IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

Data Transmission or Mailing on Security Basis Using AES Algorithm

Akshay Gaikwad[1], Prashant P Buktare[2], Chanda chouhan[3]

Student, Information Technology, Atharva College of Engineering, Mumbai, India [1, 2]

Professor, Information Technology, Atharva College of Engineering, Mumbai, India [3]

Abstract: The paper highlights the security needed door transmission of data on a wireless network, with the technology moving forward wireless communications has grown enormously. It is necessary to provide security for wireless data transfer as it is more vulnerable to the security attacks .70% of the online data transfer is in the images This implies it is important to provide security to text as well as images .Images have large data size and also has real time constraints problem hence the same cipher cannot be applied to encrypt images and text. But with some manipulation ARE can be used for this purpose. Here we modify AES by adding key stream generator (CEK) for enhanced security.

Keywords: AES, Cryptography, Image encryption, Wireless transmission.

I. INTRODUCTION

In recent years the rapid development and expansion in the digital communications has resulted in significant online transmission. This has also lead to the increase in more sophisticated and robust attacks on the data. Any unwanted person can intercept the message while transmission occurs. This activity is called as intrusion attack. However intrusion has become more easy and frequent in wireless and general communication networks. To secure sensitive data from intrusion encryption/decryption is necessary. Image differs from text message as images have more data, high redundancy and stronger correlation between pixels.

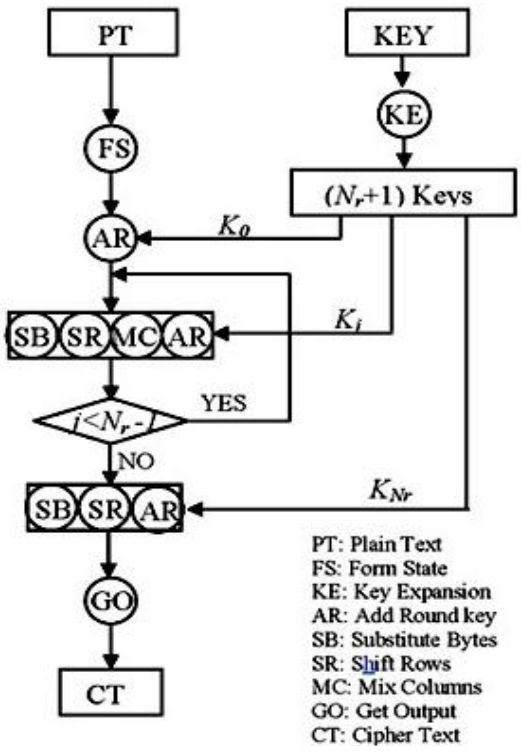
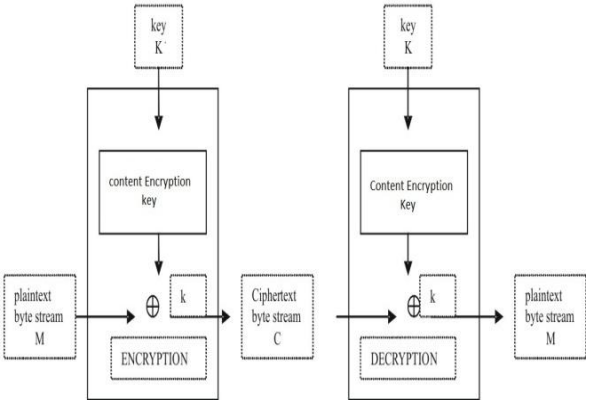


Figure-1 (AES FLOWCHART)

The conventional ciphers such as DES, IDEs are not suitable for image encryption and decryption. The AES algorithm is suitable for image encryption which is closely related to some dynamics of its own characteristics. The 128 bits AES is vulnerable to cache timing attacks, dictionary attacks. So we propose use of a key stream generator called code encryption key (CEK) which randomly generates key for every block transmitted. This increases the complexity of the system.

II. DESCRIPTION

A software DES implementation is not fast enough to process the huge amount of data generated by multimedia applications and a hardware DES implementation adds extra cost both to broadcasters and the receivers. In order to overcome such problem Advanced encryption standard (AES) was proposed. The AES cipher is in some applications that require fast processing such as smartcards, cellular phones, and image-video encrypt. The data is encrypted on the sender side with the help of AES CEK key and the encrypted key is send to receiver mail , to decrypt the data the receiver needs encrypted key which is at the at receiver mail ,with the help of the user gets original data.



DOI 10.17148/IJARCCE.2015.41106

IJARCCE

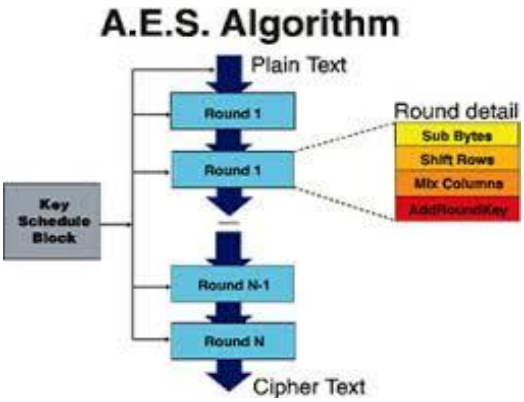
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

AES cipher algorithm is used in the proposed system because AES is the most secure algorithm. AES is used in Round structure. There are two reasons behind doing this. First, the traditional AES algorithm uses 128 bit input data but enhanced system uses 256 bits input data and secondly there are certain attacks on the AES algorithm like linear, algebraic attacks hence to increase the complexity, AES is used in Round structure. The content encryption key (CEK) is used.

III. METHODOLOGY

This work is focused on enhancement of encryption algorithm. The whole cryptographic system has been developed in this work. This includes encryption of data, key exchange and message authentication. Parameters: Throughput, CPU Usage, Encryption and Decryption Time. The AES content encryption key MUST be random generated for each instance of an enveloped-data content type. The Content Encryption key is used to encrypt the content. Key used to digitally encrypt a piece of content. The enhancement in advanced encryption standard enables nodes in the provider domain to securely exchange signaling data, and prevent attacks on the wired network. This enhanced security can help us to counter attacks likes session hijacking, Man in the middle, message replay, message forgery.



Implementation and performance evaluation

Here we are encrypting and decrypting plain text by using AES-CEK we will measure the encryption time, decryption time and calculate throughput.

Performance evaluation will be done by comparing the enhance AES with traditional AES on the basis of encryption time, decryption time and throughput.

IV. INNER WORKING OF THE ROUND

The algorithm begins with add round key stage followed by 9 rounds of four stage and a tenth round of fourth stage. This applies for encryption and decryption with the exception that each stage of a round the decryption algorithm is inverse of its counterpart in the encryption algorithm

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

The tenth round simply leaves out the Mix Columns stage.

The first nine rounds of the decryption algorithm consist of the following:

1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns

Again, the tenth round simply leaves out the Inverse Mix Columns stage. Each of these stages will now be considered in more detail. Substitute Bytes this stage (known as Sub Bytes) is simply a table lookup using a 16×16 matrix of byte values called an s-box. This matrix consists of all the possible combinations of an 8 bit sequence (28 = 16×16 = 256). However, the s-box is not just a random permutation of these values and there is a well defined method for creating the s-box tables. The designers of Rijndael showed how this was done unlike the s-boxes in DES for which no rationale was given. We will not be too concerned here how the s-boxes are made up and can simply take them as table lookups.

Again the matrix that gets operated upon throughout the encryption is known as state. We will be concerned with how this matrix is affected in each round. For this particular round each byte is mapped into a new byte in the following way: the leftmost nibble of the byte is used to specify a particular row of the s-box and the rightmost nibble specifies a column The Inverse substitute byte transformation (known as InvSubBytes) makes use of an inverse s-box.

The s-box is designed to be resistant to known cryptanalytic attacks. Especially, the Rijndael developers sought a design that has a low correlation between input bits and output bits, and the property that the output cannot be described as a simple mathematical function of the input. In addition, the s-box has no fix points (s-box (a) = a) and no opposite fixed points (s-box(a) =− a) where − a is the bitwise compliment of a. The s-box must be invertible if decryption is to be possible (Is-box[s-box(a)] = a) however it should not be its self inverse i.e. s-box(a) 6= Is-box(a)

Shift Row Transformation:-

This stage (known as Shift Rows) this is a simple permutation and nothing more. It works as follow:

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

Shift Rows stage:-

The Inverse Shift Rows transformation (known as InvShiftRows) performs these circular shifts in the opposite direction for each of the last three rows (the first row was unaltered to begin with).

This operation may not appear to do much but if you think about how the bytes are ordered within state then it can be seen to have far more of an impact. Remember that state is treated as an array of four byte columns, i.e. the first column actually represents bytes 1, 2, 3 and 4. A one byte

shift is therefore a linear distance of four bytes. The transformation also ensures that the four bytes of one column are spread out to four different columns.

Mix Column Transformation:-

This stage (known as MixColumn) is basically a substitution but it makes use of arithmetic of GF (28). Each column is operated on individually. 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 each element of the product matrix is the sum of products of elements of one row and one column. In this case the individual additions and multiplications are performed in GF(28). The MixColumns transformation of a single column j ($0 \leq j \leq 3$) of state can be expressed as:

s0 0,j = (2•s0,j)⊕(3•s1,j)⊕s2,j ⊕s3,j s0 1,j = s0,j ⊕(2•s1,j)⊕(3•s2,j)⊕s3,j s0 2,j = s0,j ⊕s1,j ⊕(2•s2,j)⊕(3•s3,j) s0 3,j = (3•s0,j)⊕s1,j ⊕s2,j ⊕(2•s3,j)

Where • denotes multiplication over the finite field GF(28).

Add Round Key Transformation:-

In this stage (known as AddRoundKey) the 128 bits of state are bitwise XORed with the 128 bits of the round key. The operation is viewed as a column wise operation between the 4 bytes of a state column and one word of the round key. This transformation is as simple as possible which helps in efficiency but it also affects every bit of state.

V. CONCLUSION

End-to-end security has been an issue in 3G networks and hence a solution has to be proposed for the same using AES CEK or a similar mechanism should be provided for security of data. Hence CEK is used here with AES as an encryption algorithm for security. The motivation behind increasing complexity is to make the system attack resistant and secure data from attackers. AES is enhanced with use of content Encryption key to make cryptography more strong.

ACKNOWLEDGMENT

We would like to acknowledge the support provided by our mentor and my colleague for successfully carrying out this work. I thank the institution for all the facilities and infrastructure they provided me.

REFERENCES

[1] **G**. Selim, H. M. E. Badawy and M. A. Salam, Editors, "New Protocol design for Wireless Networks security", IEEE International Conference on Computer Science and Information Technology (ICACT), **(2006)** Feb 20-22.

[2] M.B. Vishnu, S.K. Tiong, M. Zaini, S.P. Koh, "Security Enhancement of Digital Motion Image Transmission Using Hybrid AES-DES Algorithm", APCC 2008

[3] Razi Hosseinkhani, H. Haj Seyyed Javadi, "Using Cipher Key to Generate Dynamic S-Box in AES Cipher System", International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (1) : 2012

[4] E. Sabbah, A. Majeed, K. Y.-D. Kang, K. Liu and N. Abu-Ghazaleh, Editors, "An application-driven perspective on wireless sensor network security", ACM international workshop on Quality of service & security for wireless and mobile networks, **(2006)**.

[5] .Julia Juremi, Ramlan Mahmod, Salasiah Sulaiman, "A Proposal for Improving AES S-box with Rotation and Key-dependent", Cyber Warfare and Digital Forensic (CyberSec) international conference, 2012

[6] Saif Al-alak, Zuriati Ahmed, Azizol Abdullah and Shamala Subramiam "AES and ECC Mixed for ZigBee Wireless Sensor Security", World Academy of Science, Engineering and Technology 2011

[7] Anirudh Ramaswamy Ganesh, Naveen Manikandan P, Sethu S Pl, Sundararajan R, Pargunarajan K.," An Improved AES-ECC Hybrid Encryption Scheme for Secure Communication in Cooperative Diversity based Wireless Sensor networks", IEEE conference on Recent Trends in Information Technology (ICRTIT), 2011

[8] K. Bhatele, A. Sinhal and M. Pathak, Editors, "A Novel Approach to the Design of New Hybrid Security Protocol Architecture", IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), **(2012)** August 23-25, Ramanathapuram.