ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 7, Issue 2, pp: (182-184), Month: April - June 2019, Available at: www.researchpublish.com

Network Security Using Cryptographic Techniques

[1]Manmeet Singh Khalsa, [2]Siddhesh Chile, [3]Dr. Ramesh Solanki

[1,2] MCA Semester-VI Vivekananda Education Society Institute of Engineering, Chembur, Mumbai-74

[3]Asst. Professor(MCA, Vivekananda Education Society Institute of Engineering, Chembur, Mumbai-74

Abstract: **System security has turned out to be increasingly essential to PC clients, associations, and the military. With the appearance of the web, security turned into a noteworthy concern and the historical backdrop of security permits a superior comprehension of the rise of security innovation. The web structure itself took into account numerous security dangers to happen. The design of the web, when altered can diminish the potential assaults that can be sent over the system. Knowing the assault strategies, takes into account the fitting security to develop. Numerous organizations secure themselves from the web by methods for firewalls and encryption components. The organizations make an "intranet" to stay associated with the web yet verified from potential dangers.**

System Security alludes to all equipment and programming capacities, attributes, highlights, operational strategies, responsibility, measures, get to control, and authoritative and the board approach required to give a worthy dimension of assurance for Hardware and Software, and data in a system. Just a single specific component underlies a significant number of the security systems being used: Cryptographic procedures; henceforth our attention is on this zone Cryptography. Cryptography is a rising innovation, which is significant for system security. Research on cryptography is still in its creating stages and an extensive research exertion is as yet required for verified correspondence.

Keywords: **Network Security, accountability, access control, management policy, cryptography.**

1. INTRODUCTION

System Security and Cryptography is an idea to ensure system and information transmission over remote system. Information Security is the fundamental part of secure information transmission over inconsistent system. Information Security is a difficult issue of information correspondences today that contacts numerous zones including secure correspondence channel, solid information encryption procedure and confided in outsider to keep up the database. The quick advancement in data innovation, the protected transmission of secret information herewith gets a lot of consideration. The customary techniques for encryption can just keep up the information security. The data could be gotten to by the unapproved client for vindictive reason.

System security is associated with associations, endeavours, and different kinds of establishments. It does as its title clarifies: It verifies the system, just as securing and supervising tasks being finished. The most widely recognized and basic method for securing a system asset is by relegating it a one of a kind name and a relating secret phrase. System security begins with validating the client, regularly with a username and a secret key. Since this requires only one detail validating the client name — for example the secret word, which is something the client 'knows'— this is at times named one factor confirmation. With two-factor verification, something the client 'has' is additionally utilized (for example a security token or 'dongle', an ATM card, or a cell phone); and with three-factor verification, something the client 'is' is additionally utilized (for example a unique finger impression or retinal output). When verified, a firewall authorizes get to arrangements, for example, what administrations are permitted to be gotten to by the system clients.

The vast topic of network security is analysed by researching the following:

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 7, Issue 2, pp: (182-184), Month: April - June 2019, Available at: www.researchpublish.com

1. History of security in networks

2. Internet architecture and vulnerable security aspects of the Internet

3. Types of internet attacks and security methods

4. Security for networks with internet access

5. Current development in network security hardware and software.

Concepts Used In Cryptography

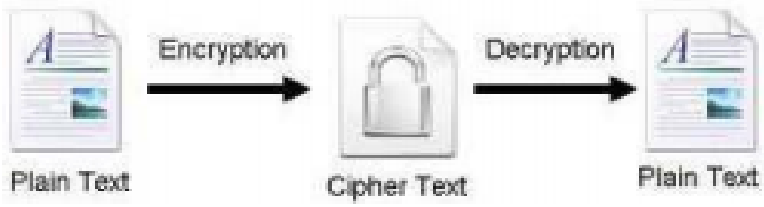
A .Plain Text: The original message that the person want to communicate is defined as plain text.

B. Cipher Text: The message which cannot be understood by anyone is defined as cipher text

C. Encryption: Converting plain text to cipher text is referred as encryption. It requires two processes. Encryption algorithm and a key.

D. Decryption: Converting cipher text to plain text is referred as decryption. This may also need two requirements Decryption algorithm and key.

E. Key: Combination of numeric or alpha numeric text or special symbol is referred as key .it may use at time of encryption or decryption .key plays a vital role in cryptography because encryption algorithm directly depends on it.



Encryption-Decryption Flow

Based on this research, the future of network security is forecasted. New trends that are emerging will also be considered to understand where network security is heading.

1. Network Security

Framework and system innovation are a key innovation for a wide assortment of utilizations. Security is urgent Network Security System and system innovation is a key innovation for a wide assortment of uses. Security is urgent to systems and applications. Despite the fact that, arrange security is a basic prerequisite in rising systems, there is a critical absence of security strategies that can be effectively executed. When considering system security, it must be underscored that the entire system is secure. System security does not just concern the security in the PCs at each finish of the correspondence chain.

When developing a secure network, the following need to be considered [1]:

1. Access – authorized users are provided the means to communicate to and from a particular network

2. Confidentiality – Information in the network remains private

3. Authentication – Ensure the users of the network are who they say they are

4. Integrity – Ensure the message has not been modified in transit

5. Non-repudiation – Ensure the user does not refute that he used the network.

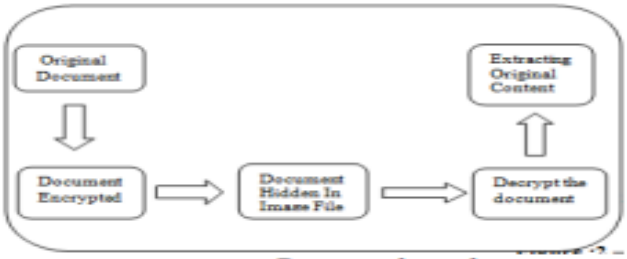
2. LITERATURE REVIEW

In this area the different presentation factor and strategy for encoding the information utilized by different papers are recorded. In the examination paper suggested that the distinctive execution components are talked about, for example, key esteem, computational speed and tenability They inferred that AES calculation is better among Symmetric calculation and RSA calculation is found as better arrangement in hilter kilter encryption procedure. In the examination paper different trial components are broke down. In light of the content records utilized and the exploratory outcome was presumed that

DES calculation devours least encryption time and AES calculation utilize least memory use, Encryption time contrasts in the event of AES calculation and DES calculation. RSA devour more encryption time and memory use is additionally high however yield byte is least if there should be an occurrence of RSA calculation. In the examination paper presumed that every one of the strategies are valuable for constant encryption. Every system is one of a kind in its own specific manner, which may be reasonable for various applications. Ordinary new encryption method is developing henceforth quick and secure traditional encryption procedures will dependably work out with high rate of security.

Proposed Work

Now a day's securing data is a very big challenge to computers users such as Business, Professionals and Home users from the intruders. In this proposed system we implemented and compared three different encryption algorithms for data encryption and then the encrypted file is hidden within an image by using LSB substitution technique.



Proposed work

Purpose of Cryptography

Cryptography provides a number of security goals to ensure the privacy of data, non-alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography.

Confidentiality: - Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

Authentication: -The information received by any system has to check the identity of the sender that whether the information is arriving from an authorized person or a false identity.

Integrity: - Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

Non-Repudiation: - Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.

Access Control: -Only the authorized parties are able to access the given information.

3. CONCLUSION

In this remote world these days, the security for the information has turned out to be exceptionally significant since the correspondence by transmitting of computerized items over the open system happen in all respects oftentimes. In this paper, it has been reviewed that the current chips away at the encryption procedures. Those encryption systems are considered and dissected well to advance the exhibition of the encryption strategies likewise to guarantee the security procedures. To whole up, every one of the systems are helpful for continuous encryption. Every method is special in its own specific manner, which may be reasonable for various applications. Regular new encryption method is developing subsequently quick and secure customary encryption procedures will dependably work out with high rate of security.

REFERENCES

[1] https://s3.amazonaws.com/academia.edu.documents/36508209/V2I600106.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1557294803&Signature=yFT4XlWUsWAP7KU%2BYs0WFOpphnk%3D&response-content disposition=inline%3B%20filename%3Dhttp_student-friendly.blogspot.com_2013.pdf

[2] https://pdfs.semanticscholar.org/a9de/08631272bec3ef1082fc5f4f532a55d131ce.pdf?_ga=2.209734738.610259626.1557291206-1515357488.1557291206