Information Security

Dr. Zia ur Rehman

Books

- Stallings, W. (2022). Cryptography and network security: principles and practice. Pearson. ISBN: 9789332585225.
- Maymi, F., & Harris, S. (2016). CISSP All-in-One Exam Guide, 7 th Edition. McGraw-Hill Education. ISBN: 9780071849272.

Your Best Strategy

- Come to every lectures
- Read every lecture after going home and prepare it well.
- Do not wait till last minute to prepare for exam or work on projects
- Enjoy the fun!

Lectures need your help!

- Ask questions
- Make suggestions!
- Read something interesting and relevant to this course? Announce it in class!

Cyber Security

- It is the protection of information that is stored, transmitted, and processed in a networked system of computers, other digital devices, and network devices and transmission lines, including the Internet.

Reader’s Guide

- The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable. —The Art of War, Sun Tzu

Cyber Security….

- As subsets of cybersecurity, we can define the following:
- **Information security**: This term refers to preservation of confidentiality, integrity, and availability of information. In addition, other properties, such as authenticity, accountability, nonrepudiation, and reliability can also be involved.

Definitions

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

Security Objectives

- **Confidentiality**: This term covers two related concepts:
  - **Data Confidentiality**: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
  - **Privacy**: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Security Objectives…

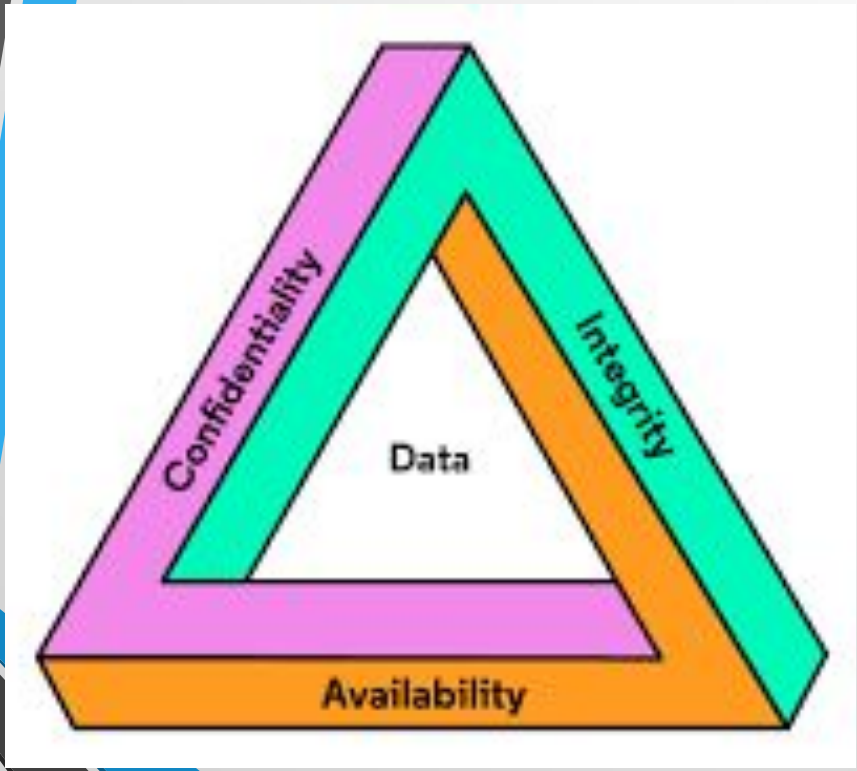
- Integrity: This term covers two related concepts:
  - **Data integrity**: Assures that data (both stored and in transmitted packets) and programs are changed only in a specified and authorized manner.
  - **System integrity**: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Sec. Obj.

- Availability: Assures that systems work promptly and service is not denied to authorized users.

Sec.. Obj...

CIA Triad



- Confidentiality
  - (Account information)
- Integrity
  - (Patient's information)
- Availability
  - (Authentication service)

Sec. Obj…

- **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.

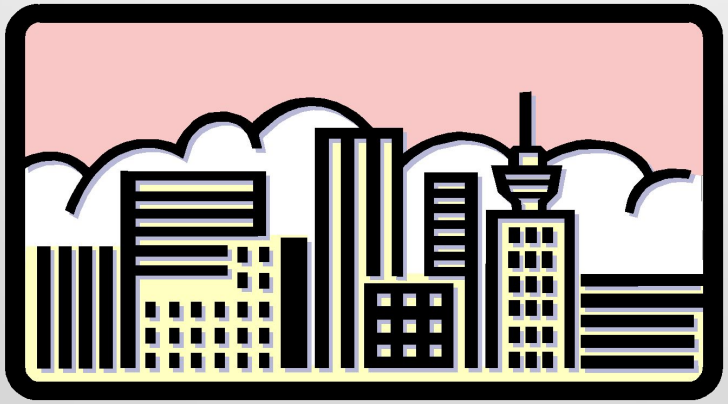
Computer Security Challenges

- not simple
- must consider potential attacks.
- procedures used counterintuitive
- involve algorithms and secret info
- must decide where to deploy mechanisms
- battle of wits between attacker / admin
- not perceived on benefit until fails
- requires regular monitoring
- too often an after-thought

  regarded as impediment to using system

OSI Security Architecture

- ITU-T X.800 “Security Architecture for OSI”
- defines a systematic way of defining and providing security requirements



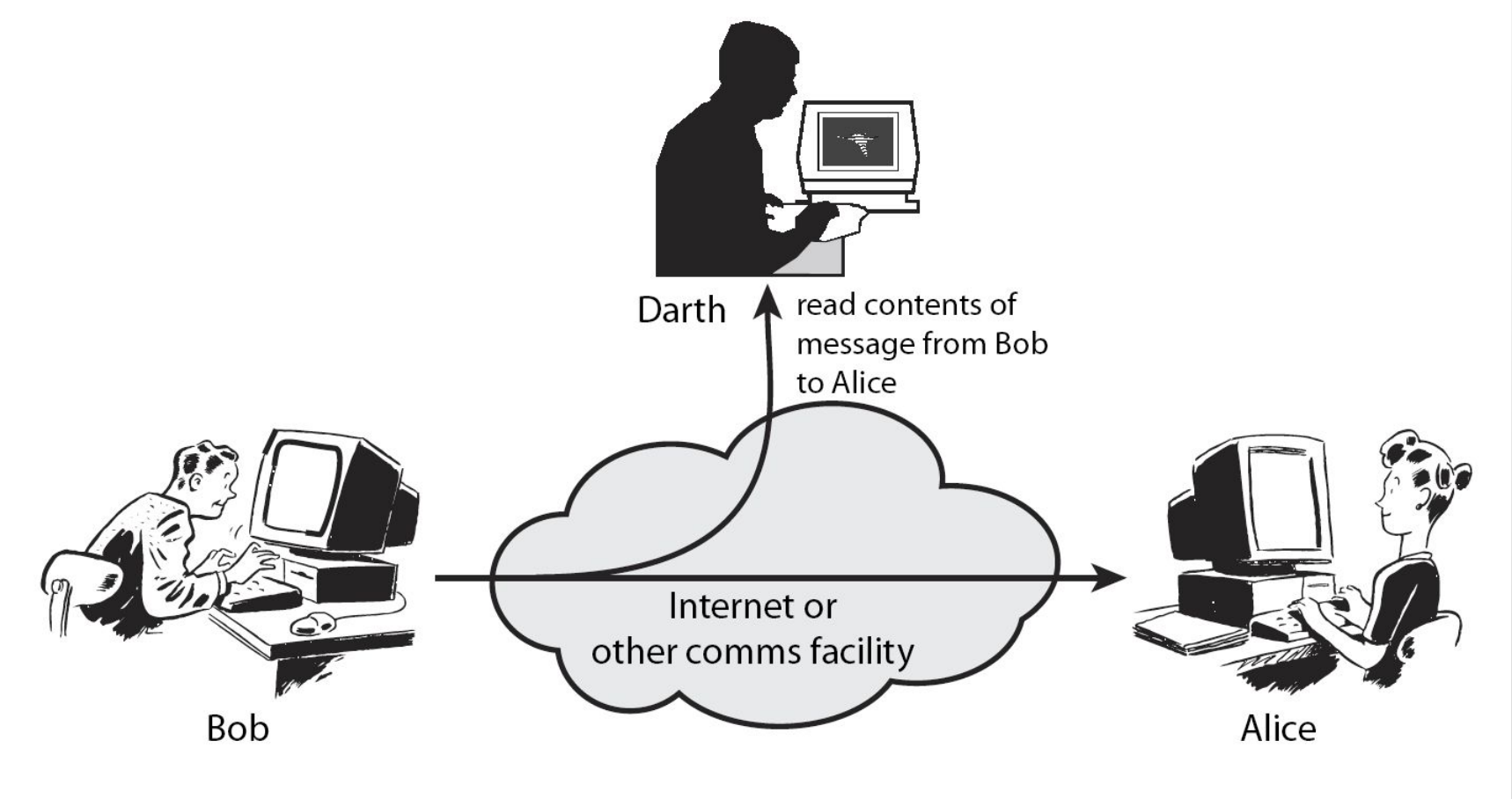
Aspects of Security

- consider 3 aspects of information security:
  - **security attack**
  - **security mechanism**
  - **security service**

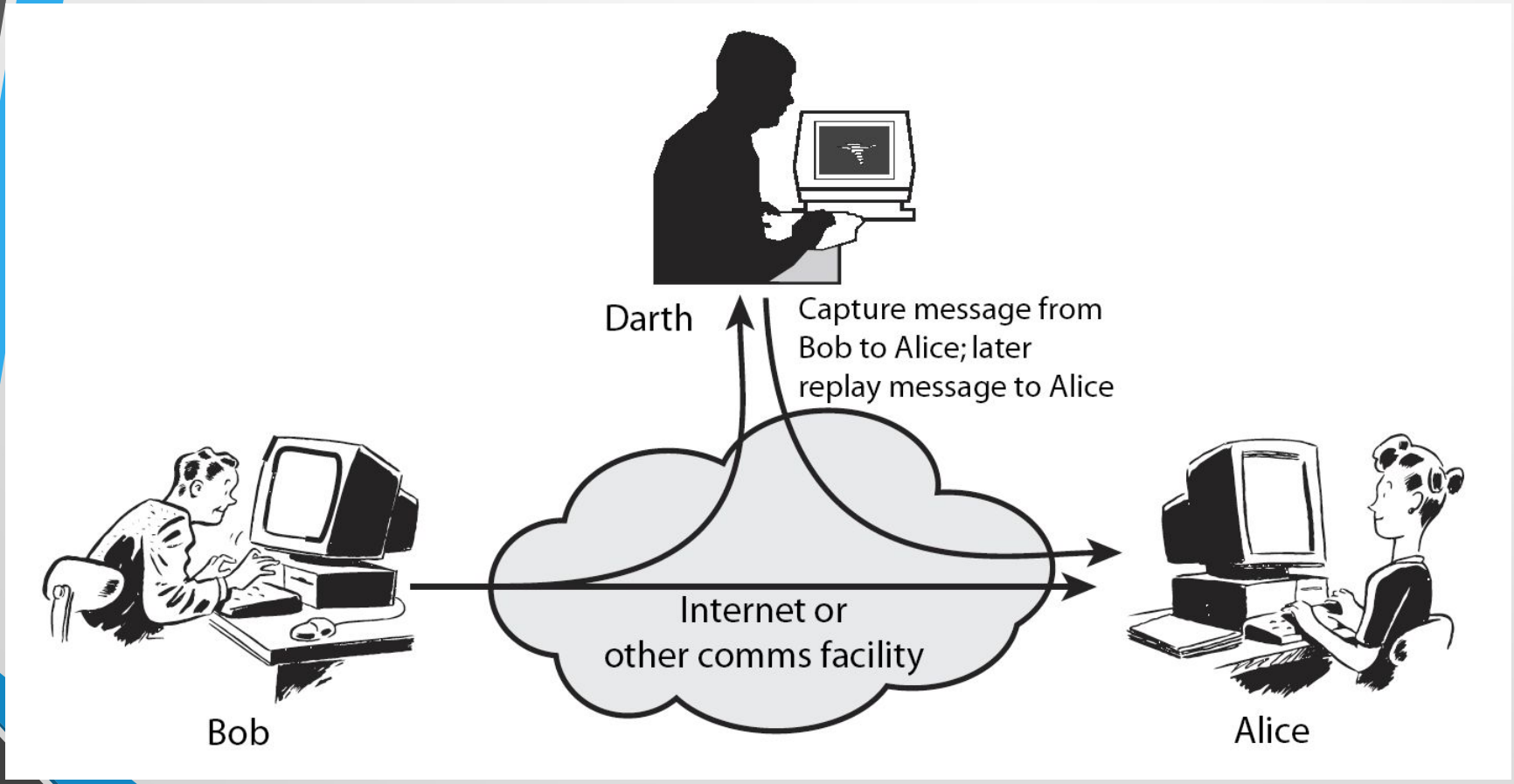
Security Attack

- Any action that compromises the security of information owned by an organization
- Information Security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- often *threat* & *attack* used to mean same thing have a wide range of attacks
- can focus of generic types of attacks
  - passive
  - active

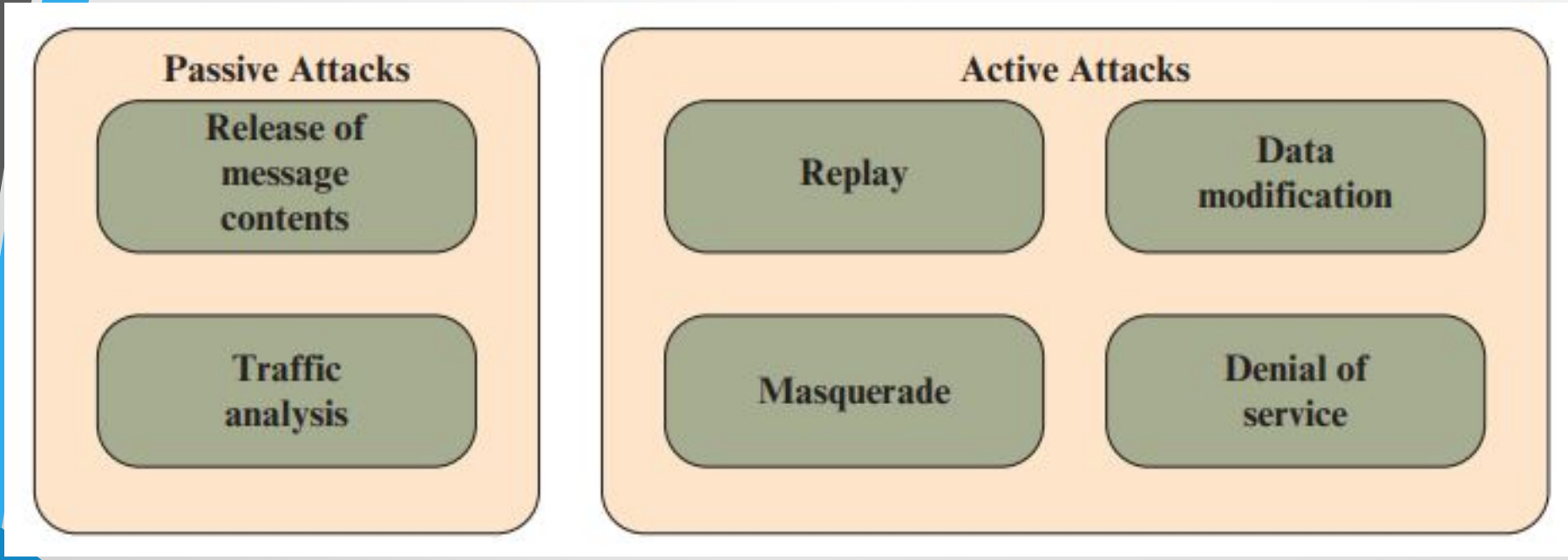
Passive Attacks



Active Attacks



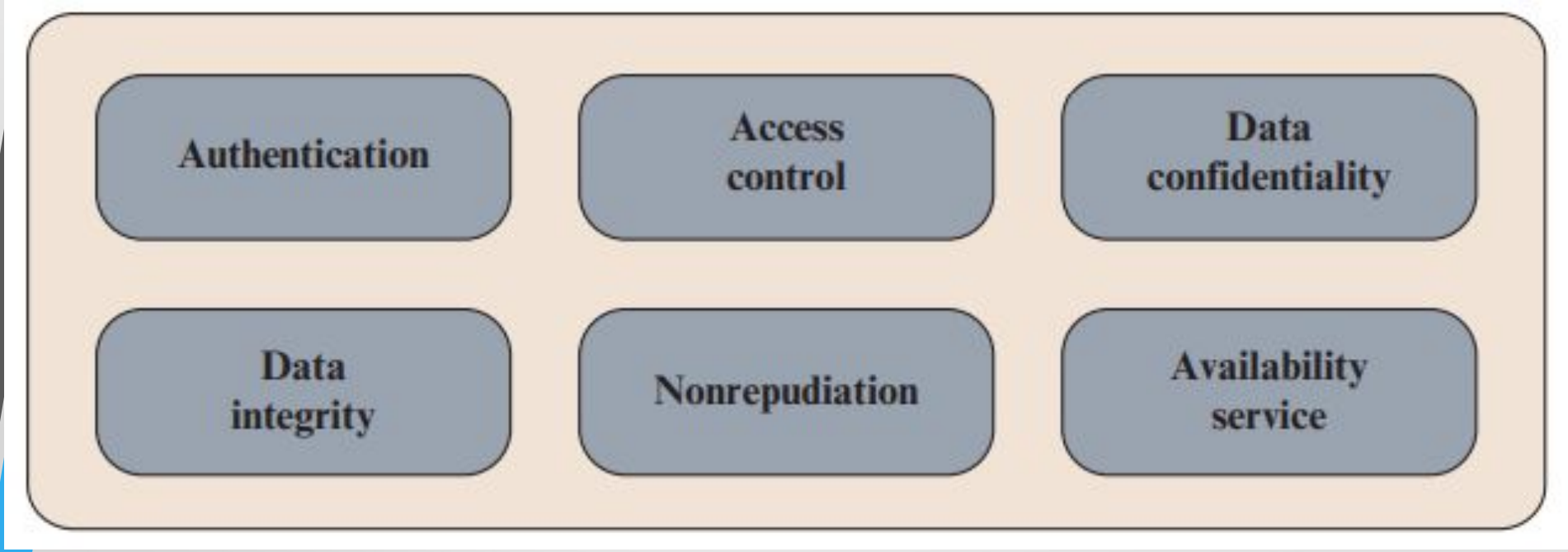
Types of Attacks



Security Service

- Enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
    - for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Security Services



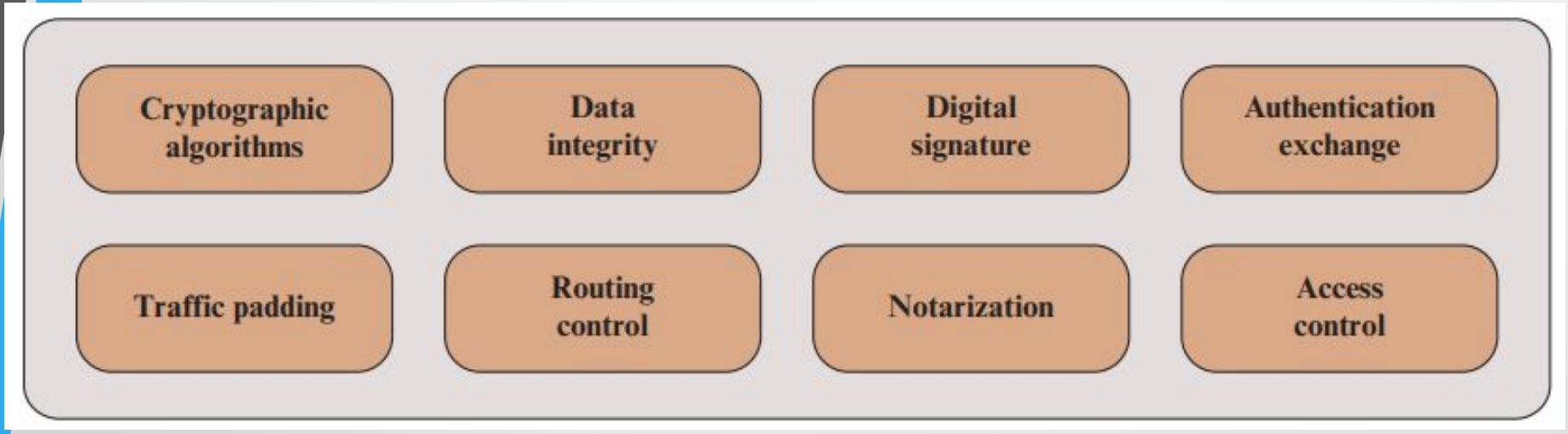
Security Services

- **Authentication** - assurance that the communicating entity is the one claimed
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication

Security Mechanism

- feature designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all services required
- however one particular element underlies many of the security mechanisms in use:
  - **cryptographic techniques**

Security Mechanism



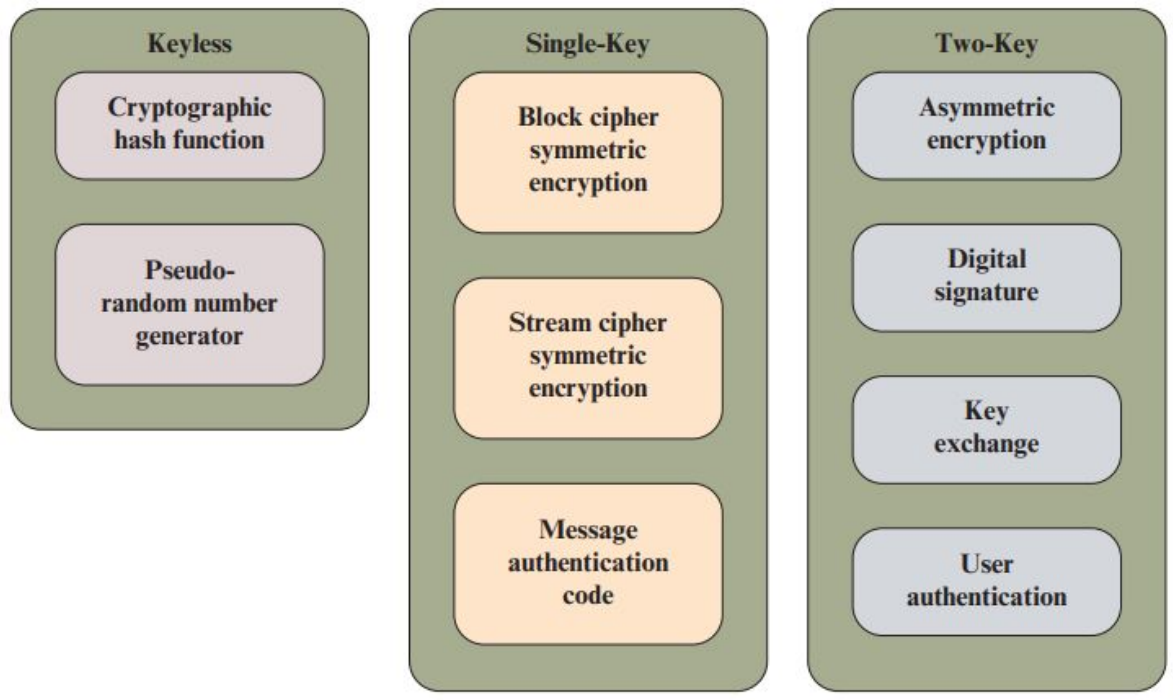
Security Mechanisms

- specific security mechanisms:
  - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- pervasive security mechanisms:
  - trusted functionality, security labels, event detection, security audit trails, security recovery

Cryptography

- It is a branch of mathematics that deals with the transformation of data.
- Cryptographic algorithms are used in many ways in information security and network security.
- Cryptography is an essential component in the secure storage and transmission of data, and in the secure interaction between parties.

Cryptographic Algorithms



Keyless Algorithms

- A **cryptographic hash function** is one that has additional properties that make it useful as part of another cryptographic algorithm, such as a message authentication code or a digital signature.
- A **pseudorandom number generator** produces a deterministic sequence of numbers or bits that has the appearance of being a truly random sequence.

Single-Key Algorithms

- **Block cipher**: A block cipher operates on data as a sequence of blocks. A typical block size is 128 bits.
- **Stream cipher**: A stream cipher operates on data as a sequence of bits. Typically, an exclusive-OR operation is used to produce a bit-by-bit transformation.
- **Message Authentication Code (MAC)**: A MAC is a data element associated with a data block or message.

Two-Key Algorithms

- A **digital signature** is a value computed with a cryptographic algorithm and associated with a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity.
- **Key exchange** is the process of securely distributing a symmetric key to two or more parties.
- **User authentication** is the process of authenticating that a user attempting to access an application or service is genuine