# Modified Advanced Encryption Standard

**Pravin Kawle, Avinash Hiwase, Gautam Bagde, Ekant Tekam, Rahul Kalbande**

***Abstract— In today's world most of the communication is done using electronic media. Data Security is widely used to ensure security in communication, data storage and transmission. Security of multimedia data is an imperative issue because of fast evolution of digital data uses the permutation step, taking from Data Encryption Standard (DES) algorithm. Theoretical analysis and experimental results prove that this technique provides high speed as well as fewer exchanges or transfer over unsecured network. Multimedia data security is achieved by methods of cryptography, which deals with encryption of data. Standard symmetric encryption algorithms provide better security for the multimedia data.***

***But applying symmetric key encryption algorithm on more complex multimedia data (mostly images); we might face the problem of computational overhead. To overcome that problem, we analyze the Advanced Encryption Standard (AES) and modify it, to reduce the calculation of algorithm and for improving the encryption performance. In modified AES algorithm instead of using Mixcolumne overheads on data. Modified-AES algorithm is a fast lightweight encryption algorithm for security of multimedia data. All above advantages make algorithm highly suitable for the images and plaintext transfer as well , than the AES algorithm.***

***Keywords- Advanced Encryption standard (AES), cryptography, DES, and symmetric key algorithms.***

## I. INTRODUCTION

It is an important aspect to protect the confidential multimedia data from unauthorized access. Multimedia content can be text, audio, still images, animation and video. Such contents are protected by multimedia security method. This is attained by techniques that are based on cryptography. These schemes facilitate communication security, piracy and to shield. Large size of text or images causes certain challenges for encryption.

Normally a typical text or image has a very large size. Using traditional encryption algorithm will make encryption difficult for large volume of multimedia data. For the encryption of any multimedia data we need such algorithms that require less computation because of large size of data.

Symmetric-key algorithms are fewer computationally serious than any Asymmetric-key algorithms. Typically, symmetric key algorithms are thousands times sooner than those of the asymmetric algorithms. So the better suitable method to encrypt the multimedia data is, to encrypt it with symmetric key encryption algorithms.One of the methods to protect any multimedia data is to encrypt that data with DES(Data Encryption Standard). DES, the encryption algorithm is very complicated and it involves very large computations. DES implementation software is not so fast to process the vast amounts of multimedia generated data. As a consequence of hardware implementation AES is very fast symmetric block algorithm. This method is known as naive approach. Applying the naive approach on enormous amount of data takes large computation and makes the encryption speed very slow due to variety of restrictions.

In particular, we make it strong using symmetric key encryption techniques(such as AES, DES) by applying on multimedia contents as sequence of binary. But unluckily when we apply these techniques on more complex multimedia (mostly images) or when the size of text data is very large, it produces significant computational overhead, i.e. required much of processing time.

Our project is concerned with optimizing the existing standards of cryptography (AES) for the text data and images encryption and decryption.

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext. It is also slanting towards exploiting the huge amount of data, in order to attain preferred speed. This edited AES is referred to as Modified-AES algorithm. The modification is done by totaling the Initial Permutation step, takes from DES (Data Encryption Standard), in order to enlarge the encryption performance. This modification indubitably increases the efficiency of encryption.

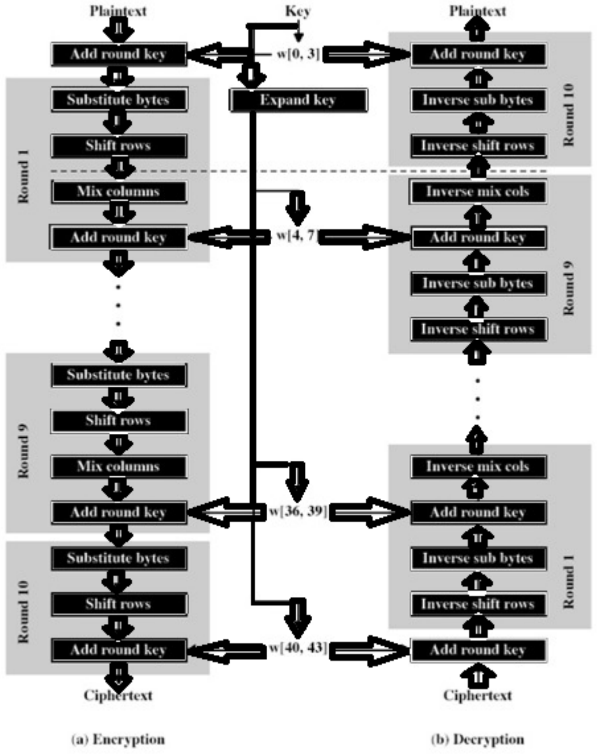

Fig.(a) Flowchart diagram for AES algorithm.

Manuscript received March. 2014

**Pravin M. Kawle**, Depatment of IT, RGCER, Nagpur University, Nagpur, Maharashtra, India.

**Avinash G. Hiwase**, Depatment of IT, RGCER, Nagpur University, Nagpur, Maharashtra, India.

**Gautam A. Bagde,** Depatment of IT, RGCER, Nagpur University, Nagpur, Maharashtra, India.

**Ekant Tekam,** Depatment of IT, RGCER, Nagpur University, Nagpur, Maharashtra, India.

**Rahul Khalbande**, Depatment of IT, RGCER, Nagpur University, Nagpur, Maharashtra, India.

*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication Pvt. Ltd.*

Joan Daemenand VincentRijmen urbanized a block cipher called Rijndael. In AES the span of each block and the key can be autonomously specified to be 128, 192, or 256 bits.The AES arrangement exploits data of 128 bits and same three key size alternatives.This 128 bit data can be divided into four operation blocks, which are represented as a squar matrix of bytes. These operation blocks are copied into a state array. The state array is organized as a 4×4 matrix.

The data is conceded through N rounds (N = 10, 12,14) for encryption. These rounds are performed by the following transformations:

- Bytesub transformation: In this process 128-bit block is replaced with another 128- bit block, for substitution purpose we use S-box..
- Shiftrows transformation: In this process we leave the first row of data, perform once shift left on 2nd row, two times shift left on 3rd row and three times shift left on 4th row..It is a simple Permutation.
- Mixcolumns transformation: Is a substitution; the bytes in the columns are linearly combined. The matrix multiplication is performed over the same GF (28) as used in the design of the S-box.
- Addroundkey transformation: When working state and expanded key are XOR with each other, process is called Addround Key.

All four layers expressed above (including key scheduling) have analogous converse methods. Procedure of encryption follows more than a few ladders. An initial addroundkey is applied. After this a round function is applied to the block. Each block consists of bytesub, shiftrows, mixcolumns and addroundkey transformation. These blocks are repeated N times, depending upon the length of the key applied. Same sequence of transformations is applied on decryption structure as which is applied in encryption structure. The transformations i.e. Inv-Bytesub, InvShiftrows, Inv-Mixcolumns, and Addroundkey permit the type of key schedules to be matched for encryption and decryption Here it must be noted that the MixColumn reverse operation requires matrix elements.

## II. METHODOLOGY

To overcome the problem of high calculation and computational overhead, we analyze the Advanced Encryption Standard (AES) and modify it, to reduce the calculation of algorithm and for improving the encryption performance. So we develop and implement a modified AES based Algorithm for all kind of data. The basic aim to modify AES is to provide less computation and better security for data. The modify AES algorithm adjusts to provide better encryption speed. In Modified-AES the block length and the key length are specified according to AES.

A.Specification.Three key length alternatives 128, 192 or 256 bits and block length of 128 bits. We assume a key length of 128 bits, which is commonly implemented. In Modified-AES encryption and decryption process resembles to that of AES, in account of number of rounds, data and key size. The round function consists of four stages. To overcome the problem of high calculation we skip the Mixcolumn step and add the permutation step. Mixcolumn gives better security but it takes large calculation that makes the encryption algorithm slow . The other three junctures remain unbothered as it is in the AES. A single 128-bit block is the input to the encryption and decryption algorithms.This block is a 4×4 square matrix consisting of 16 bytes. This block is copied into the state array. The state array is modified at each stage of encryption or decryption. Similarly the 128-bit key is also depicted into a square matrix. The 128-bit key is expressed into an array of key schedule words: each word is of four bytes. The total key schedule words for ten rounds are 44 words; each round key is similar to one state. The block diagram of the Modified-AES algorithm with 128 bits data is shown below.

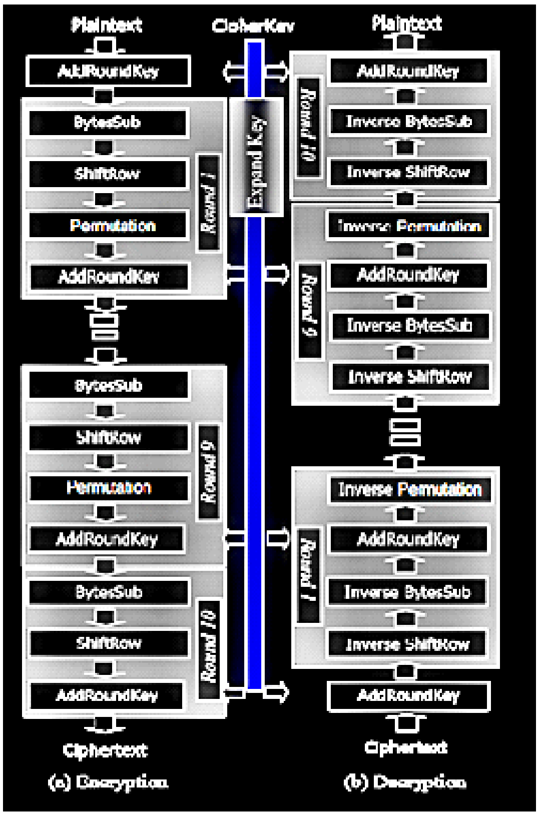

Fig.(b) Modified-AES algorithm: Encryption & Decryption Structure

The algorithm is divided into four operational blocks where we observe the data at either bytes or bit levels and the algorithm is designed to treat any combination of data and is flexible for key size of 128 bits. These four operational blocks represent one round of Modified-AES.

There are 10 rounds for full encryption.

The four different stages that we use for Modified-AES Algorithm are:

- Substitution bytes
- ShiftRows
- Permutation
- AddRoundKey

Substitution Bytes, ShiftRows and AddRoundKey remain unaffected as it is in the AES. Here the important function is Permutation which is used instead of Mixcolumn. These rounds are managed by the IP table. Permutation is widely used in cryptographic algorithms. Permutation operations are interesting and important from both cryptographic and architectural points of view. The DES algorithm will provide us permutation tables. The inputs to the IP table consist of 128 bits. Modified-AES algorithm takes 128 bits as input. The functions Substitution Bytes and ShiftRows are also interpreted as 128 bits whereas the Permutation function also takes 128 bits. In the permutation table each entry indicates a specific position of a numbered input bit may also consist of 256 bits in the output. While reading the table from left to right and then from top to bottom, we observe that the 242th bit of the 256-bit block is in first position, the 226th is in

*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication Pvt. Ltd.*

second position and so forth. After applying permutation on 128 bits we again complete set of 128 bits and then perform next remaining functions of algorithm. If we take the inverse permutation it gives again the original bits, the output result is a 128-bit cipher text. For the full decryption of Modified-AES algorithm the transformation processes are, Inv-Bytesub, Inv-Shiftrows, Inv-Permutation, and the Addroundkey, which are performed in 10 rounds as it is in the encryption process.

## III. RESULT OUTPUT AND ANALYSIS

For testing the algorithm we use a very simple code that checks the efficiency of algorithm. This test shows that the modified-AES algorithm is much better than AES algorithm. In this tutorial we have tested several files and in order to check that how fast the Modified-AES algorithm than the real AES.

To test the algorithm we take sixteen byte text compare the calculated elapsed time of both the Modified-AES with Advanced Encryption Standard (AES). Table 1 shows the comparison results performed on file size of sixteen byte text files using Modified-AES and the AES algorithm.

TABLE1: Encryption result for text file

| File Size | AES (sec) | M-AES (sec) | Efficiency (sec) |
|---|---|---|---|
| 16 byte | 1.925991 | 1.874904 | 0.051093 |

## IV. CONCLUSION

Usually lightweight encryption algorithms are very attractive for multimedia applications. Luckily we have achieved through our research a fast lightweight encryption algorithm to secure our multimedia data from unauthorized access. For the security of multimedia data, we have proposed an encryption algorithm that is based on AES using symmetric key encryption algorithm. In version of security analysis and experimental results our proposed encryption scheme is fast and on the other hand it provides good security and adds very less overhead on the data, this today is the requirement of most of the multimedia applications. Theoretical analysis and experimental results of the achievement makes it very suitable for high rate and less overhead on the data. For all these compensation it is suitable for any large scale text and image transfer.

## V. ACKNOWLEDGMENT

Many people in, **Rajiv Gandhi College of Engineering and Research (RGCER)** College have supported us from the beginning of our B.E project work. Without them, the project would obviously not have looked the way it does now. Person we would like to thank is our Project Guide Ms. **Komal Ramteke**, Professor of Information Technology, RGCER, Nagpur. She has helped us in many ways. Her enthusiastic engagements in our project work and her never-ending stream of ideas have been absolutely essential for the results, presented here. We are very grateful that she has spent so much time with us discussing different problems ranging from philosophical issues down to minute technical details.

## REFERENCE

[1] Shtewi, A.M.”An Efficient Modified Advanced Encryption Standard (MAES) adapted for image cryptosystems” IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.2,

[2] ShashiMehrotra Seth, 2Rajan Mishra,” Comparative Analysis Of Encryption Algorithms For Data Communication”, IJCST Vol. 2, Issue 2, June 2011 pp.192-192.

[3] Gurjeevan Singh, Ashwani Kumar Singla,K.S. Sandha, ”Through Put Analysis Of Various Encryption Algorithms”, IJCST Vol. 2, Issue 3.

[4] Behrouzan A. Forouzan (2010), Cryptography & Network Security, TMH Publisher, ISBN: 9780070660465.

[5] Bruce Schneier (2009), Applied Cryptography, John Wiley & Sons Publisher, ISBN:9780471117094