EFFECTIVE IMPLEMENTATION AND AVALANCHE EFFECT OF AES

Amish Kumar , Mrs. Namita Tiwari

Department of CSE MANIT-Bhopal
amish_aks@yahoo.co.in , namita_tiwari21@rediffmail.com

Abstract

Efficient implementation of block cipher is critical towards achieving high efficiency with good understandability. Numerous number of block cipher including Advance Encryption Standard have been implemented using different platform. However the understanding of the AES algorithm step by step is very typical. This paper presents the efficient implementation of AES algorithm and explain Avalanche effect with the use of MATLAB platform. Mainly use of MATLAB in Algorithm development, Data analysis, exploration, visualization, modeling, simulation, prototyping, application development including GUI building and computation.

Key Terms

AES, Avalanche effect, S-Box.

1. Introduction

Cryptography plays main role in information security. Many cryptographic algorithms have been proposed, such as the Data Encryption Standard (DES), the Elliptic Curve Cryptography (ECC), the Advanced Encryption Standard (AES) and other algorithms. Many researchers and hackers are always trying to break these algorithms using brute force and side channel attacks. Some attacks were successful as it was the case for the Data Encryption Standard (DES) in 1993, where the published cryptanalysis attack [2] could break the DES. Nowadays the Advanced Encryption Standard (AES) is considered as one of the strongest published cryptographic algorithms, where it was adopted by the National Institute for Standards and Technology (NIST) after the failing of the Data Encryption Standard (DES).

This paper discusses a Matlab implementation of the Advanced Encryption Standard (AES) [6] and show the Avalanche effect. AES is based on the block cipher Rijndael [4][5] and became the designated successor of the Data Encryption Standard (DES) [7] which has been implemented in a tremendous number of cryptographic modules worldwide since 1977. Even though this implementation is fully operational, (i. e. it can be utilized to encrypt arbitrarily chosen plaintext into cipher text and vice versa), the main optimization parameter of this implementation is understandability and avalanche effect

DOI : 10.5121/ijsptm.2012.1303

In this paper first section contains the introduction of AES algorithm and Matlab, section 2 contain the internal structure of AES with algorithm, section 3 describes Avalanche effect and Test and section 4 shows conclusion and last section is reference.

2. Internal structure of AES

AES is symmetric key block cipher. It uses a fixed 128-bit block cipher and three key lengths supported by AES as this was an NIST design requirement. The number of internal rounds of the cipher is a function of the key length according to Table 1.

key lengths	# rounds = *nr*
128 bit	10
192 bit	12
256 bit	14

Table 1:Key length and number of rounds of AES

There are three different types of layers to perform AES operation and the function of the different layers is:

1. Key Addition layer: A 128-bit round key, or sub key, which has been derived from the main key in the key schedule, is XORed to the state.

2. Byte Substitution layer (S-Box): Each (fig 1) element of the state is nonlinearly transformed using lookup tables with special mathematical properties. This introduces confusion to the data.

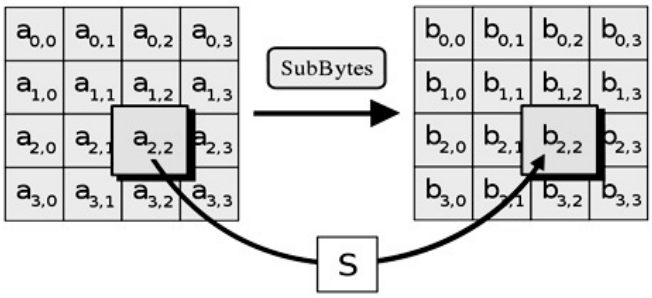

Fig 1: S-Box

3. Diffusion layer: It provides diffusion over all state bits. It consists of two sub layers, both of which perform linear operations:

(a)The Shift Rows layer provides the mechanism for shifting the rows (Fig 2) of the above layer output.

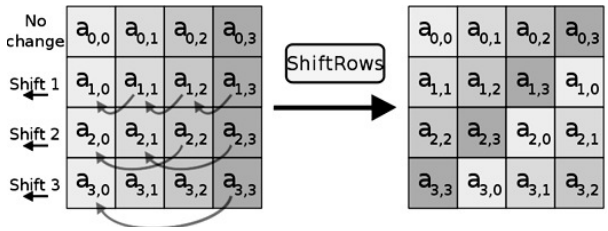

Fig 2: Shift Row

(b) The Mix Column layer is a matrix operation where each 4-byte column is considered as a vector and multiplied by a fixed 4×4 matrix. The matrix contains constant entries (Fig 3).

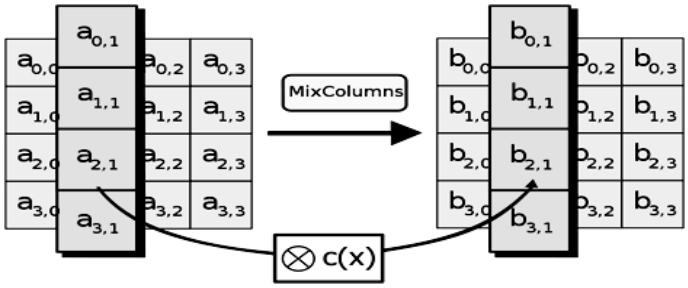

Fig 3: Mix Column

The complete process of the AES is depicted in the (fig 4).Last round of the AES does not contain mix column step which makes it more strong. Decryption process is reverse of encryption processes which perform inverse byte substitution operation, inverse shift row and inverse mix column

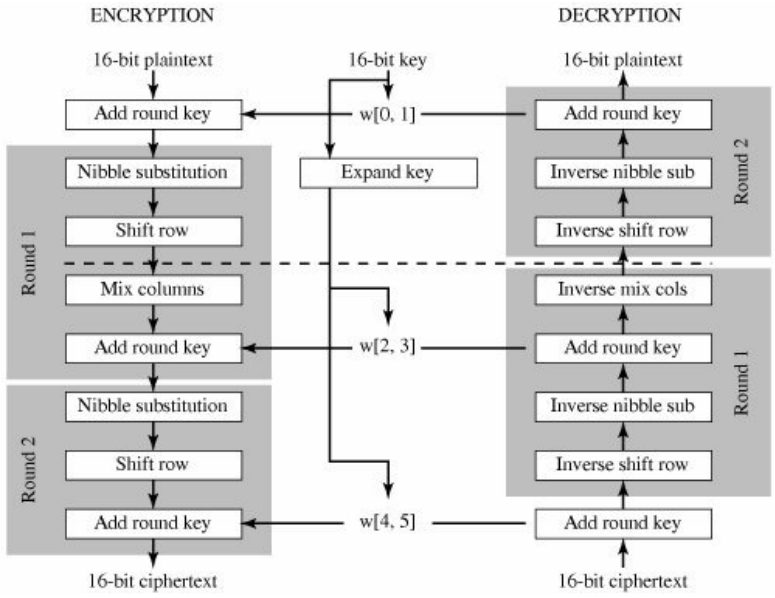

Fig 4: Bloch diagram of the AES working process

Algorithm:AES-Cipher
input: Byte $A[4 \times nb]$, Word $K[nb \times (nr + 1)]$;
output: Byte $C[4 \times nb]$,

Byte *state*[4, *nb*]; *state* := *A*;
AddRoundKey(*state*, *K*[0, *nb* − 1];
for *round* := 1 to *nr* − 1 do SubBytes(*state*);
ShiftRows(*state*);
MixColumns(*state*);
AddRoundKey(*state*,*K*[*round*×*nb*,*nb*(*round*+1)) SubBytes(*state*); ShiftRows(*state*);
AddRoundKey(*state*, *K*[*nr* × *nb*, *nb*(*nr* + 1) − 1]);
C := *state*; return *C*; end

In this algorithm A shows the input plaintext which is the size of 128 bit, K shows key which is either 128 bit, 192bit or 256 bit long, C shows the cipher text which is of the length 128 bit long. The number of rounds depends upon the size of the key which varies from 10 to 14.

3. Avalanche Effect and Test

Avalanche effect is important characteristic for encryption algorithm. This property can be seen when changing one bit in plaintext and then watching the change in the outcome of at least half of the bits in the cipher text. One purpose for the avalanche effect is that by changing only one bit there is large change then it is harder to perform an analysis of cipher text, when trying to come up with an attack. First we start calculate avalanche effect for AES S-box. To perform the test we change plaintext bit to "10" instead of "11" and "12" instead of "11" and "10" instead of "00" the result obtained is is 0.4375 and 0.5153 and .4453 respectively

Plain text	Cipher text	Avalanche effect
11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11	79 f8 cc 24 01 82 dd 7f 2d 89 f7 e7 78 b7 ee 30	.4375(56)
11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 10	9d 4c 1d b4 6a 93 27 b5 20 64 37 d1 3d 9d 2a	
11 22 33 66 55 44 55 44 77 88 99 66 44 45 36 12	4a a9 16 11 e2 8a 9f 67 35 30 1f 80 16 c5 b7 cd	.5153(66)
11 22 33 66 55 44 55 44 77 88 99 66 44 45 36 11	D7 00 43 2d 51 78 f7 65 50 03 03 75 b1 e4 2d a0	
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	C6 a1 3b 37 87 8f 5b 82 6f 4f 81 62 a1 c8 79	.4453(57)
10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0d 19 33 06 27 42 fe 01 9c fe 06 e1 a8 1a a0 01	

Table 2: Avalanche Test of Basic AES

Observation: from the above result we can see the cipher text is very strong for very simple plaintext.

4. Conclusion:

This paper presents the basic implementation of AES algorithm which also shows the Avalanche effect and understandability of the AES.AES is the very strong cipher and impossible to break without knowing the key so the importance of AES algorithm is high security. The complex process of AES algorithm can be comfortably implemented in MATLAB

Reference:

[1] Amish Kumar,Namita Tiwari, PERFORMANCE EVALUATION OF AES METHODS: REVIEW,ICCC 2012,paper id 1365

[2] Biham,Eli and Adi Shamir,Differential Cryptanalysis of the Data Encryption Standard, SpringerVerlag,1993.

[3] The Mathworks: Matlab,The Language of Technical Computing. http://www. mathworks.com/products/matlab,(2001).

[4] V.Rijmen: The block cipher Rijndael.http://www.esat.kuleuven.ac.be/rijmen/rijndael/,(2001).

[5] J.Daemen,V.Rijmen: AES proposal: Rijndael.http://www.esat.kuleuven.ac.be/~rijmen/rijndael/rijndaeldocV2.zip,(1999).

[6] National Institute of Standards and Technology: Specification for the Advanced Encryption Standard(AES). http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf,(2001).

[7] National Institute of Standards and Technology: Data Encryption Standard (DES). http://csrc.nist.gov/publications/fips/fips46- 3/fips46-3.pdf,(2001).

[8] Radu Tomoiaga, Mircea Stratulat AES Performance Analysis on Several Programming Environments,Operating Systems or Computational Platforms", 2010 Fifth International Conference on Systems and Networks Communications.

[9] Chirag Parikh, M.S. Parimal Patel, Ph.D." Performance Evaluation of AES Algorithm on Various Development Platforms".

Author

Amish Kumar,
M.Tech (Information security)
NIT-Bhopal, India