International Journal of Innovations & Research Analysis (IJIRA)
ISSN :2583-0295, Impact Factor: 5.449, Volume 03, No. 01(II), January- March, 2023, pp 73-78

A REVIEW PAPER ON CRYPTOGRAPHY IN NETWORK SECURITY

Pratiksha Mishra*

ABSTRACT

Cryptography is the study and practice of techniques for secure communication in the presence of third parties called adversaries.With the increasing growth in the internet, Network Security has become a big concern and threat for organizations whose private network is connected to the internet. Information security is the most extreme basic issue in guaranteeing safe transmission of data through the web.In order to secure data transmission and network, cryptography and network encryption are used. Cryptography ensures that the content of messages remain confidential. Network Security has become one the major concerns as the world transitions to digital world. Network security provides security for administrator managed data.Network security is setup to guard against unauthorized access, alteration, or modification of information, and unauthorized denial of service. In this paper, we have discussed about cryptography process, security mechanism, security services, attacks, types of cryptography, Steganography.

Keywords: *Cryptography, Network Security.*

Introduction

In today's world, cryptography plays a major role in protecting the information of technology. Nowadays private information is being shared of a user on many platforms like E-commerce websites, e-banking, hospitals etc. so, there should be a way to protect user information from being misused.

Cryptography is used to convert the data into a form so that it cannot be understood, in this readable data is converted to unreadable forms through algorithms which makes the data secure. For example, Rohan is a sender who will send data or a message and Yogesh is the receiver. Rohan uses insecure communication methods like telephone lines or computer networks. This message can be interpreted by the hackers and even they can modify the message during its transmission and Rohan and Yogesh will remain unaware of the changes made to the message. In this survey,many cryptography encryption methods and techniques have been reviewed and discussed.

Network Security is modern and growing technology. Network Security refers to the measures taken by any organization to secure its computer network and data using both hardware and software systems. Network Security problems can be divided into four categories:

- Secrecy
- Authentication
- No Reputation
- Integrity Control

* Lecturer, Department of Computer Science, S.S. Jain Subodh P.G. Mahila Mahavidyalaya, Jaipur, Rajasthan, India.

We will discuss these problems in detail in this review. The aim is to secure the confidentiality and accessibility of the data. Some of the network security principles are Confidentiality, Authentication, Integrity, Access control, and Availability. Many people think that to educate and train people about network security they should think like a hacker, it gives them an edge to make correct decisions. Cryptography is used for Network Security. In cryptography, if data can be read easily is called Plain Text and the method through which plain text is converted into unreadable text is called encryption and encrypted text is called Cipher Text. A key is required to convert the cipher text to plain text so, by this we can prevent hacker to steal users' data. The process of converting cipher text to plain text is called Decryption.

There are three general classes of NIST-approved cryptographic algorithms, which are defined by the number or types of cryptographic keys that are used with each.

- Symmetric Algorithm
- Asymmetric Algorithm
- Hash Functions

Literature Survey

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. The term is derived from the Greek word ‘kryptos’, which means hidden. Cryptography is used to achieve Network Security. With the help of cryptography, we can achieve Network Security principles.

- **Confidentiality**

This principle states that only sender and receiver will be able to access the information that is being shared. The degree of confidentiality determines the secrecy of the information. If an unauthorized person is able to access the information then confidentiality is compromised. For example, if A wants to share some information with B that is confidential and a hacker C is able to access the information then it is said that confidentiality is compromised.

- **Authentication**

Authentication is the mechanism that is used to identify the user system or entity. It ensures the identity of the person who is trying to access the information. The authentication is mostly secured by setting username and password. The authorized person whose identity is pre registered can prove his identity and then access the sensitive information.

- **Integrity**

Integrity ensures that the data and information that is received is exact, accurate, and unaltered. If the content of the data or message is changed while data is being transmitted from sender to receiver then it is said that the integrity of the data is lost

- **Non-Repudiation**

Non-repudiation is a method that prevents the denial of the message content sent over a network. Many times the sender sends the message and later denies it. But the non-repudiation does not allow the sender to refuse the receiver. It is a mechanism that is used to ensure that the message has been sent and received by the receiver so that the recipient can’t claim that the message was not delivered.

- **AccessControl**

Access control is the process that prevents unauthorized access and use of the resources.The principle of access control is determined by role management and rule management. Role management determines who should access the data while rule management determines up to what extent one can access the data. The information displayed is dependent on the person who is accessing it.

- **Availability**

According to the principle of availability the resources will be available to authorize party at all times. Information will not be useful if it is not available to be accessed.

Importance and Approach

In cryptography, we hide the information that is in plain text form, it is also called original text. This information can be in the form of alphabets, words or numerical data or pictorial representation etc.

The original or plain text refers to the data in its original form, that is the data before the encryption or the data after the decryption has been done. for transmission and security purposes data is converted into Cipher Text. The cipher text is nothing but meaningless data without decryption. cipher text is used for the transmission of data not plain text. There are many algorithms that can be used to convert plain text into cipher text.

The algorithm of transforming plain text to cipher text is called Caesar cipher. The method of converting plain text or readable data into cipher text or in meaningless data is called encryption or encoding. when the data is encrypted it can be transmitted without the risk of a security leak of data.

The formula of encryption is:

E_n (x) = (x + n) mod 26

After the transmission, the receiver needs to decrypt the cipher text in order to read and understand it. So this process of converting cipher text into plain text is called decryption or decoding.

The formula of decryption is:

D_n (x) = (xi - n) mod 26

Where,

E denotes the encryption

D denotes the decryption

x denotes the letters value

n denotes the key value (shift value)

"i" denotes the offset of the ith number of the letters, as shown in the table below

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

For Example while Encryption

Plaintext: J → 09 , En: (09 + 3) mod 26

Now, Ciphertext: 12 → M

For Example while decryption

Ciphertext: 12 → M ,Dn: (12 - 3) mod 26

Now, Plaintext: 09 → J

Types of Cryptography

Cryptography has many types which include codes, steganography, etc. codebooks are used for codes, in steganography different methods are used to hide the plain text such as behind a picture. all these different methods of cryptography use different alphabetical, numerical, or other digitally generated ciphers.

- **Codes and Codebooks**

A code means a properly constructed phrase, sentence or symbol that can represent some other message in a hidden form.If a code is designed properly it can provide high security. Codebooks are generally used for these types of encryption but these codebooks need to be guarded well in order to maintain the secrecy of the code. But there is one more demerit of codebooks that the more a codebook is used the less secure it becomes.

- **Steganography**

In steganography we hide the existence of the message itself by using some tools like microscopic writing, hiding text or message behind a photograph etc.

Steganography is the practice to conceal or hide a message or information behind a normal message or picture such as without giving any idea of having any secret information present there.The first use of steganography is assumed to be in 440 BC by the Greeks, they used to write messages on a wooden log and used to cover it with wax to hide it from being seen in normal ways.

- **Ciphers**

Ciphers are most commonly used in cryptography because of their ease of use. There are 2 types of ciphers.

- Substitution ciphers
- Transposition ciphers

Ciphers can be defined as secret codes that are used to encode plain text. In a substitution cipher, each alphabet of plain text is replaced by a particular cipher or group of letters or symbols. whereas in transposition cipher letters of a word in plain text are jumbled or rearranged in such a manner that they are no longer readable or understandable.

- **Computer Ciphers**

Many Government agencies such as banks, hospitals, schools, and colleges need to share some crucial information from one computer to another which can turn out to be crucial information that is why it needs to be secured. such information is secured by using computer encryption methods.

- **Cryptanalysis**

This is nothing but a method to analyze the cipher text to extract the plain text or key from it. We can say that cryptanalysis is just the opposite of cryptography. Before designing any encryption system we must analyze its code-breaking.

The science of cryptography has become very developed so far. There are so many software and hardware that are able to encode and decode data in a very secure way.

Cryptographic Algorithm

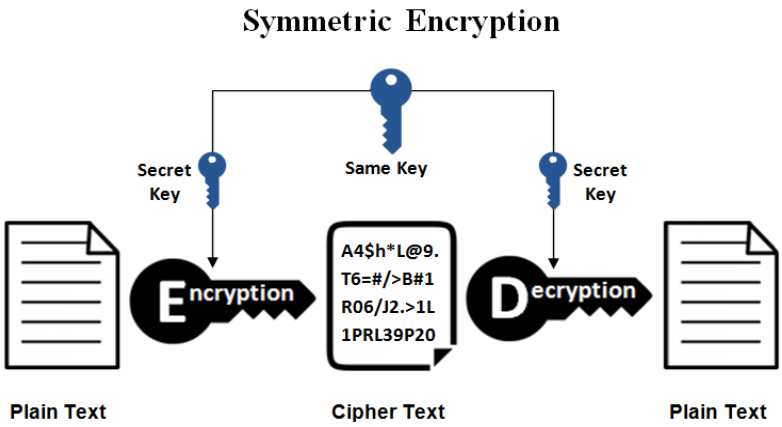
- **Symmetric Encryption**

It is an algorithm in which the sender and receiver both have the same 'key', which means the same key is used to encrypt and decrypt the message. The key used is called as Secret Key. Symmetric Encryption consists of two parts:

- Substitution Ciphers
- Transposition Ciphers

Example of Symmetric Encryption:

- Data Encryption Standard (DES)
- Triple Data Encryption Standard (Triple DES)
- Advanced Encryption Standard (AES)
- International Data Encryption Algorithm (IDEA)

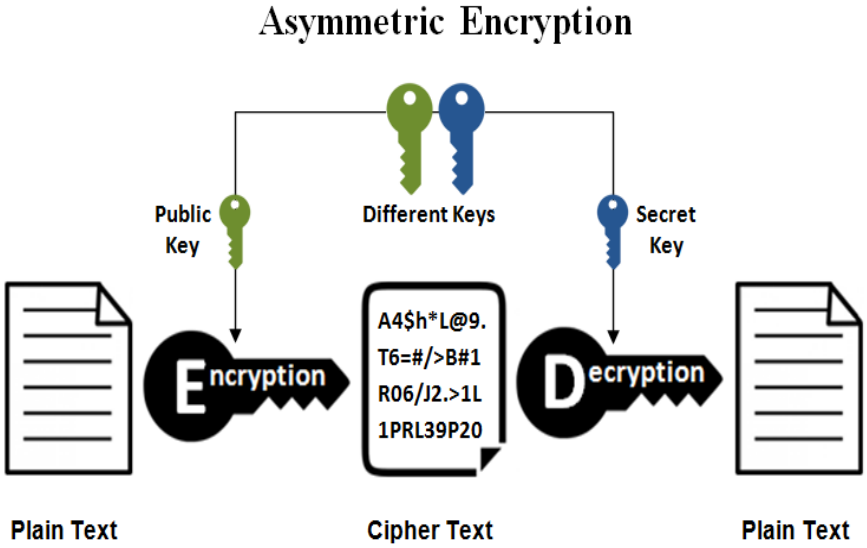


- **Asymmetric Encryption**

In Asymmetric Encryption, we use two separate keys for encryption and decryption. One key is a public key which is used for encryption and another is the private key which is used for decryption. So, in this, the receiver must have a private key or secret key which is used for decryption for converting cipher text back to plain text.

Example of Asymmetric Encryption

- Rivest Shamir Adleman (RSA)
- the Digital Signature Standard (DSS), which incorporates the Digital Signature Algorithm (DSA)
- Elliptical Curve Cryptography (ECC)
- the Diffie-Hellman exchange method
- TLS/SSL protocol



- **Hash Function**

Hash Function is a mathematical function that converts the plain text into unique ciper text of a specific length. Values that hash function returns is called digest or hash value. The definition tells s that no two data will have the same hash value if the data changes hash value also changes. Basically, it is used to ensure that the message reaches to the recipient in the same condition.

Example of Hash Function

- Secure Hash Function (SHA)
- Message Digest
- Whirlpool(512 bit)

Conclusion

Cryptography acts as a key component for providing network security. Cryptography is a great technique for providing security goals like data integrity, confidentiality, no-repudiation. Cryptography plays an important role in providing robust, reliable, and strong Network Security. In this review, we have discussed various types of cryptography that are used like Stenography, Ciphers, Cryptanalysis, Code and CodeBooks, Computer Ciphers. We have also discussed various Cryptographic Algorithms like Symmetric Encryption, Asymmetric Encryption, and Hash Function, these algorithms are used to convert plain text messages into Cipher Text so the message becomes unreadable and can be sent to the receiver securely.

References

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
3. Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Transactions on Information Theory 22, 644–654 (1976).