ISSN: 2393-8528

IJICSE
Open Access

Contents lists available at www.ijicse.in

International Journal of Innovative Computer Science & Engineering

Volume 4 Issue 4; July-August-2017; Page No. 13-16

A Survey Paper on Various Techniques used in Cryptography

V.KEERTHANA

ASSISTANT PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE

KG COLLEGE OF ARTS AND SCIENCE

Received 10 May 2017; Accepted 02 July. 2017

ABSTRACT

In Modern Era, evaluation of wireless networks and networking provides the easiest way of communication in anywhere at any time. Security is the main aspect in wireless technology. The process of cryptography plays an very important role in provide the security to the wireless networks. There are various symmetric and asymmetric cryptographic techniques used to provide the security for wireless networks. This paper is mainly deals with various types of cryptography algorithms.

Keywords: Encryption, DES, AES, Blowfish, RSA

1. Introduction

Cryptography [1, 2] is the art and science of achieving security by encoding messages to make them readable. The tremendous growth of the networking technology leads to the culture for interchanging of data very drastically. Hence it is more unsafe of duplicating of data and re-distributed by hackers. Due to the above reason the information has to be protected while transmitting it, Sensitive information like credit cards, banking transactions and social security numbers need to be protected. For this many encryption techniques are existing which are used to avoid the hacking of information. In recent days, the encryption of data plays a vital role in securing the data during online transmission. It focuses mainly on its security across the wireless. Different encryption techniques are used to protect the information from unauthorized use. Encryption is a very common technique which was used for the information security. The evolution of encryption is moving towards a future of endless possibilities .Everyday new methods of encryption techniques are discovered. This paper holds some of existing encryption techniques and their comparison.

2. Some of the terms used in cryptography are described below [1]:

2.1 Cryptography

Plain Text: Any communication in the language that we speak referred as plain text. It is understood by both the sender and the receiver and also it will understand by anyone who gets an access to that message.

Cipher Text: Cipher is also referred as secret message. When a readable text is codified as unreadable text using any suitable scheme the resulting message is called as cipher text.

Encryption: The process of encrypt the plain text into cipher text is called encryption.

Decryption: The reverse process of encryption is defined as decryption that is transforming cipher text messages back to plain text is called as decryption.

Key: It is an important aspect for performing encryption and decryption. It is the key which was used for encryption and decryption that makes the process of cryptography secure.

2.2 Uses of Cryptography

Cryptography uses for following purposes:

Confidentiality: The main principle of confidentiality specifies that only the sender and the particular receiver will able to access the contents of a message.

Authentication: The main purpose of authentication mechanisms is to establish the proof of identities. This process ensures that the origin of the message is correctly identified.

Integrity: The integrity mechanism ensures that the contents of the message remain the same when it reaches the particular receiver as sent by the sender.

Non- repudiation: It is the assurance that someone cannot deny something that is the

Corresponding author: V.KEERTHANA

sender cannot denied that he/she cannot send the message

Access Control: Access Control specifies and controls who can access what.

Availability: The main principle of availability refers that resources should be available at all the times to authorized parties.

2.3 Types of Cryptography

There are two types of cryptography:

Symmetric Key Cryptography: The same key is used for both encryption and decryption then it is referred as symmetric key cryptography.

Asymmetric Key Cryptography: In this two different keys are used , One is for encryption and other is for decryption.

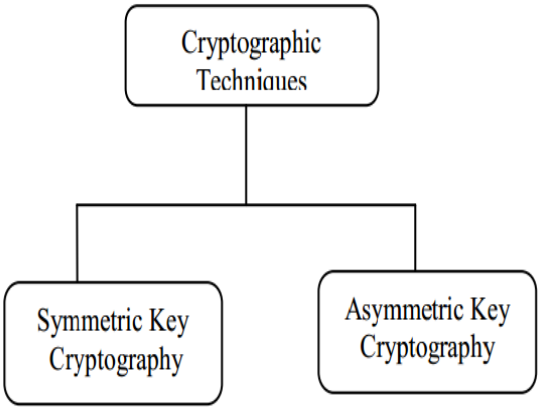

Figure 1:

3. RELATED WORKS

This subsection describes and examines previous work on most common algorithm.

3.1 DES

DES uses Block cipher method. In this it used shared secret key for both Encryption and Decryption. Davis R describes about DES algorithm. In this a fixed-length string is taken as plain text and performs some complicated and transforms as cipher text of same length. DES uses the block each block size is 64 bits. The key size of DES is 56 bits which is to customize the transformation. In this decryption is only possible to the user who knows the particular key used to encrypt the message. DES uses 16 stages of processing, each stage is considered as rounds. DES also performs initial and final permutation. In DES IP "undoes" the action of FP, and viceversa. The steps in DES are as follows [1]:

1. The 64-bit plain text message is given over to an Initial permutation (IP) function.
2. The plain text performs the initial permutation.
3. The Initial Permutation produces the result as two halves of the permuted message, Left Plain Text (LPT) and Right Plain Text (RPT).
4. Then 16 rounds of encryption process is performed through each of LPT and RPT.
5. After the rejoining of LPT and RPT final permutation (FP) is performed on the block which are combined.
6. Finally 64- bit cipher text is produced as a result..

Rounds: Each of the 16 rounds, in turn, consists of the broad level steps and shown in Figure.

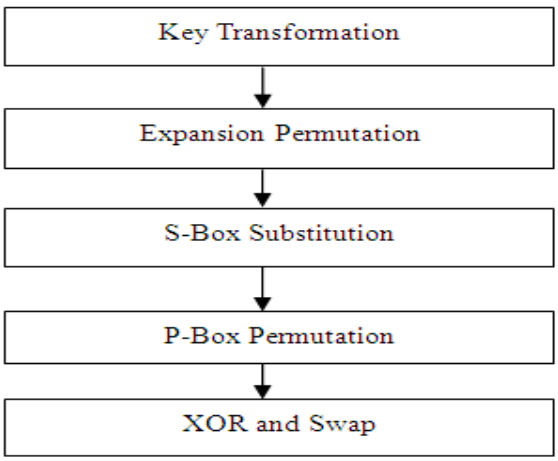

Figure 2: Details of One Round in DES

3.2. 3DES

3DES (Triple DES) is an enhancement of DES; it is 64bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original but it applies 3 times DES process to extend the secret writing level and therefore the average safe time. once Compare to alternative block cipher the 3DES is taken into account as slower. the 2 or 3 56 bit keys within the sequence Encrypt-Decrypt-Encrypt(EDE)is employed. Initially, 3 totally different keys area unit used for the secret writing formula to come up with cipher text on plaintext message,t.

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

wherever C(t) is cipher text created from plain text t,Ek1 is that the secret writing methodology mistreatment key k1, Dk2 is that the decipherment methodology mistreatment key k2Ek3 is that the secret writing methodology mistreatment key k3.Another option is to use 2 totally different keys for the secret writing formula that reduces the memory demand of keys in TDES.C(t) = Ek1(Dk2(Ek3(t))) (2)

© 2017 All Rights Reserved.

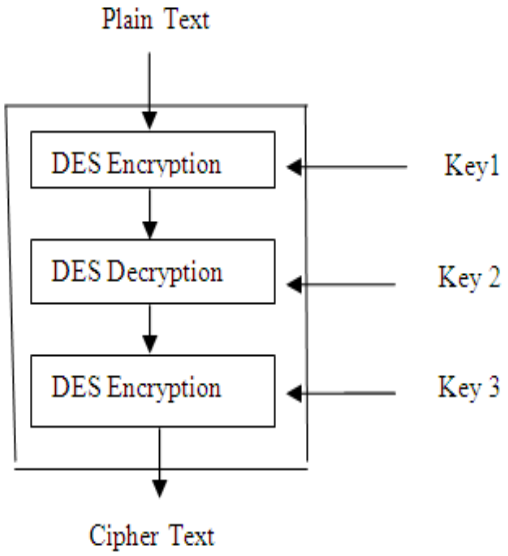

Figure 3: secret writing in 3DES

3.3 AES

The AES cipher is sort of clone of the block cipher Rijndael cipher developed by 2 Belgian cryptographers, Joan Daemen and Vincent Rijmen. The formula represented by AES may be a symmetric-key formula, which means a similar key's used for each encrypting and decrypting the information. The quantity of internal rounds of the cipher may be a operate of the key length. the quantity of rounds for 128-bit key's ten. Not like its precursor DES, AES doesn't use a Feistel network. Feistel networks don't cipher a complete block per iteration, e.g., in DES, 64/2 = thirty two bits area unit encrypted in one spherical. AES, on the opposite hand, encrypts all 128 bits in one iteration.

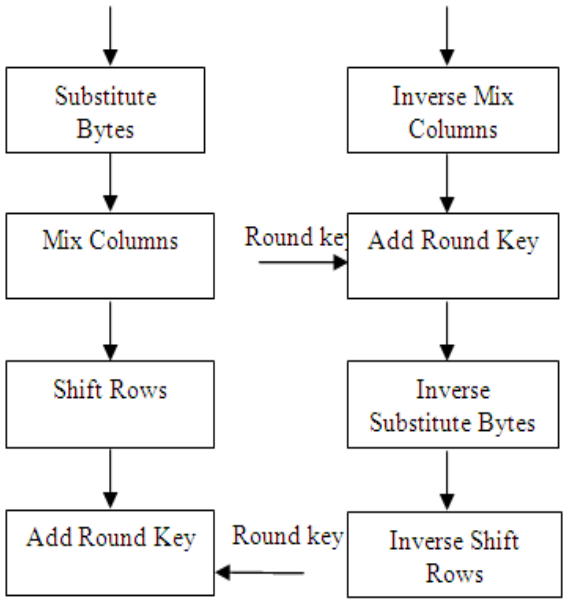

Figure 4:

3.4 Blowfish

Blowfish [5] is one in all the foremost common property right secret writing algorithms provided by Bruce Schneier - one in all the world's leading cryptologists, and therefore the president of bedding Systems, a consulting company specializing in cryptography and pc security. The Blowfish formula was initial introduced in 1993.

Operation of Blowfish:

Blowfish encrypts 64-bit block cipher with variable extent with key. It contains two parts:

- Sub key Generation: This process converts the key up to 448 bits long to sub keys to totaling 4168 bits.
- Data Encryption: This process involves the iteration of a simple function 16 times. Each circle contains a key dependent transformation and key- and data needy substitution.

Blowfish relates the applications where the key remain constant for a extensive time (e.g. communication link encryption) but not where the key changes frequently (e.g.packet switching). The blowfish encryption is shown in figure below:

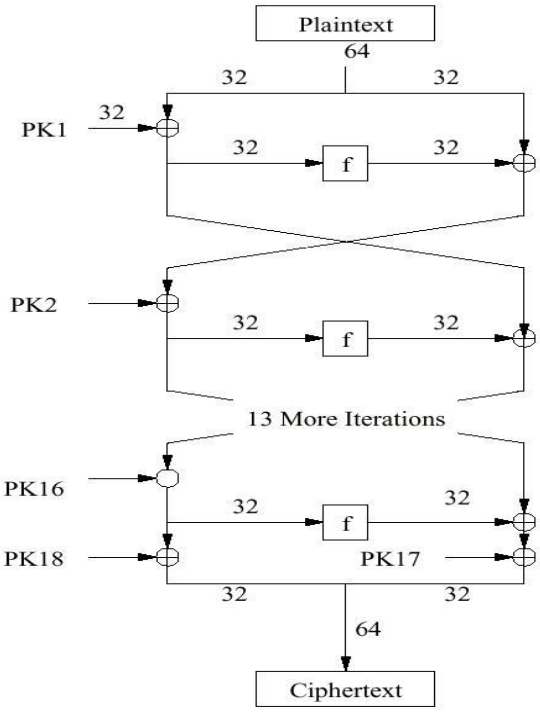

Figure 5:

3.5 Comparison

Comparative study of the cryptographic algorithms both symmetric as well as asymmetric has been done.

© 2017 All Rights Reserved.

Table 1: Comparison of Cryptography Algorithms

ALGORITHM	CREATED BY	KEY SIZE(BITS)	BLOCK SIZE (BITS)
DES	IBM in 1975	56	64
3DES	IBM in 1978	112 or 168	64
AES	JOAN DAEMEN & VINCENTRIJMEN IN 1998	256	128
BLOWFISH	BRUCE SCHNEIER IN 1993	32 - 448	64

4. CONCLUSION

In this wireless world, the security for the data has become highly important since the selling and buying of products over the open network occur very frequently. In this paper, it has been surveyed about the presented works on the encryption techniques. These encryption techniques are premeditated and analyzed well to encourage the presentation of the encryption methods also to ensure the safety actions. This paper deals with the algorithms like AES, 3DES, Blowfish and DES.

REFERENCES

1. Atul Kahate "Cryptography and Network Security",Tata McGraw-Hill Companies, 2008.
2. D. Boneh and M. Franklin, "Identity-based encryption form the weil pairing", in Advance in Cryptology (CRYPTO'01), LNCS 2139, Springer Verlag, 37, 213-229, 2011
3. Davis.R, "The Data Encryption Standard in Perspective", Proceeding of Communication Society magazine, IEEE, Vol 16, Nov 1978. [4.] 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 Chnadra Mandal "Superiority of Blowfish Algorithm," International Journal Of Advanced Research in Computers Science and Software Engineering Vol 2 Issue 9, September 2012.
5. Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.

© 2017 All Rights Reserved.