Volume 3, Issue , 2024
PP 370-379

International Journal of Futuristic Innovation in Arts, Humanities and Management (IJFIAHM)

Network security and Cryptography

Monali Sudhakar chalurkar
chalurkarmonali@gmail.com
Department of Computer Science& Engineering, Shri Sai College of Engineering & Technology, Chandrapur, India

Prof. Pushpa Tandekar
p.tandekar@yahoo.in Departmentof Computer Science & Engineering, Shri Sai College of Engineering & Technology, Chandrapur, India

Prof. Ashish Deharkar
Ashish.deharkar@gmail.com Department of Computer Science& Engineering, Shri Sai College ofEngineering & Technology, Chandrapur, India

Abstract:

With the arrival of web and ecommerce applications and social networks across the world generate huge amount of data. Network Security is the most extreme issue to guarantee safe transmission of data through the web. As large amount of user connect to internet it is attracted by huge number of cyber-attacks. Cryptography is the method of using mathematical algorithms to encrypt and decrypt the information. Store data or transfer it across unconfident networks so that it cannot be view by anyone except the conscious recipient. While cryptography is the technique of protecting data, cryptanalysis is the science of surveying and breaking secure conversation. It is basically used to convert the plain text into cipher text .In this paper we provide an overview on Network Security andCryptography.

Keywords— Cryptography, encrypt and decrypt, Cryptanalysis, Network Security.

I. INTRODUCTION

Society across the world generates a massive quantity of information day by day. Networksecurity is the maximum difficult challenge in the internet and community. Pc andcommunity security is a new and rapid moving generation and security of records can beaccomplished with the aid of an artwork called cryptography. Nowadays records protection machine includes confidentiality, authenticity, integrity, non-repudiation. It convert information of a given layout is plaintext to some other layout is cipher text, theusage of an encryption key. The operation of reversing cipher text to its authentic

undeniable text is called decryption set of rules. Reason of cryptography includes ATM cards, laptop passwords, and military, medical area.

Cryptography is the science of information security. Information security is the most extreme basic issue in guaranteeing safe transmission of data through the web. Also network security issues are now becoming important as society is moving towards digital information age. The word cryptography is derived from Greek kryptos, meaning concealed as more and more users connect to the internet it attracts a lot of cyber-attacks. Its required to protect computer and network security i.e. the critical issues. The pernicious hubs make an issue in the system. It can utilize the assets of different hubs and safeguard the assets of its own. In this paper we provide an overview on Network Security and various techniques through which Network Security can be enhanced i.e. Cryptography.

ARCHITECTURE DIAGRAM

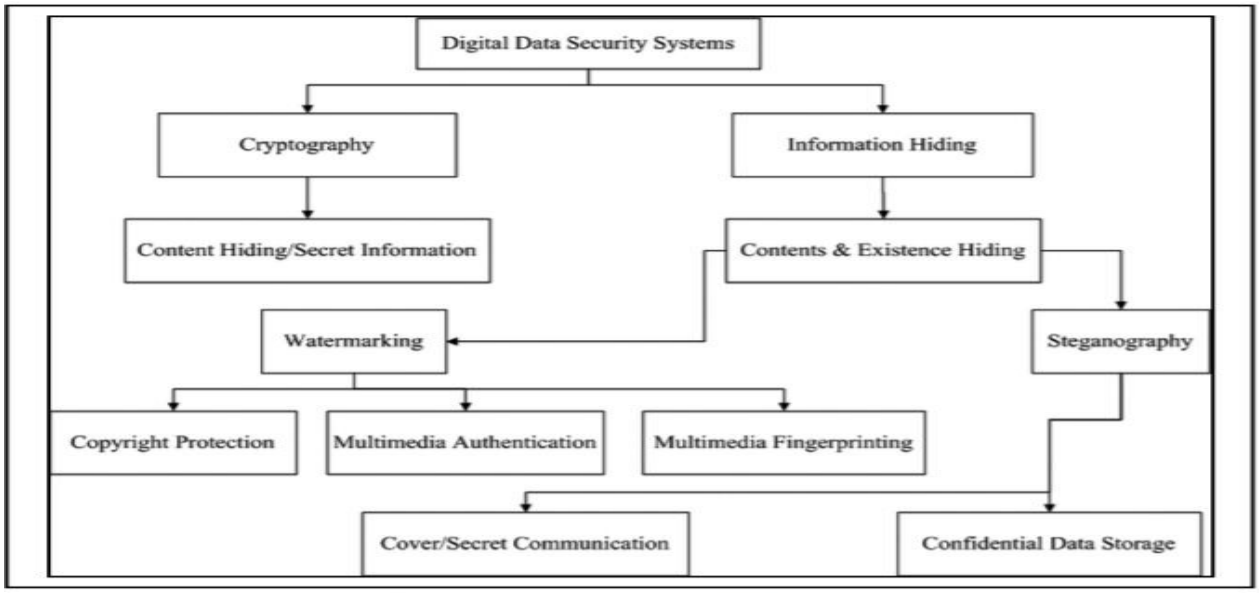

Fig1: Architectural Diagram

FIGURE 1.1 : ARCHITECTURAL DIAGRAM

METHODOLOGY

1) BASIC TERMINOLOGY OF CRYPTOGRAPHY

Cryptography Is The Conversion Of Smooth And Readable Statistics Into A Shape That Cannot Be So As To Cozy Information. The Word Cryptography Comes From The Greek Word "Kryptos", Which Means Unknown And Invisible, And "Graphikos" Which Shows Writing. Cryptography Is Related To The Approach Of Changing Normal Plain Textual Content Into Unintelligible Textual Content And Vice-Versa. It Is A Manner Of Storing And Transmitting Information For The Duration Of A Selected Shapes In Order That Most Effective The Ones For Whom It's Intended Can Examine And Procedure It.

Cryptography Now Not Only Protects Records From Theft Oralteration, But Additionally May Be Used For Consumer Authentication. The Statistics That Require To Cover, Is Known As Authentic Textual Content, It Might Be For The Duration Of A Form Of Characters, Numerical Information, Executable Applications, Pix, Or The Other Quite Information, The Records With The Intention To Be Translated Is Referred To As Cipher Text , It's A Time Period Refers To The String Of "Worthless" Records, Or Meaningless. It's Far The Information With A Purpose To Be Transmitted Specially Thru Network; Many Algorithms Are Needed To Transform Plaintext Into Cipher Textual Content.

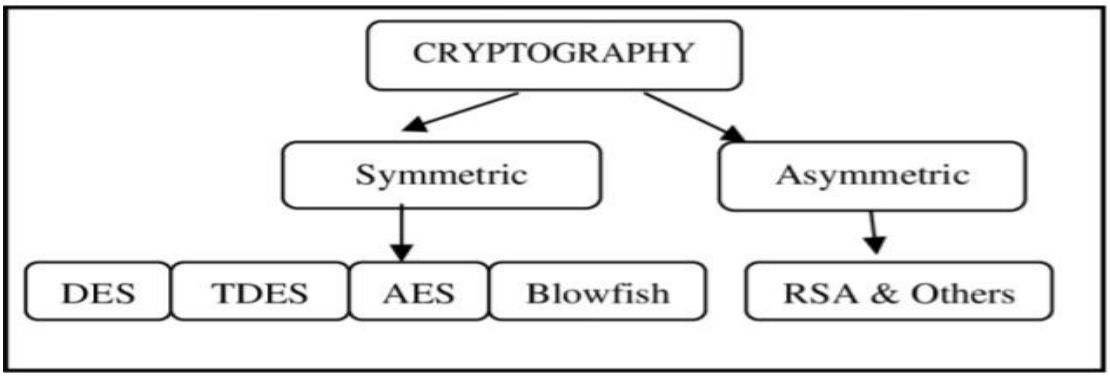

Figure 2.1 : BASIC TERMINOLOGY OF CRYPTOGRAPHY

2)SYMMETRIC KEY CRYPTOGRAPHY

It Is A Form Of Encryption Wherein Only One Key (A Secret Key) Is Used To Both Encrypt And Decrypt Digital Data. The Entities Speaking Via Symmetric Encryption Should Trade

The Key In Order That It May Be Used Within The Decryption Method.By Using The Use Of Symmetric Encryption Algorithms; Information Is Transformed To A Form That Cannot Be Understood By Means Of Every Person Who Does Not Possess The Name Of The Game Key To Decrypt It. If There Need To Be An Prevalence Of Symmetric Encryption, Same Cryptography Keys Are Carried Out For Encryption Of Plaintext And Reduce Of Discern Content. Symmetric Key Encryption Is Rapid And Much Less Hard But Their Principle Problem Is That Each The Customers Want To Transport Their Keys Safety[3, 4]

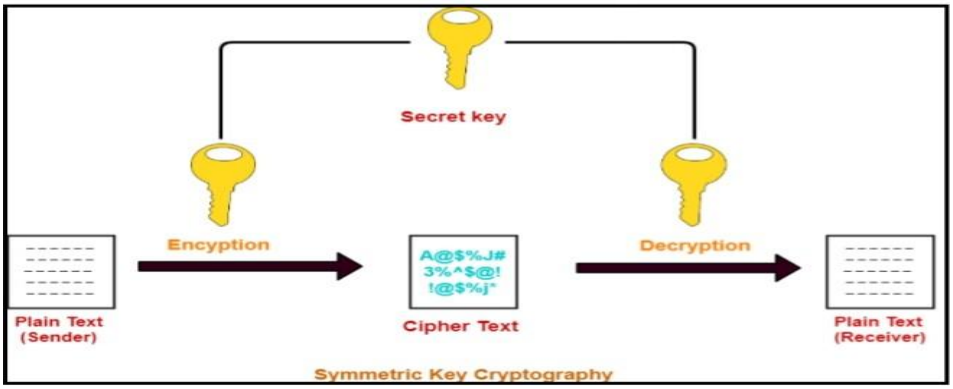

Figure 2.2: SYMMETRIC KEY CRYPTOGRAPHY

3) ASYMMETRIC KEY CRYPTOGRAPHY

Asymmetric Encryption, also referred to as public-key encryption, is a form of facts encryption where the encryption key(also known as public-key) and the corresponding decryption key(also referred to as private key) are distinctive. A message encrypted with the general public key may be decrypted best with the corresponding private key. The general public key and personal key are associated mathematically, but it's far computationally infeasible to derive the non-public key from the general public key.Consequently, a recipient should distribute the general public key extensively. Every person can use the public key to encrypt messages for the recipient and best the recipient can decrypt them. Asymmetric encryption is taken into consideration to be more at ease than symmetric encryption as it makes use of two keys for the method.
Commonplace asymmetric encryption techniques consist of RSA, DSA, and PKCS.

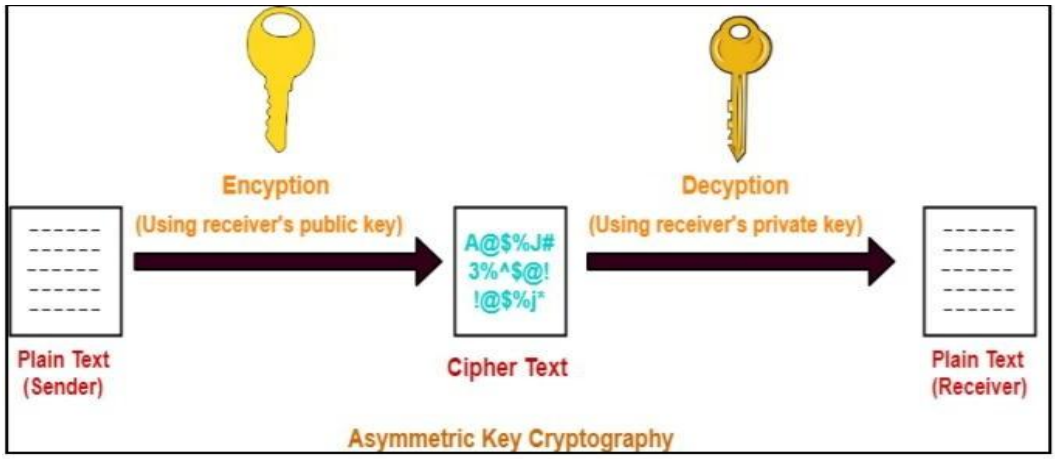

FIGURE 2.3 : ASYMMETRIC KEY CRYPTOGRAPHY

4) DATA ENCRYPTION STANDARD (DES)

Information Encryption well-known (DES) is a block-cipher algorithm that takes plain textual content in blocks of 64 bits and converts them to cipher text using keys of forty eight bits. It's far a symmetric key algorithm, which means that the equal keys used for encrypting and decrypting facts.

5) ADVANCED ENCRYPTION STANDARD (AES)

AES is a block cipher supposed to replace DES for worthwhile function. It uses a 128-bit block length and key size of 128, 192, or 256 bits. The huge style of constitutional rounds of the cipher is a function of the key length. The huge style of rounds for 128- bitsecret's 10[3].

6) PUBLIC-KEY CRYPTOGRAPHY

Public-key cryptography is a shape of cryptosystem wherein encryption and decryption are implement the unique keys—one a public key and one a private key. these keys are mathematically related despite the fact that potential of one key does no longer permit someone to clearly decide the other key. As shown in discern, the sender A makes use

of the public key of receiver B (or a few set of guidelines) to encrypt the plaintext message M and sends the cipher textual content C to the receiver. The receiver applies personal non-public key to decrypt the cipher textual content C and get better the plaintext message M. because pair of keys is wanted, this get entry to is likewise calledasymmetric cryptography.

CRYPTOGRAPHY – BENEFITS

Cryptography is a crucial data security mechanism. It provides the four most basic duty of information security –[5, 6]

- Confidentiality – Encryption method can protect the statistics and conversation from unauthorized revelation and get right of entry to of data
- Authentication – The cryptographic techniques

consisting of MAC and virtual signatures can shield statistics towards spoofing andforgeries.

- In uneven or public key, cryptography there may be no want for changing keys, thus getting rid of the key distribution trouble.
- Data Integrity –records integrity is the assurance that the virtual records is uncorrupted and might most effective be accessed or modified by the ones authorized to achieve this integrity includes retaining the consistency, accuracy and trustworthiness of information over its complete lifecycle.

- A symmetric cryptosystem is faster.
- Non-repudiation – non-repudiation refers to the capability to ensure that a celebration to a settlement or a conversation can’t deny the authenticity in their signature on a record or the sending of a message that they originated.

CRYPTOGRAPHY – DRAWBACKS

- A strongly encrypted, authentic, true, and digitally signed statistics may be tough to get right of entry to even for a legitimate users at an important time of selection- making. The employer or the laptop can be attacked and affected non-useful thru an intruder [7].

- High availability, one of the important factors of records security, can't be ensured via the usage of cryptography. Different methods are needed to guard against therisk along with denial of service or complete breakdown of facts device.

- It is predicated upon the name of the game key if you overlook the keys you can't get better statistics.

- Cryptography does now not shield against the vulnerabilities and threats that emerge from the negative layout of machine.
- Another fundamental need of data security of selective access control also cannot be realized through the use of cryptography. Administrative controls and techniques are required to be exercised for the same.

- It is always vulnerable to brute force attack.
- Symmetric cryptosystems have a hassle of key transportation. The name of the game key is to be transmitted to the receiving system before the real message is to be transmitted. Each technique of electronic communication is insecure as it is not possible to guarantee that nobody can be able to tap communiqué channels. So the handiest relaxed way of exchanging keys could be replacing them individually.

- Cryptography comes at price. The value is inphrases of money and time −o Addition of cryptographic techniques in the statistic processing ends in delay.

o The use of public key cryptography calls for setting up and up key of public key infrastructure requiring the good-looking financial budget.

- The safety of cryptographic method is primarily based on the computational difficulty of mathematical issues. Any step forward in solving such mathematical problems or developing the computing power can render a cryptographic technique inclined.

STEGANOGRAPHY

The safety of cryptographic approach is based at the computational trouble of mathematical troubles. Any breakthrough in fixing such steganography is the method of hiding secret statistics within an everyday, non-mystery file or message so that you can keep away from detection; the secret information is then extracted at its destination.

The usage of steganography can be combined with encryption as a further step fohiding

or protective statistics. The phrase steganography is derived from the Greek words stenos (which means hidden or protected) and the Greek root graph (which means to jot down). Steganography can be used to hide almost any kind of virtual content material, such as textual content, photo, video or audio content; the facts to be hidden may be hidden inner nearly some other type of virtual content material. The content material to be concealed thru steganography -- known as hidden textual content -- is frequently encrypted earlier than being incorporated into the harmless-seeming cover text record or information flow. If not encrypted, the hidden textual content is commonly processed in a few manner so that you can boom the problem of detecting the secret content.

TYPES OF STEGANOGRAPHY TECHNIQUES

Relying on the character of the quilt item (real object wherein secret records is embedded), steganography may be divided into five types.

a) Text approach: text Steganography is hiding facts within the text documents. It involves things like converting the layout of current textual content, converting words within a textual content, generating random character sequences or using context-loose grammars to generate readable texts. Numerous strategies used to hide the statistics within the textual content are:

- Format/ Layout Based Techniques
- Random and Statistical Generation
- Linguistic Method

b) Image/ picture Technique: Hiding the records by way of taking the duvet object because the picture is known as image steganography. In virtual steganography, images are broadly used cowl supply due to the fact there are a large range of bits gift in the virtual representation of an photograph. There are a number of methods to hide facts internal an photo. Commonplace methods consist of: [8]

- Masking and Filtering
- Redundant Pattern Encoding
- Encrypt and Scatter

c) Audio Technique: In audio steganography, the secret message is embedded into an audio sign which alters the binary sequence of the corresponding document. Hiding secret messages in digital/virtual sound is a far extra tough procedure when as compared to others, along with Picture Steganography. Unique techniques of audio steganography include:

- Least Significant Bit Encoding
- Parity Encoding
- Phase Coding
- Spread/unfold Spectrum

d) Video method: In Video Steganography you can hide kind of data into virtual video format. The benefit of this type is a massive amount of data may be hidden inside and the fact that it is a movingcirculation of photographs and sounds. You could consider this because the mixture of Image Steganography and Audio Steganography.

e) Network Technique: It is the technique of embedding information inside network manipulates protocols utilized in statistics transmission such TCP, UDP, ICMP etc. You can use steganography in some covert channels that you may locate inside the OSI model. For Example, you can hide information in the header of a TCP/IP packet in some
fields that are either optional.

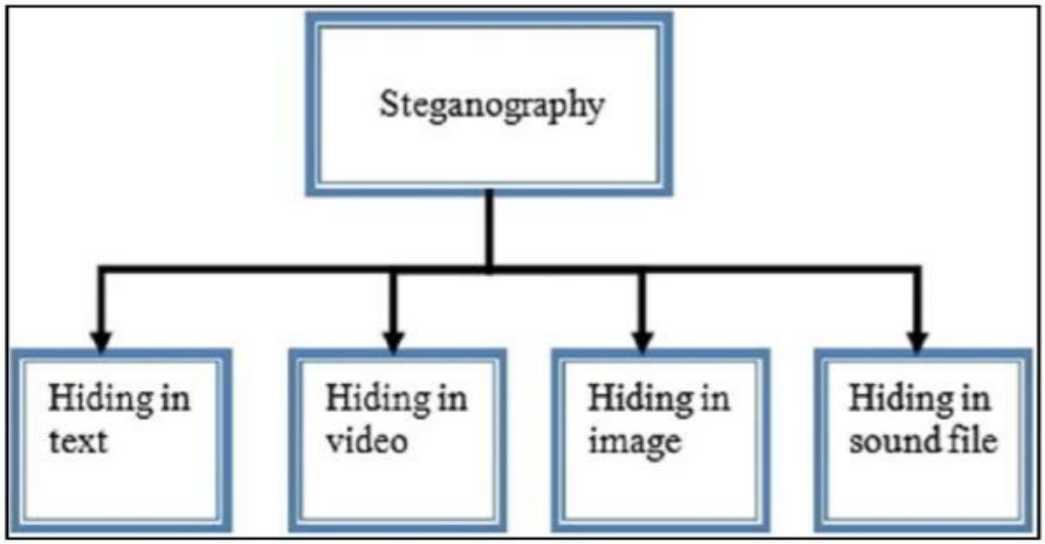

Figure 3.1 : TYPES OF STEGANO GRAPHY TECHNIQUES

CONCLUSION

In this paper we presented a classification of network security techniques and various cryptographic techniques are discussed to increase the security of network. We have also discussed about steganography and its types. Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Cryptography is used for Network security purpose. Both cryptography and steganography are well known and widely used techniques. If both the techniques: Cryptography and Steganography is combined used then the communication becomes double secured. Network security covers the use of cryptographic algorithm in network protocols and network applications. The security forthe data has become highly important.

REFERENCES

[1] Vaishnavi B. Savant, Rupali D. Kasar ― Research Journal of Engineering and Technology 12 (4), 110-114, 2021

[2] Sarita Kumari, ― A research Paper on Cryptography Encryption and Decryption‖ International Journal Of Engineering And Computer Science, 2017

[3] https://en.wikipedia.org/wiki/Cryptography

[4] Jangala. Sasi Kiran M. Anusha, A.Vijaykumar, M.Kavya ―Cryptography: The Science of Secure Communication‖ International Journal of Computer Science and Network Security (IJCSNS) 2016.

[5] Dr.Sandeep Tayal, Dr.Nipin Gupta, Dr.Pankaj Gupta, Deepak Goyal, Monika Goyal, ―A Review paper on Network Security and Cryptography‖ Advances in Computational Sciences and Technology ISSN, 2017.

[6] IEEE Standard P1363.1, ―IEEE standard specification for public key cryptographic techniques based on hard problems over lattices‖, 2009.

[7] ShyamNandan Kumar, ―Review on Network Security and Cryptography‖ in International Transaction of Electrical and Computer Engineers System, 2015, Vol. 3, No.1, 1-11