Comparative Study of Cryptography for Network Security

[1]Neha Gupta, [2]Krutibash Nayak

[1]Student, [2]Associate Professor,
[1]Computer Science and Engineering,
[1]Poornima Institute of Engineering & Technology, Jaipur, India

Abstract: This paper aims to provide a broad review of Cryptography for Network Security about how to protect data or information by providing security to them. The increased use of the website attracts many attackers to destroy our data. It requires authorization to access the data in the system which is the network administrator's control. Users opt for password and their ID assigned to them or any other authentication data that enables them to access their authority's information and programs from their authority. Security of networks concerns organizations, companies and alternatives styles of establishments. Cryptography is the technique which is used to convert the plain text into cipher text using various encryption techniques. The art and science used to introduce the secrecy in the information security in order to secure the messages are defined as cryptography. We're going to review this paper about a few latest Cryptographic algorithms which are used to enhance the security of the data and the modern use of paying with the help of the cryptography. It also focuses on various types of cryptography, encryption, decryption concepts and different cryptographic functions used for the security.

Index Terms – Cryptography, Network Security, Encryption, Decryption, Algorithm, Cipher Text, Plain Text, Modern use

I. INTRODUCTION

Network security is the most necessary segment in data security, as it is in charge of verifying all the data that is gone through arranged computers. System security refers to all equipment and programming capacities, highlights, operational techniques, responsibility, measures, get to control, and the executives and managerial strategies required to give a worthy dimension of hardware and software insurance and network data. It consists of a networked administrator's allocation and policies for preventing and monitoring uncertified access, misuse and contradiction of computer networks and network-accessible resources. Security of network covers a diversity of private and public computer networks [1] used in our daily life where businesses, government agencies, and individual conduct transactions and communication. Networks, for example within a company, can be private and public can be private, and other networks that may be open to public access. In organizations, businesses and other types of institutions, network security is involved. As title explains, it does: secure the network and protects and supervises the operations being carried out. The unique name and password is the easiest form to protect a network resource.

Cryptography is crucial for today's pc and transmission networks protective everything from business e-mails to bank transactions and the web shopping whereas traditional and fashionable cryptography appoint varied mathematical proficiency to prevent eavesdroppers from teaching encrypted content. Computer systems and networks that are storing process and human activity careful or valuable info need safety against such unauthorized access. Cryptography named Symmetric cryptography and asymmetric cryptography techniques. In symmetric key cryptosystem, a same key is used by the two users. The sender uses this key and an encryption estimation to encrypt the data. The beneficiary uses a comparable key and the relating unravelling count to decrypt the data. In upside down or open key cryptography, there are two keys i.e., public and private key are used. Cryptography is the science of the secret writing the code that can't be understood by anyone. It is a combination of code that is required for encoding and decoding of the content. When cryptography is not there in the context then, any transmission between the sender and the receiver can be easily modified or read. Every data we send from private message to your partner or information about your bank details will become open for the public examination [3].

A simple or ordinary text which is sent above the network is first off arrive and modified in to cipher text hence to the amount so that only the sender and the [2] buyer can make use of the information, In empiric terms [2], the technique in which the simple text messages get encoded in cipher text messages is recognized as encryption process. The transformation process of cipher text into ordinary text messages is recognized as the decryption process. Decryption is simply the opposite of the encryption process. In a laptop, to computer communication, the computer at senders quite commonly transforms plain text content messages in cipher text by using encryption technique. Then this message is dispatched to the receiver over the network [2]. The receiver laptop takes the encrypted message yet performs the decryption method in conformity for obtaining the plain text. The method of encoding and decoding is regarded as cryptography [2]. Encryption is the conversion process of common data (known as plain text) in incomprehensible text (known as cipher text). Decryption is the reverse that moves back from unintelligible cipher text to plaintext [1]. The Cryptosystem is an ordered list of possible finite plain text elements, possible finite cipher texts and possible finite keys, and the algorithm for encryption and decryption that match each key [1].

Example: We should perceive how cryptography can help secure the communication among Andy and Sam. While sending the message, Andy converts the message from plain text to cipher text. Here, the changes over the message to some irregular numbers. From that point onward he utilizes a key to encode his message. In cryptography, we call this cipher text. Andy then sends this non readable message or encoded message over the correspondence channel, he won't need to stress over someone highly involved with finding his private messages. Assume, Eaves here find the message and he by one way or another figure out how to alter it before it reaches Sam. Presently, Sam would require a key to decode the message to recuperate or recover the original or first plaintext. So, as to change over the ciphered content into plain content Sam would need to utilize the unscrambling key. Utilizing the key he would change over the ciphered content or the numerical incentive to the comparing plain content. In the wake of utilizing the key for unscrambling what will turn out is the first plaintext message is a blunder. Presently this mistake is critical. It is the manner in which Sam realizes that the message sent by Andy isn't equivalent to the message that he got. Therefore, we can say that encryption is vital to impart or share data over the system.

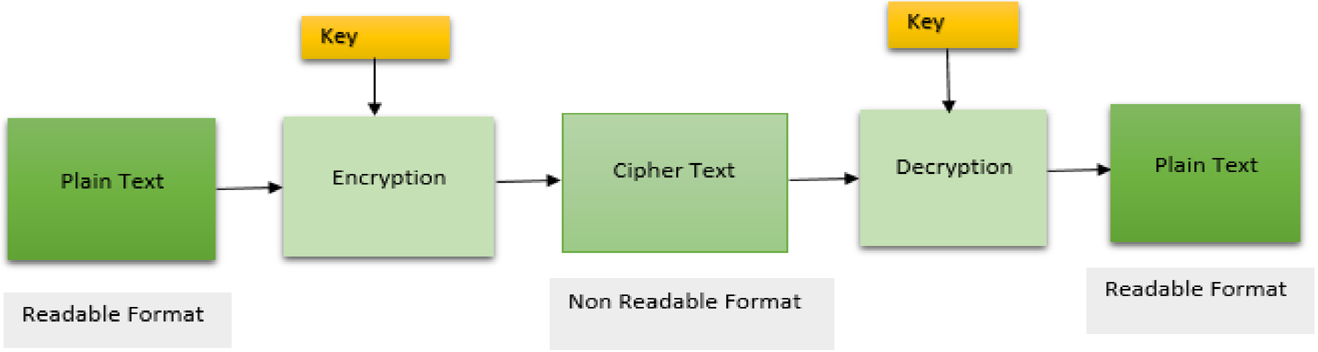

Figure 1. Cryptography Technique

II. CRYPTOGRAPHIC FUNCTIONS

Cryptography is required when communicating over any non-reliable mode such as the Internet. There are various services that are provided to ensure the security of the system. It amplifies the safety of data handling and transfer. There are basically four main ways that cryptography is used to ensure data security.

2.1 Authentication

It is a process in which the receiver needs to be sure of the originator identity. It certifies that the data accepted by the receiver has been sent only by a recognized and verified originator or sender. Authentication is a process to ensure that the customer on both ends of the connection are actually who they claim to be. We experience at least one type of authentication used on the web whenever we use a secure website, such as your company's intranet site or even Amazon. Secure websites use what is called an SSL certificate, which provides proof that the holder of the website possess a public cryptography key and exhibit that a user is connected to the correct server. Depending on the browser they use, an online user will see a closed padlock or a green URL to indicate that the website they are connected to is the one it claims to be or secure. Another example of cryptography being used for authentication purposes is Pretty Good Privacy, which is a freeware software collection that is used to supply encryption and validation for messaging, digital signatures and data compression, as well as emails and their attachments.

2.2 Non-repudiation

It keeps either sender or beneficiary from denying a transmitted message. Hence, when a message is sent, the recipient can demonstrate that the supposed sender in truth sent the message. Additionally, when a message is gotten, the sender can demonstrate that the supposed collector in truth got the message [1]. In the early days of online financial and e-commerce dealings, some users would approve an online transaction, then later claim they had never approved the transaction. Cryptographic non-repudiation tools were created to ensure that a specific user had indeed made a transaction, which could not be disclaimed later on for the purposes of a refund. This prevents online banking users from authorizing a funds transfer to an outside account, then coming back a few days later claiming they had not made the transaction and demanding the money be refunded to their account. A bank can prevent the above attempt to steal funds by putting the correct non-repudiation measures in place, which can consist of hashed data, digital certificates and more.

2.3 Confidentiality

Confidentiality, or keeping your private data private, is one of the most important security applications for any user. Safeguarding approved confinements on data access and exposure, including implies for securing individual protection and exclusive data. Lost privacy is the unapproved exposure of data [1]. Today's constant data breaches, which are usually due to a lack of proper cryptography for the task at hand, make the appropriate use of cryptography a must for any secure process.

2.4 Integrity

Cryptography can ensure that no one can change or view data while it's in transit or in storage. It can apply to a flood of messages, a solitary message, or chose fields inside a message. Lost honesty is the unapproved change or devastation of data [1]. Cryptography can ensure that a rival company, or any other party hoping to profit from data tampering, cannot screw around with the company's sensitive data and internal correspondence.

III. ENCRYPTION ALGORITHMS

In general, there are basically two types of techniques for encrypting and decrypting the protected data or information like Asymmetric and Symmetric encryption technique.

3.1 Symmetric Key Cryptographic Algorithm

Symmetric Key Algorithm is also well known as secret key cryptosystems. In this encryption structure sender and recipient of the message share a solitary key that is utilized for encrypting and decrypting the message [5]. The Symmetric key algorithm provides authentication as well as authorization to the data because data is encrypted with one of the unique keys cannot be decrypted with any other key. It is an actuality that the key should be well-known to both the sender and the recipient i.e., it is kept hidden. In symmetric key algorithms, the key used is kept confidential and not released publicly. The main problem of Symmetric Key Cryptography is the distribution of the key between sender and receiver [6]. Information Encryption Standard (DES), Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES) are the most popular Symmetric-key Algorithms which are used for the security. Symmetric Key Algorithms generally are inexpensive.

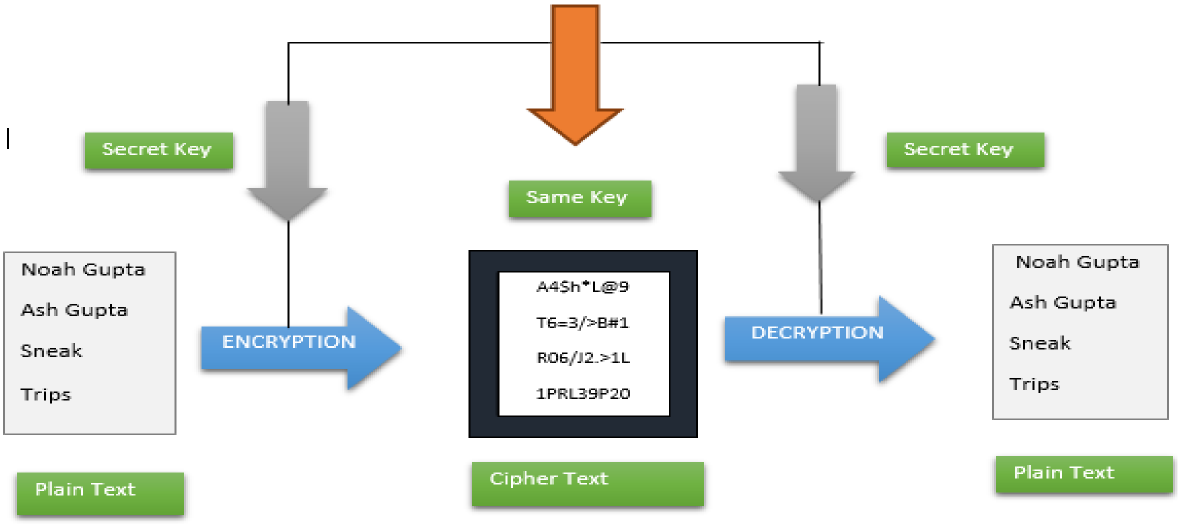

Figure 2. Symmetric Key Cryptography

3.2 Asymmetric Key Cryptographic Algorithm

Asymmetric Key Algorithms are also known as Public Key Cryptosystems. In this encryption process where we use different keys for encrypting and decrypting the data or information. These keys are extraordinary however are numerically related, with the end goal that recovering the plain content by decoding figure content is achievable. It has been considered as the form of cryptosystem where we are using two different keys [4] for encryption and decryption process. Two keys are used in the asymmetric algorithm- one is a private key and public key [4] which is kept secret. The secret key of the algorithm is interchange over a large network with ensuring that the unauthorized person does not misuse the keys. It can be used for confidentiality, authentication or both. Some of the famous examples of Asymmetric Key Cryptosystem are RSA Algorithm, Digital Signature Algorithm (DSA) and Diffie Helman Algorithm.

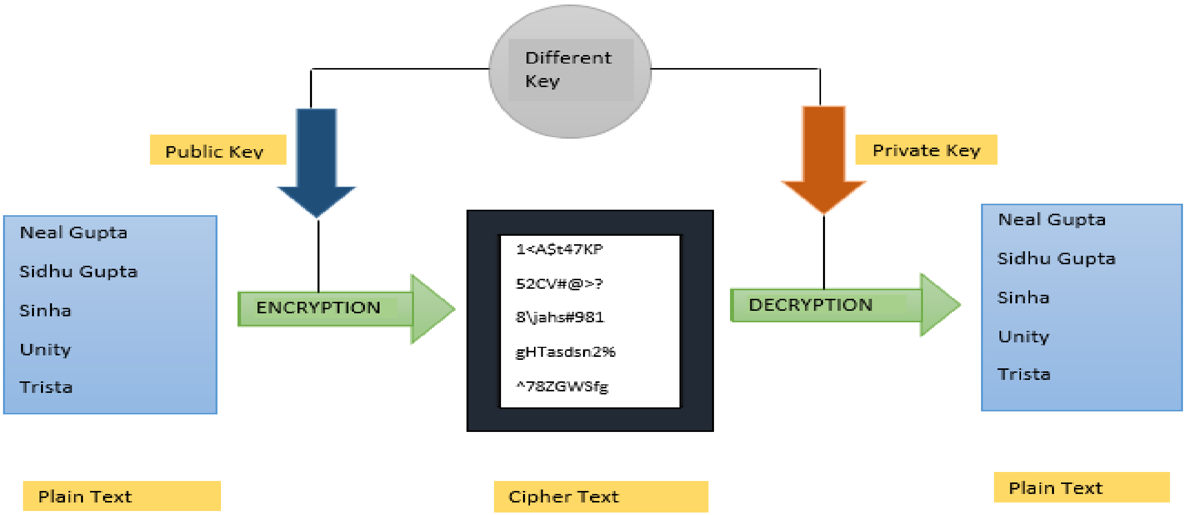

Figure 3. Asymmetric Key Cryptography

IV. MODERN USES OF CRYPTOGRAPHY

In this modern era, cryptography is used in banks, credit unions and other financial organizations to encode the data that is sent or transmitted between credit card companies, banks, their customers and other occupation. It protects the information or data during communication and when it is conserved in large databases. In our daily life, we use a credit card for secure transmission of payment for the goods. When we swipe our card at the store to pay for our purchase, there is a piece of information that is stored on the card's embedded chip or magnetic strip that is in encrypted form so that no one can read that information. The encrypted data or information that is in non-readable form is transferred to do the payment processor that make sure your credit card limit hasn't reached i.e., with another encrypted dispatch or transmission and then replies with an encoded approval code. This type of activity takes place when we use another kind of technique for payment such as debit card or NFC based forms of "touches" payment systems, like Android Pay or Apple Pay. In his transactions are carried out electronically with a net transport or shift of finance from one customer to another, which may be either credit card or debit card and can be either recognized or unnamed. Unacknowledged applications do not disclose the name of the customer that is based on the unsighted signature plan. Recognized spending plan disclose the name of the customer that is based on more common forms of signature schemes. Unnamed schemes are the electronic analog of cash, while named schemes are the electronic analog of a credit card or debit card. Encryption is used in digital money plan to protect normal transaction information or data like transaction amounts and account numbers, digital signatures can restore credit card license or handwritten signatures, and public key encryption can provide privacy or confidentiality. When data is not encrypted then data violation or breaches of data would become so usual or common that would probable or likely to happen on a day to day or even hourly basis, instead of the monthly incident they seem to be in current times. The data violation or breaches that we see in the news on a uniform or regular basis can normally be allocated due to a lack of correct encryption or to the use an especially fragile structure of cryptography to safeguard the data or information. Time stamping is a technique that can guarantee that a definite digital document communication existed or was delivered at a definite time. It uses an encryption representation called a blind signature scheme. Blind signature schemes permit a sender to get message receipt by another party without disclosing any data or information about the message to the other customer. It is very much close as sending a recorded letter by the US mail, but supply a separate level of evidence. It can show that a receiver accepts a particular document. Possible requests include copyright archives, patent applications, and contracts. It is an unfavorable request that will assist to make the transformation in electronic lawful papers possible. We can understand this by an example of our daily life, we use the credit card for the payment of groceries which has a magnetic strip or embedded chip in it, and then the card is swapped in the credit card reader that reads the encrypted information or data on the credit card. The information is sent to the payment processor in the encrypted format so that no one can read it. Payment Processor decrypts the information or data which is sent by the credit card reader which approves the transaction so that we can understand or in a readable form to approve the transaction. Then the reply is sent to the card reader with the help of the Encrypted approval code. By going through all these processes the payment gets processed and the customer gets their groceries. Given below is the figure to explain the process of cryptography in our daily life.

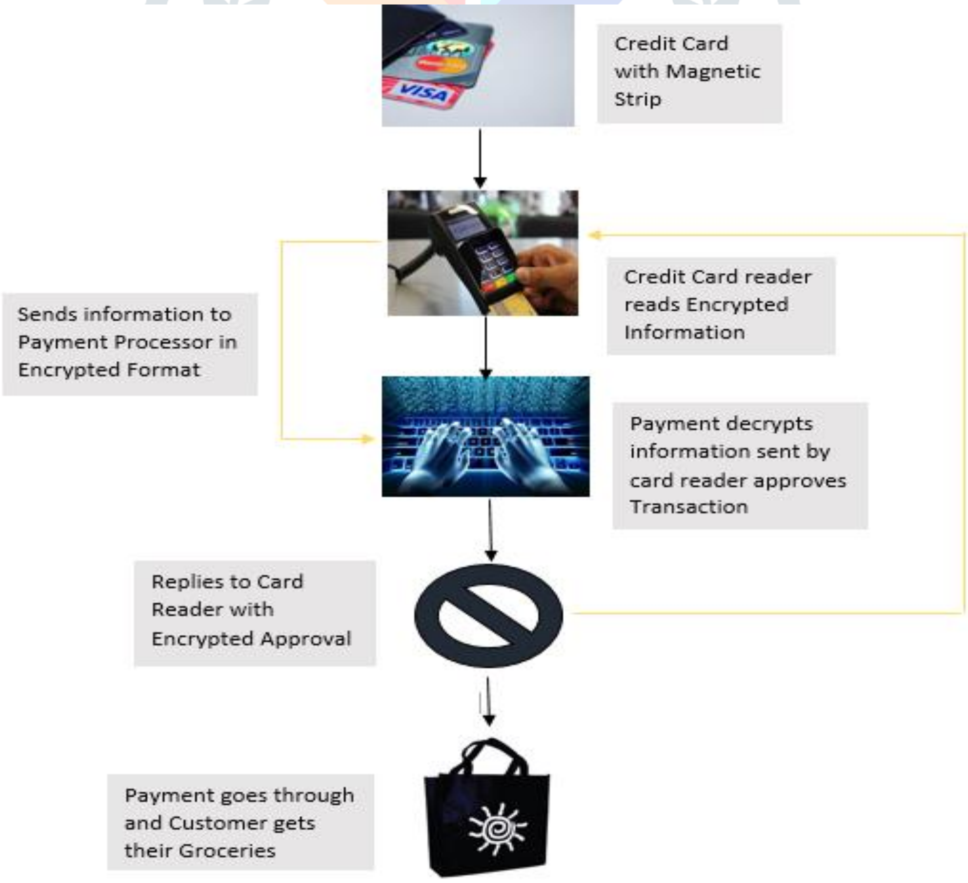
Credit Card with Magnetic Strip
Credit Card reader reads Encrypted Information
Sends information to Payment Processor in Encrypted Format
Payment decrypts information sent by card reader approves Transaction
Replies to Card Reader with Encrypted Approval
Payment goes through and Customer gets their Groceries

Figure 4. Paying for Groceries with Credit card

V. CONCLUSION

Any organization or approval whose inside the private system is appended to the server has turned out to be progressively worried in this range of Internet, arrange and digital security. Network Security uses the algorithm in network applications and protocols. We have studied various algorithm and techniques to provide data security to the network. Those who are well tested and well studies are the best algorithms. The unique "code" required to encrypt and decrypt the data will make the technique systematic form for keeping the data safe from prying eyes. The big usage of the internet for business and individual communications makes encryption a must for any diplomatic data. Without cryptography, any message you send on the internet could be intercepted and read. The paper discusses the various schemes which are used to secure the Network system. In this paper, we can discuss how the symmetric key algorithm is faster than the asymmetric key algorithm. However, asymmetric key cryptosystems are progressively adaptable and give more confirmation and non-revocation. But we need more algorithm to provide security for the encryption of the data or information to provide security from the theft or attack by the hacker. We have also discussed the modern use of cryptography in our daily life.

REFERENCES

[1] Pubs.sciepub.com Review on Network Security and Cryptography, Shyam Nandan Kumar, International Transaction of Electrical and Computer Engineers System, 2015, Vol. 3, No. 1.

[2] ijsrcseit.com Study on Cryptography and Techniques, Shivani Sharma, Yash Gupta, International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2017 IJSRCSEIT | Volume 2 | Issue 1 | ISSN : 2456-3307.

[3] Sarah Zanafi, Noura Aknin, Maurizio Giacobbe, Marco Scarpa, Antonio Puliafito. "Enabling Sustainable Smart Environments Using Fog Computing", 2018 International Conference on Electronics, Control, Optimization and Computer Science (ICECOCS), 2018.

[4] www.ripublication.com A Review paper on Network Security and Cryptography, Dr. Sandeep Tayal, Dr. Nipin Gupta, Dr. Pankaj Gupta, Deepak Goyal, Monika Goyal, ISSN 0973-6107 Volume 10, Number 5 (2017) pp. 763-770.

[5] Study on symmetric key encryption: An Overview by Dharitri Talukdar, International Journal of Applied Research 2015.

[6] An Overview of Cryptography an article by Gary C. Kessler, Embry-Riddle Aeronautical University - Daytona Beach, March 2016.