International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 04 | April - 2021 ISSN: 2582-3930

Network Security and Cryptography

Sweta Chourasia[1], Prof Arvind Kumar Pandey[2]

1. M.C.A. Student, ARKA JAIN University,

2. Professor, ARKA JAIN University,

ABSTRACT:

Cryptography and Network Security are used to prevent network and data transfers occurring over a wireless network. Providing data security is one of the key features of data transfer over a reliable wireless network. Network security issues are now becoming more important as the public moves towards the digital information age. As more and more users connect to the internet it attracts more cyber-attacks. The need for wireless network security is very important and is provided by network coverage and security. In this paper we have discussed cryptographic terms, types of cryptosystem and cryptographic model and its algorithm. It is about privacy, authenticity and integrity while disclosing personal information.

Keywords: Cryptography, Security, transmission, Encryption, Decryption.

I. INTRODUCTION

Network Security is responsible for providing security for all information transmitted over the Internet from one computer goes to another. Network Security refers to all software and hardware functions, liability, features, management and control, steps, features, access control, network information and Operating systems are an acceptable level of protection for software and hardware. Cryptography is one of the emerging phenomena technology used to provide data security. The authorized user must provide the user ID and password or otherwise another unique data access secure data. He was keeping the information safe and secure. Four network security issues: anonymity, confidentiality, privacy and authentication. Secret is a word used keeping data confidential without being accessed by unauthorized users. Authentication requires data storage more sensitive. Frequent repentance goes hand in hand with signing. Message Integrity was used to ensure secure communication between sender and receiver. Cryptography is a process of encryption. Cryptography has many facets applications such as computer passwords, ATM cards, e-commerce, electronic transactions, business plans and in other applications. Cryptography is not something that is closely related to cryptology and cryptanalysis. Two technologies are used in cryptography. Encryption used on the sender side and encryption is applied to the receiver side. Encryption cannot do without encryption. Cryptanalysis is used to “break code”. The place where we have cryptanalysis and cryptography is called cryptology. A lot Strong strategies but among them AES is one of the most powerful and effective methods. Use of Cryptography many algorithms and other principles.

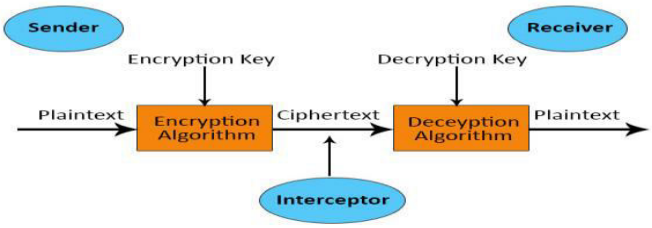

Fig-1 Crypto System

II. CRYTOGRAPHIC PRINCIPLES

A. Redundancy

Cryptographic guideline 1: The entire encoded message contain some excess, there is no need of understanding the message by data.

B. Freshness

Cryptographic rule 2: Timestamp is utilized in each message. For example the time stamp is of 10sec for each message. The beneficiary keeps the message around 10sec to get the message and channel the yield inside that 10sec. The message surpasses the timestamp it is toss out.

III. CRYPTOGRAPHY MECHANISM

Cryptography is a methodology for taking care of and communicating data in a particular casing so those for whom it is normal can peruse and deal with it. The term is consistently associated with scrambling plaintext message (standard substance, sometimes suggested as clear text) into cipher text (a strategy called encryption), at that point back again (known as deciphering). There are, generally speaking, three kinds of cryptographic plans regularly used to accomplish these goals: secret key (or symmetric) cryptography, open key (or hilter kilter) cryptography, and hash works, every one of which is depicted under.

Cipher Text: Cipher text is otherwise called scrambled or encoded data since it contains a type of the first plaintext that is ambiguous by a human or PC without the appropriate code to unscramble it.

Plain text: In cryptography, plaintext as a rule implies decoded data forthcoming contribution to cryptographic calculations, generally encryption calculations. This typically alludes to information that is communicated or put away decoded

Encryption: A system of changing over plain substance into figure content is called as Encryption. This technique requires two things – an encryption estimation and a key. Computation suggests the framework that has been used as a piece of encryption. Encryption of data occurs at the sender side.

Decryption: A pivot methodology of encryption is called as Decryption. In this system Cipher content is changed over into Plain substance. Deciphering measure requires two things-an unscrambling computation and a key. Estimation infers the technique that has been used as a piece of Decryption. All around the two computations are same.

IV. SYMMETRIC AND ASYMMETRIC ENCRYPTIONS

There are commonly two types of techniques that are used for encrypt/decrypt the protected data like Asymmetric and Symmetric encryption technique.

Asymmetric Encryption

It utilizes two distinct keys to send and get the messages. It utilize public key for encryption and another key is utilized for unscrambling. Two client An and B needs to convey, A utilization public key of B's to scramble the message. B utilize private key to unscramble the content. It is additionally called as open key cryptosystems. Diffie-Hellman key trade produce both public and private key.

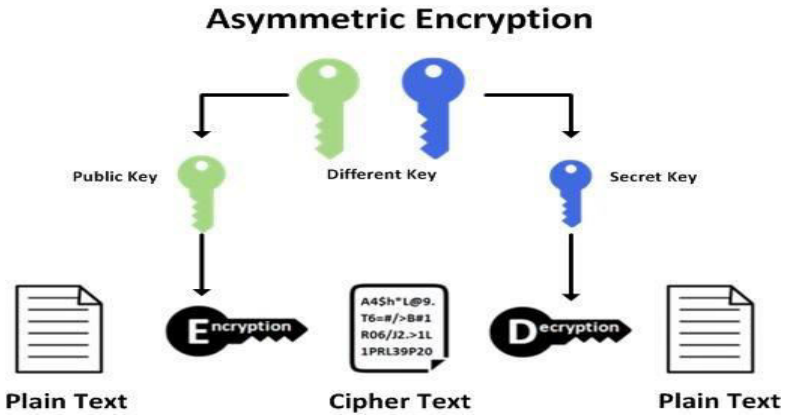

Fig 2- Asymmetric Encryption

Symmetric Encryption

In Symmetric Encryption both the enciphering and translating keys are indistinguishable or in some cases both are identified with one another. Both the key ought to be kept safer in any case in future secure correspondence won't be conceivable. Keys ought to be safer and it ought to be traded in a protected channel between two clients. Information Encryption Standard (DES) is illustration of Symmetric encryption.

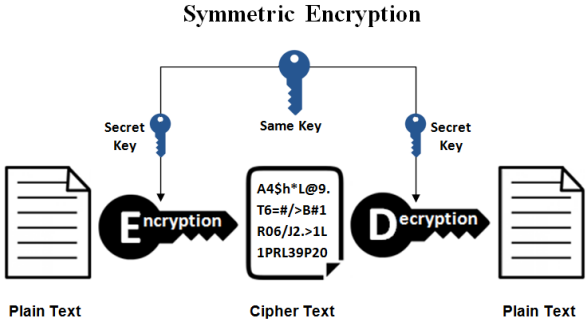

Fig 3- Symmetric Encryption

V. CRYPTOGRAPHIC MODEL

Encryption model

In the encryption model the plain content is changed over into a code text. There are two kinds of keys utilized in Encryption model. One is Symmetric key or private key and the other is public key. With a scrambled encryption just one key utilized for correspondence. Void content can be encoded utilizing a particular encryption calculation.

Decryption model

In the Decryption model the code text is changed over to plain content utilizing both Symmetric and Asymmetric mystery composing. Equivalent encryption for a solitary key is utilized for encryption and unscrambling. In the utilization oflopsided key two distinctive correspondence keys.

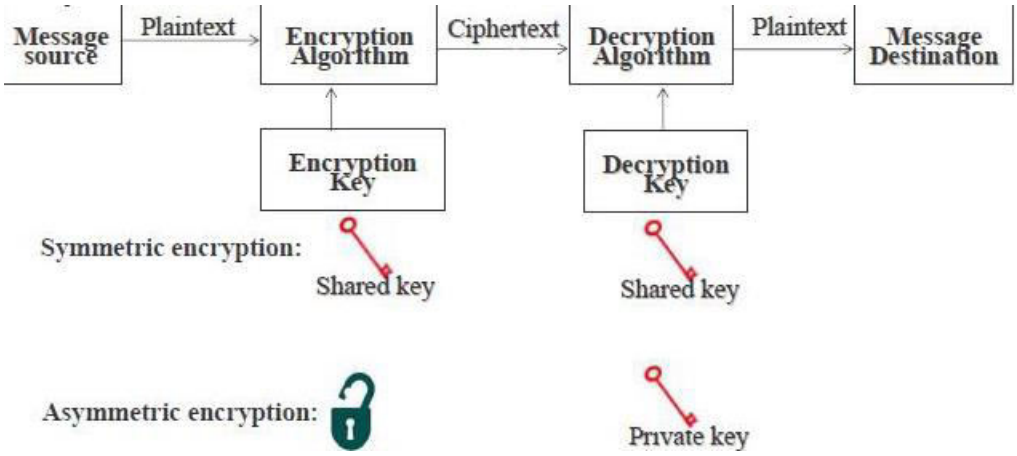

Fig 4 - Cryptographic Model

VI. ENCRYPTION TECHNIQUES

There are two types of Encryption techniques: Substitution and transposition.

Substitution technique: In which plain content letters are supplanted by other letter or by images or numbers. On the off chance that the plaintext is seen as an arrangement of pieces, replacement is incorporated rather than plaintext bit designs with figure text bit designs.

Transposition technique: The rendering method is a cryptographic strategy that changes the plain content over to encode text by performing stages on the plain content, i.e., changing each character of plain content for each round.

1. Rail fence

Rail fence is simple cipher, in which the plaintext is written your plaintext on alternate lines across the page, and then reading off each line in turn.

Plaintext = meet me at home

To encode this message with a rail fence,

we write the message as follows: m e m a h m e t e t o e

The encrypted text is MEMAHMETETOE

VII. SECURITY SERVICES

The security services are:

Confidentiality: It helps to protect information or messages from unauthorized access.

Authentication: Ensures that the source of the message or electronic document is properly identified, and that the identity is not true.

Integrity: Ensures that only authorized teams are able to modify computer assets and transmitted information. Modifications include writing, editing, deleting, creating and delaying or duplicating sent messages.

Non repudiation: It does not require the sender or recipient of the message to be able to deny the transmission.

Access control: Requires that access to sources of information can be controlled or directed by the system.

Availability: Requires computer program assets to be available from authorized groups where required.

VIII. Cryptographic Attacks

Passive attack

In inactive assault the assailant sees every one of the messages and duplicates the substance of data or messages. They center around observing all exchanges and getting information. The aggressor isn't attempting to adjust any information or information they gather. While there isn't anything amiss with the framework because of this assault, it very well may be risky for the security of your information.

Passive attack are of two sorts:

Release of message contents: Phone visit, email message and sent document may contain delicate or private data. We might want to keep the foe from perusing the substance of this exchange.

Traffic analysis: If we had encryption security set up, the rival could in any case see the message design. The foe can decide the area and personality of the correspondence executives and can see the amount and length of messages that are traded. This data can assist with foreseeing the sort of correspondence that was occurring. Minor assaults are more hard to recognize in light of the fact that they don't include information trade.

Active attack In which the assailant endeavours to change the substance of messages or data.

Active attacks are of two kinds:

Masquerade – A masquerade attack is an attack that utilizes a phony character, like an organization personality, to acquire unapproved admittance to PC data through real access ID.

Replay – includes inactive catch of an information unit and its resulting transmission to create an unapproved impact.

Change of messages – Some segment of message is alter or the messages are deferred or recorded, to create an unapproved impact.

Denial of service – (DDoS) attack when numerous PC frameworks are assaulted by an objective, like a worker, site or other organization administration, and results in the dismissal of the client's asset for the proposed asset.

IX. Hash Function

In this Hash work just some numerical strategies are utilized and no key is utilized. After encryption information can't be decoded back to plain content in this calculation. Hash work changes over a mathematical info esteem into another packed mathematical worth. The info is of discretionary length however yield is consistently of fixed length. So it is known as single direction encryption. MD5, SHA-1, and so forth might be such encryption.

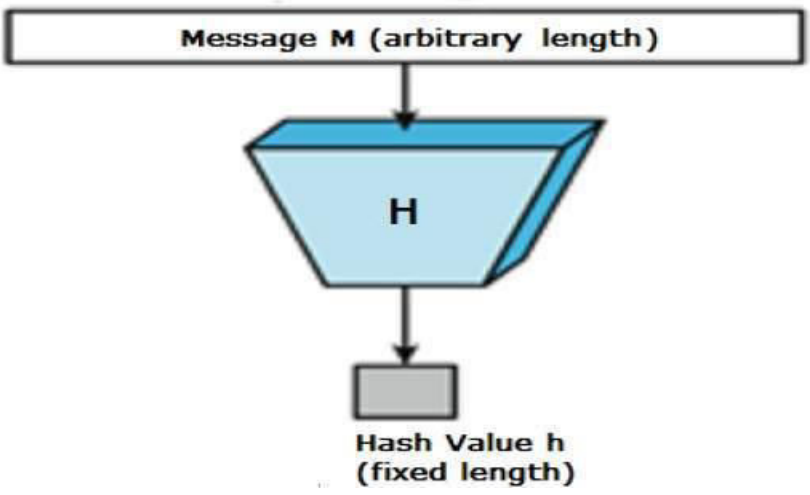

Fig-5: Hash function

X. DataEncryption Standard

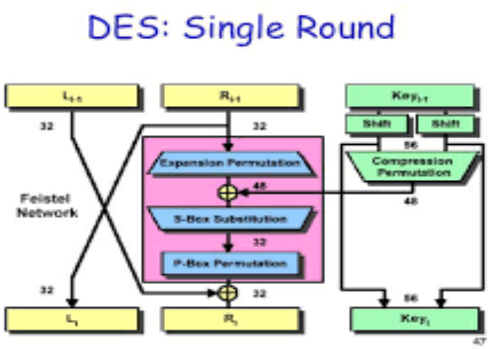

Fig-6: DES

The Data Encryption Standard is popular encryption method and countless people utilized this strategy. The DES is block figure method it utilizes a similar key for to encode and translate. The Block size DES is 64-bit and Key size DES is 56-bits. It is comprises of 16 indistinguishable stages (Rounds), Initial Permutation (IP) and Final Permutation (FP). The information encryption standard comprises of following advances:

1. In this stage 64-digit, the plaintext is consider as contribution to the IP and IP is performed on plaintext and to happen the Permuted Input it adjusts the pieces.

2. In this progression incorporates of 16-rounds of a similar capacity, and it contains replacement and stage Methods.

3. The last cycle (16) yield contains 64-pieces, and they are an element of info plaintext and key

4. The preout is delivered, subsequent to trading the yield of left and right side.

5. Finally preout is gone through IP that implies inverse of IP to make 64-bit ciphertext.

XI. Literature Review:

Sl. No.	Title	Author	Finding	Remark
1.	Data Encyption and Decryption	Ankit Fadia and Jaya Bhattacharjee	Encode information in such a manner to shield it from pariahs. meaning of encryption and decoding and clarification of how encryption	In this study I got to know that concept of cryptography, encryption and decryption algorithm.

			functions with the developing need to defend one's security in correspondence	
2.	Network Security and Cryptography	Shyam Nandan Kumar	Dynamic assault rolls out certain improvements to the information stream. The kinds of dynamic assaults are message change, administration refusal, replay and Masquerade. The latent Attack used to screen correspondence. In a Traffic assault the message is perused by an outsider	It focuses on the Active attack and Passive attack which define how attacker attacks on the messages.
3.	Security in Wireless Sensor Networks using Cryptographic Techniques	Madhumita Panda	security necessities apply to remote sensor organizations like Confidentiality, Proof of credibility, trustworthiness and accessibility. Some tangible security hindrances are utilized inside Very Limited Resources	It focuses on Wireless Sensor Network to provide wireless security communication
4.	Network Security	Prof. Mukund R.	The message	It focuses on

	with Cryptography	Joshi, Renuka Avinash Karkade	ought to be encoded at the sender side yet all the scrambled message contain some excess. The newness use timestamp to get the message.	redundancy and freshness.
5.	Origins and meaning of cryptography	Anjula Gupta	Cryptography as an approach to guarantee ID, accessibility, trustworthiness, verification, and classification of clients and their information by giving security and protection	It focuses on the security services this is use to protect and secure data.
6.	Hash function	Orman	Hash functions are playing a important role in cryptography by providing nearly number to any piece of data	Hash function converts the numerical input value into another compressed numerical.
7.	protecting computer network from attack	Bradley Dunsmore	It describes with general advice about how to set up a comprehensive system of defences. It concludes with information on the specifics of configuring several products.	It focuses on the protecting computer network from attack across the Internet, emphasizing firewall solutions from Cisco, Symantec, Microsoft, and Check Point.

XII. CONCLUSION

Cryptography is quite possibly the main factors in giving security to information interchanges inside networks. Use it to shield information from unapproved clients. The key is traded between the sender and the beneficiary accordingly done in a protected manner. The key should just know the sender and beneficiary in any case the security issue will be detected wake up. In this paper the cryptosystem and its model are examined as far as organization security. Subtleties can be pressed to diminish correspondence costs. Gloom can be kept away from after the information is reduced storage space. There are two kinds of pressure utilized by network security to pack information. It's missing again approaches to lose two different ways to pack. Some cryptographic calculations utilized for network security in provided a safe association. Key trades ought to be made safer. Cryptography and network security is utilized for information correspondence over the web to give security.

XIII. REFERENCE

1. Preneel, B. (2010, September). Cryptography for network security: failures, successes and challenges. In International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security (pp. 36-54).Springer, Berlin, Heidelberg.

2. Kumari, S. (2017). A research Paper on Cryptography Encryption and Compression Techniques. International Journal Of Engineering And Computer Science, 6(4).

3. Bhatia, P., & Sumbaly, R. (2014). Framework for wireless network security using quantum cryptography.arXiv preprint arXiv:1412.2495.

4. Tayal, S., Gupta, N., Gupta, P., Goyal, D., &Goyal, M. (2017). A Review paper on Network Security and Cryptography. Advances in Computational Sciences and Technology, 10(5), 763- 770.

5. Panda, M. (2014). Security in wireless sensor networks using cryptographic techniques. American Journal of Engineering Research (AJER), 3(01), 50-56.

6. Dhamdhere Shubhangi, T., & Gumaste, S. V. Security in Wireless Sensor Network Using Cryptographic Techniques.

7. Kumar, S. N. (2015). Review on network security and cryptography. International Transaction of Electrical and Computer Engineers System, 3(1), 1-11.

8. Kaur, S., Kaur, R., &Raina, C. K. (2017). Review on Network Security and Cryptography.

9. Duong, T., & Rizzo, J. (2011, May). Cryptography in the web: The case of cryptographic design flaws in asp. net. In Security and Privacy (SP), 2011 IEEE Symposium on (pp. 481-489). IEEE.

10. Stallings, W. (2006). Cryptography and Network Security, 4/E. Pearson Education India.

11. Krishnamoorthy, Dr, and S. Chidambaranathan. "Clever Cardnovel Authentication Protocol (NAUP) in Multi-Computing Internet of Things Environs." (2017).