International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 4, Special Issue 1 (September '2018)
Special Issue on 2nd National Conference on Advanced Computing and Communication Technologies,
Conference held at Siri PSG Arts and Science College for Women, Sankari,Tamilnadu,India.

A COMPARATIVE STUDY OF A VARIETY OF CRYPTOGRAPHIC TECHNIQUES

M.Thulasimani,
Research Scholar,
Department of Computer Science,
Vivekanandha College for Women,
Tiruchengode, Tamilnadu,India.

M.Valarmathi,
Head of the Department
Department of Computer Science,
Vivekanandha College for Women,
Tiruchengode, Tamilnadu,India.

Abstract: In today's communication is very important role which help in growth of new technologies. Whatever we want to send file from one location to another location in the network, many unauthorized users are illegally access the information .So security is an important parameter to be considered. The study of both encryption and decryption is known as cryptography. So these technology is used to secure the data. The process of transforming the original information into an unreadable format is known as encryption. The process of converting the unreadable format in to the original information is known as decryption. These techniques and algorithm are used to which is better algorithm for communication purpose.

Keywords: Encryption, Decryption, AES, DES, RSA.

I.INTRODUCTION

Cryptography is a most important of securing electronic documents. Its use two techniques such that Encryption and Decryption. Encryption is the process of encoding information (plaintext) to make it unreadable without special knowledge. While encoding, the meaning of the message is not obvious. Decryption is the reverse process. The process of decoding or transforming an encrypted message (cipher text) back to its readable and original form (plain text) is called decryption. In other words, encryption helps us to hide the meaning of the original message so that we can send it safely, and decryption helps us reveal the original message from the secret message. In encryption, we use various techniques to encode the message whereas in decryption, the prior knowledge of key or password is required to decode the message. Thus, encryption and decryption help in secure transmission of the message and in protecting the message from unauthorized persons. The cryptography is used in various fields like wired networks and wireless networks etc. The important objectives of cryptography are confidentiality, authentication, integrity, non-repudiation, access control and availability. In order to perform encryption and decryption the various cryptographic techniques are used such as AES, DES, 3DES, Blowfish and RSA.

1.1 TERMINOLOGIES:

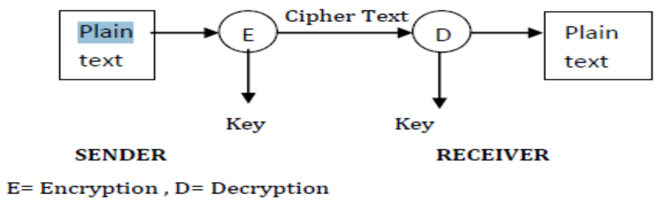


Figure-1.1:*General figure of cryptographic system*

- Plain Text: It is the original form data that a sender wants to send to the receiver. It is an original understandable message that is input to the algorithm.
- Cipher text: Cipher text is the scrambled content or message in its coded human unreadable form. The cipher text is the output of encryption process and input of decryption process If two different keys used for encryption of a message, then two different cipher texts are produced.
- Encryption Algorithm: It performs different techniques such as substitution and transformation on the plaintext to obtain cipher text.
- Decryption Algorithm: It is the exactly opposite procedure of encryption technique. To obtain original plaintext it uses cipher text and secret key.
- Secret Key: The secret key is input to an encryption process. The key value is independent of plaintext and algorithm. Depending on the key being used, the algorithm gives various output. The exact operation performed on that algorithm depend on the key.

1.2 Purpose of cryptography:

- Confidentiality: Its main feature is that only sender and receiver should access the contents of message or data. A loss of confidentiality leads to the unauthorized revelation of data.
- Authentication: The authentication is the important feature of being authentic and it is verified and trusted. This method guarantees that the sender of the message should correctly identify.
- Integrity: This property guarantees that the data in the message do not change when it reaches to the

receiver. A loss of integrity is an unauthorized modification of message contents.

- Non-repudiation: Gives security against denial by one of the parties required in a communication of having taken an interest in all or part of the correspondence.
- Access Control: Its main function is to prevent illegal use of resources.
- Availability: It guarantees that system will work good and service given to only authorized users

II. DIFFERENT CRYPTOGRAPHY TECHNIQUES:

There are two types of cryptography techniques, and they are as follows:

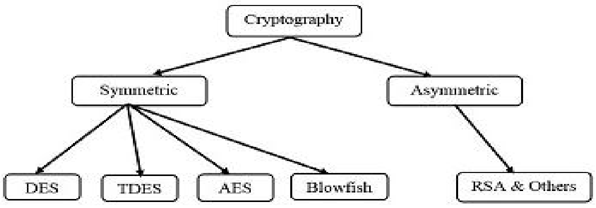
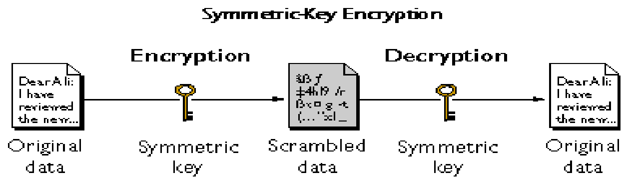


Figure 2: classification of cryptography techniques

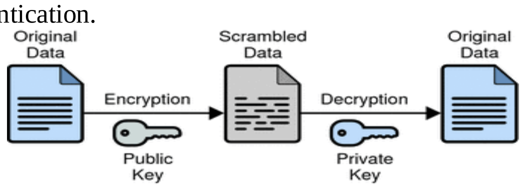
2.1. *Symmetric Key Cryptography:*

Symmetric cryptography, the similar key is used for together encryption and decryption. Symmetric cryptography also provides data encrypted with one symmetric key cannot be decrypted with any other symmetric key. Therefore symmetric key is kept secret by the two parties using it to encrypt communications, each party can be sure that it is communicating with the other the decrypted messages continue to make sense.



2.2. A*symmetric Key Cryptography:*

It is known as public key cryptography. In asymmetric key encryption, two dissimilar keys are used for encryption and decryption - public and private key. The public key of the recipient is used to encrypt the plain text and only the authorized person can be able to decrypt the cipher text through his own private key. Private key is kept secret. This technique is more suitable and provides better authentication.



III. COMPARISON TABLE FOR DIFFERENT SYMMETRIC KEY ALGORITHMS:

	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

❖ DES:

Data encryption standard (DES) is a symmetric key algorithm which was found by IBM in the year 1977.DES is a cipher, meaning it operates on plaintext blocks of a given size (64-bit) and returns ciphertext blocks of the same size. Thus, DES results in a combination among the 2^{64} possible arrangements of 64-bits, each of which may be either 0 or 1. DES operates on the 64-bit blocks using key sizes of 56-bit. The keys are really stored as being 64 bits long, but each 8th bit in the key is not used (i.e. bits numbered 8,16,24,32,40,48,56,64).DES uses 56-bit key out of 64-bit because the 8 bits are used for parity checking, so the effective key size is 56 bits.

Advantages:

a) DES was introduced long time ago in 1977, so no real weakness was found.

b) A DES is likewise an ANSI and ISO standard so anybody can learn and execute it.

Disadvantages:

a) It's key size.

b) It is fast in Hardware implementation as compared to software implementation.

❖ Triple DES:

It is three times slower than the regular DES, but can be billions of times more secure if used properly. Triple DES much wider use than DES since DES is so easy to break with today's fast advance technology. In 1998, the DES cracker managed to break Des in less than 3 days. Triple DES is another mode of DES operation. It takes three 64-bit keys, for an on the whole key length of 192 bits.

Advantages:

a) TDES is a technique to reuse DES executions, by falling three examples of DES (with particular keys).

b) TDES is secure up to no less than 2112 security, so it is unbreakable with today's innovation.

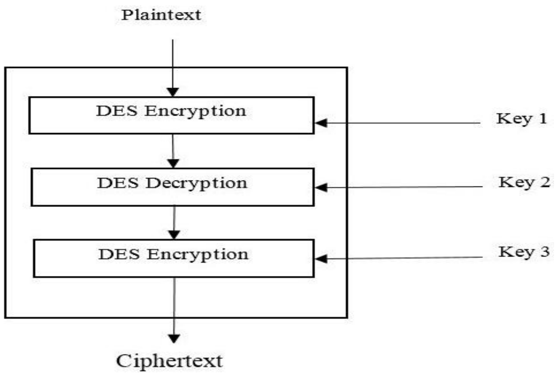
Disadvantages:

a) It is moderate, particularly in programming.

b) It has low performance.

The TDES Encryption has following steps:

1. The First key is for encryption of plaintext
2. The Second key is for decryption of encrypted message produced by Step 1.
3. The Third key is for encryption of decrypted message produced by Step 2.



Triple DES Encryption

❖ *AES*

It is a symmetric block cipher developed by two Belgian cryptographers Joan Daemen and Vincent Rijmen in 1998.The AES stands for Advanced Encryption Standard and based on design method called as a substitution-permutation network. The AES-128, AES-192, and AES-256 block ciphers are included in it. Every cipher encodes and decodes information in the block of 128-bits utilizing cryptographic keys of 128-bits, 192-bits, and 256-bits respectively. The AES is a symmetric cipher and it uses the identical key to perform encryption and decryption on message. For 10 rounds, 12 rounds and 14 rounds AES use 128-bits, 192-bits and 256-bits keys are used respectively.

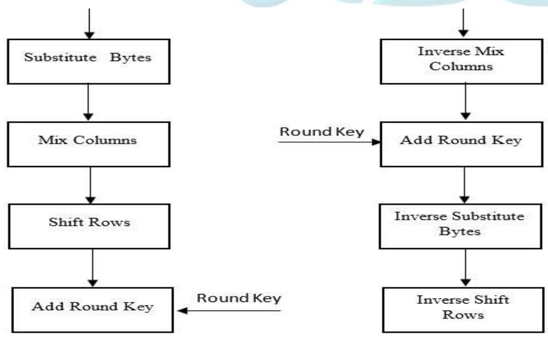


Figure. 3 AES process for Single Round

The AES Encryption, Decryption, and processing round have following 4-stages:

1. Substitute byte: To carry out a byte-by-byte substitution of the block it uses an S-box.
2. Shift rows: A simple permutation.
3. Mix column: A substitution that makes utilize of arithmetic over GF(28).
4. Add round key: A simple bitwise XOR of the current block with a portion of expanded key.

Advantages:

a) This method is more secure as compared to other techniques.

b) It supports larger key size than DES and TDES.

Disadvantages:

a) It has low performance.

❖ *Blowfish*

It is a designed by Bruce Schneier in 1993. It is symmetric block cipher technique. Its block size is 64-bit, and key length is variable. Its variable key length ranges from 32-bits to 448-bits. It is one of the fastest technique which has developed up to date [4]. This algorithm is unpatented and placed in the public domain due to which it can be used freely by anyone. Blowfish algorithm contains two parts Key Expansion and Data Encryption. The key of the Blowfish calculation is 448 bits, so it requires 2448 mixes to look at all keys.

Advantages:

a) It is symmetric block cipher and used as an option for DES.

b) As it uses variable length key from 32-bits to 448-bits making it suitable for both residential and exportable use.

c) Since it released in 1993 so the Blowfish code is not cracked up till now.

d) It has faster performance than other encryption algorithms.

Disadvantages:

a) It requires more space for the cipher text because of difference between key size and block size

❖ *RSA*

This algorithm was developed at MIT in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman (RSA). It is public-key cryptosystem used for secure data transmission. This algorithm uses two keys, first to encrypt second to decrypt. The public key used for encryption of messages and decrypted by using the private key. In this method, any one key is kept secret.

Advantages:

a) The Public Key encryption and increased security is major advantage of RSA algorithm.

b) As it uses two keys, then public key is used for encryption and private key for decryption.

c) In RSA algorithm, the private keys are never transmitted nor revealed.

d) It provides a method for digital signature and that cannot repudiate.

Disadvantages:

a) The speed is a major disadvantage of the public key system.

b) The Public Key Cryptography might be defenseless against mimic, regardless of the fact that client's private keys are not accessible.

V.CONCLUSION

In this paper DES and TDES are easily hack the message for today advancing technologies comparing with Blowfish algorithm. In Blowfish algorithm is very secured and it can't break the any type of messages easily. Therefore Blowfish algorithm are better for hidden data.

VI.REFERENCES

[1]. A William Stallings "Network Security Essentials (Applications and Standards)", Pearson Education, 2004.

[2]. Atul Kahate "Cryptography and Network Security", Tata McGraw-Hill Companies, 2008.

[3]. Gurjeevan Singh, Ashwani Kumar Singla, K.S.Sandha "Performance Evaluation of Symmetric Cryptography Algorithms," International Journal of Electronics and Communication Technology Volume 2 Issue 3, September 2011.

[4]. Pratap Chandra Mandal "Superiority of Blowfish Algorithm," International Journal of Advanced Research in Computers Science and Software Engineering Vol 2 Issue 9, September 2012.

[5]. Mitali, Vijay Kumar and Arvind Sharma "A Survey on Various Cryptography Technique", International Journal of Emerging Trends & Technology in Computer Science, Volume 3, Issue 4, July-August 2014 .

[6]. O.P Verma, RituAgarwal, DhirajDafouti and ShobhaTyagi, "Peformance Analysis Of Data Encryption Algorithms", IEEE Delhi Technological University , India,2011. [2] voices.yahoo.com/comparing-symmetricasymmetric-key-encryption-6329400.html.