Algorithms Used in Cryptography and Role of Cryptography in Network Security

Arun Murugesan , Pradeepkandhasamy Jawahar, Karuppaiah Parameswaran.

Abstract- In this modern world, we cannot live without these two things. One is technology and other one is security. Even these two cannot stand alone, they depend on each other. Technology without security and security without technology leads the world into destroying path. Day by day the technology is improving and also the security. In the technology field, the network plays an important role. Every system in the world depends on the network. So the network has been secured before it sends to the relevant people. By this problem can lead us to create a new method called Cryptography. The work of cryptography is to convert the sending message into encryption method by using some key and the receiver receives the encrypted message. The receiver decrypt the message by the key which is used to encrypt the message. In this paper, we discuss how network security works with cryptography and algorithm used for cryptography.

Keywords : Cryptography, DES, Encryption, Decryption, AES, Blowfish

.

I. INTRODUCTION

The term cryptography was mainly used with cipher and code, for securing the secrets. The two important thing that deals with cryptography, they are encryption and decryption. In words we can say that cryptography is art of writing by using some secrets in codes. In late years 1970's this concept was used in all governments to preserve the data. The cryptography was taken into development and it was named as "Cryptanalysis". The reason for development is to break the codes and do cipher. The main function of the cryptography is to convert a readable message into unreadable format and then again it converts to readable one. By using this the data is not visible to the outsiders and visible to sender to receiver. Network security is one of the topic discussed in recent because the data transmission via network are misused, theft by strangers. So protect such activities which are occurring in both private and public and also in all the private organizations and in government cryptography is used. Since the use of internet is used in all over the world it must that all the data stored and transferred via internet must be safe and also be more secured for this reason the concept cryptography is used. In the cryptography the encryption technique is mainly used in providing information security to the data. Thus the encryption is not easy to hack for this purpose it is mainly used. In this paper some of the major algorithm used in cryptography and how the cryptography plays a key role in the field of network security are discussed in this paper.

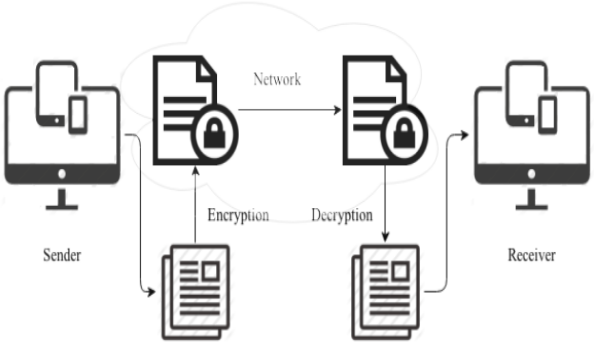

Fig 1. Transformation process for data

II. LITERATURE SURVEY

Mr. Joseph Amalraj made their survey about the cryptographic techniques. In his perspective Email system requires security, so they implemented the cryptographic techniques to apply the defensive system to the network. According to the survey, Public Key Infrastructure has some key issues but it can implemented for the security purpose and also being a efficient system for the Email service. The aim of this paper is to provide a Email security to the common users. We can use more number of cryptographic techniques to reach the secure communication network.

Prof. Mukund R. Joshi discussed in his paper about the protection of network and transmission of data through the wireless network. In networks, the data only can accessible by the authorization is provided by the network administrator. These types of network security are used in various organizations and institutions. In Cryptography implements the security in the authorization to access the data in the unreliable network. The data transmissions processed over the network can be restrained by administrator of the unreliable network. Network security provides both private access and public access in the network.

Mr. Gurjeevan Singh analyzed about the various types of algorithms that can be implemented for the information security in Network application and Internet. In that paper he evaluated the four different algorithms frequently used for data encryption in the networks. The evaluation explains the performance of the four different algorithms based on their encode time, decode

Revised Manuscript Received on December 05, 2019.

***** Correspondence Author

Mr.Arun Murugesan*,Department of Computer Applications, Kalasalingam Academy ofResearch and Education, Krishnan Koil, Tamil Nadu, India. Email: m.arunvincent@gmail.com.

Mr. Pradeepkandhasamy Jawahar, Department of Computer Applications, Kalasalingam Academy ofResearch and Education, Krishnan Koil, Tamil Nadu, India. Email: honey.kanda@gmail.com.

Mr. Karuppaiah Parameswaran, HCL Technologies , Madurai. Tamil Nadu. India. Email : karuppaiahkp1995@gmail.com.

time and throughput. These algorithms are sustainable for the wireless network.

Mr. Hassouna discussed about the certificate less cryptography based on secure mail service. The Standard security system is not much efficient as proposed mailing service. In Proposed mailing service, the messages are encrypted by PKI (Public Key Infrastructure) encryption algorithm to implement security. Private keys and public keys of the PKI encryption algorithm can be accessed by both source and destination.

Dr. Kusum Lata bharti and Dr. Varun Tiwari explained in his paper about the internet are used in the several things that can be the estimation of networking and wireless network which has been given the better information and communication. The main function of the network is to secure the internet with the mode of cryptography. To increase the security and capability of the communication system accept the PKI (Public Key Infrastructure) method to behead the security, but this PKI based system go through from valuable certificate management and problem in scalability. The main aim of this process is to understand the security of email and its need to the general computer users. There are many cryptographic techniques are here to reach the safe communication. The upcoming email system is safer against the regular security model.

In this paper Monika Agarwal and Pradeep Mishra said that the internet usage is grows all over the world and the main thing of the issue for the society is security. Previous security was the important problem for military application but now they are developed and place over the web. Cryptographic is the technique which is created to give the secure transformation between the senders and receivers by using the method called Encryption and Decryption. These process that send the messages without any changes and only the authorized person can access these message. There are more number of cryptographic methods to reach the high safe communications.

III. VARIOUS TYPES OF ALGORITHM USED IN CRYPTOGRAPHY

A. *Triple DES*

This DES was reinstate for authentic DES (Data Encryption Standard) algorithm. Once upon a time, Threefold DES was endorsed standards which are frequently used in industry as a wide range.

Three personal keys with each of 56 bits are used in Threefold DES. Upto 168 bits can be add into the entire length of the key, but the experts scabble that 112-bits of the vitality of the key is the higher like it.

Threefold DES takeover to create a trustworthy hardware encryption result for financial utility and other industries.

B. *RSA*

Rivest-Shamir-Adleman (RSA) is a mutual-key algorithm and the common for sending the data over the internet. It appear to be one of the approach used in PGP and GPG programs.

By using of the couple of keys, RSA is treated an asymmetric algorithm. The conclusion of RSA encryption is a giant cluster of mumbo jumbo that takes mugger entirely a portion of time and deal with power to crack.

C. *Blow fish*

The replacement for the DES algorithm is Blowfish. This symmetric nonentity crack into section of 64 bits messages and independently encrypts them.

Blowfish is noted for both its great agility and overall performance. In the meantime, merchant took sufficient gain of its free opportunity in the public realm.

Blowfish initiate in software division ranging from e-commerce platforms to password authority apparatus for securing the payments. It's absolutely be the one of the more malleable encryption technique possible.

D. *Two fish*

The Expert of computer security Bruce Schneider is the mastermind of his successful creation Blowfish and its replacement Two fish. Up to 256 bits of key in length is used in this algorithm and as a symmetric approach, and there is only one key is enough.

The obesrvation Twofish is to be one of the agile of its kind, and optimal for use in both hardware and software situations. Like Blowfish, Twofish is also applicable for free to everyone.

E. *AES*

The AES(Advanced Encryption Standard) algorithm is trusted by the U.S. Government and numerous organizations as the standard.

AES is used for heavy duty encryption purposes, uses the keys of 192 and 256 bits.

AES is treated impassable to every attacks, with the omission of brute force, which try to decipher the entire messages by using the every possible waysin 128, 192 or 256-bit cipher. Eventhough, the experts in security believe that the AES will be hailed the de facto standard for encrypting the data in the confidential zone.

IV. ROLE OF CRYPTOGRAPHY IN NETWORK SECURITY

The world before cryptography, the every type of organisations and even the government were facing the top issues to keeping the secrets from the unauthorized persons. All these days the main concern in the network security is the dissolution of the business operations and the advancement of the computer network. In advance of concerning the security, most of the network in the organisations are accidently expect to appear, and also these accidents can't be predictable but the security will stop it. Finally cryptographic technique is involved with the network security. Some of the beasic needs of cryptography in the network security is:

A. *Confidentiality* – All the informations when it transfers to the particular person, it should probably be important to them. When the transfering informations accessed in a illegal manner by the unauthorized person, it should not be well. So the transfering data should be confidential when it comes under the security by the method of cryptography. The sending data could be encrypted and then send to the particular person by using the key in the method of cryptography.Important files tranferred through the internet using these security methodology to avoid the unauthorised access by the unauthorised person or unautjorisation organisation.confidentiality approaches encryption.

B. ***Integrity*** - cryptography methodology is demanded security syatem for file transfer through the internet and file storage in the cloud service provider,But the cryptography methodology needs integrity fpr the encryption and decryption processed on the files used in the cryptography process.Integrity is process of securing the encrypted files from the unauthorized parties.Hash values needs the integrity in the cryptography.Integrity ensures whether the data is accurate, real and unmodified content from the unauthorized parties.Many integrity constraints are used in the cryptography methodology.Integrity needs accuracy to secure the data from the unauthorized parties.

C. ***Availability*** – Availability in other words means authetication.Availability is a verification taking a process of file or data accessed by the authorized person. cryptography approaches authentucation for particular security purpose and the purpose is whether the file or data reaches the right person or authorized person or not. This is the verification process of the availability principle in cryptography methodology.Availiability secures the file or data from the various attack from the unauthorized parties.Files may be abused by unauthorized parties and it is avoided by the availability.The major morality of availability is the user can access the file or data by the authorized user in a right time when they needed.

V. CONCLUSION

In this paper, we inquiry different algorithms used in the cryptography and roles of the cryptography algorithm.DES and AES major algorithms are used for the secure encryption and decryption of the Files transferred through the internet.Hashing algorithms are safer than the other algorithms because they have more accuracy in the key value of both encryption and decryption of the files.RSA algorithm is widely used algorithm and it is first pulic-key cryptosystem and it universally for secure data transformation in the internet.Blowfish algorithm is pitched-in to cryptosystems in exchange of DES algorithm.Twofish algorithm is also pitched-in to encryption in exchange of theDES algorithm but Blowfish algorithm is safer than the Twofish algorithm.There are three principles are present in the cryptography system and principle has some unique features and roles are performed in the cryptography methodology.Finally we concluded that the algorithm used in the cryptosystem and the roles of the cryptosystem are must need the regural update on the algorithms and that may avoid the various attacks performed on the files by the unauthorised parties in illegal abusing of the file s in the internet.
Updation of the algorithms and various security level processed on the algorithm can secure the files from various malicious attacks on the internet.

REFERENCES

1. A. Joseph Amalraj , Dr. J. John Raybin Jose" A SURVEY PAPER ONCRYPTOGRAPHY TECHNIQUES", International Journal of Computer Science and Mobile Computing, Vol.5 Issue.8, August-2016, pg. 55-59.
2. Prof. Mukund R. Joshi, Renuka Avinash Karkade "Network Security with Cryptography", , International Journal of Computer Science and Mobile Computing, Vol.4 Issue.1, January- 2015, pg. 201-204.
3. Pratap Chandra Mandal "Superiority of Blowfish Algorithm", International Journal of Advanced Research in Computers Science and Software Engineering Vol 2 Issue 9, Sep 2012.
4. M. Hassouna, N. Mohamed, B. Barry, and E. Bashier, "An end-to-end secure mail system based on certifticateless cryptography in the standard security model", International Journal of Computer Science Issues, 10, 264-272, 2013.
5. Dr. Kusum Lata Bharti [1], Dr. Varun Tiwari [2]," A Brief Survey of Cryptography Techniques", International Journal of Computer Science Trends and Technology (IJCST) – Volume 6 Issue 2, Mar - Apr 2018.
6. Monika Agrawal, Pradeep Mishra", A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol.4 May 2012.
7. E.Thmbiraja, G.Ramesh, Dr.R.Umarani, "A survey on various most common encryption techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 7, July 2012.
8. Daemen.J and Rijmen, The Advanced Encryption Standard, Dr. Dobb's Journal, March 2001.
9. D. S. A. Elminaam, H. M. A. Kader, and M. M. Science, Menoufia University, Egypt in 2008. He Hadhoud, "Evaluating the performance of symmetric encryption algorithms," International Journal of Network Security, vol. 10, no. 3, pp. 213-219, 2010.
10. A. Nadeem, "A performance comparison of data encryption algorithms," IEEE Information and Communication Technologies, pp. 84-89, 2006.

AUTHORS PROFILE

Mr. M. Arun, Assistant Professor, Department of Computer Applications, Kalasalingam Academy of Research and Education have more than 12 years of Teaching Experience. He completed his Under Graduation in Computer Applications at Madurai Kamarajar University and Post Graduation in Computer Applications at Anna University, His Major research area is Network Security.

Mr. J. Pradeepkandhasamy, Assistant Professor, Department of Computer Applications, Kalasalingam Academy of Research and Education have more than 7 years of Teaching Experience. He completed his Under Graduation in Computer Science at Bharathidasan University and Post Garduation in Master of Computer Applications in Kalasalingam University, His Major research area is prediction and classification in Data Mining

Mr. K. P. Karuppaiah, Software Engineer , HCL Technologies Madurai. He completed his Under Graduation and Post Graduation in Computer Applications at kalasalingam Academy of Research and Education. His area of interest in Network Security.