ISSN:0975-9646

Implementation of Advanced Encryption Standard Algorithm

H. B. Pethe[1], Dr. S. R. Pande[2]

[1]*Department of Electronics and Computer Science, RTM Nagpur University, Nagpur(MH), India.*

[2]*Department of Computer Science, Shivaji Science College, Congress Nagar, Nagpur(MH), India.*

Abstract **- Cryptography plays an important role in the network security to maintain the CIA triad that is Confidentiality, Integrity, Authentication and non-repudiation of information. The use of internet is increasing day-by-day; therefore information security is the major issue today. To keep our data secure over the internet, the use of cryptography is important. Cryptography makes the data like text, image, audio and video unreadable during transmission and the main goal is to keep data secure from unauthorized access. There are various algorithms used for cryptography and they are algorithms broadly divided into two types symmetric and asymmetric. This paper deals with an implementation on ICDAR-UK using MATLAB2011b and analysis of Advanced Encryption Standard Algorithm (AES) which is the symmetric key cryptographic algorithm and encrypts the text embedded in the image.**

Keywords **- Symmetric key cryptography, Advanced Encryption Standard, CIA triad.**

I. INTRODUCTION

Cryptography is the process of hiding information. Steganography, Computer passwords and transferring data from one place to another are done by using cryptography. It is the science of using mathematics to encrypt and decrypt data. It enables to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient.

Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form that is not recognizable by its attackers while stored and transmitted [2]. Data cryptography mainly is the scrambling of the content of data, such as text, image, audio, video and so forth to make the data unreadable, invisible or unintelligible during transmission or storage called Encryption. The main goal of cryptography is keeping data secure form unauthorized attackers. The reverse of data encryption is called data decryption.

The original data which is readable and that is to be transmitted or stored is called plaintext whereas the data which is unreadable, neither by human nor by machine is called ciphertext. A system that provides encryption and decryption is called cryptosystem which uses encryption algorithms to determine how simple or complex the encryption process will be.

The security of an encryption algorithm is measured by the size of its key. Larger the size of the key, the more time the attacker will require to do the exhaustive search of the key. Thus larger size key provides higher security level. In the symmetric key encryption the key is same for both encryption and decryption. Key is a piece of information (sequence of bits) that specifies the particular transformation of plaintext to ciphertext or vice versa. The strength of the encryption algorithm depends on how secret is the key, length of the key, the initialization vector and how they all work together. Cryptographic algorithms are either symmetric or asymmetric. Symmetric algorithms uses symmetric keys also called secret keys. Asymmetric algorithms uses asymmetric keys also called public and private keys.

This paper discusses the symmetric key cryptographic algorithm called Advanced Encryption Standard Algorithm. This algorithm uses a block cipher, which is the method of encrypting data in which a cryptographic keys and algorithms are applied to the block of data rather than to one bit at a time [3].

II. ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM

An AES is a block oriented symmetric key encryption algorithm. It is developed in 2000 and considered to be more secure than Data Encryption Standard (DES) algorithm. AES is based on the design principle known as substitution permutation network.

It operates on a 128 bit data block at a time and uses 128, 192 or 256 bits key length and uses 10, 12 or 14 rounds [4,5]. A data block is partitioned into an array of bytes. Such bytes are interpreted as a finite field elements using polynomial representation. The input is divided into 16 bytes and then arranged into a 4x4 matrix column wise [6]. This matrix is known as the state matrix. The original 128-bit key is also divided in to 16 bytes as like 128 bit data and arranged in the form of 4x4 matrix. This matrix is called keyMatrix.

The algorithm starts with an Addroundkey stage followed by 9 rounds of four stages and a tenth round of three stages.

Both these matrices form the necessary inputs to the algorithm.

AES encryption includes,

1) An initial round(0)
2) Nine general rounds (1 to 9) and
3) A final round (10)

In round (0) the two matrices are simply XORed under AddRoundKey transformation. The output of Round0 is given as the input to Round 1. Each round composed of four distinct, uniform and invertible transformations: Subbytes, ShiftRows, MixColumn and AddRoundKey as shown in fig1.

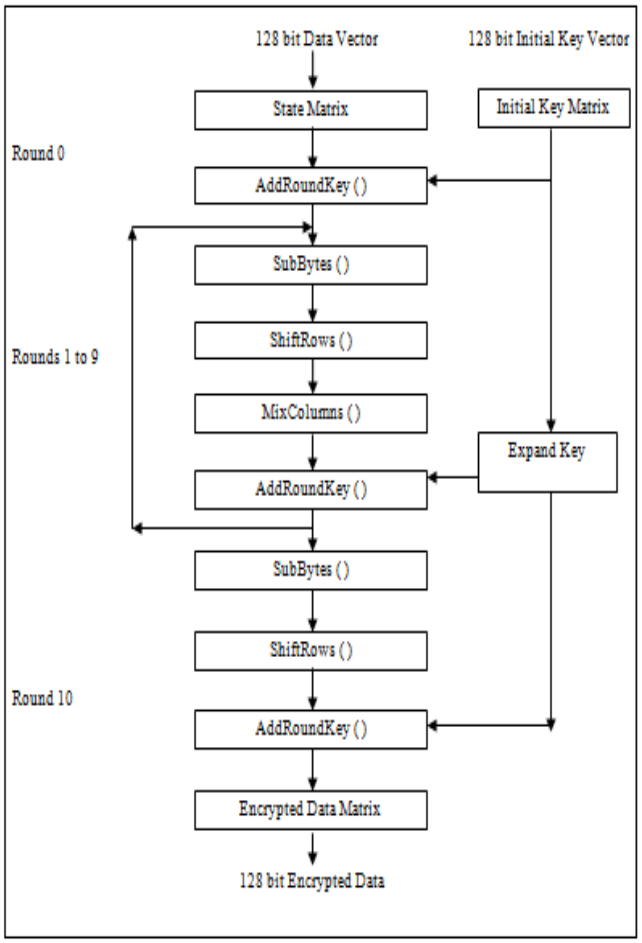

Fig. 1 : Structure of AES Encryption

A. Subbytes

This stage also known as Substitute Bytes, it is simply a table lookup using a 16x16 matrix of byte values called s-box. This matrix consists of all the possible combinations of an 8 bit sequence (2^8 =16x16 = 256).

It is a non-linear byte substitution operation designed to give the required amount of Confusion. It operates independently on each byte of the State matrix using a substitution table S-box. Each byte is substituted by corresponding byte in the S-box [7].

B. ShiftRows

This stage is also known as Shift Row Transformation. It works as follows:

1) The first row of state is not altered.
2) The second row is shifted 1 bytes to the left in a circular manner.
3) The third row is shifted 2 bytes to the left in circular manner.
4) The fourth row is shifted 3 bytes to the left in a circular manner

It is a transposition step that gives the required amount of Inter – word Diffusion and operates individually on each of the last three rows of state matrix shifting cyclically a certain number of bytes. The first row is left unchanged. The second row is left rotated by one byte, third row by two bytes and fourth row by three bytes as shown in fig 2.

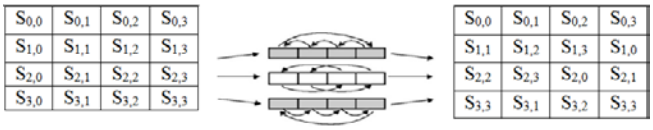

Fig : 2 ShiftRows stage

C. MixColumn

This operation gives intra-word Diffusion and operates on each column of the state matrix individually, combining the four bytes in each column using multiplications and additions in GF (2^8).

Each byte of a column is mapped into a new value that is a function of all four bytes in the column. The transformation can be determined by the following matrix multiplication on state as shown in the following fig:

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{pmatrix} = \begin{pmatrix} S'_{0,0} & S'_{0,1} & S'_{0,2} & S'_{0,3} \\ S'_{1,0} & S'_{1,1} & S'_{1,2} & S'_{1,3} \\ S'_{2,0} & S'_{2,1} & S'_{2,2} & S'_{2,3} \\ S'_{3,0} & S'_{3,1} & S'_{3,2} & S'_{3,3} \end{pmatrix}$$

The MixColumn transformation of a single column j (0<=j<=3) of state can be expressed as follows:

$$S'_{0,j} = (2 \bullet S_{0,j}) \oplus (3 \bullet S_{1,j}) \oplus S_{2,j} \oplus S_{3,j}$$
$$S'_{1,j} = S_{0,j} \oplus (2 \bullet S_{1,j}) \oplus (3 \bullet S_{2,j}) \oplus S_{3,j}$$
$$S'_{2,j} = S_{0,j} \oplus S_{1,j} \oplus (2 \bullet S_{2,j}) \oplus (3 \bullet S_{3,j})$$
$$S'_{3,j} = (3 \bullet S_{0,j}) \oplus S_{1,j} \oplus S_{2,j} \oplus (2 \bullet S_{3,j})$$

Where • denotes multiplication over the finite field GF(2^8).

D. AddRoundKey

It is designed to provide Key Dependency and Asymmetry. It operates independently on each byte of the State matrix by adding it with the corresponding byte of the Subkey using bitwise XOR. For each round, a Subkey is derived from the main key using the keyexpansion function. Each subkey has the same size as the state matrix [8].

The final round includes all the transformations except MixColumn. After completing all the ten rounds the output is 128 bits in encrypted format called cipher text.

AES Key Expansion

Key expansion is an important for both encryption and decryption. The AES key expansion algorithm takes as input a 4-word (16 bytes) key and produces a linear array of 44 words (176 bytes).This is sufficient to provide a 4-word round key for the initial Add Round Key stage and each of the 10 rounds of the cipher.

The following figure shows pseudo code for generating the expanded key from the actual key.

```
KeyExpansion (byte key [16], word w [44])
{
   Word temp
for(i=0;i<4;i++)
w[i]=(key[4*i], key[4*i+1], key[4*i+2], key[4*i+3]);
for(i=4;i<44;i++)
{
        temp=w[i-1];
        if(i mod 4=0)
        temp=SubWord(RotWord(temp)) ⊕ Rcon[i/4];
        w[i]=w[i-4] ⊕ temp;
 }
 }
```

Fig 3: Key expansion psuedocode

The key is copied into the first four words of the expanded key. The remainder of the expanded key is filled in four words at a time. Each added word w[i] depends on the immediately preceding word, w[i-1], and the word four positions back w[i-4]. In three out of four cases , a simply XOR is used. For a word whose position in the w array is a multiple of 4, a more complex function is used. Fig 4 illustrates the generation of the first eight words of the expanded key using the symbol g to represent that complex function.

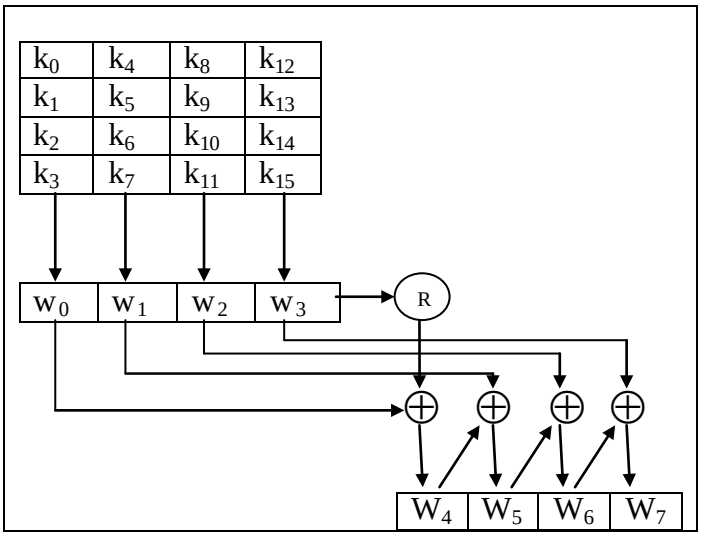

Fig 4: AES key expansion

The function g consists of the following subfunctions:

1. RotWord performs a one-byte circular left shift on a word. This means that an input word [b0, b1, b2, b3] is transformed into [b1, b2, b3, b0].
2. SubWord performs a byte substitution on each byte of its input word, using the s-box.
3. The result of steps 1 and 2 is XORed with round constant, Rcon[j].

The round constant is a word in which the three rightmost bytes are always 0. Thus the effect of an XOR of a word with Rcon is to only perform an XOR on the leftmost byte of the word. The round constant is different for each round and is defined as Rcon[j] = (RC[J],0,0,0), with RC[1] = 1, RC[j]=2•RC[j-1] and with multiplication defined over the field GF(2^8).

The key expansion was designed to be resistant to known cryptanalytic attacks.

Decryption Algorithm

The decryption process involves the transformations InvSubBytes, InvShiftRows, InvMixColumns and AddRoundKey. The name AddRoundKey is same in both encryption and decryption since AddRoundKey is its own inverse [9][10].

III. EXPERIMENTAL RESULTS

The algorithm is implemented in MATLAB 2011B and the image files taken from the ICDAR-UK database.

TABLE I

Encryption & Decryption Time for different image files.

Images	Encryption Time	Decryption Time
img1	18.111	30.81
img2	26.738	36.613
img3	22.948	42.932
img4	23.12	37.743
img5	25.475	36.176
img6	26.286	34.102
img7	19.471	41.621
img8	15.647	28.252
img9	18.05	30.998
img10	20.202	33.696
img11	20.358	37.627
img12	20.109	29.562
img13	21.903	42.12
img14	23.946	34.148
img15	22.183	38.563

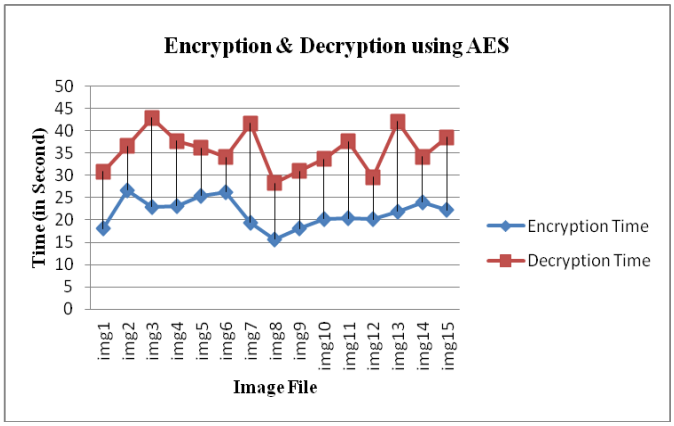

Fig 5 : Time required for encryption and decryption using AES

IV. CONCLUSIONS

Implementation of Advanced Encryption Standard (AES) algorithm involves the functions for encryption such as AddRoundKey (), SubBytes (), ShiftRows (), MixColumns (). After analysing the result it is found that the time required for encryption is less than the time required for decryption and as the file size increases the time required for encryption and decryption is also increases. For two files having same size, if one of the file contains blur image, then the time required for encryption and decryption is more.

REFERENCES

[1] Bruce schneier "Applied Cryptography" 2nd Edition published by John Wiley & Sons Inc.

[2] DiaasalamaAbdElminaam, HatemMohamadAbdual Kader, Mohly Mohamed Hadhoud, "Evalution the Performance of Symmetric Encryption Algorithms", *international journal of network security vol.10,No.3,pp,216-222,May 2010.*

[3] Shraddha Soni, Himani Agrawal, Dr. (Mrs.) Monisha Sharma "Analysis and Comparison between AES and DES cryptographic algorithm" *International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012.*

[4] A. Nadeem, "A performance comparison of data encryption Algorithms", *IEEE information and communication technologies, pp.84-89, 2006.Bn*

[5] R. Rivest, A. Shamir, L.Adleman."A method for obtaining digital signatures and public-key cryptosystems". Communications of the ACM, Feb 1978.

[6] T. Saravanan, V. Srinivasan, R, Udayakumar "MATLAB-Simulink Implementation of AES Algorithm for Image Transfer" *Middle-East Journal of Scientific Research 18(12) 1709-1712, 2013.*

[7] P. Karthigaikumar, Soumiya Rasheed "Simulation of Image Encryption using AES Algorithm" *IJCA 2011.*

[8] Akash Kumar Mandal, Chandra Parakash, Mrs. Archana Tiwari "Performance Evaluation of Cryptographic Algorithms: DES and AES" *IEEE Students' Conference on Electrical, Electronics and Computer Science 2012.*

[9] William Stalling "Cryptography and network security" *Pearson education, 2nd Edition.*

[10] Sumitra " Comparative Analysis of AES and DES security Algorithms" *International Journal of Scientific and Research Publications, Volume 3, Issue 1, January 2013 1 ISSN 2250-3153.*