Smart Symmetric Key Encryption Algorithms

R.Raja[1], Dr.V.Dhanakoti[2]
[1, 2] Department of Computer Science and Engineering
[1, 2]Valliammai Engineering College, Chennai

Abstract- *Security is an important aspect for everything. Internet and network application are increasing manner day-by-day. And also the amount of information to be transferred over the internet or other media types are increasing. The better solution for providing the protection against the attackers or man in the middle or intruders is cryptography. Cryptography is converts the data or information from normal form into an unreadable form by using encryption and decryption technique. Cryptography provides a facility and ensure the data to be sent securely and is able to open and read a message by only the authorized person. Cryptographic techniques basically divide into two techniques, they are Symmetric and Asymmetric. Data security is the important key factor for network communication. The traditional methods of encryption is maintain only data security so modern cryptography is consider and needed to enhance the data security and faster communication. The following are some of the encryption techniques that is used for efficient encryption and enhance data security.*

Keywords- Cryptography, Encryption, Decryption, AES, DES, TRIPLEDES, Blowfish.

I. INTRODUCTION

A. Cryptography

Cryptography is the form of secret writing. It is the way of secret writing. Cryptography is used to protecting the information by converting it into an unreadable format and only the intended recipient will be able to convert it into original text. The main objective is to keep the data secure from unauthorized access. Data can be read and understood without any special measures is called plaintext. The method of convert plaintext to hide its substances is called encryption. Encrypting plaintext results is unreadable format called cipher text. The process of changing cipher text to original plaintext is called decryption. The system provides both encryption and decryption is called cryptosystems. This paper explains some of the encryption techniques and security issues.

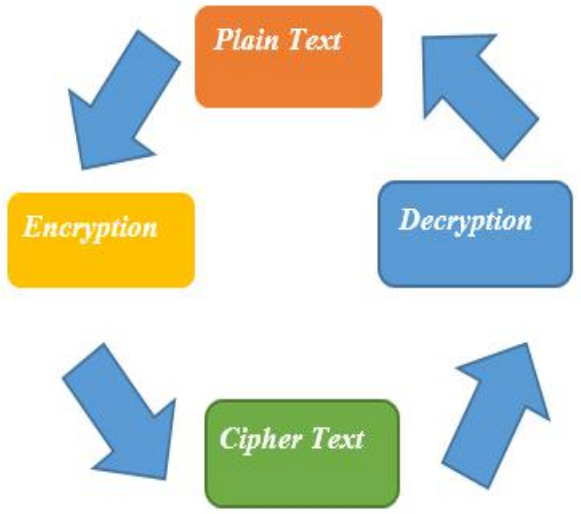

Fig.1 Cryptosystems

Cryptography consider the security goals and to ensure the privacy of data, on-alteration of data and so on. Cryptography is the methods that allow data or information to be sent securely in network and only the authorized person able to retrieve this information. Network security is majorly based on cryptography. Cryptography is the method of hiding the information by encrypting the message using algorithms. The cryptography system is performs encryption and decryption process. In todays, the cryptography is considered all fields such as mathematics, computer science, information theory, computer security, and engineering. The security level of cryptography is determined by the key space (size of key).

B. Goals of Cryptography

a) Confidentiality:

Confidentiality is the word defines the information transmitted in computer and has to be accessed only by the authorized person and not by anyone else.

b) Authentication

To check the identity of whether the authorized sender sends the information or a false identity and also to check the identity of whether the authorized receiver receives the information.

c) Data Integrity

To Ensuring the information has not been altered by any unauthorized or unknown persons. (i.e.,) no one in between the sender and receiver are allowed to alter the message.

d) Access Control

Authorized persons are only able to access the given information.

C. Basic Terminology used in cryptography

a) Plain Text

The original message which is to be sent from sender to the receiver. For example: if Ramesh wants to send a message "hello world" to Suresh then it is consider as a plain text.

b) Cipher Text

Cipher text is produced after using encryption process. Cipher text is a text which is to be sent from sender to receiver and it is not understandable by anyone. For example: "hello world" is the plain text and its cipher text is "*@97K&A%L#1".

c) Encryption

It is the process of converting a plain text into cipher text by using encryption key and an algorithm.

d) Decryption

It is the process of converting a cipher text into a plain text by using decryption key and an algorithm.

e) Keys

Key is a numeric or alpha numeric text or may be a special symbol.

II. CLASSIFICATION OF CRYPTOGRAPHY

Cryptography majorly divided into two category based on the use of key.

A. Symmetric Encryption (Private Key Encryption)

In this type of encryption same key is used both encryption and decryption. The key plays a vital role for in this type of encryption. The key distribution has to be made before the transmission of data or information starts.

Example: DES, 3DES, BLOWFISH, AES etc.

B. Asymmetric Encryption (Public Key Encryption)

Different key is used for encryption and decryption. Two different keys are generated, one key is used for encryption and another key is used for decryption. Receiver side key is send before transmission starts. Example: RSA algorithm.

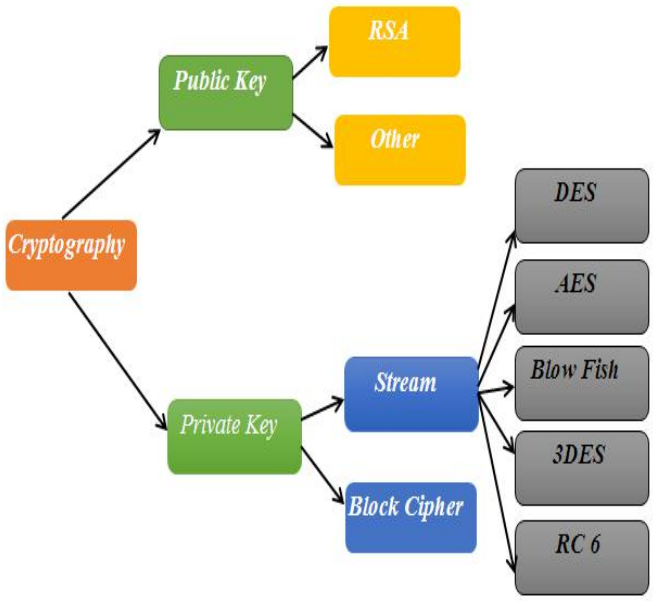

Fig.2 Cryptography

III. SYMMETRIC KEY ENCRYPTION ALGORITHM

A. Data Encryption Standard (DES)

DES was the first encryption algorithm to be published by NIST (National Institute of Standards and Technology). After that it was further designed by IBM based on their Lucifer Cipher. At initially, 56 bits keys are selected from the initial 64 by permuted choice(1). The remaining eight bits may discarded or used as parity check bits. Further that the 56 bits are divided into two 28-bit halves. In successive rounds, both halves are rotated left by one or two bits and then 48 sub key bits are selected by permuted choice(2), 24 from the right half and 24 bits from the left. The key schedule for decryption is similar, the sub keys are in reverse order compared to encryption.\

B. Advanced Encryption Standard (AES)

AES is a symmetric block cipher. The same key is using for both encryption and decryption. AES is developed by National Institute of Standards and Technology (NIST) in December 2001. It is a non Feistel cipher that encrypts and decrypts a data block of 128 bits. The key size may be 128,192, or 256 bits, depends on the number of rounds. It uses 10, 12, or 14 rounds. If both block length and key length are 128 bits, AES will perform 9 processing rounds.

- Block and key are 192 bits - AES will perform 11 processing rounds

- Block and key are 256 bits- AES performs 13 processing rounds.

One single processing rounds involves four steps:

• Substitute bytes: S-box is used to perform a byte by byte substitution of the block.

• Shift rows: A simple permutation.

• Mix column: data in each column from the shift row is multiplied by the algorithm's matrix.

• Add round key: processing round Key is XOR'ed with the data. A number of AES parameters depend on the key length. At present the most common key size likely to be used is the 128 bit key.

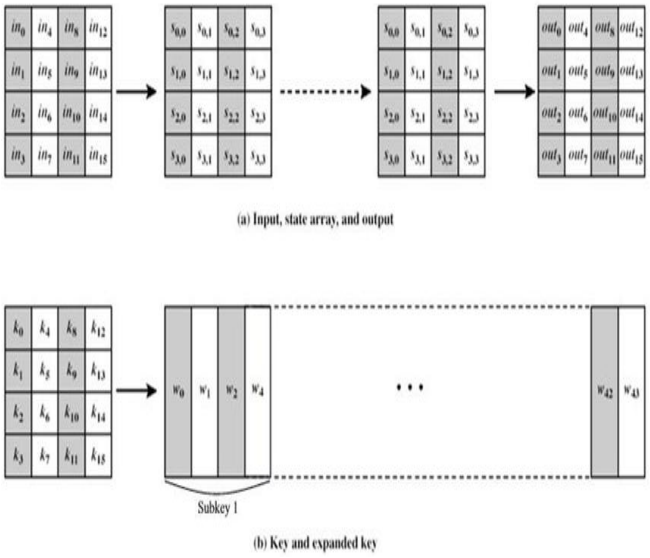

Fig.3 Data structures in the AES algorithm.

C. Triple DES

TRIPLE DES is the short name for Triple Data Encryption Algorithm block cipher, which applies the Data Encryption Standard cipher algorithm three times to each data block. The DES cipher's original key size is 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES increasing the key size of DES to protect against such attacks. It takes three 64- bit keys, for an overall key length of 192 bits. In Triple DES,

- The data is encrypted with the first key
- Decrypted with the second key
- Finally encrypted with the third key

Triple DES is runs 3 times slower than DES, but it provide more secure. The procedure for decrypting and encryption is the same, except it is executed in reverse.

D. Blowfish

Blowfish was developed in 1993 by Bruce Schneier and is this method of algorithm is designed for fast, free alternative to existing encryption algorithms. Blowfish is a symmetric block cipher method that effectively used for encryption and protecting of data. Variable-length key is taken, from 32 bits to 448 bits, making it ideal for securing data. The block size is 64 bits, and key can be any length up to 448 bits. It is more faster than most encryption algorithms when implemented on 32- bit microprocessors. The algorithm consists of two parts:

• A key expansion part and
• A data-encryption part.

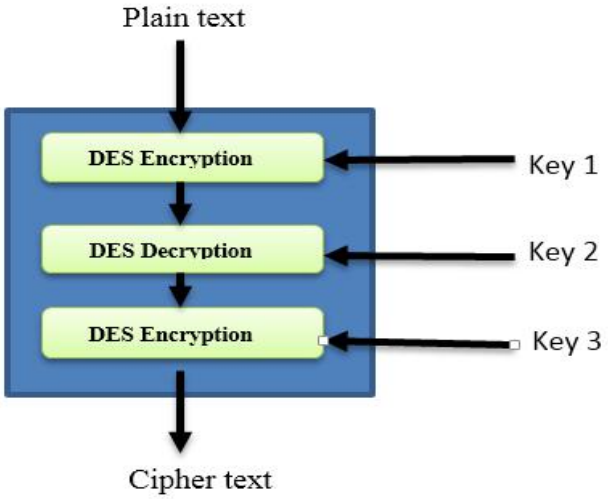

Fig.3 Data structures in the AES algorithm

IV. CONCLUSIONS

This paper discuss the symmetric key encryption algorithms like AES, DES, TRIPLEDES and BLOWFISH. When compared to those algorithms the Blowfish algorithm uses a variable number of bits ranging from 32 to 448 bits and encrypts the data 16 times. In this type of algorithm is not possible for the hacker to decrypt it. Data security is one of the import key for communication. Security in network can be achieved by using cryptography. There is so many algorithms is available for cryptography. The selection of one of the best algorithm is also very important. The algorithm can be selected based on the type of data being communicated. Those encryption techniques are analyzed to enhance the data security. As the day passes modern encryption is needed to promote the data security.

REFERENCES

[1] W. Stallings, "Cryptography and Network Security Principles and Practices Fourth Edition", Pearson Education, Prentice Hall, 2009.

[2] Tingyuan Nie, and Teng Zhang , "A Study of DES and Blowfish Encryption Algorithm", IEEE, 2009.

[3] Singh, S preet, and Maini, Raman "Comparison of Data Encryption Algorithms", International Journal of Computer science and Communication,vol.2,No.1,January-June 2011,pp.125-127.A.

[4] Atul khate, Cryptography and Network Security, 2nd Ed, Tata Mcgraw hill, 2009, pp.87-2004.

[5] Himani Agrawal and Monisha Sharma, "Implementation and analysis of various Symmetric Cryptosystems", Indian Journal of science and Technology vol.3, No.12, December 2012.

[6] Y.Wang and M. Hu, ―Timing - evaluation of the known cryptographic algorithms, in proc. International Conference on Computational Intelligence and Security, Beijing, China Dec 2009.

[7] International Journal of Computer Theory and Engineering, Vol. 5, No. 4, August 2013 Multiphase Encryption: A New Concept in Modern Cryptography by Himanshu Gupta and Vinod Kumar Sharma.

[8] International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July 2012 A Survey on Various Most Common Encryption Techniques by E.Thambiraja, G. Ramesh and Dr. R. Umarani.

[9] Coppersmith, D. "The Data Encryption Standard (DES) and Its Strength Against Attacks."I BM Journal of Research and Development, May 1994, pp. 243 -250.

[10] Mohammed Abutaha, Mousa Farajallah, Radwan Tahboub & Mohammad Odeh Survey Paper: Cryptography Is The Science Of Information Security International Journal of Computer Science and Security (IJCSS), Volume (5): Issue (3) : 2011 298

[11] IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011 Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures by Yogesh Kumar1, Rajiv Munjal2, Harsh Sharma3

[12] Simar Preet Singh, and Raman Maini "COMPARISON OF DATA ENCRYPTION ALGORITHMS" International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 125-127

[13] Shashi Mehrotra Seth, 2Rajan Mishra," Comparative Analysis of Encryption Algorithms for Data Communication", IJCST Vol. 2, Issue 2, June 2011 pp.192- 192.

[14] Diaa Salama Abd Elminaam1, Hatem Mohamed Abdual Kader2, and Mohiy Mohamed Hadhoud2," Evaluating The Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vol.10, No.3,5-17.