IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Volume-5, Issue-2 E-ISSN: 2347-2693

A Survey on Different Cryptographic Techniques

Mathew L.R.

Dept. of CSE, St. Thomas College of Engineering and Technology, Kozhuvalloor, India

*Corresponding Author: leenu2leenu@gmail.com

Available online at: www.ijcseonline.org

Received: 26/Jan/2017 Revised: 31/Jan/2017 Accepted: 23/Feb/2017 Published: 28/Feb/2017

***Abstract*— Data transmission over the Internet for various purposes has become a necessary part of technology nowadays. But, the data sent over the Internet or the data to be retrieved can be hacked by any other party in several ways. To provide security, various cryptographic schemes have been developed. Among the different schemes the data integrity cannot be ensured in a number of aspects. Cryptography ensures that the message should be sent without any alternation and only the authorized person can be able to open and read the message. Cryptographic techniques can be broadly classified into two methods, namely symmetric and asymmetric. This paper focus mainly on the different kinds of the existing encryption techniques, and a comparative study of different algorithms.**

Keywords-Encryption,Cryptography,Symmetric,Asymmetric

I. INTRODUCTION

Cryptography is a method of storing and transmitting data in a special form so that only those for whom it is concerned can read and process it. It is a combination of encryption and decryption of data which provide security or authenticity to the encrypted data over the Internet. Cryptography is basically scrambling of data for ensuring secrecy and authenticity of information. The data sent over the Internet in the form of encrypted data is transformed into the cipher text from the plain text to hide the original form of data from any fraudulent users. Cryptography can also change the form of data from one state to another which can never be understood without its proper decryption. Hence, it can provide authenticity to the data which has to be sent over the network and to hide it from its misuse. The primary goal of cryptography is entirely based on the capability to hide the message from any insecurity. Essentially, the principle of cryptography is to offer secret and secure communication. Cryptography enables us to transmit data in secure networks so that it cannot be read by anyone expect the authorized recipient. When the user defined input may in any of the format such as text, or an image which is plain, is converted into a scrambled or unintelligible form called as the cipher text or cipher image. This process is referred to as encryption. The reversible process in which the cipher text is converted in to the original form is called as the decryption process [1].

Steganography and cryptography are the two approaches that make the communication secure. They are closely related. Cryptography plays a major role in protecting the secret information in various applications. Steganography is the art and science to hide data in a cover which can be text, audio, image, video etc. Cryptography is secret writing. The main aim of Steganography is to keep the message undetectable from any unauthorized access. The concept of cryptography is not always as sufficient to provide the secure communication. The applications such as e-banking, e commerce, medical databases, e-mail, military and some more, all of them require the exchange of confidential information.

II. CRYPTOGRAPHY GOALS

A. Cryptography

The main goals provided by cryptography are[2]:

1. Authentication: Process in which the identity of the sender is checked to prove that the information is coming from authorized users.
2. Confidentiality: This ensures that the encrypted data can only be understood by authorized users.
3. Data Integrity: This ensures that the receiver receives data which is secured and unaltered.
4. Non-Repudiation: It guarantees that the sender has already sent the message, so that he can't be blamed for not sending the message. [1]
5. Access Control: Process of preventing an unauthorized user from accessing the resources. If one can access, under which restrictions and conditions the access be occurred, and what is the permission level of a given access.

III. CRYPTOGRAPHICAL ALGORITHMS

There are two types of encryption algorithms: symmetric encryption algorithm and asymmetric encryption algorithm [3].

In symmetric key encryption sender and receiver will have the same key for the process of encryption and decryption of data.

In asymmetric key encryption algorithm two different keys are used: one to encrypt the plain text and one to decrypt the cipher text at the sending and receiving site. It is called asymmetric cryptography because it is used as a pair of keys: one is the public key that can be given by the owner to the

required user and the other one is the private key and it is known only by the owner.

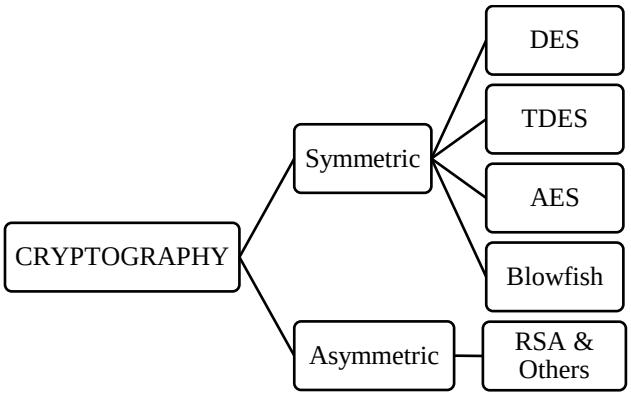

Figure1: Classification of cryptographic algorithms .

IV. RELATED WORKS

This section describes and examines previous work done in field of data encryption.

A. DES

DES is a block cipher operating on fixed-length groups of bits, called *blocks*, with an unvarying transformation that is specified by a symmetric key. 64bit of plain text goes as the input to DES, which produces 64 bits of cipher text. The keys length is 56 bits [4]. It divides the original message into 64-bit blocks. Each block is then permutated to change the order of its bits. Two 28-bit halves is divided by 56-bit key. Each half is than circular-shirted to the left, reconnected and enlarged to 48 bits. Then the half in right plain text blocks is also expanded to 48-bits.

The drawback of this algorithm is that it can be easily prone to brute force attack in which the hacker can break the key by applying all possible combination. In DES there are only 256 possible combinations which are quite easy to crack. So DES is not so secure [5].

B. Triple Data Encryption Standard(3DES)

The triple DES (3DES) algorithm was needed as a replacement for DES due to advances in key searching .TDES uses three rounds of DES encryption and has a key length of 168 bits (56*3). The 56-bit DES key used for encrypting the data first, then another 56-bit DES key is for decrypting, and finally the original 56-bit DES key is used for encrypting again. 3 DES contains several levels of encryption and it can better protect against middle attacks.

The disadvantage of this algorithm is that it is too time consuming.

C. Advanced Encryption Standard(AES)

AES is a variable bit block cipher and uses variable key length of 128,192 and 256bits. Depending on size of the key, the standard name is modified to AES-128, AES- 192 or AES- 256 correspondingly. Key length is dependent on number of AES parameters. If both the block length and key length are 128 bits. AES will perform a processing round, if the key size used is 192, the number of rounds is 12 whereas it is 14 for 256 bits respectively. It is noted that, if there is a longer keys, it is difficult to crack, but it will take more time for computation.

D. Blowfish

Blowfish is a 64 bits block cipher with variable length key from 32bit (4 byte) to 448 bits (56 bits) [6]. The algorithm has two parts key expansion and data encryption. First step converts 448key into 4168 bytes. A P array of size18 and four S –boxes which is of size 256 is made. XOR each entry in P array and S boxes with 32 bits of the keys [7]. There are total 16 rounds of data encryption. In each round a 32 bit sub key is XORed with leftmost 32 bits of plaintext and the result is then passed to the F functions of blowfish. This result becomes rightmost32 bits for the next round and the output of F functions XORed with the original rightmost 32 bits of plaintext becomes leftmost 32 bits for the next round and so on.

The key used is 448 bits, so that it requires 448 combinations to examine all keys [8]. The advantage of this algorithm is that it is highly secure and has not been cracked yet. It is simple to implement since all operation carried out are XOR and addition. Speed of encryption and decryption is also faster.

E. RSA

RSA is a most popular asymmetric cryptography algorithm. It has two keys (public and private) and both keys will be used for encryption and decryption process. Sender will encrypt the data using receiver's public key and then receiver will decrypt the data using his own private key. It uses two prime numbers for generating private key and public key.

Disadvantages of RSA algorithm is that it takes more time for computation process. RSA takes more memory than AES and DES.

V. PERFORMANCE METRICS

Performance metrics and criteria for cryptographic research are security and time. The algorithms should perform the encryption and decryption of the input text/other multimedia file. For that some of the parameters and measures are to be considered. They are encryption computation time, decryption computation time, and key size and block size.

Metrics might be used for evaluating and comparing cryptographic algorithms.

1. Encryption Time: Time taken to encrypt the data from plaintext to cipher text. It is used to calculate Encryption throughput.
2. Decryption Time: Time taken to decrypt the data. It is used to calculate Decryption Throughput.

3. Key size**:** A size of the key which is measured in bits and will depend on algorithm. The security of any algorithm is highly based on the length of key being used [9].

VI. OBSERVATIONS

The following observations can be identified from the previous sections:

1) Short length single key is not capable to provide secured cryptographic model and long length key can be able to provide secured cryptographic model.

2) Asymmetric keys are used and preferred for high level security.

3) There should be a proper key arrangement in order to achieve secure cryptographic model.

VII. COMPARISON OF DIFFERENT CRYPTOGRAPHIC ALGORITHMS

Performance of different algorithms are evaluated by considering the following parameters.

A. Stimulation Time: Time taken during the process is to be noticed. Encryption time is the time taken to produces a cipher text from plain text. Decryption time is the time taken to produce a plain text from cipher text.

B. Buffer Size: Variation in memory usage is referred as buffer size.

Table1: Comparison of various packet sizes for DES, AES and RSA

Sl. No	*Algor*	*Pack Size (kB)*	*Encrypt Time (Sec)*	*Decrypt Time (Sec)*	*Buff Size*
1	DES	153	3.0	1	157
	AES		1.6	1.1	152
	RSA		7.3	4.9	222
2	DES	118	3.2	1.2	121
	AES		1.7	1.2	110
	RSA		10.0	5.0	188
3	DES	196	2.0	1.4	201
	AES		1.7	1.24	200
	RSA		8.5	5.9	257
4	DES	868	4.0	1.8	888
	AES		2.0	1.2	889
	RSA		8.2	5.1	934

CONCLUSION

This survey paper dealt with the basic concepts in cryptography, symmetric and asymmetric types, performance metrics and some of the important parameters that are used in cryptography to secure the system to achieve high level of security. From Table1, it was observed that the encryption time (1.6, 1.7, 1.7, 2.0 Sec) and decryption time (1.1, 1.2, 1.24, 1.2 Sec) is lesser for AES algorithm compared to the DES and RSA algorithms for the different pack sizes (153, 118, 196, 868 kB) considered. It is also observed that RSA consume longest encryption time. AES is found to outperform the DES and RSA in all the four pack sizes as far as stimulation time and buffer size is considered. Hence it can be concluded that, proper selection of a suitable encryption algorithm is important for a secured information system that can defeat several attacks efficiently.

ACKNOWLEDGMENT

I would like to take this opportunity to express my profound gratitude and deep regards to the HOD and staff, Department of Computer Science and Engineering, St. Thomas College of Engineering and Technology for the constant encouragement throughout the duration of the survey.

REFERENCES

[1] Stallings W., “Cryptography and Network Security”, 2nd Edition, Prentice Hall, 1999.

[2] Sharma A., Thakur R S and Jaloree S., "Investigation of Efficient Cryptic Algorithm for image files Encryption in Cloud", International Journal of Scientific Research in Computer Science and Engineering, Vol.4(5), pp. 5-11, Oct 2016

[3] Dipti K. S., Neha B., “Proposed System for Data Hiding Using Cryptography and Steganography”, International Journal of Computer Appilcations, Vol.8(9), pp.7-10, Oct 2010.

[4] Schneier B., “Description of a New Variable Length Key, 64 Bit Block Cipher (Blowfish)” International Workshop on Fast Software Encryption, Cambridge Security Workshop proceedings, pp.191-204, Dec 1993. ISBN 978-3-540-48456-1

[5] Minaam D. S. A., Abdual-Kader H. M., Hadhoud M.M, “Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types”, International Journal of Network Security, Vol.11(2), pp.78-87, Sep 2010.

[6] Nigam A, Singh V., "Securing Data Transmission in Cloud using Encryption Algorithms", International Journal of Computer Sciences and Engineering, Vol.4(6), pp.21-25, Jun -2016

[7] Rin M. C. J., Lin Y. L., “A VLSI implementation of the Blowfish Encryption/Decryption Algorithm”, ASP-DAC '00 Proceedings of the 2000 Asia and South Pacific Design Automation Conference, Jan 2000. ISBN:0-7803-5974-7

[8] Mathew M, Sumathi D., Ranjima P, Sivaprakash P., "Secure Cloud Data Sharing Using Key-Aggregate Cryptosystem", International Journal of Computer Sciences and Engineering, Vol.2(8), pp. 121-123, Aug -2014

[9] Agarwal M., Mishra P., “A comparitive survey on Symmetric Key Encryption Techniques” International Journal on Computer Sciences and Engineering, Vol.4(5), pp.877-882, May 2012.

Authors Profile

Mrs.Leenu Rebecca Mathew pursed Bachelor of Technology from College of Engineering Chengannur in 2011 and Master of Technology from Federal Institute of Science and Technology in year 2013. She is currently working as Assistant Professor in Department of Computer Science, at St Thomas college of Engineering and Technology. She has 3.5 years of teaching experience .

