Cryptography Introduction

Sachin Tripathi

IIT(ISM), Dhanbad

Course Coverage

Unit No.	Topics to be Covered	Lecture Hours	Learning Outcome
1.	Cryptography: Introduction, Security requirements, Attacks, Security techniques, modes of operation	6	Learning the basics of cryptography and security
2.	Mathematical backgrounds: Modular Arithmetic, Group, Ring, Field, elliptic curve	5	Understanding the basics of mathematics used in cryptography
3.	Classical encryption techniques, Block ciphers, Public-key ciphers, Elliptic curve cryptography	6	Learning about the classical as well as public ciphers techniques, elliptic curve cryptography
4.	Message authentication, Cryptographic hash algorithms, Digital Signatures	6	learning about message authentication hash algorithms and digital signatures
5.	Network Security: Network layer security (IPSec)- Authentication header (AH), Encapsulated security payload (ESP), Security association (SA), Internet security protocol (IKE).	7	Understanding the network layer security and the protocols
6.	Transport layer security: Secure socket layer (SSL)- SSL architecture, Four protocols, SSL message formats, TLS	6	Understanding the transport layer security and the protocols
7.	E-mail security: Introduction to E-mail architecture, PGP (Pretty Good Privacy), S/MIME	6	Understanding the application layer security and the protocols

Course Outcome

1.Describe the fundamentals of networks security, security architecture, threats and vulnerabilities.

2.Apply the different cryptographic operations of symmetric cryptographic algorithms.

3.Explain the different cryptographic operations of public key cryptography.

4.Apply the various Authentication schemes to simulate different applications.

5.Discuss the various Security practices and System security standards.

Cryptography

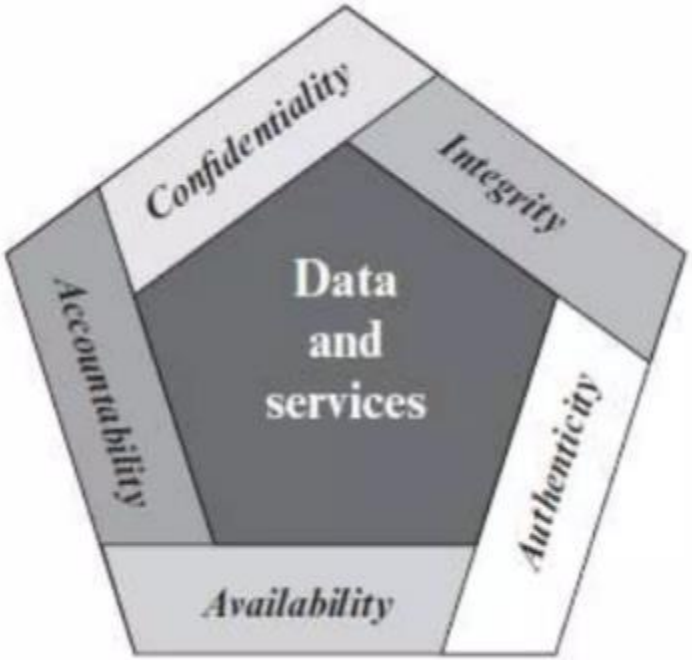
- Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents.
- The term is derived from the **Greek word kryptos,** which means hidden.
- Cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading **private messages**

Cryptographic Algorithms & Protocols

Cryptographic algorithms and protocols can b
grouped into **four main areas**:

- **Symmetric encryption:** Used to conceal the contents of blocks or streams of data of any size, including messages, files, encryption keys, and passwords.
- **Asymmetric encryption:** Used to conceal small blocks of data, such as encryption keys and hash function values, which are used in digital signatures.
- **Data integrity algorithms:** Used to protect blocks of data, such as messages, from alteration.
- **Authentication protocols:** These are schemes based on the use of cryptographic algorithms designed to authenticate the identity of entities.

Essentials Network and Computer Security Requirement



- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for **protecting personal privacy and proprietary information.**
- **Integrity:** Guarding against **improper information modification or destruction**, including ensuring information nonrepudiation and authenticity.
- **Availability:** Ensuring **timely and reliable access** to and use of information.
- **Authenticity:** The property of being **genuine and being able to be verified and trusted confidence** in the validity of a transmission, a message, or message originator.
- **Accountability:** The security goal that **generates the requirement for actions of an entity** to be traced uniquely to that entity.

Need of Security at Multiple Level

- The field of ***Network and Internet security*** consists of measures to deter, prevent, detect, and correct security violations that involve the transmission of information

OSI Security Architecture

- It is a systematic way of defining the requirements for the security
- It characterize the approaches to satisfy the various security products and polices
- **X.800 security architecture** of OSI defines such a systematic approach
- OSI security architecture is useful for **organizing the task of providing security**

- Since this architecture was developed as an **international standard**, Computer and Communications vendors have **developed security features for their products and services** that relate to **this structured definition of services and mechanisms**

- The OSI security architecture focuses on
  - Security Attacks
  - Security Mechanism
  - Security Services

Security Attacks

❖ **Security Attacks:**

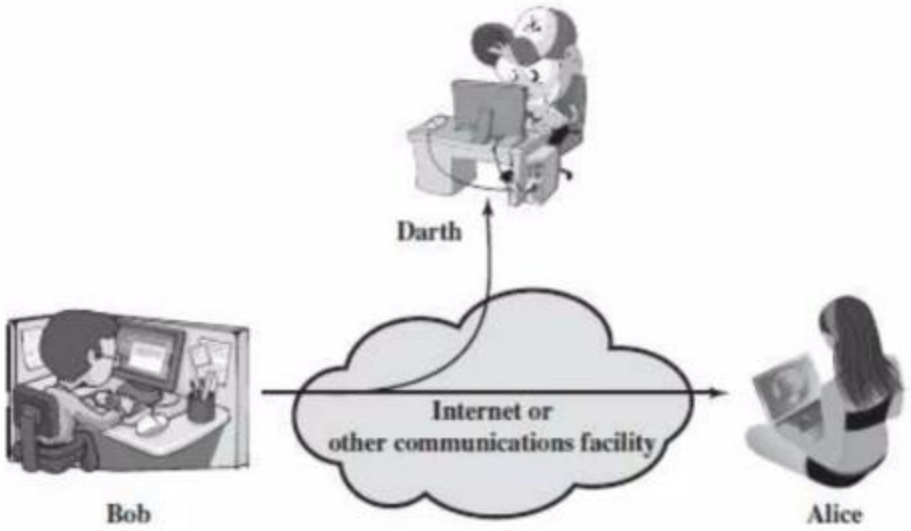
- Any action that **compromises the security** of information owned by an organization

❖ Classifications:

- *Passive attacks*
- *Active attacks*

Passive Attack

- Passive attacks are in the nature of **eavesdropping on**, or **monitoring of**, transmissions.



Passive Attacks

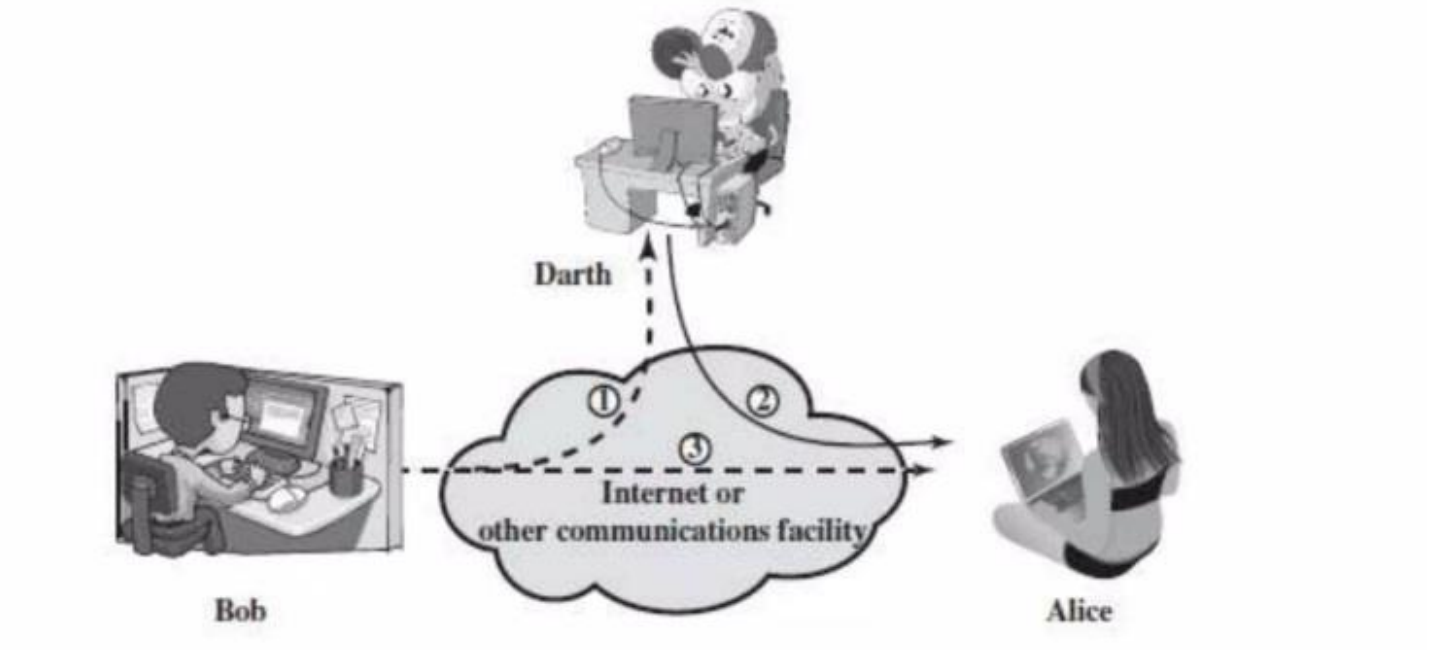
- The goal of the opponent is **to obtain information** that is being transmitted.
- Two types of passive attacks are
  - Release of message contents
  - Traffic analysis.

Passive Attacks

- **Release of message contents**
  - capture and read the content.
  - A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.
- **Traffic analysis**
  - Can't read the information, But observe the pattern
  - Determine the location and identity of communicating parties
  - Observe frequency and length of communication

Active Attacks

- Active attacks involve some modification of the data stream or the creation of a false stream



Active Attacks

- It can be subdivided into four categories:
  - Masquerade
  - Replay
  - Modification of messages
  - Denial of service

➢ Masquerade

- A **masquerade** takes place when one entity pretends to be a different entity
- Masquerade is a type of attack where the attacker **pretends to be an authorized user** of a system in order to gain access to it or to gain greater privileges than they are authorized for.

➢ Replay

- A replay attack also known as playback attack.
- Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

Active Attacks

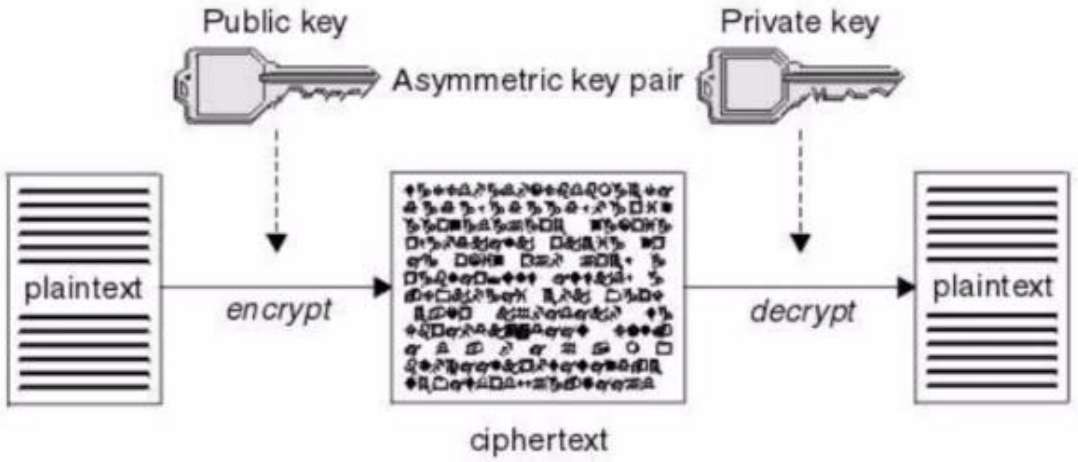
- **Modification of messages**
  - It simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect
- **Denial of service**
  - A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service

Security Mechanism

- **Security mechanism:**
  - A process that is designed to detect, prevent, or recover from a security attack
- The following are some security mechanisms defined in X.800
  - *Encipherment*
  - *Access Control*
  - *Digital Signature*
  - *Data Integrity*
  - *Authentication Exchange*
  - *Traffic Padding*
  - *Routing Control*
  - *Notarization*

Encipherment

- The use of mathematical algorithms to transform data into a form that is not readily intelligible.
- The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

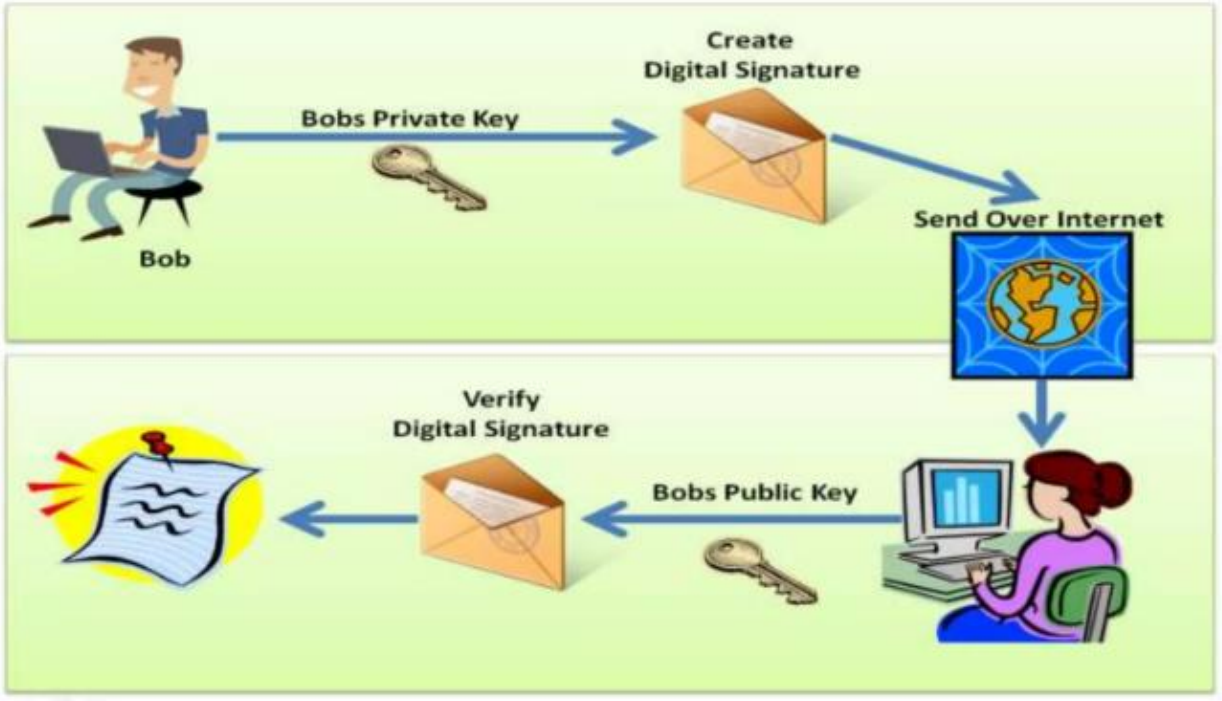


Access Control

– A variety of mechanisms that enforce access rights to resources.

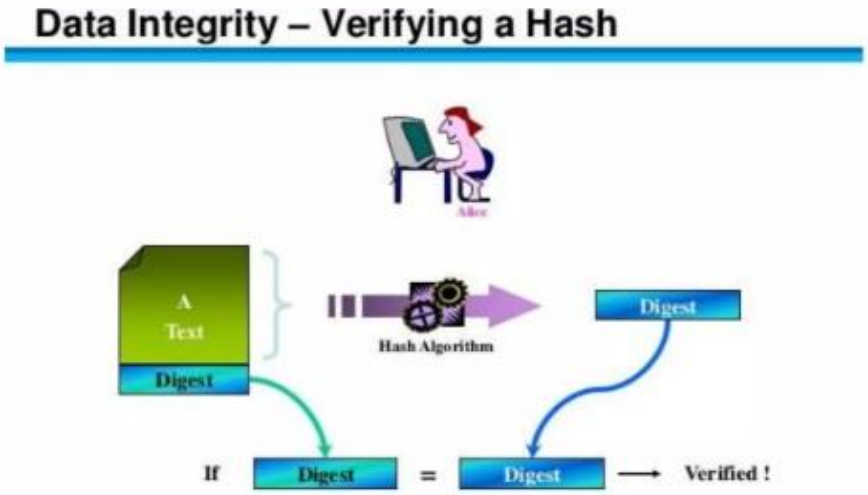
Digital Signature

- Here the sender can electronically sign the data and the receiver can electronically verify the signature.



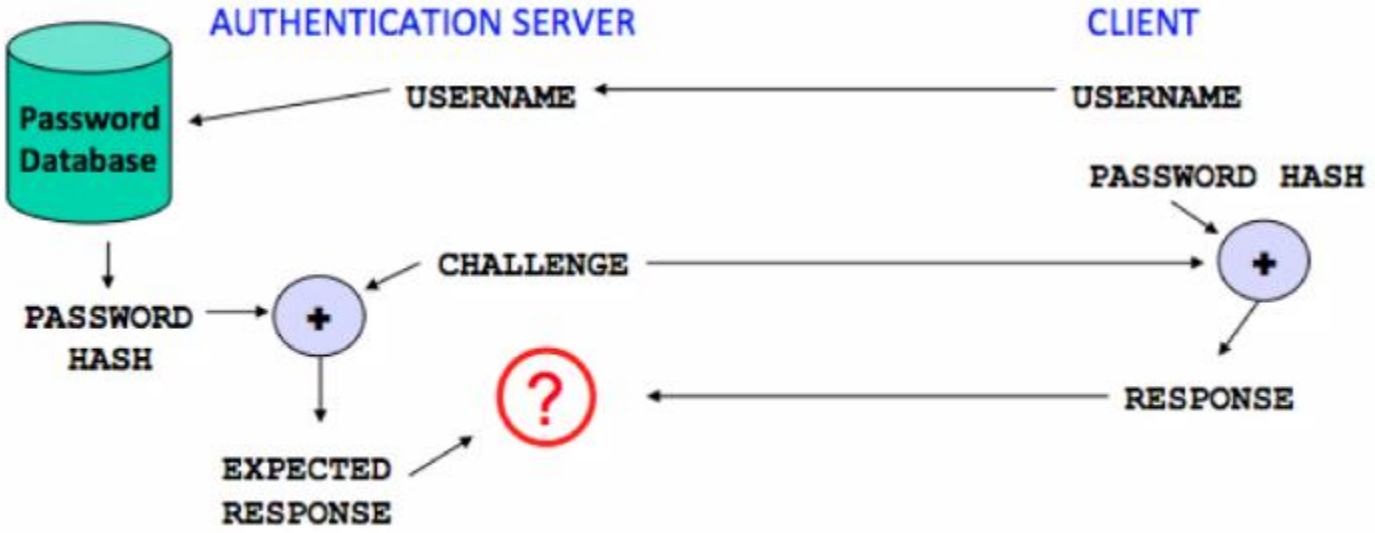
Data Integrity

- The assurance that the data has not been altered in an unauthorised manner since the time that the data was last created, transmitted, or stored by an authorised user.
- A variety of mechanisms used to assure the integrity of a data unit or stream of data units.



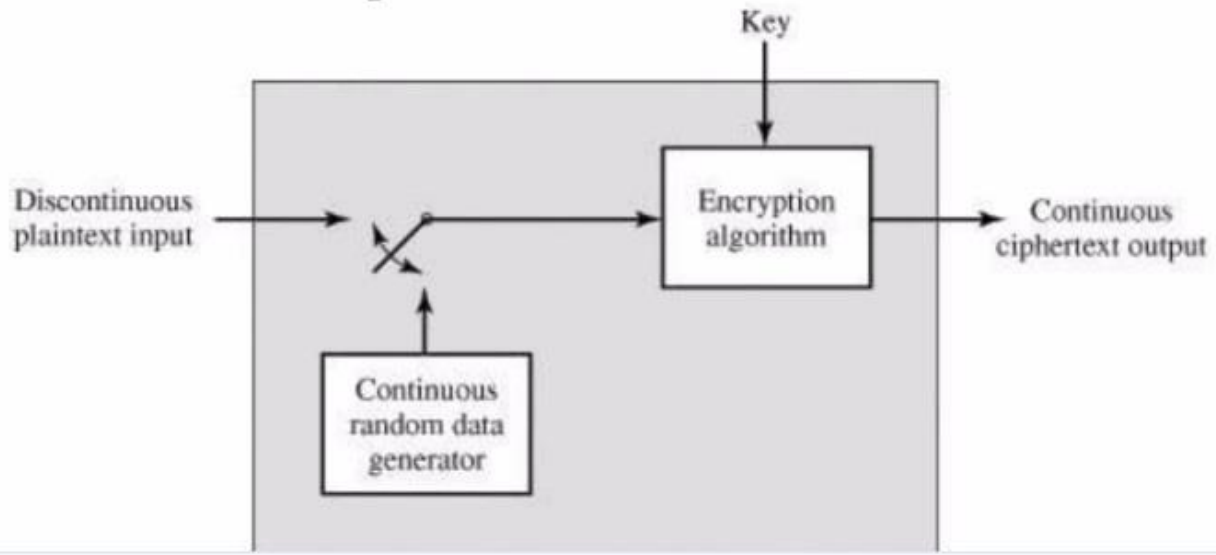
Authentication Exchange

– A mechanism intended to ensure the identity of an entity by means of information exchange.



Traffic Padding

- The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts
- Traffic padding may be used to hide the traffic pattern, which means to insert **dummy traffic into the network** and present to the intruder a different traffic pattern.



Routing and Notarization

- **Routing Control**
  - Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.
- **Notarization**
  - The use of a trusted third party to assure certain properties of a data exchange.

Notarization Example

– The use of a trusted third party to assure certain properties of a data exchange.

Security Services

- It is a processing or communication service that is provided by a system to give a **specific kind of protection to system resources.**
- Security services implement ***security policies*** and are implemented by ***security mechanisms***.
- X.800 divides these services into **five categories and fourteen specific services**

Services Categories

- The five categories are
  - **Authentication**
  - **Access Control**
  - **Data Confidentiality**
  - **Data Integrity**
  - **Nonrepudiation**

Authentication

- The authentication service is concerned with **assuring that a communication is authentic**
- Two specific authentication services are defined in X.800:
  - Peer entity authentication
  - Data origin authentication

- **Peer entity authentication**
  - Used in association with a logical connection to provide **confidence** in the ***identity of the entities connected.***
- ***Data origin authentication***
  - In a connectionless transfer, provides **assurance** that the ***source of received data is as claimed***

- The prevention of ***unauthorized use of a resource.***

(i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do)

Data Confidentiality

- Confidentiality is the protection of transmitted data from passive attacks
  - ❖Connection Confidentiality
  - ❖Connectionless Confidentiality
  - ❖Selective-Field Confidentiality
  - ❖Traffic-Flow Confidentiality

Data Confidentiality

- Connection Confidentiality
  - The protection of all user data ***on a connection***
- Connectionless Confidentiality
  - The protection of all user data ***in a single data block***
- Selective-Field Confidentiality
  - The confidentiality of ***selected fields*** within the user data on a ***connection or in a single data block***.
- Traffic-Flow Confidentiality
  - The protection of the information that might be **derived from observation of traffic flows**

Data Integrity

- The **assurance** that data received are **exactly** as sent by an authorized entity (i.e., **contain no modification, insertion, deletion, or replay**).
  - Connection Integrity with Recovery
  - Connection Integrity without Recovery
  - Selective-Field Connection Integrity
  - Connectionless Integrity
  - Selective-Field Connectionless Integrity

Data Integrity

- Connection Integrity with Recovery
  - Provides for the **integrity of all user data on a connection** and detects any modification, insertion, deletion, or replay of any data **within an entire data sequence**, with **recovery attempted.**
- Connection Integrity without Recovery
  - As above, but provides **only detection without recovery**
- Selective-Field Connection Integrity
  - Provides for the integrity of **selected fields within the user data of a data block transferred over a connection** and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Data Integrity

- Connectionless Integrity
  - Provides for the ***integrity of a single connectionless data block*** and may take the form of detection of data modification.
  - Additionally, a limited form of replay detection may be provided.
- Selective-Field Connectionless Integrity
  - Provides for the integrity of **selected fields within a single connectionless data block**; takes the form of determination of whether the selected fields have been modified

Non-Repudation

- Provides **protection against denial** by one of the entities involved in a communication of having participated in all or part of the communication
- **Nonrepudiation Origin**
  - **Proof** that the message was **sent by the specified party.**
- **Nonrepudiation, Destination**
  - **Proof** that the message **was received by the specified party.**

Relation Between Security Services and Mechanisms

SERVICE \ MECHANISM	Enchipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			