Enhance Security with AES cryptography algorithm: a Survey

Meena kumari
M.Tech CSE Deptt.BPSMV khanpur kalan (sonipat)
E-Mail: meena.boora24@gmail.com

Abstract

Advancement of network technology and various communication techniques, like email, twitter, faceboook etc. However many hackers and malicious groups also increased with the advancement on network Technology. So security is most challenging issue in the world. There for many Different data security methods like cryptography, hashing, and steganography etc, have been developed for protecting data from unauthorized access. This paper provides a survey in between some symmetric algorithms like Data Encryption Standard (DES), Triple DES (3DES), Blowfish and (AES) Advanced Encryption Standard. Comparison of these algorithms is provided on the basis of various factors like key size, block size, attacks, security and number of rounds required for its implementation. Existing symmetric algorithms AES provide better data security. AES involves the sequence of four functions like: Sub Bytes, Shift Rows, Mix Column and Add Round Key.

Keyword

Encryption, Decryption, Cryptography, Symmetric algorithms: Data Encryption standard (DES), 3DES, Blowfish, AES,

1. Introduction

Advancement of network needs some technique to face challenges in networking security. To overcome this problem in network security, “Cryptography” is the best techniques for securing information. Cryptography is way of data hiding it changing original text into secretes form by sender and decoded by only receiver who has authority to open it [1]. Cryptography algorithms are very important for information security. Cryptography divided into two types Symmetric and Asymmetric key Cryptography. In Symmetric key algothim same key are used for encryption and decryption the data. And in asymmetric key algorithm different key are used for sender and receiver. Key is an important aspect in encryption and decryption. If a weak key is used in the algothim than unauthorized person can easily decrypt (access) the data. If a week key or small length is used in the algorithm then easily data can be decrypted. Symmetric key algorithms consume some amount of computing resources as battery power, CPU time, etc. [2].

There are some goals of cryptography:

1. Authentication: Sender and data receiver must be confirming each other's identity before sending and receiving data.

2. Confidentiality: only authenticated user, can access the messages.

3. Integrity: there is no modification amid sender and receiver of data.

4. Non-Repudiation: sender and receiver cannot deny that they had sent a message.

5. Service Reliability: Attacker (hacker) can attacks on secure systems, which may affect the service of user [3].

1.1 Encryption and Decryption

Encryption is the process of converting original information (called plaintext) into secretes form (called cipher text).Decryption is the reverse process, converting from cipher text to plain text [4].

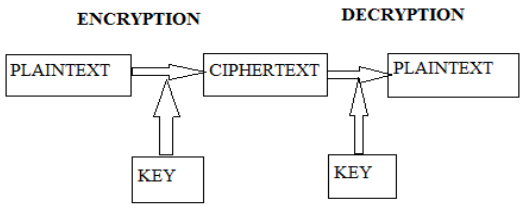

Fig. 1 Encryption & Decryption process [5].

1.2 Background and Terminology

Plaintext: An original message (text) send by sender is called Plain text.

Cipher text: An original message converting into secretes witting is called Cipher text.

Encryption: It is change the original text into cipher text

Decryption: Decryption converts Cipher text into Plaintext.

Key: Combination of numeric, alpha numeric text or special symbol.

Cryptanalysis: is recovering the plaintext of a message without access to the key [4].

2. Encryption Algorithms

2.1 DES (Data Encryption Standard):

One of the symmetric block encryption algothim is DES (Data Encryption Standard). It was the first encryption algorithm published by NIST. It uses 64 bits key, out of 64 bits key 56 bits are independent key, which determine the exact cryptography transformation, and remaining 8 bits are used for error detection. The main operations of DES are bit permutation and substitution in one round of DES. Six different permutation operations are used in key expiration part and cipher part. Decryption is similar to encryption in DES algorithm but differences only round key are applied in reverse order. Many attacks and methods recorded the weakness of DES, so it is an insecure block cipher key [2].

Encryption Process

1. The input key is used to derive sixteen 48-bit keys. Each round uses these keys.

2. Expansion of right half from 32 bits to 48 bits using different fixed table.

3. The result is combined with the sub key that round using the XOR operation.

4. Using the S-boxes 48 resulting bits are transformed over again in to 32 bits, which is again permutated using another fixed table. In next round, this combination is used as the new left half [6].

2.3 Triple DES

Triple DES is an enhancement of data encryption standard. It uses 64 bit block size and 192 bits of key size. The encryption process of 3DES is similar to original DES but applied 3 times to increase the encryption level and average safe time [2].except that the three keys are used in the following order

1. 1st key is used for encryption.
2. 2nd key is used for decryption.
3. 3rd key is used for again another encryption.

Even though 3DES is more secure than DES, one of the observable disadvantages is that 3DES takes three times long as DES for encryption and decryption [6].

2.4 Blowfish

It is one of the most public domain encryption algorithms. Blowfish was designed by Bruce Schneider in 1993. Blowfish is faster than to existing encryption algorithms (DES, 3DES etc). Blowfish is a symmetric key block cipher that uses a 64 bit block size and 32 bits to 448 bits variable key length. Blowfish has variants of 14 rounds or less [7]. It is faster than DES on a Pentium/PowerPC-class machine.

2.5 AES (Advanced Encryption Standard)

The AES algorithm is a symmetric block cipher. AES block ciphers that can process data blocks 128 key bits, using cipher keys lengths 128,192,256 bits with 10,12,14 rounds . The algorithm may be used with the three different key lengths that may be referred to as “AES-128”, “AES-192”, & “AES-256” [8].it work with low complexity and high security on data.

Algorithm Steps: These steps used to encrypt 128-bit block

1. Set the round keys from the cipher key.
2. Initialize state array and add the initial round key.
3. Execute Usual Round = 1 to 9:
4. Execute Final Round.
5. Matching cipher text chunk output of Final [9].

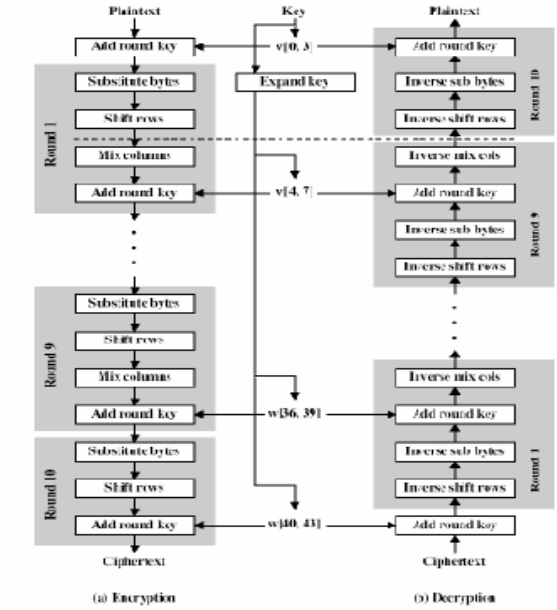

Figure 2: AES encryption and decryption [10]

The AES organizes the data block in four-row and row-major ordered matrix.

When AES encryption and decryption the data it uses the round function. Those round steps are:

1. Key Expansion using Rijndael key schedule

2. Initial Round

3. Encryption Round

3.1. Sub bytes: it is a non linear substitution step where each byte replaced with to a lookup table for encryption.

3.2. Shift rows: a transposition step each row of the state is shifted cyclically in left side.

3.3. Mix columns: This operation operate on the columns of the state, combining four bytes in each state.

3.4. Add round key: each bytes of states is combined with the round key; all round

3.5. Key is derived from cipher key using a key schedule.

4. Final Round: it not uses Mix columns round.

4.1 Sub Bytes

4.2 Shift rows

4.3 Add Round Key [11]

Decryption: Decryption involves reversing all the steps of encryption, using the inverse functions [9].

Algorithm	Created by	Year	Key size	Block	Round	flexible	feature
DES	IBM	1995	64 bits	64 bits	16	No	Not strong Enough, better in H/W then S/W
3DES	IBM	1978	112 or 168 bits	64 bits	48	Yes	Replaced for DES, Adequate security
Blowfish	Bruce Schneier	1993	32-448 bits	64 bits	16	Yes	Fast cipher in SSL
AES	Joan Daemen & Incent Rijmen	1998	128,192,256 Bits	128 bits	10,12,14	Yes	Replaced for 3DES.Excellent security,

Table1.Comparison between DES, 3DES, Blowfish and AES [4]

3. Conclusion

In this paper a new comparative study between DES, 3DES, blowfish and AES were present. Which are key length, cipher type, block size, developed, flexible, security, possibility key, and all these features proved the AES is better than DES, 3DES.and blowfish.

References

[1].Swati Kashyap, Er. Neeraj Madan, " A Review on: Network Security and Cryptographic Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, April 2015,pp1-5.

[2].Mamta. Juneja, and Parvinder S.Sandhu, "A Review of Cryptography Techniques and Implementation of AES for Images", International journal of computer Science and Electronics Engineering (IJSEE) Volume 1, Issue 4 (2013),pp 1-5.

[3].Anjula Gupta[1,] Navpreet Kaur Wali[2], "Cryptography Algorithms: A Review", International Journal of Engineering Development and Research **(www.ijedr.org),**2014 IJEDR | Volume 2, Issue 2,pp 1-6.

[4].M.Chanda Mona,S.Banu Chitra,V.Gayathri, " A SURVEY ON VARIOUS ENCRYPTION AND DECRYPTIO ALGORITHS",International Journal of security(IJS) Singraporem Journal of scientific Research(SJSR), available at:www.iaaet.org/sjsr,Vol.no.6 2014.pp 1-12.

[5]. Geeta D. Rote1, Dr. A. M. Patil2, "Steganography with Cryptography Technique For Data Hiding", International Journal of Science and Research (IJSR), Volume 4 Issue 1, January 2015,pp1-7.

[6]. Ali Makhmali, Hajar Mat Jani, "Comparative Study On Encryption Algorithms And Proposing A Data Management Structure", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 2, ISSUE 6, JUNE 2013,pp 1-7.

[7]. Pratap Chandra Mandal, "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish", Journal of Global Research in Computer Science Volume 3, No. 8, August 2012, pp1-4.

[8]. A.Sriram, G.Yuvaraj "Sub Pipelined Architecture for Self-Test Techniques of Crypto Devices Based on AES with High Throughput" International Journal of Innovations in Engineering and Technology (IJIET), Vol. 1 Issue 4 Dec 2012, pp 1-6.

[9]. Manjesh.K.N* R K Karunavathi, "Secured High throughput implementation of AES Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013,pp1-6.

[10] Uzzal Kumar Prodhan1, A.H.M. Shahariar Parvez2, Md. Ibrahim Hussain2,Yeasir Fathah Rumi2,Md. Ali Hossain3, "PERFORMANCE ANALYSIS OF PARALLEL IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD (AES) OVER SERIAL IMPLEMENTATION", International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.6, November 2012,pp 1-16.

[11]. Subashri T^1, Arunachalam R^2, Gokul Vinoth Kumar B^3, Vaidehi V^4, "Pipelining Architecture of AES Encryption and Key Generation with Search Based Memory International journal of VLSI design & Communication Systems (VLSICS) Vol.1, No.4, December 2010,pp1-13.