AES, and the modified AES Shift-Row transformation in time delay, has shown marginal change. In the standard AES, the Shift-Row transformation uses a single key for encryption and decryption process, while the modified AES uses five different keys in each round for both operations.

2 The principle of the AES algorithm

The AES accepts 128 bits of plaintext and master key blocks of size 128, 192 or 256 bits. Let us denote the AES with these different key sizes as AES-128, AES-192 and AES-256, respectively. The 128-bit ciphertext block is produced after the plaintext block is processed by the round function a number of times. This number is 10, 12 and 14 for AES-128, AES-192 and AES-256, respectively. The plaintext, ciphertext and intermediate state blocks can be depicted as two-dimensional rectangular array of bytes with dimension 4 × 4. The master key can also be represented in this form but the number of rows is fixed to four. The number of columns equals the key length divided by 32.(3)

The cipher process uses the following functions:

- Sub Bytes - a non-linear substitution function that operates independently on each byte of the State, using a substitution table (S-box)
- Shift Rows - the bytes in the last three rows of the state array are cyclically shifted. The row number gives the shift number and the first row is not shifted
- Mix Columns - operates on the state column-by-column, treating each column as a four-term polynomial
- Add Round Key - a round key is added to the state using a XOR operation.

The Inverse cipher uses the same functions as the Cipher, but inverted. The order is : inverted shift rows, then inverted sub byte, inverted mixed columns, add round key. At the end of the state process an Output array (cipher text or PlainText) is obtained.

3. ShiftRows Transformation

ShiftRows is a transposition step where each row of the state is shifted cyclically a certain number of times . The purpose of this step is to provide diffusion of the bits over multiple rounds. The row 0 in the matrix is not shifted, row 1 is circular left shifted by one byte, row 2 is circular left shifted by two bytes, and row 3 is circular left shifted by three bytes as shown in Figure(1). The importance of this step is to avoid the columns being linearly independent, in which case, AES degenerates into four independent block ciphers.(4)

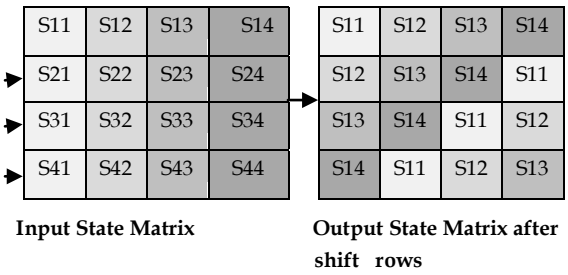


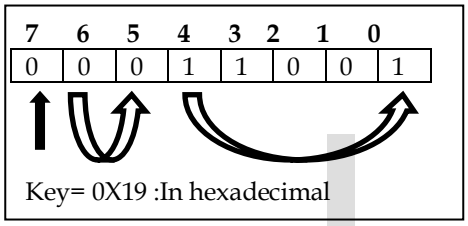
Figure (1) ShiftRow Transformation in AES Algorithm

The **inverse shift row transformation**, called InvShiftRows, performs the circular shifts in the opposite direction for each of the last three rows, with a 1-byte circular right shift for the second row, and so on.(5)

4.Multi Keys ShiftRows Transformation in AES

The AES shift row transformation is a byte oriented while the proposed algorithm is bit oriented , five keys have been used to increase the complexity of the ShiftRows transformation in each round. The keys are generated randomly, If the number of rounds is 10 So the number of keys is 50.

The encryption and decryption processes are performed either on rows or columns. The description details of each key used demonstrate in Figure(2) and Table(1) , while Algorithm(1) demonstrate the modified ShiftRow transformation steps.



Figure(2) One byte key example

Table(1) Details of one byte key

Bits index	Description
0,1,2,3,4	Numbers of bits to be shifted cyclically (25)
5,6	The index of either row or column to be shifted(22)
7	=0 apply on column =1 apply on row

Algorithm (1) Modified ShiftRow transformation

Input *:plaintext Block message {State[Row][Column],Row, Colum= 1,2,3,4}* ,Shift_Key[Round][5]={..,..,..,…..},Round=1,2,…..,depend on key length.

Output: *ciphertext Block message {State[Row][Column],Row, Colum=1,2,3,4}*

For every Block message to be ciphered in AES algorithm do
Step1: Repeat for each State[Row]{Column} using Shift_Key[Round][j], j=1,2,…..,5}
Step2: for each key (one byte=8 bits {0,1,….,7}) find the following:
RC: only one bit which indicate choosing either ROW or COLUMN
Index_RC: the index of either the row or column to be shifed(two bits)
Shift_No: number of bits to be shifted (five bits)
Step3: Encrypt the State matrix each round five times depend on

5 Results and Discussion

The present work is aimed to achieve higher complexity compared to original AES keeping the required time for encryption and decryption processes near the same. Such complexity was justified by applying the Modified ShiftRow transformation . The proposed algorithm has been applied to the variable length sizes of audio files ,Table (2) gives comparison between standard AES, the modified AES ShiftRow transformation in time ,while Table (3) gives a summary for comparison between standard AES, the modified AES ShiftRow transformation for different factors.

Table (2) Comparison between Standard AES and modified AES in time

	SIZE ON DISK	Standard AES-ENC	Modified AES-ENC	Standard AES-DEC	Modified AES-DEC
FILE 1	108 KB	0.197 SEC	0.325 SEC	0.434	0.561
FILE 2	23.4 MB	0.318 SEC	0.528 SEC	0.728	0.908

Table (3) Comparison between the standard AES and the modified ShiftRow AES algorithms

	Standard AES	Modified AES
Block length	16 bytes	Same
2- Numbers of rounds	10//12//14	Same
3-Key length	16//24//32	Same
4-Single round details	AddRoundKey, SubByte,MixColum, ShiftRow	Same Functions + using5 keys selected randomly within ShiftRow in each round
5-Complexity ShiftRow	One key /one round	5 keys/one round
6-Complexity ShiftRow	16!	16! * 5!

6 Conclusions

Based on the results, the following conclusions can be drawn:
The Functions ShiftRow has been modified in original AES to achieve higher complexity keeping the required time for encryption and decryption processes near the same.
In standard AES the ShiftRow transformation use a single key for encryption and decryption process, while the modified AES using five different keys in each round for both operations .
The keys set length used in encryption and decryption process is randomly selected by the user and by five keys at each round, so the number of key set depends on the length of the key used in AddRound function, ex. If the AES algorithm has 10 (for a 128-bit key), 12 (for a 192-bit key), or 14 rounds (for a 256-bit key) then the keys set are50,60 and 70 respectively

References

[1]- K. Kazlauskas, J. Kazlauskas, "Key-Dependent S-Box Generation in AES Block Ciphe System ",Informatica, Vol. 20, No. 1, 23–34, 2009.
[2]- AN0033 - Application Note,2013," AES Ci pher Modes with EFM32"
[3] - Isa H.,Bahari I., Sufian H., Z'aba M. R., (2011), "AES: Current Security and Efficiency Analysis of its Alterna tives", IEEE.
[4] Sachdev A, Bhansali M.,(2013) " Enhancing Cloud Compu ting Security using AES Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 67– No.9.
[5] William Stallings. 2012. Cryptography and Network Se curity Principles and Practice. Fifth Edition, Prentice Hall.