CHAPTER EIGHT

8. Data Security And Integrity

8.1. Fundamentals of secure networks;

Network Security deals with all aspects related to the protection of the sensitive information assets existing on the network. It covers various mechanisms developed to provide fundamental security services for data communication. This tutorial introduces you to several types of network vulnerabilities and attacks followed by the description of security measures employed against them. It describes the functioning of most common security protocols employed at different networking layers right from application to data link layer. After going through this tutorial, you will find yourself at an intermediate level of knowledge regarding network security.

Network security is not only concerned about the security of the computers at each end of the communication chain; however, it aims to ensure that the entire network is secure. Network security entails protecting the usability, reliability, integrity, and safety of network and data.

Effective network security defeats a variety of threats from entering or spreading on a network.

The primary goals of network security are Confidentiality, Integrity, and Availability.

Activity 8.1

Why we need to secure our network communication?

Discuss some techniques which help to the network?

Do you know about cyber security? Discuss with your classmates?

8.2. Goals of Network Security

As discussed in earlier sections, there exists large number of vulnerabilities in the network.

Thus, during transmission, data is highly vulnerable to attacks. An attacker can target the communication channel, obtain the data, and read the same or re-insert a false message to achieve his nefarious aims.

Network security is not only concerned about the security of the computers at each end of the communication chain; however, it aims to ensure that the entire network is secure. Network security entails protecting the usability, reliability, integrity, and safety of network and data. Effective network security defeats a variety of threats from entering or spreading on a network.

The primary goals of network security are Confidentiality, Integrity, and Availability. These three pillars of Network Security are often represented as CIA triangle.

Confidentiality – The function of confidentiality is to protect precious business data from unauthorized persons. Confidentiality part of network security makes sure that the data is available only to the intended and authorized persons.

Integrity – This goal means maintaining and assuring the accuracy and consistency of data. The function of integrity is to make sure that the data is reliable and is not changed by unauthorized persons.

Availability – The function of availability in Network Security is to make sure that the data, network resources/services are continuously available to the legitimate users, whenever they require it.

Achieving Network Security

Ensuring network security may appear to be very simple. The goals to be achieved seem to be straightforward. But in reality, the mechanisms used to achieve these goals are highly complex, and understanding them involves sound reasoning.

International Telecommunication Union (ITU), in its recommendation on security architecture X.800, has defined certain mechanisms to bring the standardization in methods to achieve network security. Some of these mechanisms are –

En-cipherment – This mechanism provides data confidentiality services by transforming data into not-readable forms for the unauthorized persons. This mechanism uses encryption-decryption algorithm with secret keys.

Digital signatures – This mechanism is the electronic equivalent of ordinary signatures in electronic data. It provides authenticity of the data.

Access control – This mechanism is used to provide access control services. These mechanisms may use the identification and authentication of an entity to determine and enforce the access rights of the entity.

Having developed and identified various security mechanisms for achieving network security, it is essential to decide where to apply them; both physically (at what location) and logically (at what layer of an architecture such as TCP/IP).

Security Mechanisms at Networking Layers

Several security mechanisms have been developed in such a way that they can be developed at a specific layer of the OSI network layer model.

• Security at Application Layer – Security measures used at this layer are application specific. Different types of application would need separate security measures. In ordern to ensure application layer security, the applications need to be modified.

It is considered that designing a cryptographically sound application protocol is very difficult and implementing it properly is even more challenging. Hence, application layer security mechanisms for protecting network communications are preferred to be only standards-based solutions that have been in use for some time.

An example of application layer security protocol is Secure Multipurpose Internet Mail Extensions (S/MIME), which is commonly used to encrypt e-mail messages. DNSSEC is another protocol at this layer used for secure exchange of DNS query messages.

• Security at Transport Layer – Security measures at this layer can be used to protect the data in a single communication session between two hosts. The most common use for transport layer security protocols is protecting the HTTP and FTP session traffic.

The Transport Layer Security (TLS) and Secure Socket Layer (SSL) are the most common protocols used for this purpose.

• Network Layer – Security measures at this layer can be applied to all applications; thus,

they are not application-specific. All network communications between two hosts or networks can be protected at this layer without modifying any application. In some environments, network layer security protocol such as Internet Protocol Security (IPsec) provides a much better solution than transport or application layer controls because of the difficulties in adding controls to individual applications. However, security protocols at this layer provide less communication flexibility that may be required by some applications.

Incidentally, a security mechanism designed to operate at a higher layer cannot provide protection for data at lower layers, because the lower layers perform functions of which the higher layers are not aware. Hence, it may be necessary to deploy multiple security mechanisms for enhancing the network security.

In the following chapters of the tutorial, we will discuss the security mechanisms employed at different layers of OSI networking architecture for achieving network security.

8.3. Cryptography

Human being from ages had two inherent needs – (a) to communicate and share information and (b) to communicate selectively. These two needs gave rise to the art of coding the messages in

such a way that only the intended people could have access to the information. Unauthorized people could not extract any information, even if the scrambled messages fell in their hand.
The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography.
The word ‘cryptography’ was coined by combining two Greek words, ‘Krypto’ meaning hidden and ‘graphene’ meaning writing.

History of Cryptography

The art of cryptography is considered to be born along with the art of writing. As civilizations evolved, human beings got organized in tribes, groups, and kingdoms. This led to the emergence of ideas such as power, battles, supremacy, and politics. These ideas further fueled the natural need of people to communicate secretly with selective recipient which in turn ensured the continuous evolution of cryptography as well.
The roots of cryptography are found in Roman and Egyptian civilizations.

Context of Cryptography

Cryptology, the study of cryptosystems, can be subdivided into two branches –

• Cryptography
• Cryptanalysis

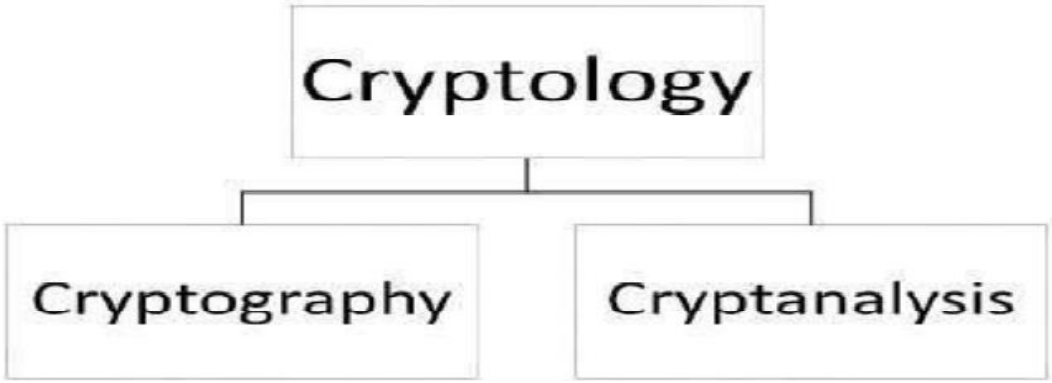

Figure 8.1 Cryptography branches

What is Cryptography?

Cryptography is the art and science of making a cryptosystem that is capable of providing information security.
Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. You can think of cryptography as the establishment of a large toolkit containing different techniques in security applications.

What is Cryptanalysis?

The art and science of breaking the cipher text is known as cryptanalysis.
Cryptanalysis is the sister branch of cryptography and they both co-exist. The cryptographic process results in the cipher text for transmission or storage. It involves the study of cryptographic mechanism with the intention to break them. Cryptanalysis is also used during the design of the new cryptographic techniques to test their security strengths.

Security Services of Cryptography

The primary objective of using cryptography is to provide the following four fundamental information security services. Let us now see the possible goals intended to be fulfilled by cryptography.

Confidentiality

Confidentiality is the fundamental security service provided by cryptography. It is a security service that keeps the information from an unauthorized person. It is sometimes referred to as privacy or secrecy.
Confidentiality can be achieved through numerous means starting from physical securing to the use of mathematical algorithms for data encryption.

Data Integrity

It is security service that deals with identifying any alteration to the data. The data may get modified by an unauthorized entity intentionally or accidently. Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user. Data integrity cannot prevent the alteration of data, but provides a means for detecting whether data has been manipulated in an unauthorized manner.

Authentication

Authentication provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified and verified sender.
Authentication service has two variants –

• Message authentication identifies the originator of the message without any regard router or system that has sent the message.
• Entity authentication is assurance that data has been received from a specific entity, say a particular website.

Apart from the originator, authentication may also provide assurance about other parameters related to data such as the date and time of creation/transmission.

Non-repudiation

It is a security service that ensures that an entity cannot refuse the ownership of a previous commitment or an action. It is an assurance that the original creator of the data cannot deny the creation or transmission of the said data to a recipient or third party.
Non-repudiation is a property that is most desirable in situations where there are chances of a dispute over the exchange of data. For example, once an order is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation service was enabled in this transaction.

Cryptography Primitives

Cryptography primitives are nothing but the tools and techniques in Cryptography that can be selectively used to provide a set of desired security services –

• Encryption
• Hash functions
• Message Authentication codes (MAC)
• Digital Signatures

The following table shows the primitives that can achieve a particular security service on their own.

Table 8.1: Security Services of Cryptography

Primitives ⇨ Service ⇩	Encryption	Hash Function	MAC	Digital Signature
Confidentiality	Yes	No	No	No
Integrity	No	Sometimes	Yes	Yes
Authentication	No	No	Yes	Yes
Non Reputation	No	No	Sometimes	Yes

A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a **cipher system.**

Let us discuss a simple model of a cryptosystem that provides confidentiality to the information being transmitted. This basic model is depicted in the illustration below –

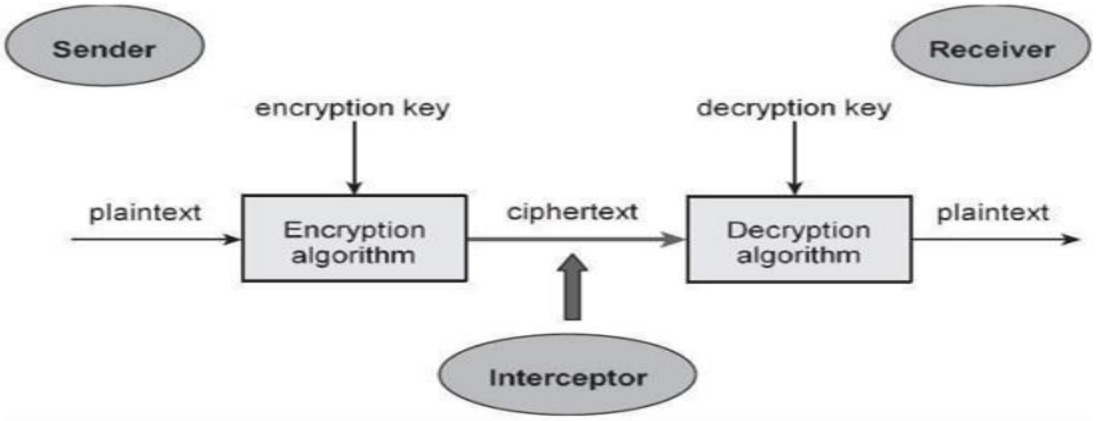

Figure 8.2 Simple model of Cryptography

The illustration shows a sender who wants to transfer some sensitive data to a receiver in such a way that any party intercepting or eavesdropping on the communication channel cannot extract the data.
The objective of this simple cryptosystem is that at the end of the process, only the sender and the receiver will know the plaintext.

Components of a Cryptosystem

The various components of a basic cryptosystem are as follows –

• **Plaintext.** It is the data to be protected during transmission.
• **Encryption Algorithm.** It is a mathematical process that produces a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.
• **Ciphertext.** It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The ciphertext is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.
• **Decryption Algorithm,** It is a mathematical process, that produces a unique plaintext for any given ciphertext and decryption key. It is a cryptographic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.
• **Encryption Key.** It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.
• **Decryption Key.** It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext.

For a given cryptosystem, a collection of all possible decryption keys is called a **key space.**
An **interceptor** (an attacker) is an unauthorized entity who attempts to determine the plaintext. He can see the ciphertext and may know the decryption algorithm. He, however, must never know the decryption key.

8.4. Types of Cryptosystems

Fundamentally, there are two types of cryptosystems based on the manner in which encryptiondecryption is carried out in the system –
• Symmetric Key Encryption
• Asymmetric Key Encryption

The main difference between these cryptosystems is the relationship between the encryption and the decryption key. Logically, in any cryptosystem, both the keys are closely associated. It is practically impossible to decrypt the ciphertext with the key that is unrelated to the encryption key.

Symmetric Key Encryption

The encryption process where same keys are used for encrypting and decrypting the information is known as Symmetric Key Encryption.

The study of symmetric cryptosystems is referred to as symmetric cryptography. Symmetric cryptosystems are also sometimes referred to as secret key cryptosystems.
A few well-known examples of symmetric key encryption methods are – Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.

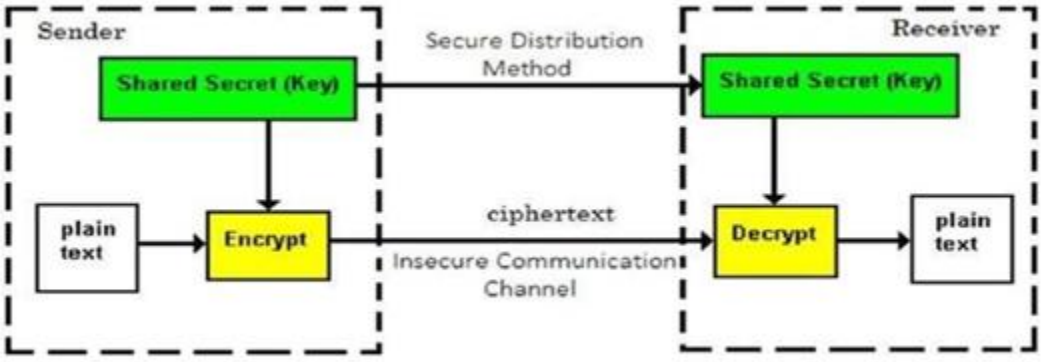

Figure 8.3 Symmetric key encryption

Prior to 1970, all cryptosystems employed symmetric key encryption. Even today, its relevance is very high and it is being used extensively in many cryptosystems. It is very unlikely that this encryption will fade away, as it has certain advantages over asymmetric key encryption.
The salient features of cryptosystem based on symmetric key encryption are –

• Persons using symmetric key encryption must share a common key prior to exchange of information.
• Keys are recommended to be changed regularly to prevent any attack on the system.
• A robust mechanism needs to exist to exchange the key between the communicating parties. As keys are required to be changed regularly, this mechanism becomes expensive and cumbersome.
• In a group of n people, to enable two-party communication between any two persons, the number of keys required for group is $n \times (n – 1)/2$.
• Length of Key (number of bits) in this encryption is smaller and hence, process of encryption-decryption is faster than asymmetric key encryption.
• Processing power of computer system required to run symmetric algorithm is less.

Challenge of Symmetric Key Cryptosystem

There are two restrictive challenges of employing symmetric key cryptography.
• Key establishment – before any communication, both the sender and the receiver need to agree on a secret symmetric key. It requires a secure key establishment mechanism in place.
• Trust Issue – since the sender and the receiver use the same symmetric key, there is an implicit requirement that the sender and the receiver 'trust' each other. For example, it may happen that the receiver has lost the key to an attacker and the sender is not informed.

These two challenges are highly restraining for modern day communication. Today, people need to exchange information with non-familiar and non-trusted parties. For example, a communication between online seller and customer. These limitations of symmetric key encryption gave rise to asymmetric key encryption schemes.

Asymmetric Key Encryption

The encryption process where **different keys are used for encrypting and decrypting the information** is known as Asymmetric Key Encryption. Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting ciphertext is feasible. The process is depicted in the following illustration –

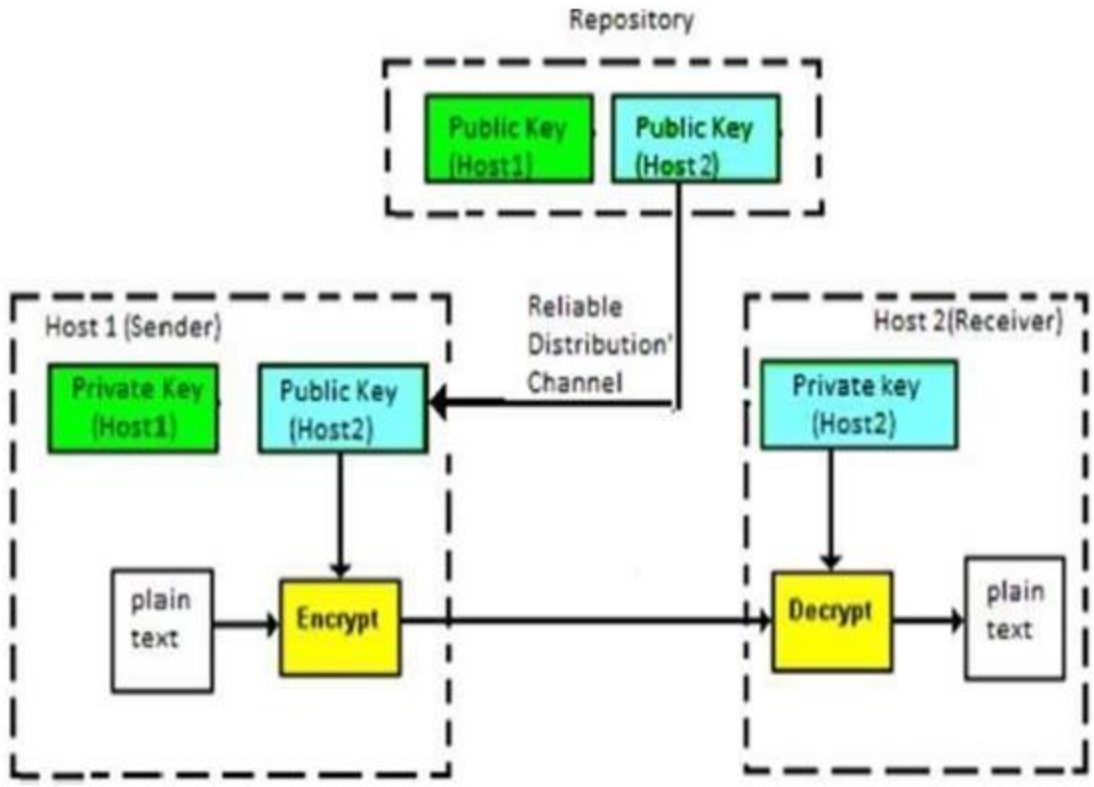

Figure 8.4 Asymmetric key encryption

Asymmetric Key Encryption was invented in the 20th century to come over the necessity of preshared secret key between communicating persons. The salient features of this encryption scheme are as follows –

• Every user in this system needs to have a pair of dissimilar keys, **private key and public key**. These keys are mathematically related – when one key is used for encryption, the other can decrypt the ciphertext back to the original plaintext.
• It requires to put the public key in public repository and the private key as a wellguarded secret. Hence, this scheme of encryption is also called **Public Key Encryption**.
• Though public and private keys of the user are related, it is computationally not feasible to find one from another. This is a strength of this scheme.

• When Host1 needs to send data to Host2, he obtains the public key of Host2 from repository, encrypts the data, and transmits.
• Host2 uses his private key to extract the plaintext.
• Length of Keys (number of bits) in this encryption is large and hence, the process of encryption-decryption is slower than symmetric key encryption.
• Processing power of computer system required to run asymmetric algorithm is higher.

Symmetric cryptosystems are a natural concept. In contrast, public-key cryptosystems are quite difficult to comprehend.

Challenge of Public Key Cryptosystem

Public-key cryptosystems have one significant challenge – the user needs to trust that the public key that he is using in communications with a person really is the public key of that person and has not been spoofed by a malicious third party. This is usually accomplished through a Public Key Infrastructure (PKI) consisting a trusted third party. The third party securely manages and attests to the authenticity of public keys.
When the third party is requested to provide the public key for any communicating person X, they are trusted to provide the correct public key.

The third party satisfies itself about user identity by the process of attestation, notarization, or some other process – that X is the one and only, or globally unique, X. The most common method of making the verified public keys available is to embed them in a certificate which is digitally signed by the trusted third party.

Relation between Encryption Schemes

Table 8.2 Summary of basic key cryptosystem

	Symmetric Cryptosystems	Public Key Cryptosystems
Relation between Keys	Same	Different, but mathematically related
Encryption Key	Symmetric	Public
Decryption Key	Symmetric	Private

Due to the advantages and disadvantage of both the systems, symmetric key and public-key cryptosystems are often used together in the practical information security systems.

Private Key

In Private key, the same key (secret key) is used for encryption and decryption. In this key is symmetric because the only key is copy or share by another party to decrypt the cipher text. It is faster than the public key cryptography.

Public Key

In Public key, two keys are used one key is used for encryption and another key is used for decryption. One key (public key) is used for encrypt the plain text to convert it into cipher text and another key (private key) is used by receiver to decrypt the cipher text to read the message. Now, we see the difference between them:

Table 8.3 Difference between public and private key

S.NO	Private Key	Public Key
1.	Private key is faster than public key.	It is slower than private key.
2.	In this, the same key (secret key) and algorithm is used to encrypt	In public key cryptography, two keys are used, one key is used for encryption