A Comparative Survey on Symmetric Key Encryption Techniques

Monika Agrawal
Department Of Computer Science
Shri ShankaraCharya Institute Of Technology & Management
Bhilai, India
monika.agrawal1986@gmail.com

Pradeep Mishra
Department Of Computer Science
Shri ShankaraCharya College Of Engineering & Technology
Bhilai, India
pradeepmishra4u@gmail.com

***Abstract*— Nowadays, the use of internet are growing increasingly across the world, security becomes a prime concern of issue for the society. Earlier security was a major issue for military applications but now the area of applications has been enhanced since most of the communication takes place over the web. Cryptography is an area of computer science which is developed to provide security for the senders and receivers to transmit and receive confidential data through an insecure channel by a means of process called Encryption/ Decryption. Cryptography ensures that the message should be sent without any alterations and only the authorized person can be able to open and read the message. A number of cryptographic techniques are developed for achieving secure communication. There are basically two techniques of cryptography- Symmetric and Asymmetric. This paper presents a detailed study of most of the symmetric encryption techniques with their advantages and limitations over each other.**

Keywords- Symmetric Encryption; Asymmetric Encryption; Cipher Text; Plain Text; Key

I. INTRODUCTION

In today's corporate world where access to information in lesser time is required with the goal of running the enterprise smoothly and efficiently, it is very important to give right information to right people at right time. What actually the information has been sent should be the same information been received. Suppose one person is sending an important file to the other person who is sitting at some other site office then the message passes through an insecure channel and may be possible that anyone in the middle can retrieve the message and modify it and then passes it to the destination. This will lead to many undesirable side-effects and the company may suffer a big loss in economical terms. Cryptography plays a very vital role in keeping the message safe as the data is in transit. It ensures that the message being sent at one end remains confidential and should be received only by the intended receiver at the other end.

Cryptography converts the original message in to non readable format and sends the message over an insecure channel. The people who are unauthorized to read the message try to break the non readable message but it is hard to do it so. The authorized person has the capability to convert the non readable message to readable one.

A. Basic Terms Used in Cryptography

- Plain Text
  The original message that the person wishes to communicate with the other is defined as Plain Text.
  In cryptography the actual message that has to be send to the other end is given a special name as Plain Text. For example, Alice is a person wishes to send "Hello Friend how are you" message to the person Bob. Here "Hello Friend how are you" is a plain text message.
- Cipher Text
  The message that cannot be understood by anyone or meaningless message is what we call as Cipher Text. In Cryptography the original message is transformed into non readable message before the transmission of actual message. For example, "Ajd672#@91ukl8*^5%" is a Cipher Text produced.

- Encryption
  A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. The process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.
- Decryption
  A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption
  algorithm are same.
- Key
  A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it. For example, if the Alice uses a key of 3 to encrypt the Plain Text "President" then Cipher Text produced will be "Suhvlghqw".

B. Purpose of Cryptography

Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography. [1]

- Confidentiality
  Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.
- Authentication
  The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity.
- Integrity
  Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.
- Non Repudiation
  Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.
- Access Control
  Only the authorized parties are able to access the given information.

C. Classification of Cryptography

Encryption algorithms can be classified into two broad categories- Symmetric and Asymmetric key encryption.

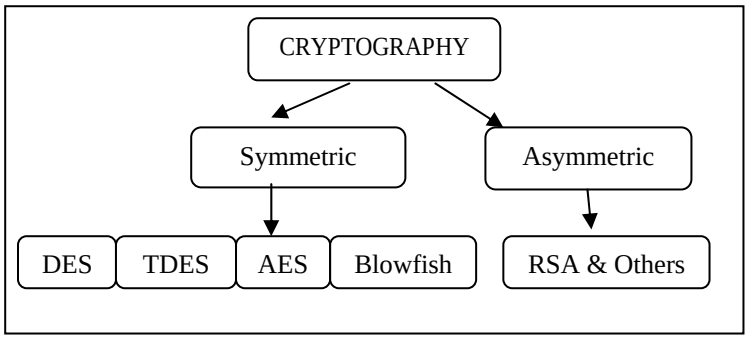

Figure 1. Classification Of Cryptography

- Symmetric Encryption
  In symmetric Cryptography the key used for encryption is similar to the key used in decryption. Thus the key distribution has to be made prior to the transmission of information. The key plays a very important role in symmetric cryptography since their security directly depends on the nature of key i.e. the key length etc. There are various symmetric key algorithms such as DES, TRIPLE DES, AES, RC4, RC6, BLOWFISH. [2]

- Asymmetric Encryption

In Asymmetric Key encryption, two different keys are used for encryption and decryption- Public and Private. The public key is meant for general use so it is available to anyone on the network. Anyone who wants to encrypt the plaintext should know the Public Key of receiver. Only the authorized person can be able to decrypt the cipher text through his own private key. Private Key is kept secret from the outside world.

For example, A wants to send message to B. The following steps are involved-

a) A and B should know public key of each other but private keys are kept secret.
b) A encrypts a Plain Text message for B by using B's public key.
c) A transmits the encrypted message (Cipher Text) to B.
d) B receives the cipher text and decrypts it using its own private key.
e) B gets the Plain Text message.

Symmetric Encryption Algorithm runs faster as compared to Asymmetric key algorithms. Also the memory requirement of Symmetric algorithm is lesser as compared to asymmetric. [3]

TABLE I. Equivalent Strength Table

Encryption bits	***Symmetric Algorithm***	***ASymmetric Algorithm (RSA)***
112	3DES	K=2048
128	AES-128	K=3072
192	AES-192	K=7680
256	AES-256	K=15360

The above table shows that for encrypting 256 bits of text, an RSA based encryption uses 15360 bits of key to provide as much security as that of AES with 256 bits. This shows that Symmetric algorithms are superior as compared to Asymmetric encryption algorithms.

II. PROBLEM DESCRIPTION

Cryptography came into existence due to the four fundamental problems exists while communication. They are Security, Authentication, Non Repudiation and Integrity Control. Consider the problem of a person wants to buy something on the web. When credit card number is transmitted over the network for online cash payment then security is a big concern for the buyer. On the other hand the vendor has to be sure that the credit card number is of legitimate user. So cryptography plays here a very important role of authenticating the identity of the buyer. Assuming the vendor accepts the transaction, how can they prove that you really did order the item and won't claim it wasn't you when the bill comes due? This is the non repudiation problem. Finally after the transaction, how can the vendor and buyer be sure that our communication is not being altered by any malicious interceptor?

Encryption is the process of converting the original plain text into non readable format. There are various encryption techniques exist in the cryptography such as DES, Triple DES, AES, RSA etc. But the problem arises in choosing the encryption technique is to select the algorithm with better key length. The second difficulty is to make choice on the implementation of cryptosystem or protocol. There are dozens of encryption algorithms available. But how to find which algorithm is better for encrypting the plain text will depend on the advantages and disadvantages of each algorithm.

Symmetric Encryption uses the same key concept to encrypt as well as decrypt. There are a number of benefits of this approach. Performance is relatively high. There are two aspects of this algorithm. The first is the encryption algorithm and the other is the key. The encryption algorithm is a process of transformations take place on the plain text with the key itself. At the time of decryption the same process of encryption is followed in a reverse manner with the same key. A strong algorithm should depend on its key entirely. These algorithms can be directly implemented on hardware easily. The weakness of symmetric algorithms is in sharing of symmetric key between sender and receiver.

Asymmetric encryption uses two different keys for encryption and decryption. The private key can only decrypt the encrypted message. No key other than private key can be used for decryption. The key exchange is not a problem in this approach. The public key can be known to anyone because it can be used only for encrypting the message. So anyone can encrypt the message but only the legitimate person can decrypt the message by using its own private key. Performance is relatively low as compared to symmetric key encryption. The problem of asymmetric encryption is it works slower as compared to symmetric encryption. Most asymmetric algorithms depend on the properties of hard problems in mathematics. These problems usually work intensive in one direction and nearly impossible in the other direction. For example, factoring the product of two large prime numbers. If one of the prime number is known then factoring becomes easy. But by knowing only the product it is very difficult to factorize and find the prime numbers.

III. METHODOLOGIES

A. DATA ENCRYPTION STANDARD (DES)

DES was the first encryption standard designed in 1973 and was recommended by NIST (National Institute of Standards and Technology) to be the most efficient method for encryption of data in 1976. This was the most widely used standard all across the world. [4]

It is a block cipher which encrypts 64 bit plaintext at a time and uses 56 bit key. This was based on symmetric key algorithm which means that the same key will be used for both encryption and decryption. DES can operate in CBC, ECB, CFB and OFB modes. DES has 16 rounds which mean a total of 16 processing steps are being applied on the input plaintext to produce cipher text. First, 64 bit data is passed through the initial permutation phase and then 16 rounds of processing takes place and finally the last step of final permutation is carried out on the input plain text which results in 64 bit cipher text.

The drawback of this algorithm is that it can be easily prone to Brute Force Attack in which the hacker attempts to break the key by applying all possible combinations. In DES there are only 2^56 possible combinations which are quite easy to crack. So DES is not so secure [7].

B. TRIPLE DES

The triple DES (3DES) algorithm was needed as a replacement for DES due to advances in key searching. [5] TDES uses three rounds of DES encryption and has a key length of 168 bits (56 * 3). Either two or three 56 bit keys are used in the sequence Encrypt-Decrypt-Encrypt (EDE). First option is to use three different keys for the encryption algorithm to generate cipher text on plaintext message t.

$$C(t) = E_{k1}(D_{k2}(E_{k3}(t))) \quad (1)$$

where C(t) is the cipher text of plaintext message t, E_{k1} is the encryption method using key k1, D_{k2} is the decryption method using key k2 and E_{k3} is the encryption method using key k3.
Another option is to use two different keys for the encryption algorithm. This reduces the memory requirement of keys in TDES.

$$C(t) = E_{k1}(D_{k2}(E_{k3}(t))) \quad (2)$$

TDES with three keys requires 2^168 possible combinations and that of two keys requires 2^112 possible combinations to be tried out for brute force attack is practically not possible. This provides TDES as a strongest encryption algorithm which gives its application in banking industry. The disadvantage of this algorithm is that it is too time consuming [1].

C. ADVANCED ENCRYPTION STANDARD (AES)

The US National Institute of Standards and Technology (NIST) recommended the use of Advanced Encryption Standard to replace Data Encryption Standard in 1998. AES is a variable bit block cipher and uses variable key length of 128, 192 and 256 bits. If both the block length and key length are 128 bits, AES will perform 9 processing rounds. If the block and key are of 192 bits, AES performs 11 processing rounds. If the block and key are of length 256 bits then it performs 13 processing rounds [6].
Each processing round involves four steps:

- Substitute bytes – Uses an S-box to perform a byte by byte substitution of the block,
- Shift rows – A simple permutation,
- Mix column – A substitution method where data in each column from the shift row step is multiplied by the algorithm's matrix and
- Add round key – The key for the processing round is XORed with the data.

AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices.

D. BLOWFISH

Bruce Schneier designed Blowfish algorithm in 1993 [4]. Blowfish is a 64 bit block cipher with variable length key from 32 bit (4 bytes) to 448 bits (56 bytes). The advantage of this algorithm is that it is highly secure and has not been cracked yet. It is suitable and efficient for hardware implementation.
The algorithm has two parts- Key expansion and Data Encryption. The key expansion step converts 448 bit key into 4168 bytes. A P array of size 18 and four S boxes whose size is 256 each of which are initialized to hexadecimal digits of π. XOR each entry in P array and S boxes with 32 bits of the key [9].

There are total 16 rounds of data encryption [8]. In each round a 32 bit subkey is XORed with leftmost 32 bits of plaintext and the result is then passed to the F function of Blowfish. This result becomes rightmost 32 bits for the next round and the output of F function is XORed with the original rightmost 32 bits of plaintext becomes leftmost 32 bits for the next round and so on.

1. Divide X into two 32-bit halves: XL, XR
2. For i = 1 to 16
XL = XL ⊕ Pi
XR=F(XL) ⊕ XR
Swap XL and XR
3. Swap XL and XR (Undo the last swap)
4. XR=XR ⊕ P17
5. XL = XL ⊕ P18
6. Concatenate XL and XR

Figure 2. Blowfish Encryption Algorithm

The F function is the kernel and distinguishing feature of Blowfish and is applied as follows [10].First Divide XL (32 Bits) into four 8-bit quarters: a, b, c, and d. Then apply the formula

$$F(XL)=\{(S1[a] + S2[b]) \oplus S3[c]\} + S4[d])\} \quad (3)$$

where + means addition modulo 2^32 , and $\oplus$ means exclusive OR and S1, S2, S3, S4 are four substitution boxes.

The key of the Blowfish algorithm is 448 bits, so it requires 2^448 combinations to examine all keys [11]. The advantage of blowfish algorithm is that it is simple to implement since all operations carried out are XOR and addition. Moreover the speed of encryption and decryption are also known to be faster than other popular existing algorithms [9].

IV. COMPARISON

A comparison of popular encryption algorithms based on block size, key size, number of rounds and attacks if occurred is shown on Table II.

TABLE II. Comparison of DES, Triple DES, AES and Blowfish algorithm

	Symmetric Encryption Algorithms			
	DES	***TDES***	***AES***	***BLOWFISH***
Block Size	64 bit	64 bit	128 bit	64 bit
Key size	56 bit	168 bit	128,192, 256 bit	32-448 bit
Created By	IBM in 1975	IBM in 1978	Joan Daeman in 1998	Bruce Schneier in 1998
Algorithm Structure	Fiestel Network	Fiestel Network	Substitution Permutation Network	Fiestel Network
Rounds	16	48	9,11,13	16
Attacks	Brute Force Attack	Theoretically possible	Side Channel Attacks	Not Yet

The security of any algorithm is highly based on the length of key being used. In the above table it is clear that the key size of blowfish algorithm is high and that of DES is lesser. Hence it can be said that security of Blowfish is far better than the other algorithms. Also DES and other algorithms are vulnerable to possible attacks but Blowfish algorithm has not been cracked till date.

V. CONCLUSION

This paper gives a detailed study of the popular symmetric key encryption algorithms such as DES, TRIPLE DES, AES, and Blowfish. Symmetric Key algorithms run faster than Asymmetric Key algorithms such as RSA etc and the memory requirement of Symmetric algorithms is lesser than Asymmetric encryption algorithms. Further, the security aspect of Symmetric key encryption is superior than Asymmetric key encryption. The comparison table of popular encryption algorithms clearly shows the supremacy of Blowfish algorithm over DES, AES and Triple DES on the basis of key size and security. The F function of Blowfish algorithm provides

a high level of security to encrypt the 64 bit plaintext data. Also the Blowfish algorithm runs faster than other popular symmetric key encryption algorithms.

ACKNOWLEDGMENT

The authors would like to thank anonymous reviewers for their valuable comments and suggestions that improve the presentation of this paper.

REFERENCES

[1] O.P Verma, Ritu Agarwal, Dhiraj Dafouti and Shobha Tyagi, "Peformance Analysis Of Data Encryption Algorithms",IEEE Delhi Technological University India, 2011.
[2] Diaa Salama, Abdul. Elminaam, Hatem Mohamed, Abdul Kader and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", International Journal of Computer Science and Network Security, vol.8 No.12, December 2008.
[3] Ketu File white papers, "Symmetric vs Asymmetric Encryption", a division of Midwest Research Corporation.
[4] Tingyuan Nie and Teng Zhang," A Study of DES and Blowfish Encryption Algorithm", IEEE, 2009.
[5] Aamer Nadeem and Dr M. Younus Javed , "A Performance Comparison of Data Encryption Algorithms", IEEE, 2005.
[6] Himani Agrawal and Monisha Sharma, "Implementation and analysis of various symmetric cryptosystems", Indian Journal of Science and Technology Vol. 3 No. 12, December 2010.
[7] Diaa Salama, Abdul Minaam, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud, "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types", International Journal of Network Security, PP.78-87, Sept. 2010.
[8] Allam Mousa, "Data Encryption Performance Based on Blowfish", 47th International Symposium ELMAR-2005.08-1 0, June 2005.
[9] Russell K. Meyers and Ahmed H. Desoky, "An Implementation of the Blowfish Cryptosystem", IEEE, 2008.
[10] Noohul Basheer Zain Ali and James M Noras, "Optimal Datapath Design for a cryptographic processor: The Blowfish Algorithm", Malaysian Journal of Computer Science, Vol. 14 No. 1, pp. 16-27, June 2001.
[11] Michael C.-J. Lin and Youn-Long Lin, "A VLSI Implementation of the Blowfish Encryption/Decryption Algorithm", IEEE, 2000.

AUTHORS PROFILE

Monika Agrawal, Assistant Professor at Shri Shankaracharya Institute Of Technology & Management, Bhilai, India obtained her B.E in Computer Science from Bhilai Institute Of Technology, Durg in 2008.She is pursuing M.E in Computer Technology Application from S.S.C.E.T Bhilai, India.

Pradeep Mishra, Assistant Professor at Shri Shankaracharya College Of Engineering & Technology, Bhilai, India obtained his M.E (Computer Technology Applications) from SSCET, Bhilai, India in 2008.