Network Security and Cryptography

Pooja Verma

Assistant Professor, Department of Computer Science and Engineering,
Roorkee College of Engineering, Roorkee, Uttarakhand, India

Abstract

Communication technology is now at its peak. Security of the information transmission between the source and the destination has become very important. Security of transmission of information is very important because it protects the information from the invader from the invader information from the invader from the invader. In this article we explain the network security Technologies such as authentication, honesty control, non-rejection and privacy. We have two popular security mechanisms namely ***Cryptography*** *and* ***Steganography****. These technologies are widely used in network security. In Cryptography data is sent in an encrypted form using the encryption key using the encryption key at the receiving end decryption algorithms are used to decrypt the information with the help of decryption keys. Steganography is a process of hiding data into a cover file.*

Keywords: - *decryption, Cryptography network security, encryption steganography.*

1. Introduction

In these days a huge amount of data transmitted via wireless network or internet. The data may contain sensitive personal information, thus the information is at risk of being attacked by the unauthorized person. Sometimes To access and use the services a user have to enter the personal data on an application or on a website therefore user need a secure communication system to protect his information from invaders. To protect information from unauthorized access and use, Data integrity and confidentiality is very important. Network security is classified into 4 parts confidentiality authentication projection and integrity checking. Confidentiality refers to the security of information against unauthorized users, which means that unauthorized users should not be able to read and understand the information. Authentication refers that the sender can verify the Identity of receiver and receiver can verify the information and validate the identity of the sender. in context of rejection, sender cannot deny to send a particular message. Integrity refers that the receiver can confirm that the message has not been modified during transmission, which is used to secure information from counterfeiting.

2. SECURITY REQUIREMENTS

A) Confidentiality: -
Information should be available only for the desired receivers, which saves the information from invaders. Here we can get security using the following two techniques - cryptography and steganography. Cryptography involves written or generated codes that allow information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user. Cryptography contains two main components, coding and decoding and decoding. Following two algorithms are used to encrypt a data public key cryptography and symmetric key cryptography. Steganography refers the hiding of information within another file so that the presence of the hidden message is indiscernible. Another file can be an image, audio, video or text file.

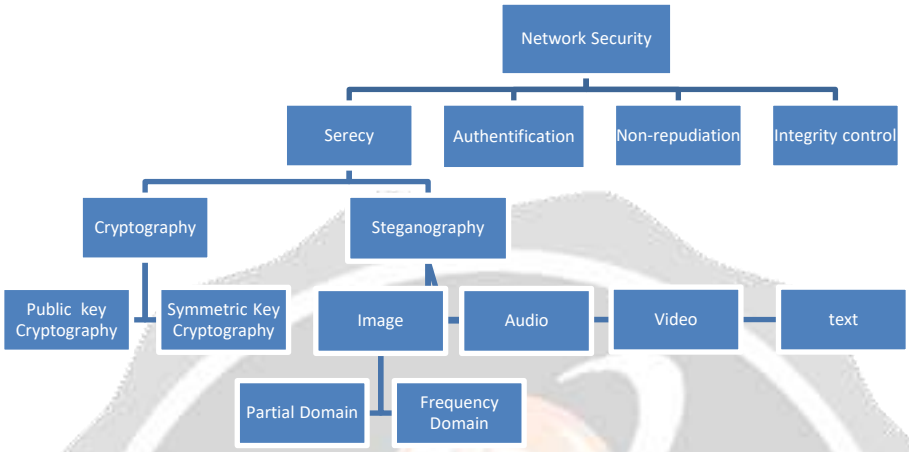
B) Authentication: -
Authentication refers the identification process of user based on the username and password. Through this process only authorized users can access information.

C) Non-repudiation: -

Non-repudiation is the assurance that someone cannot reject something. Non-repudiation is a legal concept that is widely used in information security. It refers to a service, which provides proof of the origin of data and the integrity of the data.

D) Data integrity: -

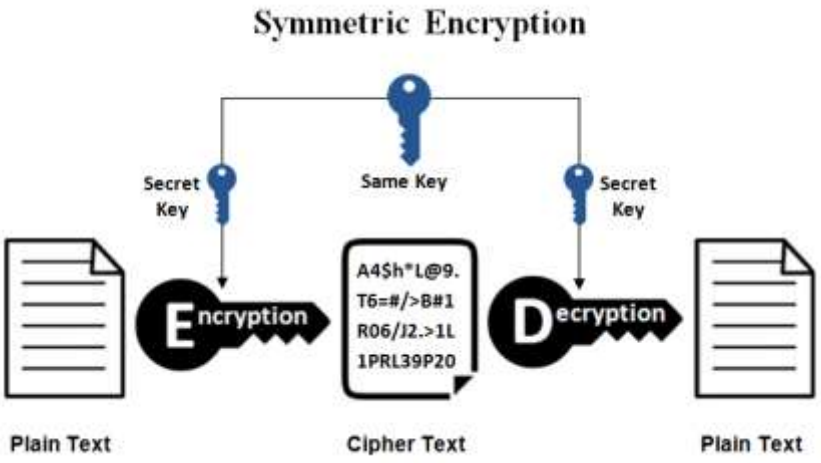
in the context of Networking, data integrity refers to the complete, accuracy and stability of data. Data integrity must be implemented when sending data. With the help of probe and correction protocols the errors can be overcome.



Classification of Network security algorithm

3. CRYPTOGRAPHY

Cryptography helps us to secure the information from being encrypted and readable. In cryptography information is transmitted over the Internet after the implementation of the encryption algorithm, which makes the intruder unable to attack on confidential information. There are two terms used in cryptography: encryption and decryption. Encryption refers to the conversion of information into encrypted text, where decryption refers the conversion of encrypted text into the original information.



1. **Plain text: -** This term stands for original basic form information, which may contain confidential data such as credit card number, passwords, bank account number, secret expression, digital signature and other important data.

2. **Cypher text**: -
   The cipher text stands for the encrypted form of basic information that is altered by mathematical algorithms. These coded texts are inconceivable, which is sent to the receiver.
3. **Key**: -
   The key is a mathematical value or formula used to encrypt or decrypt the information. The information can only

be decrypted by the key.

Cryptography algorithm

Cryptographic algorithms are the expression which is used to encrypt to encrypt plain text into cypher text. The process of converting plain text into cipher text with the help of cryptographic algorithms is called coding (encryption), and the process in which we decode the cipher text and convert it into plain text is called decryption. There are two categories of cryptographic algorithms categories of cryptographic algorithms.

1. Stream algorithm: - In this algorithm Only One byte is operated at once and converted into letters, numbers or special character. This is a slow and inefficient process.

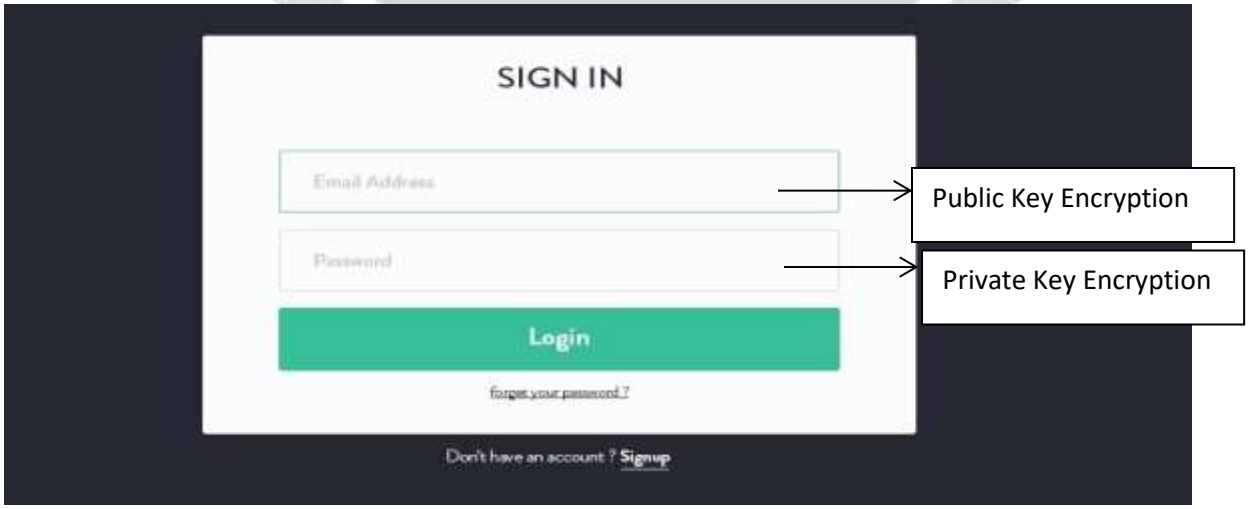
2. Block algorithm: - In this algorithm a set of bytes of bytes set of bytes algorithm a set of bytes of bytes set of bytes of bytes operated at once this that is called block. For modern algorithm the general size of a block is 64 bytes. This size is perfect for operate at once and enough difficult to break. But breaking the 64-bit algorithm with the brute force is possible with the current microprocessor speed.

Types of cryptography

- **Private Key cryptography**: -
  In this Cryptography the sender and the receiver use the same key to encrypt and decrypt the data. It is also known as secret key cryptography. This algorithm is used for symmetric key encryption. Symmetric algorithms are divided into two parts stream encryption and block encryption. Stream encryption is used to create the encryption key and encrypt the data in the form of streams, and the block encryption algorithm operates the data blocks, where data in the form of blocks are used independently. Some algorithms are following:
  - Triple Data Encryption standard
  - International Data Encryption Algorithm
  - blowfish Encryption Algorithm
  - Data Encryption standard(DES)
  - advanced encryption standard(AES)
  - Twofish Encryption Algorithm

B. Public key cryptography: -
In this algorithm both sender and receiver generate two keys, one key is used to encrypt the data and send it to the user, this key is called public key, and another key is used to decrypt the message which is a private key. Some algorithms are following

- Diffie Hellman
- Rivest- Shamir- Adelman(RSA)
- Digital signature algorithm(DSA)



In Hash Function mathematical changes occur in Irreversible encryption information. A hash function is used in cryptography to maintain the integrity of message. The digital framework is delivered through the hash value message and the hash value massage is also ensures that the message is not altered by intruders. This is an efficient

algorithm because the probability of the same hash value produced by two different plain text messages is very low.

PROS and CONS of cryptography

Pros: -
1. Cryptography hides information and keeps it safe.
2. No one can understand the message until the key of the code is not present.
3. It allows you to write whatever you want; even the secret code of the information will be encrypted.

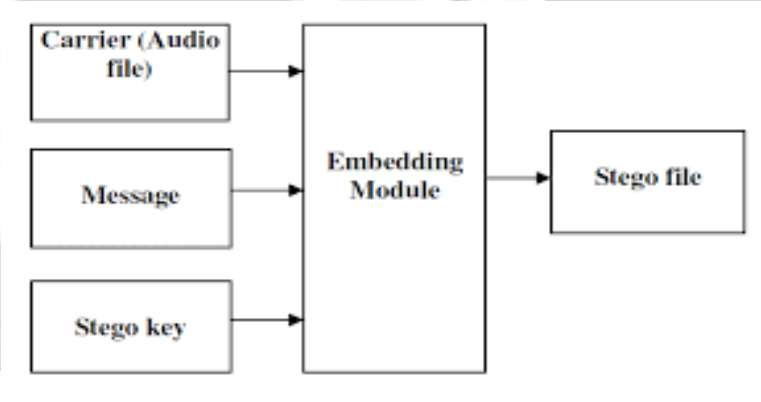
Cons: **-**
1.It requires a long time to operate the code.
2. Understanding code takes a lot of time.
3. It is always vulnerable to brute force attack.

Steganography

In Steganography, sensitive data is hidden behind the common data, which makes it difficult to find the existence of hidden message. Steganography is used to hide information so that no one can know about it. If they get suspicious data then the goal is lost. Different types of data can be used to hide the information such as video, audio, text and images etc.

1. The carrier image: - It stands for the data in which the information will be hidden. It is also called the cover object.

2. **The message**: - Sensitive data and information that is to be hidden.
3. **The key: -** It is a method or the instructions that is used to decode and understand the data.



PROS and CONS of steganography

Pros: -
a) It is difficult to identify the data, only the receiver can detect the data.
b) The speed of steganography can be boost up with the help of software.
c) It secures data sharing over the LAN, MAN and WAN.

Cons:-
a)This technique can be very dangerous for us, if fallen into wrong hands like terrorists and criminals.
b)Anybody can doubt on a large number of data and huge size files.

CONCLUSION

This article summarizes the network security technology. The demand for security and privacy is increasing day by day, which requires techniques that secure the information and data, and many techniques are being developed. In this article we have discussed about cryptography and steganography techniques, both technologies are well known and widely used technologies. These Technologies provide us a secure and very convenient communication environment. The combination of cryptography and steganography makes our communication more secure and safe.

REFERENCES

[1] STALLINGS Cryptography and Network Security Principle by Menezes, Paul C. Van Oorschot, And Scott A. Vanstone CRC Press. Hardware Security(HARDSEC) : Design , Threats and Safegaurds by Debdeep Mukhopadhyay and Rajat Subhra Chakraborty, CRC Press, Taylor and Francis Group.
[2] HilalAlmara'beh "Steganography Techniques - Data Security Using audio and Video", International journal of Advance Research Of computer Science and Software Engineering Volume 6, Issue 2, Feb 2016.
[3] Marwa E. Saleh, Abdelmgeid A. Aly, Egypt Fatma A. Omara, "Data Security Using Cryptography and Steganography Techniques" in (IJACSA), International journal Of Advance Computer Science and Applications, Vol. 7, No. 6, 2016.
[4] Vishnu S babuand Prof. Helen KJ, "A Study of Cryptography and Steganography" in IJRSCSE, International journal Of Research Studies in Computer Science and Engineering, Vol.2, Issue 5, May 2015, PP 45-49.
[5] Aarti Mehndritta, "Data Hiding System Using Cryptography and Steganography: A Comprehensive Modern Investigation" in International journal Of Engineering and Technology (IRJET), Volume:02 Issue: 01 Apr-2015.
[6] ShyamNadan Kumar, "Review on Network Security And Cryptgraphy" In international Transection Of Electrical and Computer Engineering System, 2015, vol. 3 , no. 1, 1-2011.
[7] Md. Khadil Imam Rahmani and KamiyaAroramNaina Pal, "A Crypto-Steganography: A Survey in" in (IJACSA) International journal Of Advance Computer Science and Applications, Vol. 5, No. 7, 2014.
[8] Rakhil, Suresh Gwande2 "A REVIEW ON STEGANOGRAPHY METHODS", International Journal of Advance Research in Electrical and instrumentation Engineering Vol.2 Issue 10, October 2013.