Special Issue of Engineering and Scientific International Journal (ESIJ)
Technical Seminar & Report Writing - Master of Computer Applications - S. A. Engineering College (TSRW-MCA-SAEC) - May 2016
ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

Network Security using AES Algorithm by Cryptographic Technique

S. Rajakumari [#1], R. Anitha[*2]

[1]*Master of Computer Applications, S.A. Engineering college, Chennai-77.*
rajakumari17011995@gmail.com
[2]*Asst. Prof., Department of Computer Applications, S.A. Engineering College, Chennai-77.*
anithar@saec.ac.in

Abstract— Network security is the vital component which used for protecting all details approved throughout networked security. The Cryptography technique plays an essential role in the field of network security. Only one particular element underlies many of the security mechanism in use - Cryptographic technique and hence our focus is on this area. This is very important for network security and this security is the main issue of this generation of computing, because many types of intruders are increasing day by day. Establishing a network is not a big issue but protecting the entire network is a big issue. This paper mainly focuses on symmetric encryption algorithms such as DES, triple DES and AES. These algorithms are compared and their performance is evaluated by means of encipher and decipher time, throughput, and memory usage.

Keywords— Network security; Cryptography.

1. Introduction

Network security and cryptography is a concept to secure network and data transmission over wireless communication [2]. Network security covers a variety of computer networks. The conservative systems of encryption can only preserve the data safety. The information could be accessed by the wrong user for malicious purpose. The most common and simple way of protecting a network resources is by giving user name and password. Network security starts with authenticating the user, commonly with a username and a password. Enciphering of records is the the majority ordinary means of giviing security. Cryptography is the mainly imperative devices that facilitates e-commerce because cryptography creates it probable to defend electronic records [1]. Many algorithms are obtainable and used in records security. They can be sorts into public and private key encryption. Public key is utilized for encryption and confidential key is utilized for decryption. Connection between two hosts using a network is to maintain privacy. It is the process by which digital information are protected, the goals of security are to protect confidentiality, maintain integrity, and assure availability.

In 1995, the U.S. National Institute of standards and technology began the search for a new encryption algorithm. The new search becomes the Advance Encryption Standard, or AES [5]. It is the symmetric-key encryption standard. This algorithm uses the key sizes of 128,192 and 256 bits. The algorithm's name is resulting from the initiators names, Vincent Rijmen and Joan Daemen [3]. It is a fast algorithm that can be implemented easily on simple processors. It is strong mathematical foundation, it primarily uses substitution, transposition, and the shift, exclusive OR, and addition operation. Like DES, AES uses replicate cycles.

2. Structure of AES Algorithm

The algorithm commences with an Add around key level pursued by 9 cycles of four levels and a tenth cycle of three phases in fig.1. This relates for together encipher and decipher with the omission that each phase of a surrounding the decipher algorithm is the contrary of it's complement in the encryption algorithm [4].

2.1 Step in AES Algorithm

The four stages are as follows:

- The Substitute bytes.
- The Shift rows.
- The Mix Columns.
- The Add Round Key.

The tenth round simply leaves out the Mix Columns stage. The first nine rounds of the decipher algorithm consist of the following:

- The Inverse Shift rows.
- The Inverse Substitute bytes.
- The Inverse Add Round Key.
- The Inverse Mix Columns.

Once more, the tenth encircling merely leaves out the contrary Mix Columns phase.

A. Byte Substitution

It uses substitution box structure. Substituting each byte of 128-bits block according to substitution table. Every

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

byte in the state is replaced by another one. Every byte in the matrix is restored with an 8-bit s-box. This is a directly dispersion procedure. Every byte in the state is reinstate with its entrance in a permanent 8-bit search for table, S;b_{ij}=S(a_{ij}) [7].

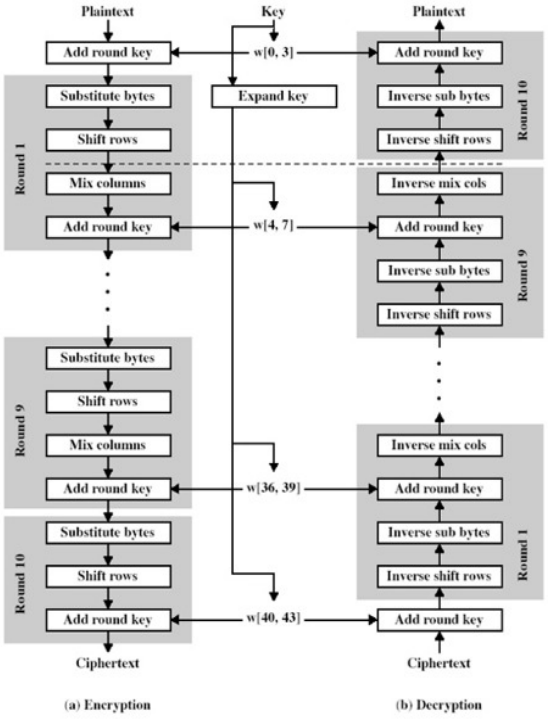

Fig. 1: Overall structure of the AES algorithm.

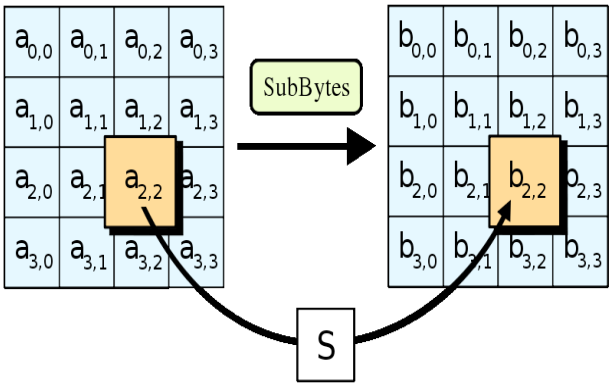

Fig. 2: Byte substitution

The analogous replacement pace used throughout decipher is called InvSubBytes.

B. Shift Row

This step is show in figure:3. It uses transposition step. For 128- and 192-bit block sizes, row n is shifted left circular (n - 1) bytes. For 256-bit blocks, row 2 is moved by 1 byte and rows 3 and 4 are shifted 3 and 4 bytes, respectively. This is a straight confusion operation [7].

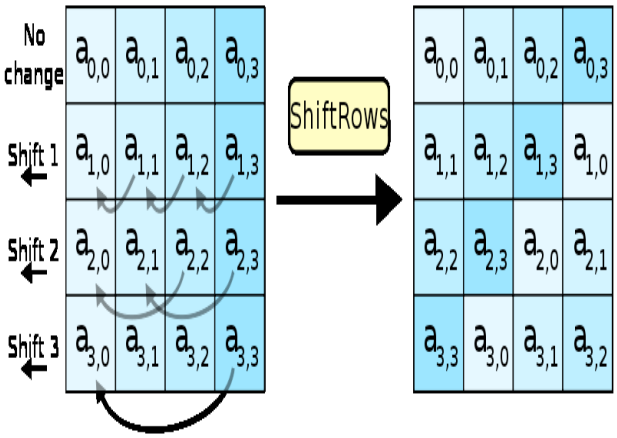

Fig. 3: Shift row

- The first row of state have no change.
- The second row is moved by 1 bytes to the left.
- The third row is moved by 2 bytes to the left.
- The fourth row is moved by 3 bytes to the left in a circular manner.

During decipher the transformation is denoted by InvShiftRows for Inverse Shift-Row Transformation.

C. Mix Column

This step involves shift left and exclusive-ORing bit with themselves. This step replaces each byte of a column by all the bytes in the same column. The mix columns function takes four bytes as input and outputs four bytes, where each input byte affects all four output bytes. This provides both diffusion and confusion [7].

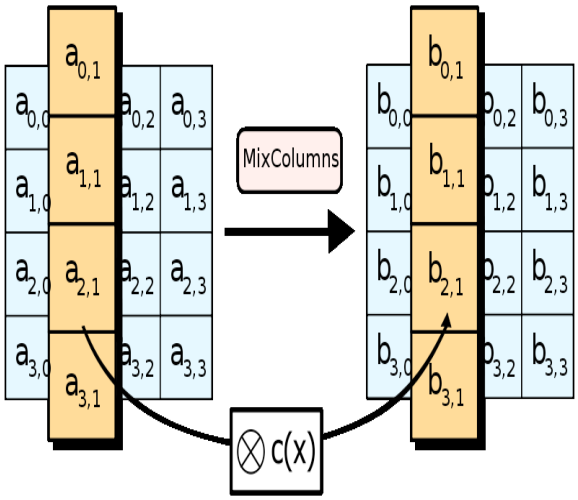

Fig. 4: Mix column

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

The corresponding transformation during decode is stands for inverse mix column transformation.

D. Add Round Key

In the added round key step, the sub-key is shared with the state. For each round, a subkey is derived from the main key; each subkey have the same size as the state. The subkey is summed by joining each byte with the corresponding byte of the subkey using bitwise Exclusive-OR. The process is sight as a feature shrewd process among the 4 bytes of a position column and one utterance of the round key. This alteration is very simple, which assists in more protected but it also possessions each bit of state [7].

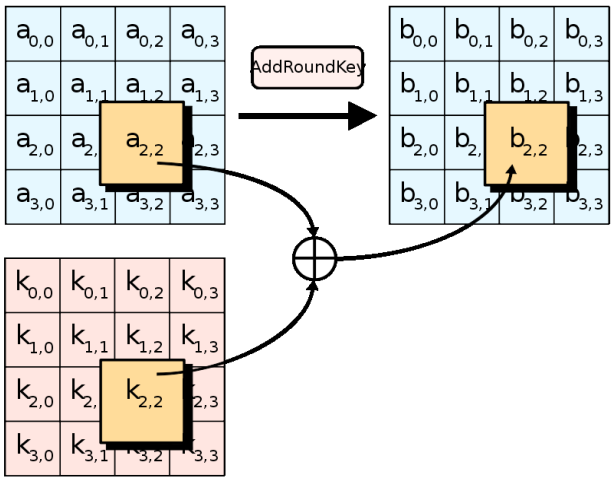

Fig. 5: AddRoundKey

The corresponding step during decode is denoted by inverse add round key transformation.

2.2 AES Algorithm

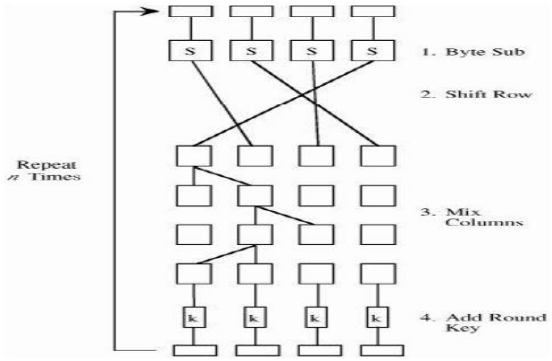

Fig. 6: AES algorithm

AES algorithm uses these four steps for encryption and decryption [6].

3. Conclusion

This paper examines the network security using cryptographic algorithm. The AES has become the defacto standard for encrypting network data. AES is better than DES, the repeat cycles is less than DES. TripleDES needed more time to encrypt/ decrypt, used less memory, and has low throughput. AES has similar time to encrypt/decrypt and better throughput. AES algorithm takes much more time to find the original message therefore AES has better security than DES and Triple DES.

4. Future Work

RSA has been the subject of extensive cryptanalysis, and no serious flaws have yet been found. RSA examine the role of keys in encryption. It was a ways to allow the key to be public but still protect the message. The basis for public key encryption is to allow the key to be public but to keep the decryption technique secret.

References

[1] Arjen K. Lenstra Citibank, and Eric R. Verheul "Selecting Cryptographic Key Sizes", Jornal of cryptology Research Volume 10, 2006, pp.278-290.
[2] http://rijndael.info/ audio/rijndael -pronunction.wav.
[3] Punita Mellu and Sitender Mali, "AES: Asymmetric key cryptographic System", International Journal of Information Technology and Knowledge Management, Volume 6, 2011, pp.427-432.
[4] Rohtak, Harayana, Yogesh Kumar "Comparative Study of Different Symmetric Key Cryptography Algorithms", International Journal of Application or Innovation in Engineering & Management, Volume 2, Issue 7, 2013, pp.56.
[5] John Daemen,Vincent Rijmen, "The Design of Rijndael: AES-The Advances Encrypting Standard", Springer, 2002, pp.42.
[6] http;//www.springerlink.com/index /UVX5NQGNN55L 199.pdf.
[7] Revathi. R.R, Tamilarasi.P and Vigneshwari.D, "Image Steganography for Secure the Data using Least Significant Bit", Special Issue of Engineering and Scientific International Journal, Technical Seminar & Report Writing - Master of Computer Applications - S. A. Engineering College, May 2015, PP.83-86.

S.Rajakumari is holding a Under Graduation Degree in B.C.A from Soka Ikeda College of Arts And Science for Women and pursuing Post-Graduation in master of computer applications from S.A Engineering College. This paper is a part of curriculum covered under in (MC7413) Technical Seminar and Report Writing.

R. Anitha is a Assistant Professor, Department of Computer Applications at S.A. Engineering College, Chennai. She has published many articles in the National and International Journals and presented papers in many Conferences.