Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 7, July 2013, pg.146 – 151

REVIEW ARTICLE

A Comparative Security Study Review on Symmetric Key Cryptosystem Based Algorithms

SSVR Kumar Addagarla[1], Babji Y[2]

[1]Assistant Professor, Department of Computer Science, VITS College of Engineering, Vizag, India
[2]Assistant Professor, Department of Computer Science, VITS College of Engineering, Vizag, India

[1] ssvrkumar.research@gmail.com; [2] babji.research@gmail.com

***Abstract—** With the vast growth of the internet various kind of applications are developed for the different kinds of the users. Due to the decreasing cost of the internet and increasing the availability from a large amount of devices and applications the impact of attacks more significant. In such cases security is required to protect the data during the transmission. Generally let us say user 'A' transmits the sensitive information to the remote located user 'B'. In the process an unauthorized intruder let say 'I' may monitor the transmission and able to capture, modify and retransmit the information to the next party. To overcome this kind of security vulnerability in the transmission we required to implement the cryptography techniques likes the Symmetric key cryptology and/or Asymmetric key cryptology. In this paper we discussed the security dependencies and its vulnerabilities of the symmetric key crypto algorithms like DES, 3DES, AES, and IDEA.*

***Key Terms: -** Spoofing; Encryption; Decryption; Keysize; DES; TDES; AES; IDEA*

I. INTRODUCTION

Sensitive user Information is constantly transported between sessions after valid authentication and hackers are putting their best effort to steal them. Here we discuss the methods of the act of session hijacking in the network level mainly. Generally users are communicates using TCP/IP (Transmission control protocol) which is defined in RFC 739 [1] (Request for Comments). Intruders often target the source/destination machines using IP Spoofing and technique called the Man In the Middle Attack (MIMA).

a) IP Spoofing:

Spoofing is pretending to be someone else. That is nothing but assuming the identity of some one. This is a technique used to gain unauthorized access to the computer with an IP address of a trusted host.

b) Man in Middle Attack (MIMA):

It involves using a packet sniffer to intercept the communication between client and server. Packet sniffer has two categories, which are active sniffer and passive sniffer. Passive sniffer monitors and sniffs packet from a network having same collision domain. Active sniffer works with switched LAN network by ARP Spoofing. That is by sending the malicious ARP (address resolution protocol) packets mapping its MAC (media access control) Address to the default gateway address, so as to update ARP cache on the client to redirect the traffic to Intruder.

The security problems in the network level can overcome by using symmetric and asymmetric key encryption algorithms. In this paper we have discussed several symmetric key encryption algorithms and its security vulnerabilities. Whereas the symmetric algorithms uses the single shared key for the encryption and decryption process. In this paper we have discussed about the several single shared key algorithms like DES, TDES, AES and IDEA and their level of security in the present world scenario. The Symmetric key scenario can be shown in Fig .1.

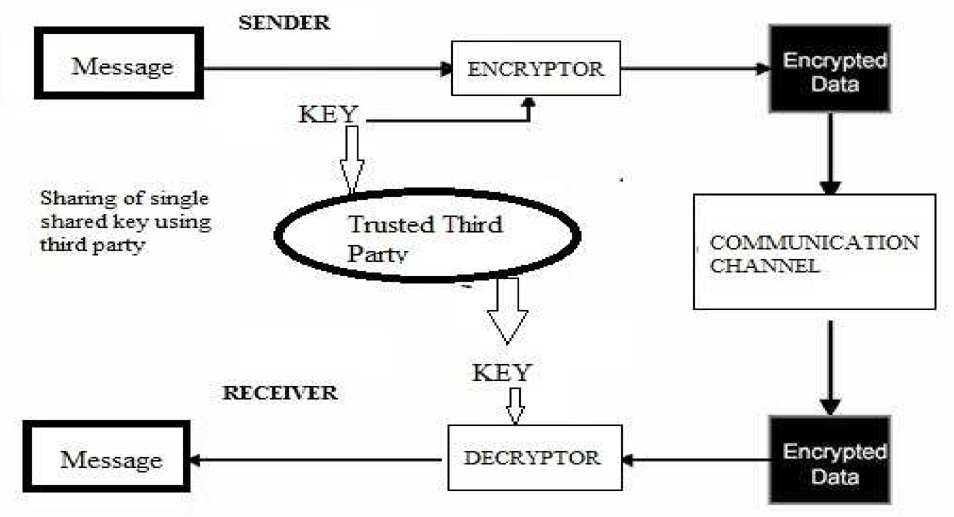

Fig .1. Symmetric Key Encryption Model

II. DES (DATA ENCRYPTION STANDARD)

The Basic process in enciphering a 64 bit data block and 56 bit key size using in DES. The round process is based on the horst Feistel network based on the Lucifer design developed by IBM in 1973 [1].

Process of DES:

- DES uses 16 rounds of Feistel network[2] process to generate the cipher text
- The plain text been divided into each 64bit blocks.
- For each round we use 48bit key as an input for the round generation from the 56bit key using permutation and left circular shit operations.
- In the DES the entire security is depends up on the 16 round generation process and shown in Fig.2

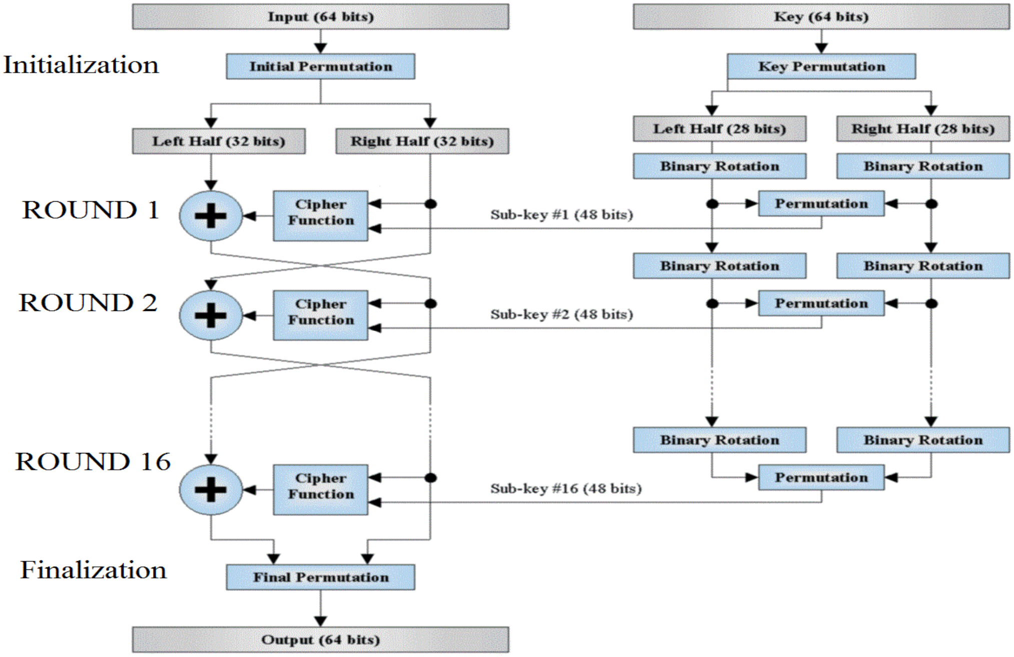

Fig.2. Data Encryption Standard Process

Security Vulnerability in DES

- The structural vulnerabilities of DES are its key size, and its short block size: with n-bit blocks, some encryption modes begin to have problem when 2n/2 blocks are encrypted with the same key.
- Hardware implementations of DES are very fast but DES was not designed for software and hence runs relatively slowly.

III. TRIPLE DES OR TDES OR 3DES

Triple DES was first standardized for use in financial applications in ANSI standard in 1985. It was incorporated of the Data encryption standard in 1999.[2]

Process of TDES:

It uses 3 keys and 3 executions of the DES algorithm.

i.e., C = E (K3, D (K2, E (K1, P)))

In the TDES it uses the 168 bit key length, so that Brute Force attacks are effectively impossible. The key usage for encryption and decryption are shown in Fig. 3

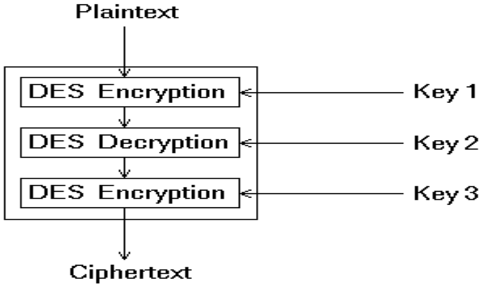

Fig.3. Triple DES Encryption

Security Vulnerability in TDES

3DES still suffers from the block size issues of DES and also, it is quite slow (DES was meant for hardware implementations, not software, and 3DES is even three times slower than DES).

IV. AES (ADVANCED ENCRYPTION STANDARD)

The original DES was designed for mid-1970's [2] for hardware implementation and doesn't produce efficient software code. Triple DES which was correspondingly slower than DES. So there is a need to produce a secure standard algorithm for Data Security while in transmission. NIST (National Institute for Standards and Technology) selected 15 algorithms and asked the cryptographic community to comment on them in a series of forums and workshops.[1] In 2000 the list had been reduced to five finalists:MARS (the IBM entry), RC6 (from RSA Laboratories), Rijndael (from Joan Daemen and Vincent Rijmen), Serpent and Twofish. Eventually **Rijndael** was selected to be the AES and the official announcement that it was the new standard was made on Dec. 4, 2001 (to be effective March 26, 2002). [5] Which is also approved by FIPS (Federal information processing standard publication).

Process of AES:

- AES is also based on the block cipher and the block size is 128bit
- In AES the key size varies from 128bit, 192 bit and 256bit.
- As we specified above for the round process it adopts the concept of Rijndael algorithm. In the actual Rijndael algorithm the block size also varies from 128,192, and 256bits.[1]
- AES uses 10, 12, 14 rounds. The key size which can be 128, 192, 256 bits depends on number of rounds.
- In the AES we have uses the total of 44 32bit word keys can be used if you select the key size of 128 bit as a standard.
- We initially started to covert bits into block to state matrix conversion and the to perform a pre-round transformation round followed by 10 rounds, where are as in the 9 rounds, same

operations are need to perform and in the 10th round we have a slight variation from the reaming rounds, that we need to remove 'Mix Column' operation from that.

- In the key generation initially we need to produce 4 32 bit words from the 128 bit key (Lets Say). This has to be given input to the pre-transformation round.
- For to generate remaining 40 32bit word keys we need to perform the following three operations :
    - ✓ Perform 1-bye circular rotation of 4 byte word on the last key of the previous round.[1]
    - ✓ Perform byte substitution for each byte of the word using S-box look up table.[1]
    - ✓ Perform an XOR (Exclusive-OR) operation with a Round constant Rcon(i) and this can be found by using the polynomial function based on the GF(2^8). [4]

Inner Round process

The AES begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of its Counterpart in the encryption algorithm. The four stages are as follows [5]:

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.

The process diagram and the round diagrams can be shown in the Fig .4

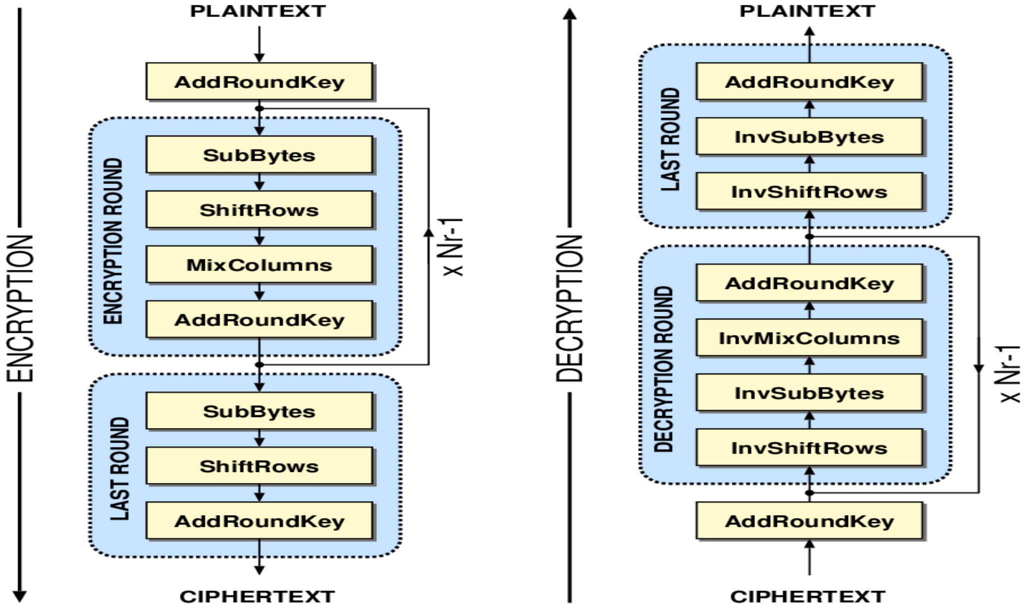

Fig.4. Advance Encryption Process

Security Vulnerability in AES

- The resistance of AES towards differential and linear cryptanalysis comes from a better "avalanche effect" (a bit flip at some point quickly propagates to the complete internal state) and specially crafted, bigger "S-boxes" (a S-box is a small lookup table used within the algorithm, and is an easy way to add non-linearity; in DES, S-boxes have 6-bit inputs and 4-bit outputs; in AES, S-boxes have 8-bit inputs and 8-bit outputs).[1] The design of the AES benefited from 25 years of insights and research on DES.

- Until May 2009, the only successful published attacks against the full AES were side-channel attacks on some specific implementations. The National Security Agency (NSA) reviewed all the AES finalists, including Rijndael, and stated that all of them were secure enough for U.S. Government non-classified data. In June 2003, the U.S. Government announced that AES could be used to protect classified information.[4]
- The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths. The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use. [5]

V. IDEA (INTERNATIONAL DATA ENCRYPTION STANDARD)

The algorithm was designed to achieve high data through put for use in real time communication system, especially for wireless communications. This is superior to DES algorithm. This algorithm also included in PGP (pretty good privacy) mail system. [6] It already becomes de-facto standard for encryption worldwide. It is also based on the block cipher. This symmetric block cipher was developed by XuejiaLai and James Messy in 1991. [6]

Design Principles:

IDEA uses the Block size of 64 bit and key size of 128 bit. [6] IDEA utilizes the 3- basic operations to achieve the process.

- Bit by Bit Exclusive OR operation
- Addition of unsigned integer modulo 2^{16} (65536)
- Multiplication of unsigned integer modulo 2^{16}+1(65537)

The Algorithm consists of eight identical rounds followed by a final transformation round. The 64bit plain text input is divided into 4 block of 16 bit each. Each round takes as 4 16bit blocks and 6 16bit sub keys and generates 4 16 bit blocks. In final round of transformation takes 4 16bit blocks and only takes 4 16bit sub keys and generates the cipher text. A total of 52 subkeys can be generated from the 128 bit using left circular shift operation randomly.

Round Process:

The plaintext block is divided into four 16 bit blocks say (P1, P2,P3, and P4) after ROUND1 you get the partially encrypted cipher text say (C1, C2,C3, and C4) which is given as input for the next round. Each of the rounds undergoes the below fourteen steps: (multiply means multiplication modulo 2^{16} + 1, and add means addition modulo 2^{16}) to get the final cipher text. The identical round process can be shown below.

1. Multiply P1 and the first subkey K1
2. Add P2 and the second subkey K2
3. Add P3 and the third subkey K3
4. Multiply P4 and the fourth subkey K4
5. XOR (results of steps 1 and 3)
6. XOR (results of steps 2 and 4)
7. Multiply (result of step 5, K5)
8. Add (results of steps 6 and 7)
9. Multiply (result of step 8, K6)
10. Add (results of steps 7 and 9)
11. C1:=XOR (results of steps 1 and 9)
12. C2:=XOR (results of steps 3 and 9)
13. C3:=XOR (results of steps 2 and 10)
14. C4:=XOR (results of steps 4 and 10)

At the end of round 8, final output transformation phase goes through these four steps:

1. Multiply X1 and the subkey, K49
2. Add X2 and the subkey, K50
3. Add X3 and the subkey, K51
4. Multiply X4 and the sub key, K52

Here X1, X2, X3 and X4 are the resultant four sub blocks after round8 and K49, K50, K51, K52 are the four 16 bit subkeys. Concatenating the resultant four sub blocks we get the final 64 bit cipher text. The 7 identical round processes can be shown in Fig.5

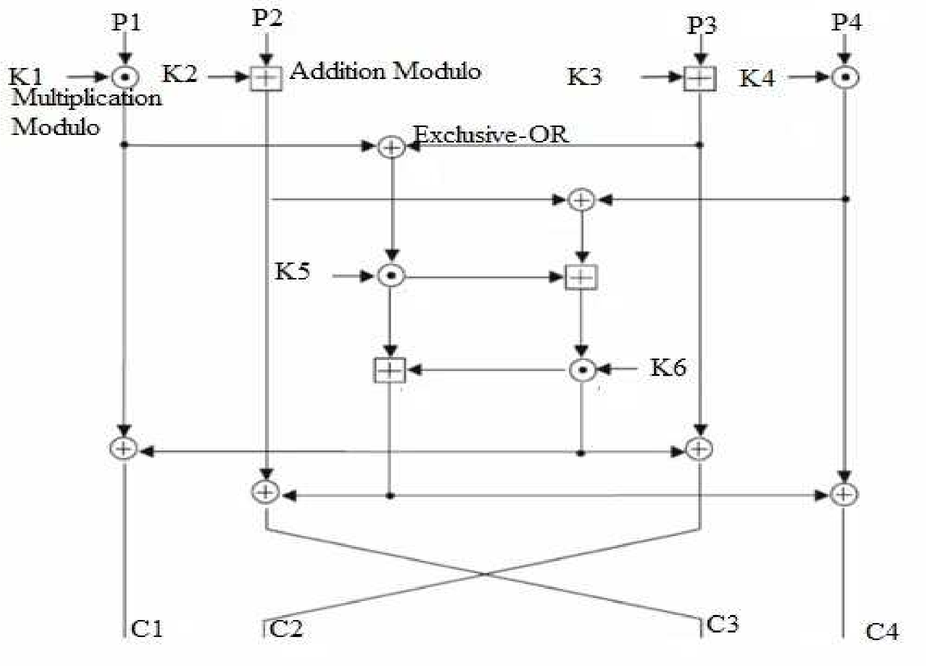

Fig.5. IDEA Round Process

Security Vulnerability:

As IDEA uses 128 bit key, which is double the key size of DES, 2^{128} encryption operation would be required to break idea [6]. Due to its strength against cryptanalytic attacks and due to its incorporation in many cryptographic packages, IDEA is widely used. Thus IDEA (International Data Encryption Algorithm) can be considered as one of the strongest block-cipher.

VI. CONCLUSION

This paper gives the detailed descriptions of the symmetric algorithms like DES, TDES, AES and IDEA. In the entire process of our review on these algorithms, we found that AES and IDEA are still strong based on its block, key size and the complexity of round process to make intruder gets harder to break the message. But still the use of the symmetric key encryption process are not alone are sufficient to send a secret information over a network now a days. In recent studies says that hackers can crack up to the 300 decimal digits or 700 bit key size in 2010 [7]. So we required and need to implement these algorithms along with the asymmetric key encryption algorithms like RSA with 2048 bit key size and MD5 for the use of sophisticated applications around the world.

REFERENCES

[1] W. Stallings -Cryptography and Network Security Principles and Practices Fourth Edition, Pearson Education, Prentice Hall, 2009.
[2] W. stallings, An Essential for Network Security-Applications and standards, 3rd Edition Pearson Education, Prentice Hall, 2009
[3] National Bureau of Standards, “Data Encryption Standard,” FIPS Publication 46, 1977
[4] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[5] Lynn Hathaway (June 2003). "National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information
[6] Lai, Xuejia, and Massey, James L, A Proposal for a New Block Encryption Standard, Advances in Cryptology EUROCRYPT ’90, Lecture Notes in Computer Science, Springer-Verlag, 1991: 389-404.
[7] http://en.wikipedia.org/wiki/Key_size