Methods of Symmetric-Key Encryption: A Survey and Comparison

Mr S VARA VINOD UNGARALA[1], Ms Kotikalapudi Devi Dhana Lakshmi[2], POSIMSETTI T CHIRANJEEVI SWAMY[3]
Asst. Professor[1,2,3]
Dept. of Computer Science and Engineeering,
Bhimavaram Institute of Engineering and Technology, Bhimavaram, Andhra Predesh, India.
E.mail id: satyamtech12@gmail.com, devibiet517@gmail.com, chiranjeevi.pt@gmail.com

***Abstract*—** With the proliferation of internet usage throughout the globe, protecting its users has become an urgent social priority. Security used to be a big concern for military applications, but now that most of the communication happens online, the field has expanded greatly. Cryptography is a subfield of computer science that uses a technique called encryption and decryption to ensure the privacy of data while transmission across an unsecured channel. Using cryptography, you may be certain that your communication will reach its intended recipient unaltered and that only they will be able to decipher and read it. Multiple cryptography methods are created to ensure confidential transmissions. Symmetric and asymmetric cryptography are the two main approaches to the field. This document compares and contrasts the strengths and weaknesses of the most popular symmetric encryption methods currently in use..

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

I. INTRODUCTION

It is crucial to get the correct information to the right people at the right time in today's fast-paced business environment so that the firm may function smoothly and effectively. It is expected that the information supplied and received are same. Let's say two people at different sites need to share a crucial file, but they're separated by an unsecured channel that may allow a third party to intercept the transmission, alter it, and resend it. Many unfavorable consequences will follow, and the organization might potentially incur significant financial loss as a result. The use of cryptography is crucial to ensuring the confidentiality of communications while data is in transit. It guarantees that only the intended recipient, on the other end, will be able to read the message you send.

Using cryptography, a message is transformed into an unreadable format before being sent across an unsecured channel. Those who aren't supposed to be able to read the message attempt to crack the code, but they have a hard time doing so. If the right individual is given access, they can decipher an unreadable communication.

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.

•Just the Facts
Plain text refers to the unaltered, as-sent communication between two parties.
Plain Text is a term used in cryptography to refer to the actual message that must be sent. For instance, Alice wants to ask Bob how he is doing by sending the message "Hello Friend how are you?" The simple sentence "Hello Friend how are you" is seen below.

Coded Message
Cipher text refers to any communication that is unintelligible or has no real-world significance. Before sending a message, cryptography converts the original text into an unreadable version. Cipher texts like

"Ajd672#@91ukl8*5%" are only one example.

• Encryption

Encryption is defined as the procedure by which Unencrypted Text is transformed into Cipher Text. Encryption is used in cryptography to convey secret information through a less-than-secure network. In order to encrypt data, two things are needed: an encryption technique and a key. The process of encrypting data is referred to as an encryption algorithm. The sender is responsible for the encryption process.

• Decryption

Decryption refers to the process of unencrypting data. It's the method used to decipher encrypted messages. Decryption is the process used by the recipient of a cryptographic communication to recover the original message from the encrypted one (Cipher Text). Both a Decryption algorithm and a key are needed for the decryption process to work. When we talk about a Decryption algorithm, we're referring about the method actually used. In most cases, the same algorithm is used for both encryption and decryption.

• Key

A Key may be a string of numbers, letters, or symbols. The Key is utilized both during the encryption of the Plain Text and the decoding of the Cipher Text. In Cryptography, the key selection is crucial since it directly affects the safety of the encryption technique. If Alice encrypts the plaintext "President" using a key of 3, the resulting ciphertext will read "Suhvlghqw."

B. Cryptography's Original Intent

To protect sensitive information and prevent unauthorized changes, cryptography offers a variety of safeguards. Cryptography is frequently employed now because of the considerable security benefits it provides. The many motivations for using encryption are listed below. [1]

• Confidentiality

The recipient of a transmission of data stored in a computer system must be the only person permitted to see the data.

• Authentication

Any system receiving data must verify the identity of the sender to determine whether the data is coming from a trusted source.

• Integrity

The recipient is the only one who can make changes to the data being sent. Between the sender and the recipient, no one may change the message in any way.

* Non-Refutation

Makes it such that neither the sender nor the recipient may claim they never received the communication.

• Managing Entry/Exit

The information is restricted to those who have been granted access.

Cryptography Classification

There are two major types of encryption techniques, called symmetric and asymmetric key encryption.

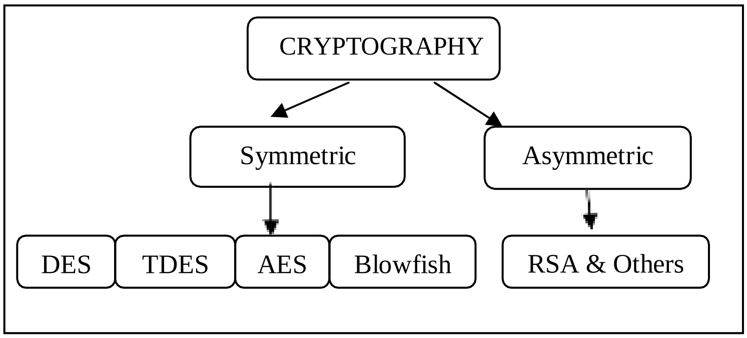

Figure 1. Classification Of Cryptography

- Symmetric Encryption

In symmetric cryptography, the encrypting and decrypting keys are the same. Therefore, key distribution must occur before data can be sent. In symmetric cryptography, the key is crucial since the strength of the encryption relies on the specifics of the key, such as its length and complexity. DES, TRIPLE DES, AES, RC4, RC6, and BLOWFISH are only a few examples of symmetric key algorithms. [2]

Encryption with Different Keys

With Asymmetric Key encryption, you'll need two keys—a public one and a private one—to encrypt and decode data. The public key's intended audience is the whole network community. The plaintext can only be decrypted by those who have the receiver's Public Key. The encrypted text may be decrypted using the authorized party's private key. The private key is protected from public knowledge.

Let's say A has a message he or she needs to convey to B. The process includes the following actions:

a) A and B must have each other's public keys, but keep their private keys secure.

b) Using B's public key, A encrypts a Plain Text message for B.

c) A sends B the decrypted version of the message (called the Cipher Text).

d) Once B has received the encrypted text, it may decode it with its own private key.

f) The Plain Text message is sent to B.

There is a performance advantage for symmetric encryption methods over their asymmetric counterparts. Symmetric algorithms also have lower memory requirements than asymmetric ones. [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

The four main issues with communication that led to the development of cryptography. They are privacy, confidentiality, availability, and trust. Think about the challenge faced by someone who wants to make an online purchase. Customers worry about their personal information being compromised whenever their credit card number is sent over the internet to make an online cash purchase. However, the store must verify that the credit card number belongs to a real person. Therefore, encryption plays a crucial function in establishing the buyer's credibility. What guarantees does the seller have that you really placed the purchase and won't try to pass the buck when the bill arrives? The non repudiation dilemma is this. After the deal is done, how can the buyer and seller be confident that their communications have not been tampered with?

During encryption, the plain text is transformed into an unreadable code. The field of cryptography is home to several different types of encryption methods, including the DES, Triple DES, AES, RSA, and many more. The challenge that emerges when deciding on an encryption method is picking an algorithm with an adequate key length. The second challenge is the selection of an appropriate cryptosystem or protocol for implementation. Numerous algorithms for secure communication are at your disposal. Consider the benefits and drawbacks of each algorithm to determine which one is best for protecting the plain text.

Symmetric To both encrypt and decode, encryption relies on the same basic idea. The advantages of this method are many. The efficiency is above average. This algorithm may be broken down into two parts. The first is the method of encryption, while the second is the secret key. The key is used in an algorithm to perform a series of transformations on the plaintext. When decrypting, the same key is used to perform the encryption process in reverse. The key is the most important part of every powerful algorithm. These algorithms lend themselves well to direct hardware implementation. Sharing a symmetric key between the sender and recipient is a security hole in symmetric algorithms.

To encrypt and decode data, asymmetric encryption employs two separate keys. The encrypted communication is unreadable without the secret key. Decryption requires the private key and no other key will work. In this method, exchanging keys is not a concern. Since the public key can only be used to encrypt the message, anybody with access to the internet may learn it. The communication may be encrypted by anybody, but only the intended recipient, using their own private key, can read it. When compared to symmetric key encryption, performance is subpar. Asymmetric encryption suffers from being less efficient than symmetric encryption. Most asymmetric algorithms rely on certain mathematical features of very challenging situations. These issues often require substantial effort in one direction yet are intractable in the other. For instance, dividing by two very big primes to get a smaller number. Factoring is straightforward if a single prime number is known. However, factoring and locating the prime numbers when just the product is known is an extremely challenging problem.

III. METHODOLOGIES

A. DATA ENCRYPTION STANDARD (DES)

The National Institute of Standards and Technology (NIST) deemed DES to be the best effective technique of data encryption in 1976, after it had been the first encryption standard created in 1973. Across the globe, this was the gold standard. [4]

It is a block cipher that employs a 56-bit key to encrypt 64 bits of plaintext all at once. The same key will be used for both encryption and decryption since this method is based on a symmetric key technique. DES may function in four different modes: CBC, ECB, CFB, and OFB. There are 16 rounds in DES, which means that the input plaintext goes through 16 iterations of processing before any encrypted text is produced. The input plain text is permuted 64 times, then processed 16 times, and finally the final permutation is performed, yielding encrypted text that is also 64 bits in length.

The downside of this approach is that it is vulnerable to Brute Force Attacks, in which hackers try all conceivable combinations of input data in an effort to crack the key. DES is easily broken since it only uses 256 potential combinations. Therefore, DES is not very safe [7].

TRIPLE DES B.

Due to developments in key searching, the triple DES (3DES) algorithm was required as a substitute for DES.

[5] TDES employs 168-bit (56 * 3) keys and three iterations of DES encryption. Encrypt-Decrypt-Encrypt (EDE) use a series of two or three 56-bit keys. The first possibility is to produce cipher text from plaintext message t using three separate keys for the encryption process.

Assume that (1) C(t) = Ek1 (Dk2 (Ek3 (t))

where Ek1 is the encryption technique with key k1, Dk2 is the decryption method with key k2, and Ek3 is the encryption method with key k3.

Alternatively, you may choose a system that requires two separate encryption keys. This decreases the space needed for TDES keys in the computer's memory.

Ek1 (Dk2 (Ek3 (t)) = Ek3 (t) (2)

In order to try all 2168 potential combinations for a three-key TDES, and 2112 for a two-key TDES, a brute-force approach is almost impossible. Because of this, TDES may be used in the financial sector as a robust encryption technique. The major drawback of this technique is its lengthy execution time [1].

C. HIGH-GAIN ENCYPTION STANDARD (AES)

When Data Encryption Standard was phased out in 1998, the US National Institute of Standards and Technology (NIST) suggested using Advanced Encryption Standard instead. Key lengths of 128, 192, and 256 bits may be used with AES, since the cipher is a variable-bit block cipher. For 128-bit block and key sizes, AES uses 9 rounds of processing. With a 192-bit block and key, AES uses 11 rounds of processing. It takes 13 iterations of processing if the block and key are both 256 bits in length [6].

There are four stages in each processing cycle:

- Substitute bytes - Makes use of an S-box to replace the block's bytes one by one
- Swap Rows - A Basic Sort

Each column's data from the shift-row step is multiplied by the algorithm's matrix and then substituted.

Data is XOR'd with the round key, which is added, to create the final output.

AES encryption is both quick and adaptable, meaning it may be used in a wide variety of contexts and devices, particularly those with limited resources.

D. BLOWFISH

Blowfish is an algorithm that was created in 1993 [4] by Bruce Schneier. Blowfish is a block cipher that uses a 64-bit key that may be anywhere from 32 bits (4 bytes) to 448 bits (56 bytes) in length. This algorithm's main benefit is that it has not been broken into. It can be efficiently implemented in hardware and serves its intended purpose.

Key expansion and data encryption are the two main components of the technique. In the process of key enlargement, a 448-bit key becomes a 4168-byte one. Initialized to the hexadecimal value of are a P array of size 18, as well as four S boxes of size 256. 32-bit XOR operation between P array and S boxes [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
        $XL = XL \oplus Pi$
        $XR=F(XL) \oplus XR$
        Swap XL and XR
3.  Swap XL and XR (Undo the last swap )
4.  $XR=XR \oplus P17$
5.  $XL = XL \oplus P18$
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

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

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

Popular symmetric key encryption algorithms including DES, TRIPLE DES, AES, and Blowfish are thoroughly analyzed in this work. When compared to Asymmetric Key algorithms like RSA, etc., Symmetric Key algorithms are more efficient and need less memory to perform. Symmetric key encryption also offers a higher level of security than its Asymmetric counterpart. In terms of both key size and security, the Blowfish algorithm is much superior to other common encryption algorithms like DES, AES, and Triple DES, as seen in the comparative table below. Since the Blowfish algorithm has a F function, it also superior safety while encrypting the 64-bit plaintext. When compared to other well-known symmetric key encryption techniques, the Blowfish algorithm is also noticeably quicker.

REFERENCES

The following is an excerpt from "Peformance Analysis Of Data Encryption Algorithms" by O.P. Verma, Ritu Agarwal, Dhiraj Dafouti, and Shobha Tyagi, published in 2011 by IEEE Delhi Technological University in India.

In December 2008, the International Journal of Computer Science and Network Security published "Performance Evaluation of Symmetric Encryption Algorithms" by Diaa Salama, Abdul. Elminaam, Hatem Mohamed, Abdul Kader, and Mohie Mohamed Hadhoud.

[3] Ketu File white papers, "Symmetric vs. Asymmetric Encryption," published by Midwest Research Corporation.

As an example, see [4] "A Study of DES and Blowfish Encryption Algorithm" by Tingyuan Nie and Teng Zhang from the IEEE in 2009.

In 2005, the IEEE published "A Performance Comparison of Data Encryption Algorithms" by Aamer Nadeem and Dr. M. Younus Javed.

According to [6] "Implementation and analysis of various symmetric cryptosystems" by Himani Agrawal and Monisha Sharma in the December 2010 issue of the Indian Journal of Science and Technology, Volume 3, Number 12.

According to [7] "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types," published in the September 2010 issue of the International Journal of Network Security, pages 78–87.

According to [8] Allam Mousa, "Data Encryption Performance Based on Blowfish", 47th International Symposium ELMAR-2005.08-1 0, June 2005.

In 2008, IEEE published "An Implementation of the Blowfish Cryptosystem" by Russell K. Meyers and Ahmed H. Desoky.

In June 2001, the Malaysian Journal of Computer Science published "Optimal Datapath Design for a Cryptographic Processor: The Blowfish Algorithm" by Noohul Basheer Zain Ali and James M. Noras.

Using a very low-power integrated circuit, Michael C.-J. Lin and Youn-Long Lin were able to publish "A VLSI Implementation of the Blowfish Encryption/Decryption Algorithm" in IEEE in 2000.