International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Different Reviews and Variants of Advance Encryption Standard

Reena Mehla[1], Harleen Kaur[2]

[1]Assistant Professor, Department of Electronics and Communication, Kurukshetra University, Haryana, India

[2]Student (M. Tech), Department of Electronics and Communication, Kurukshetra University, Haryana, India

Abstract: ***Safe storage and transmission of digital images over the network has its importance in the communication system and in the confidential video conferences. Large use and growth of internet results in extensive use of images. To fulfill the conditions of safe and confidential transmission over the network, there is a requirement of new algorithm which gives the high level of security. AES is a encryption algorithm having several advantages in data encryption. This paper presents different reviews of AES (Advance Encryption Standard)***

Keywords: Advanced Encryption Standard (AES), Shift Row Transformation, Mix column Transformation

1. Introduction

A large number of users generate and exchange a large amount of information in various fields like financial, medical, banking via internet. The exchange of information requires a special security for transmission of information over the internet and for the storage of information. For this encryption and decryption of the data at respective sender and receiver side is applicable. Sensitive data transmission requires a fast , secure and non reproductive exchange of information. Cryptography is a mean, which provides authenticate and secure transmission over the insecure networks. The transmission over the channel is to be so secure, so that unauthorized person cannot access the data transmitted over the network. Earlier, DES (Data Encryption Standard) was considered as a basic for symmetric key encryption, having a key length of 56 bits. This key length is considerably small and can be broken. Also the traditional image encryption schemes like DES [8]has low level of efficiency when the size of the image becomes large. Algorithm like Triple DES or Blowfish are not been used to transmit large data. Large data make them complex and slows down their execution time. This is why; they cannot be applicable to real time scenario. AES is an advanced scheme of encryption which provides a higher security and higher speed.

2. Advanced Encryption Standard

AES is a symmetric block cipher. The block size of AES is fixed and it is 128 bits. But the key length may be of 128, 192 or 256 bits. Since block size of 128 bits is fixed i.e. of 16 bits, the rectangular state array dimension is 4x4. Different transformation operations are performed on state array. With the beginning of encryption or decryption, the input bytes array is first mapped to the state array. At the end the final value is mapped to the output array bytes.

AES has following transformation steps performed on to the state array:

1. Sub Byte Transformation
2. Shift Rows Transformation
3. Mix Column Transformation
4. Add Round Key

Sub Byte Transformation

In this step a S-Box or Substitution Box is used as a look up table for substituting the values in the state array. S-Box is a 16x16 table of hexadecimal value.

Shift Rows Transformation

Next the shifting operation is performed on the values of state. The criterion used behind shifting is explained as:

Row 1 is kept unchanged.
Row 2 is shifted cyclically one byte to the left.
Row 3 is shifted cyclically two bytes to the left.
Row 4 is shifted cyclically three bytes to the left.

Mix Columns Transformation

Mix column transformation is performed on the state array column by column. In this each column of the state is considered as a four-term polynomial over GF(2^8) and thus multiplied by g(x) modulo x^4+1.

Where g(x) is given by $\{03\}x^3+\{01\}x^2+\{01\}x+\{02\}$

Add Round Key Transformation

In this transformation step a round key is added to the state by performing a bitwise XOR operation between them both.

It is important to mention here that among the total Nr rounds performed in AES, in the first Nr-1 rounds the total of the 4 transformation discussed above are applied, whereas the final round excludes the Mix Column Transformation.

Flow Diagram of AES

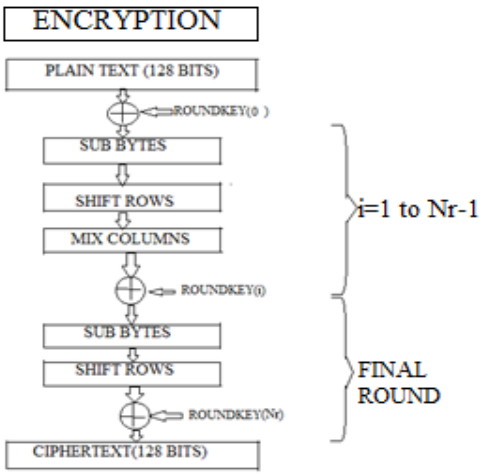

Figure 1: Encryption in AES

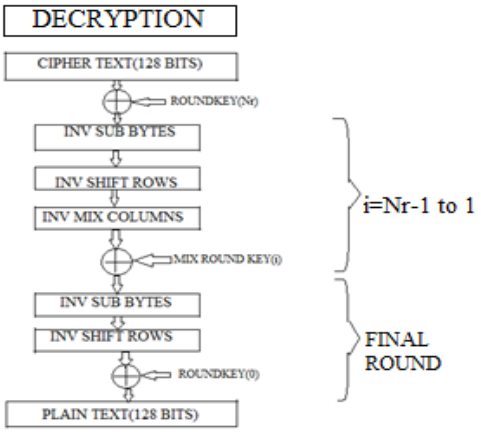

Figure 2: Decryption in AES

3. Related Work

Different cryptographic algorithms have been proposed. Kuo [1] proposed image encryption algorithm which adds the phase spectra of the plain image with the key image to obtain the encrypted image. From safety point of view, this method is good, but in this no image compression is considered. Chin –Chen Chang [2] proposed a compression technique for cryptosystems in which images are firstly decomposed into vectors and sequentially encoded vector by vector. Fridrich [3] presented two dimensional standard chaotic map using symmetric block encryption technique. Pankesh Bamotra[4] demonstrated the idea of encryption of grayscale images using pixel shuffling method . the image to be encrypted is converted into matrix of grayscale values. Then according to the value of encryption required , the matrix is divided into sub-matrices which are then randomly shuffled. This method provides good results if the size of the image is small. But for the considerably large images, it became more time consuming. Abdulkarim Amer Shtewi, Hasan and Hegazy [5] proposed an efficient modified Advanced Encryption Standard adapted for image cryptography. This modified AES proposes shift row adjustment in original AES, so as to give better results in terms of security and encryption time. B. Subramanyam, Vivek Chhabria , TG Shankar Babu[6] proposed AES with high encryption quality and less computational time and to make the key sensitivity of the algorithm resistant towards attacks. The weak point of Advance Encryption Standard is provided by static substitution box (S-Box). Luminita and Petre-Daniel[7] proposed modified S-Box provided by the modified mathematical function operate on Galois Field to make the algorithm more secure , taking less computational time and improved under the attacks from external sources.

4. Proposed Work

On the discussion of the above methods demonstrated earlier, the proposed work reduces the computational time for encryption of large images. The proposed work is focused on the modification in the key expansion and shift row transformation step of Advance Encryption Standard (AES) algorithm so as to make the respective algorithm more robust towards attacks and to reduce the computational time is take for the encryption of images and give the better performance of Advanced Encryption Standard (AES) and to make it more bandwidth efficient.

References

[1] C.J.Kuo , Novel image Encryption Technique and its application in progressive transmission. Journal of electron imaging 24 1993 pp 345-351.
[2] Chin-Chen Chang , Min –Shian Hwang, Tung-Shou Chen, " A new encryption algorithm for image cryptosystems", The Journal of Systems and Software 58(2001), 83-91.
[3] Fridrich Jiri, Symmetric ciphers based on two dimensional chaotic maps, Int. J. Bifurcat Chaos 8 (1998) (6), pp. 1259-1284.
[4] Pankesh Bamotra, International Journal of Advanced Research in Computer Science and Software Engineering 2(12), December -2012, pp. 279-282.
[5] Abdulkarim Amer Shtewi, Bahaa Eldin M. Hasan, Abd El Fatah .A. Hegazy, "An Efficeint Modified Advanced Encryption Standard Adapted for Image Cryptosystems", IJCSNS, International Journal of Computer Science and Network Security, VOL. 10 No.2, February 2010. Pp. 226-232.
[6] B. Subramanyam , Vivek.M.Chhabria, T.G. Shankar Babu, "Image Encryption Based on AES Key Expansion", 2011 Second International Conference on Emerging Applications of Information Technology, pp. 217-220.
[7] Luminita Scripcariu, Petre- Daniel Matasaru, "On the substitution Method of the AES Algorithm", 2013, IEEE.
[8] Chan A: A Security framework for privacy- preserving data aggregation in wireless sensor networks. ACM transactions on sensor networks 7(4) (2011).

Author Profile

Reena Mehla is working as Assistant Professor in Electronics And Communication Department, Doon Valley Institute of Engineering and Technology, Kurukshetra University, Haryana, India

Harleen Kaur is student in Department of Electronics And Communication, Doon Valley Institute of Engineering and Technology, Kurukshetra University, Haryana, India.