Aim of Course

- Our focus is on Security that consists of measures to:
  - Prevent,
  - detect,
  - and correct (if it is possible)
    - security violations

Chapter Objectives

After studying this chapter, you should be able to:

- Describe the **key security requirements**: Confidentiality, Integrity, and Availability (CIA triad).
- Describe **key organizations involved in cryptography standards.**
- Describe the **security architecture for OSI (X.800)**.
- Discuss **the different types of security threats and attacks**.
- Explain **the fundamental security design principles**.

Background

- Traditionally, security were provided by physical and administrative mechanisms
- Information Security requirements have changed in recent times:
  1) Growing Computer **use requires automated tools to protect files and other stored information**
  2) Use of networks and communications links requires measures to protect data during transmission

Computer Security

- The protection afforded to an automated information system in order to attain the applicable objectives of preserving:
  - Integrity
  - Availability
  - Confidentiality
    - of information and system resources.
    - The protection includes hardware, software, information/data, and telecommunications

Aspects of Security

- The OSI security architecture focuses on 3 aspects o information security:

1) **Security services**

1) **Security attack;**

   Any action that compromises the security

1) **Security mechanism;**

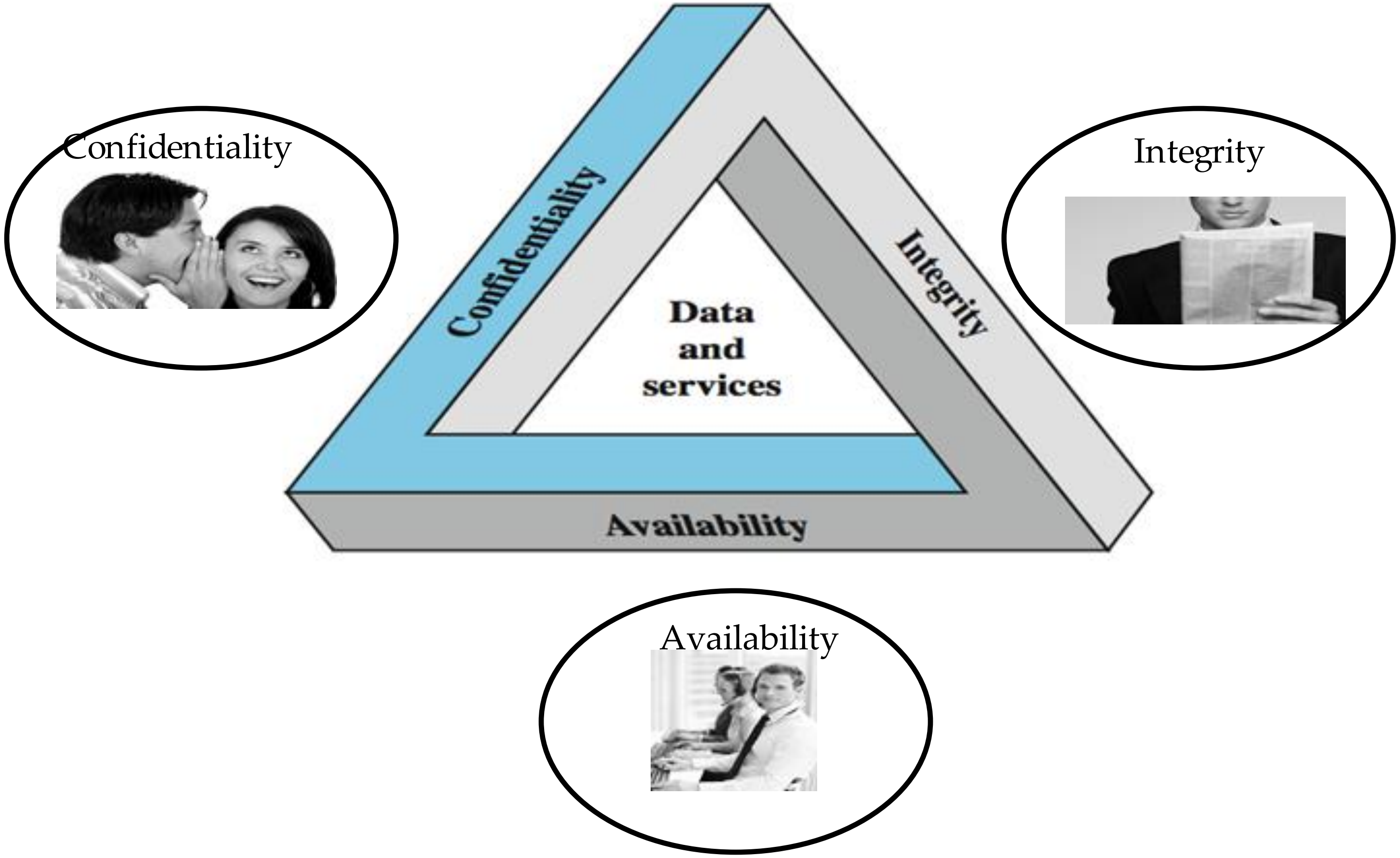
   A process that is designed to **prevent, detect, or recover** fro security attack

Security Services

- Enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms

Key Security Concepts
(Heart of computer security)

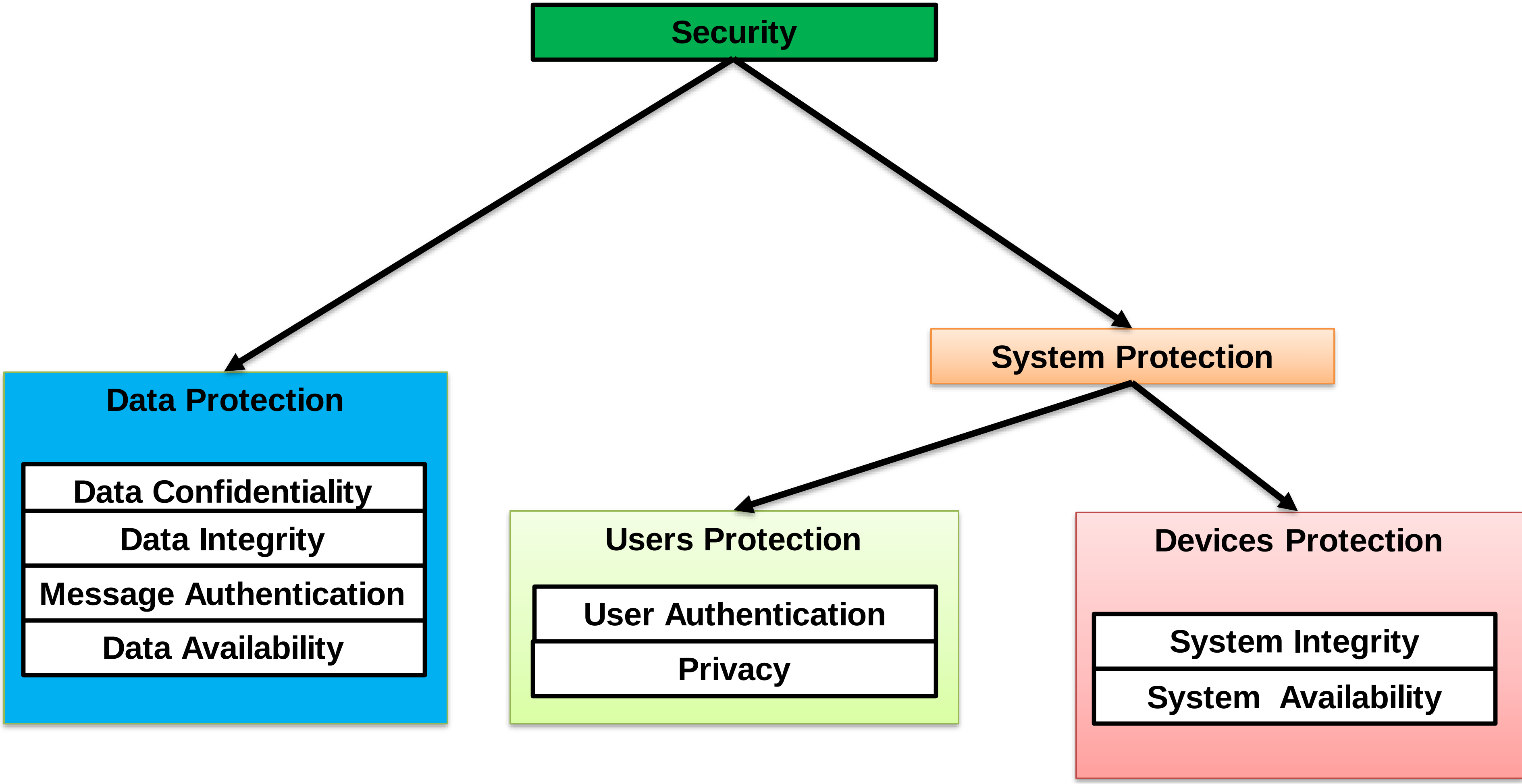
Three key objectives that are at the heart of computer security:



Security Services

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

Global viewpoints



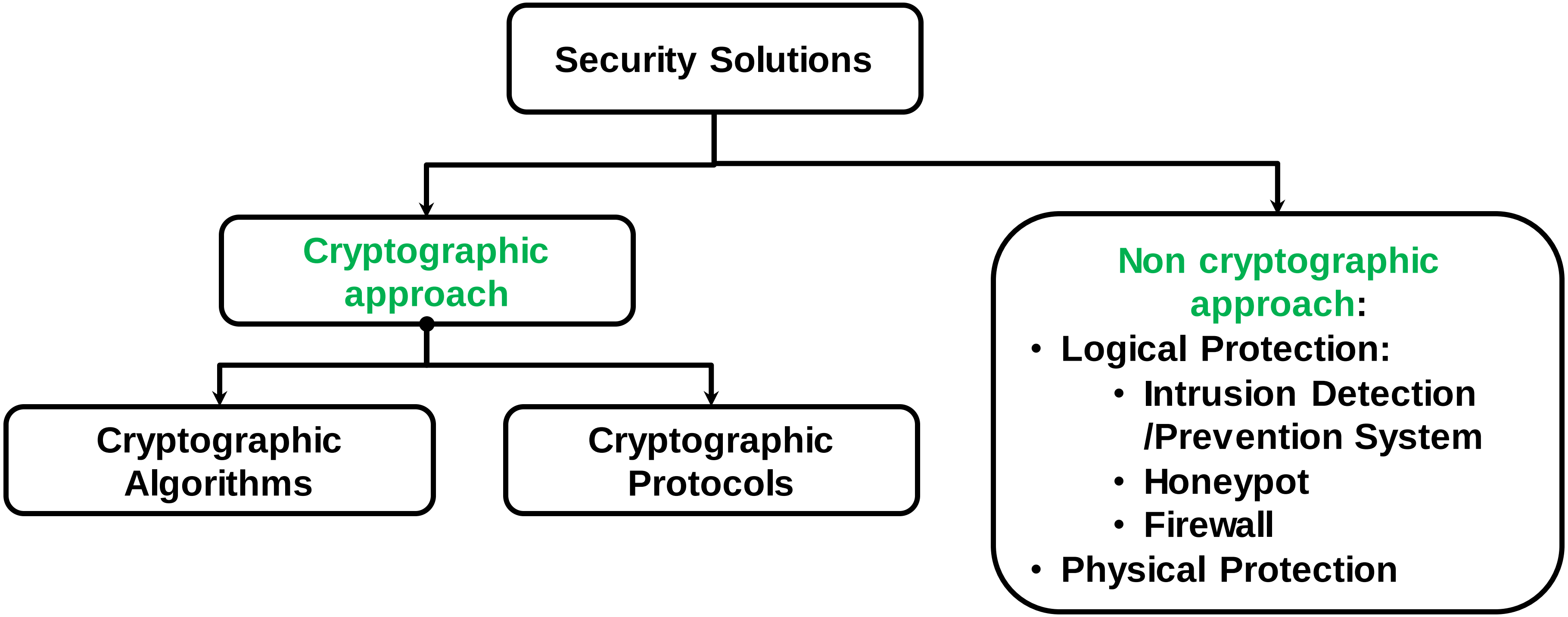
Security Mechanisms

- Designed to detect, prevent, or recover from a security attack
- **no single mechanism** that will support all ***required security services***
- However one particular element underlies many of the security mechanisms in use:
  - **cryptographic techniques**
- Hence **our focus on this topic**

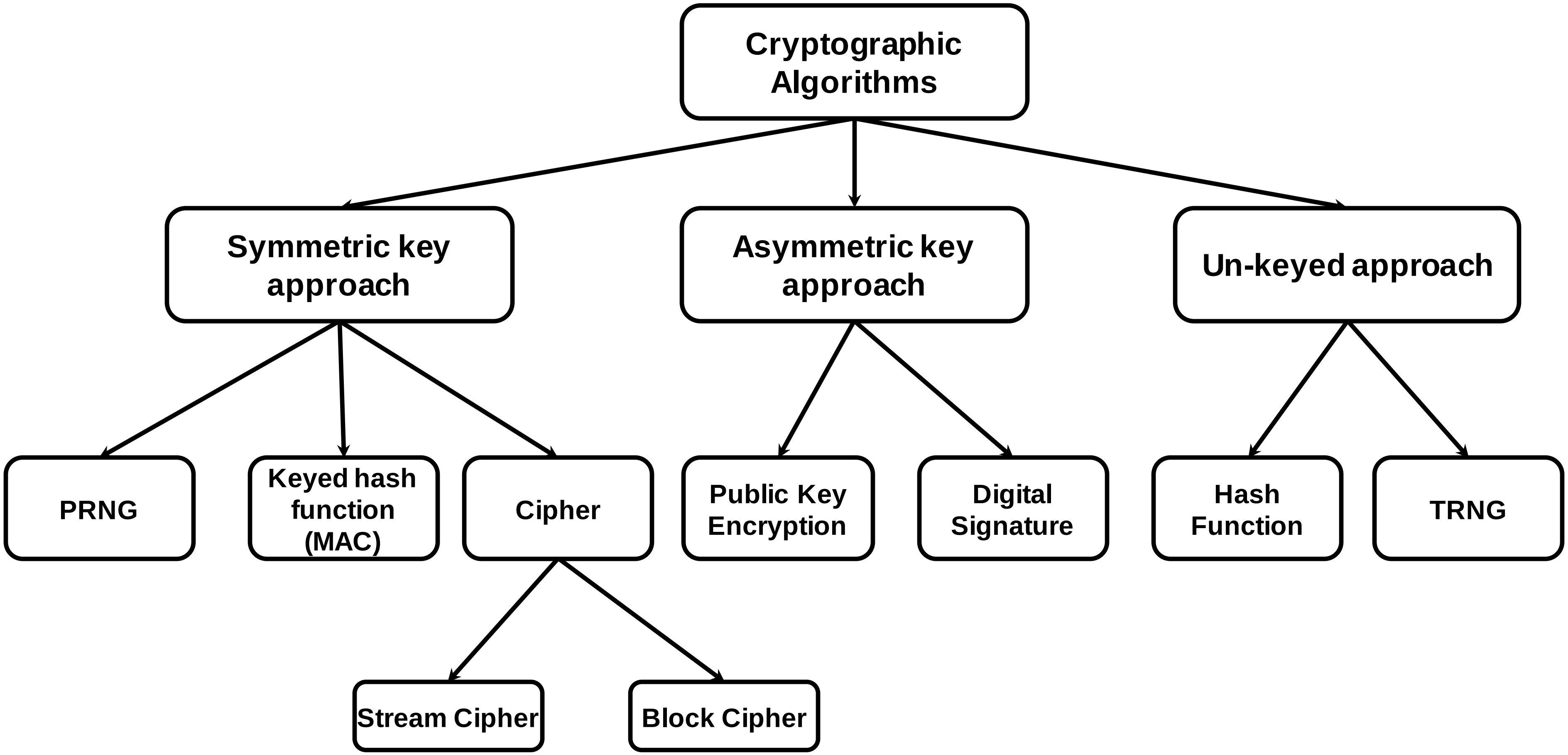
Security Mechanisms (Solutions)

1) Any application or system have to introduce security
2) Security solutions can be divided into two main classes:

   1) Cryptographic techniques
   2) Non-cryptographic techniques



Cryptographic Algorithms



[1] Katz, Jonathan, and Yehuda Lindell. *Introduction to modern cryptography*. CRC press, 2014.

Another Cryptographic Classification

- Cryptographic techniques can be grouped into four main areas:

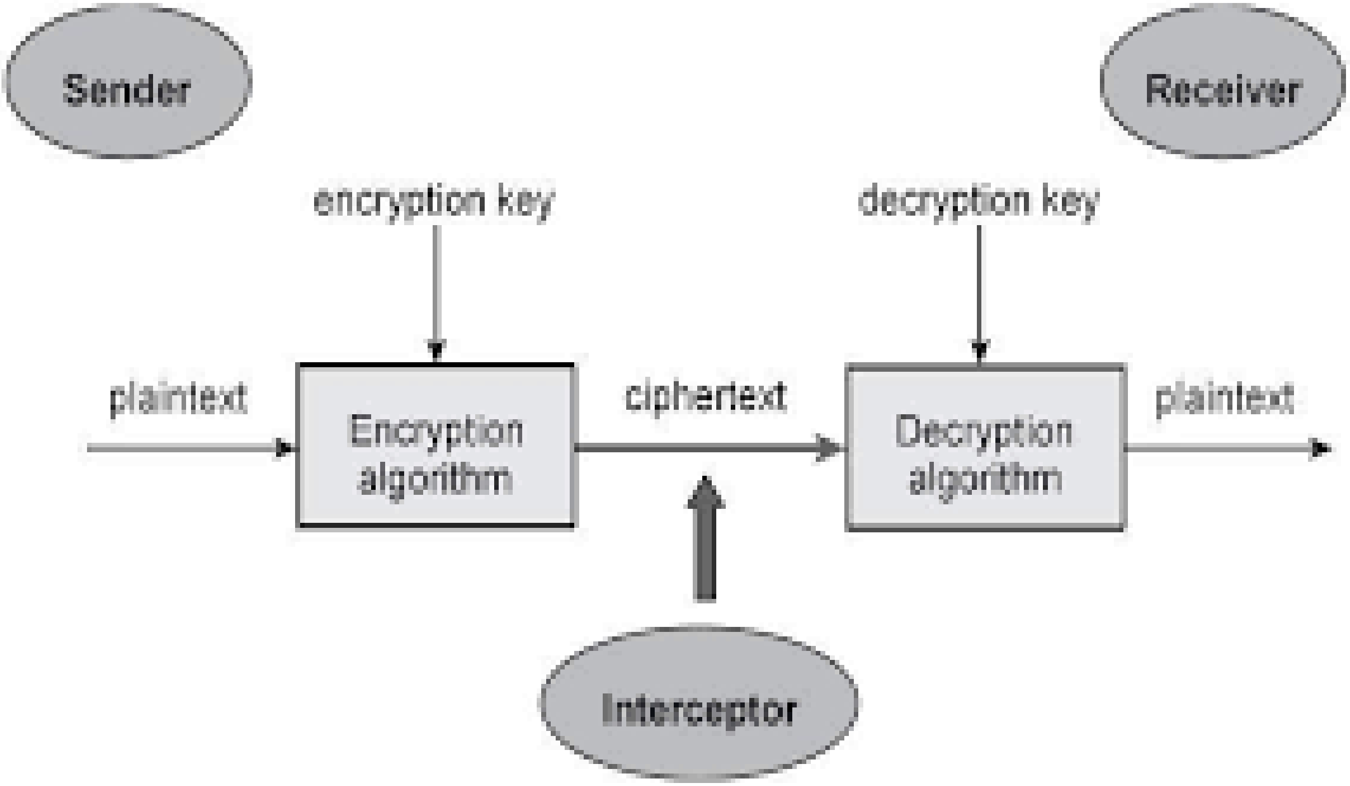
1) **Symmetric encryption**: Used to conceal streams of data of any size, including messages, files.

1) **Asymmetric encryption**: Used to conceal **small blocks of data**, such as encryption keys and hash function values.

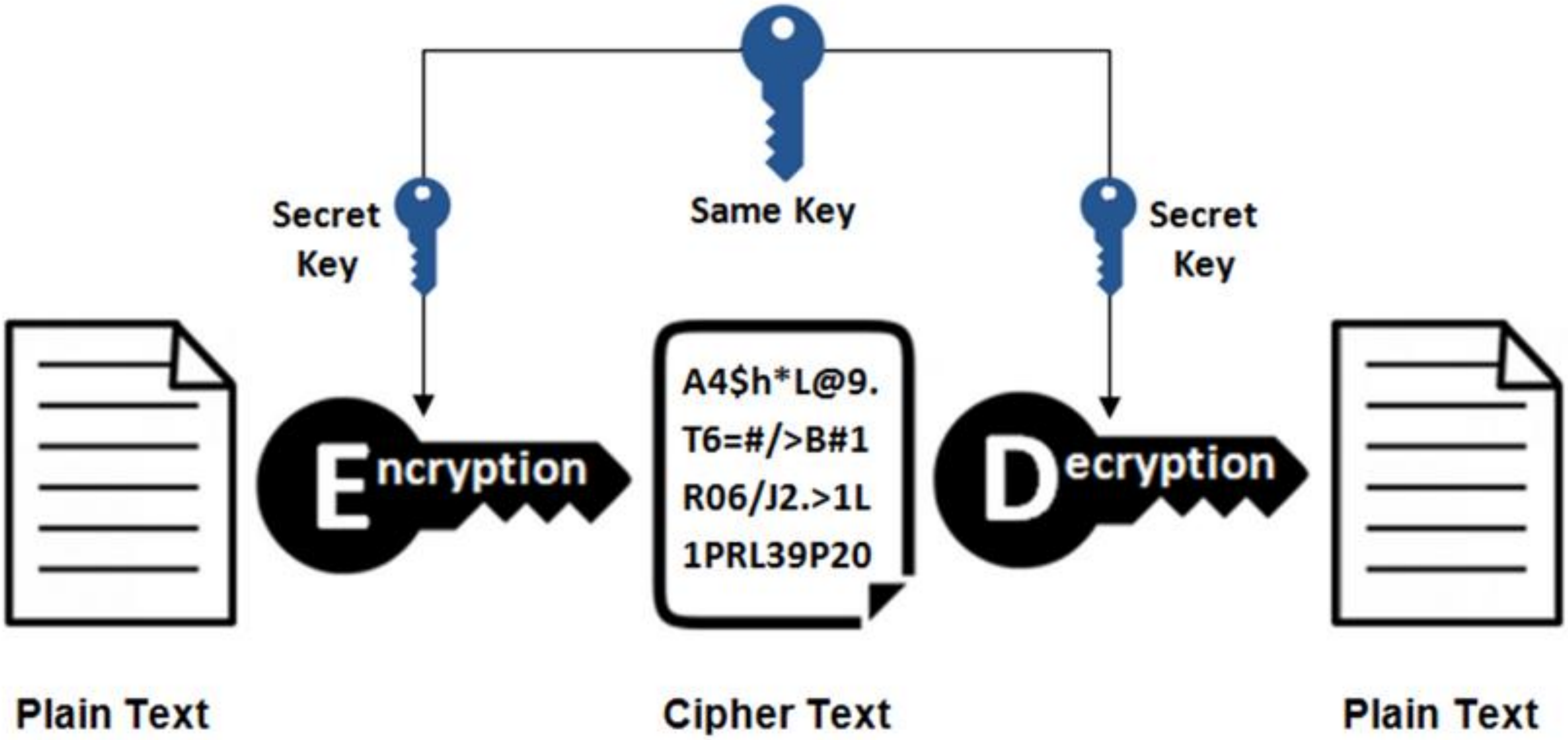
1) **Data integrity algorithms**: Used to protect blocks of data, such as messages, **from alteration**.

1) **Authentication protocols**: These are schemes **based on the use of cryptographic algorithms** designed **to authenticate the identity of entities**.

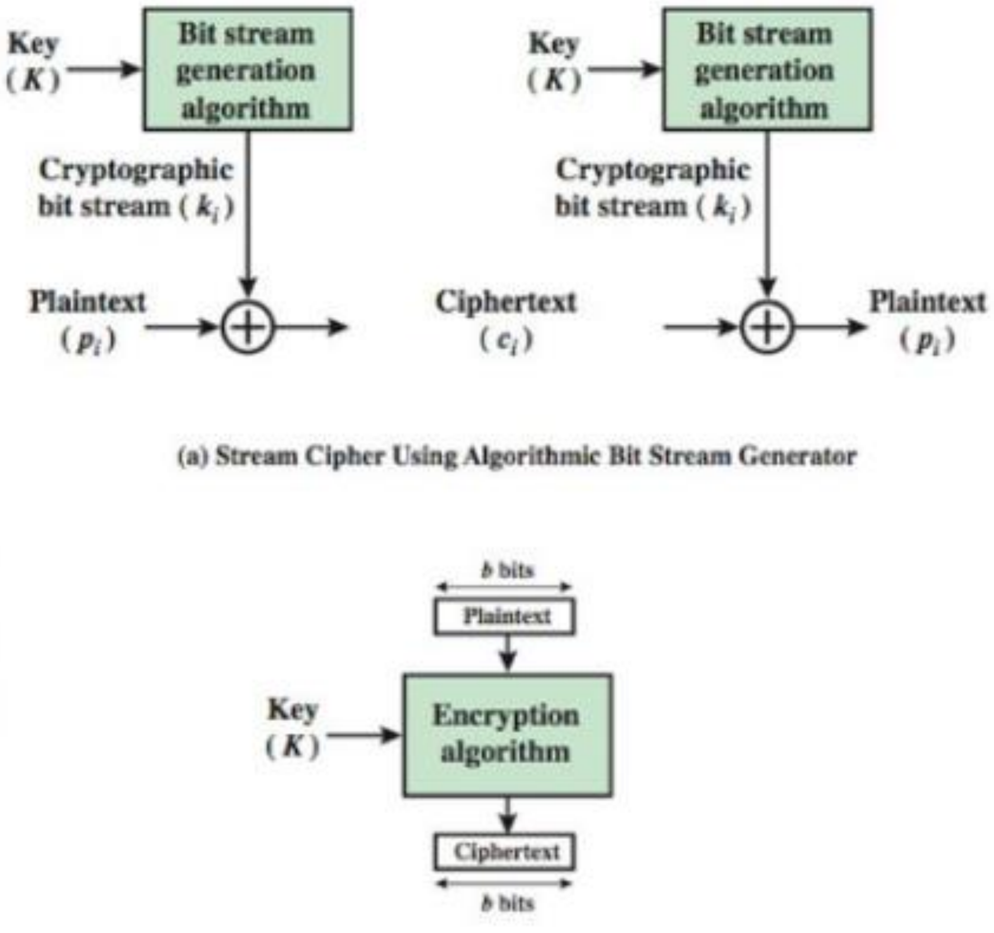
Secure Communication



Symmetric Encryption



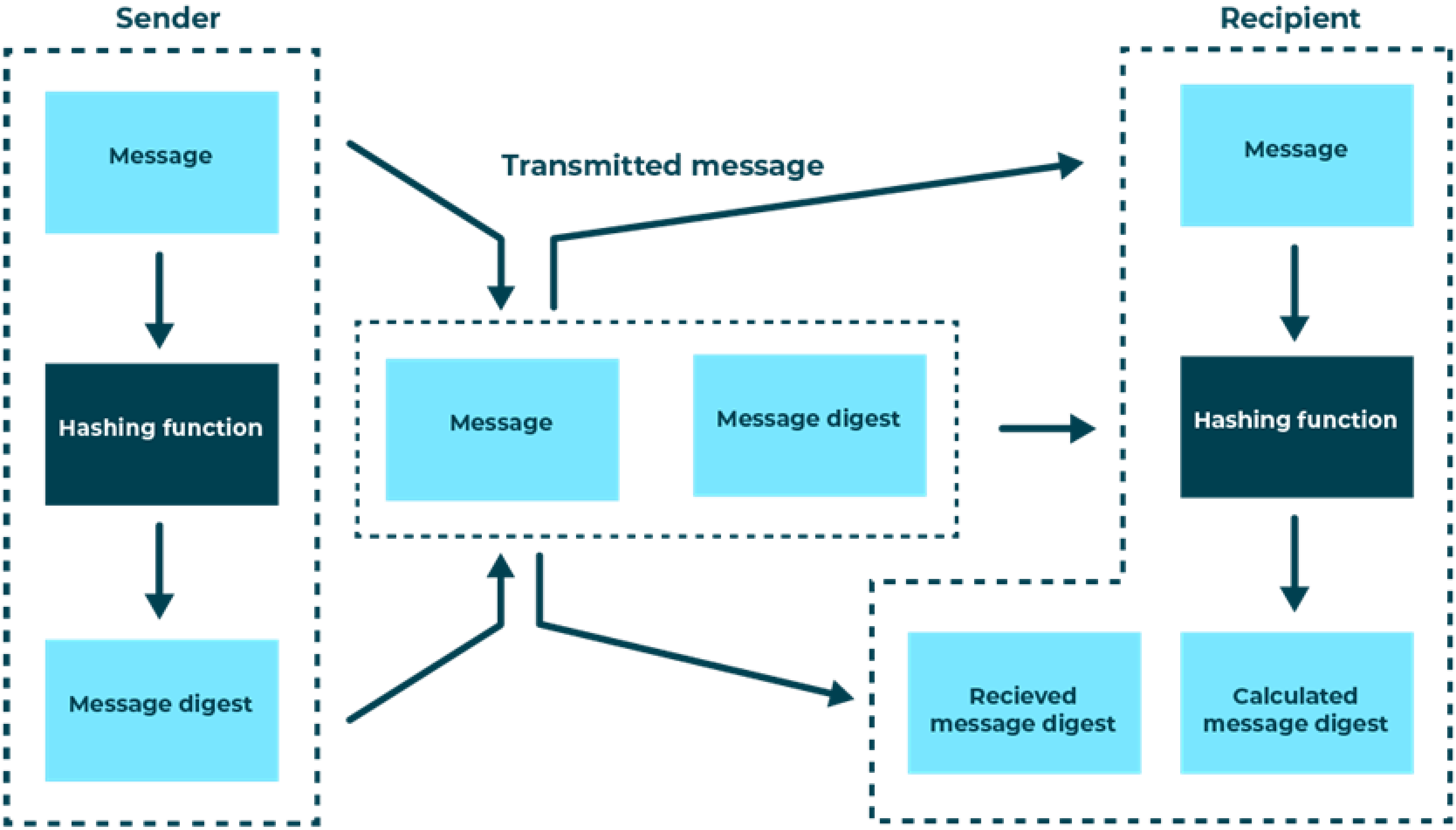
Block cipher vs Stream cipher



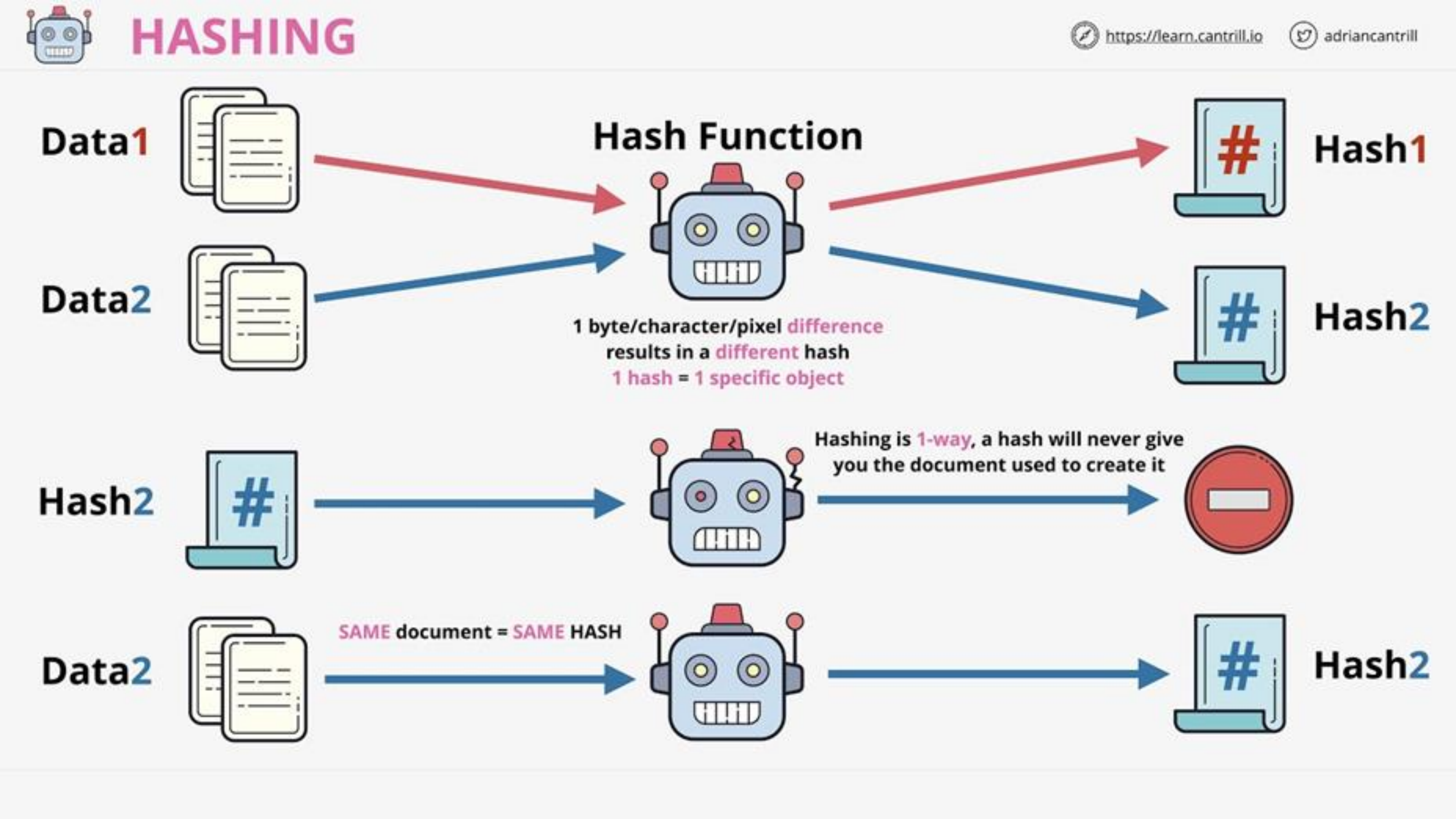
(a) Stream Cipher Using Algorithmic Bit Stream Generator

(b) Block Cipher

Hash function (Keyed or unkeyed)

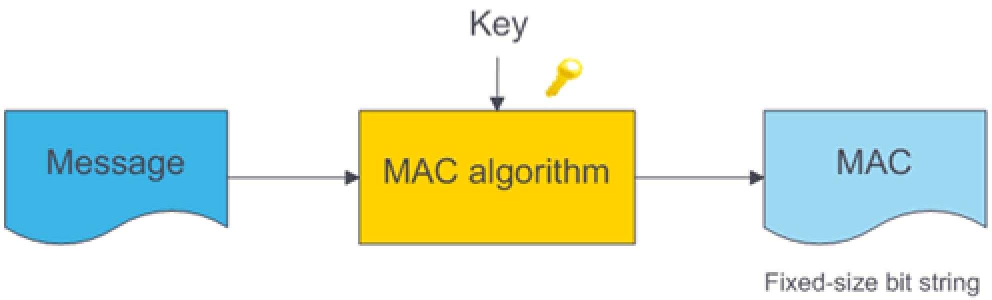


Hash Function (cont’d)

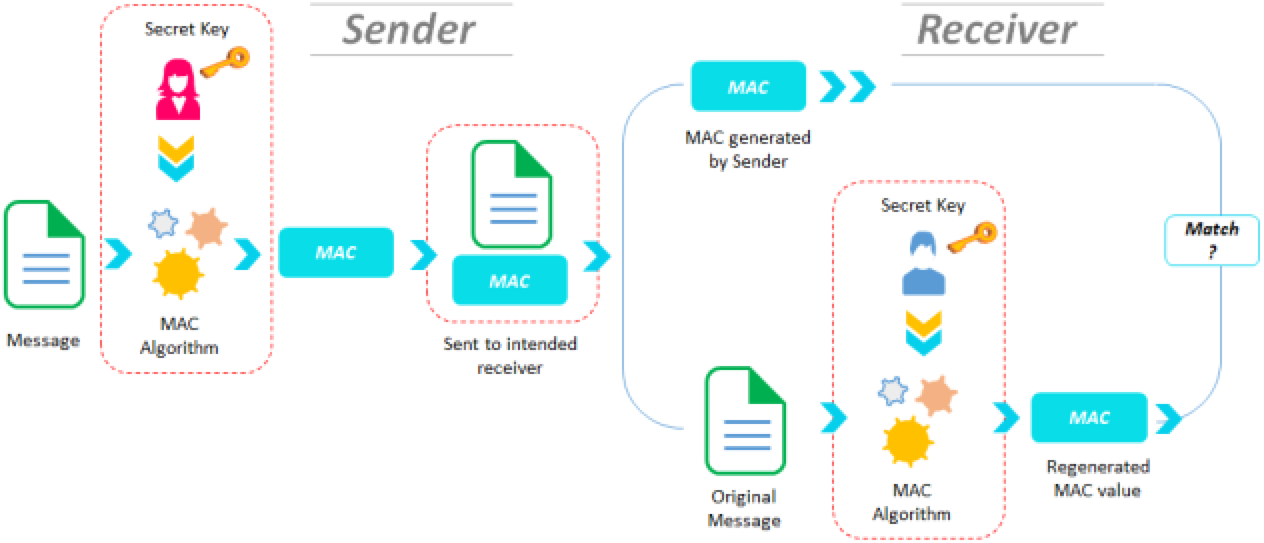


HASHING
https://learn.cantrill.io
adriancantrill
Data1
Data2
Hash Function
Hash1
Hash2
1 byte/character/pixel difference
results in a different hash
1 hash = 1 specific object
Hash2
Hashing is 1-way, a hash will never give
you the document used to create it
Data2
SAME document = SAME HASH
Hash2

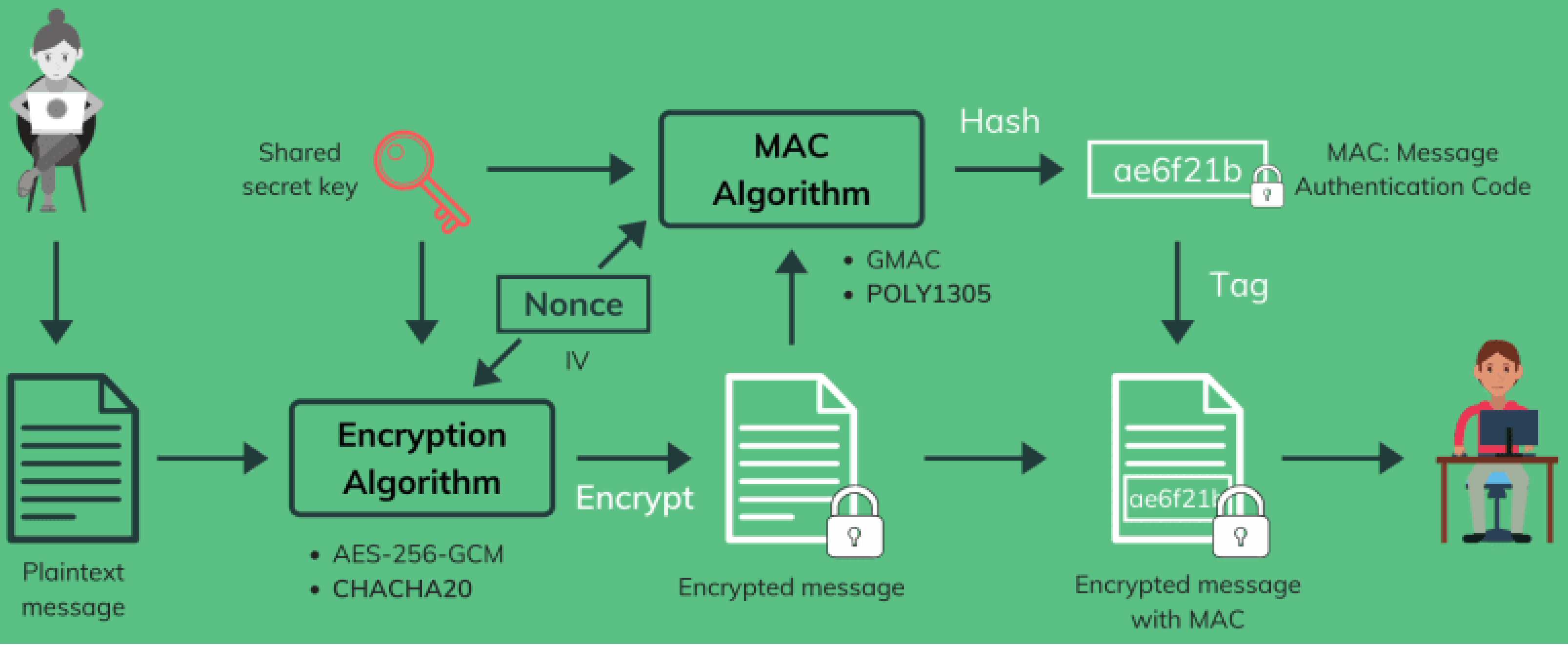
Message Authentication Algorithm



MSv38409V1



AUTHENTICATED ENCRYPTION



Shared secret key

MAC Algorithm

Hash

ae6f21b

MAC: Message Authentication Code

- GMAC
- POLY1305

Tag

Nonce

IV

Plaintext message

Encryption Algorithm

- AES-256-GCM
- CHACHA20

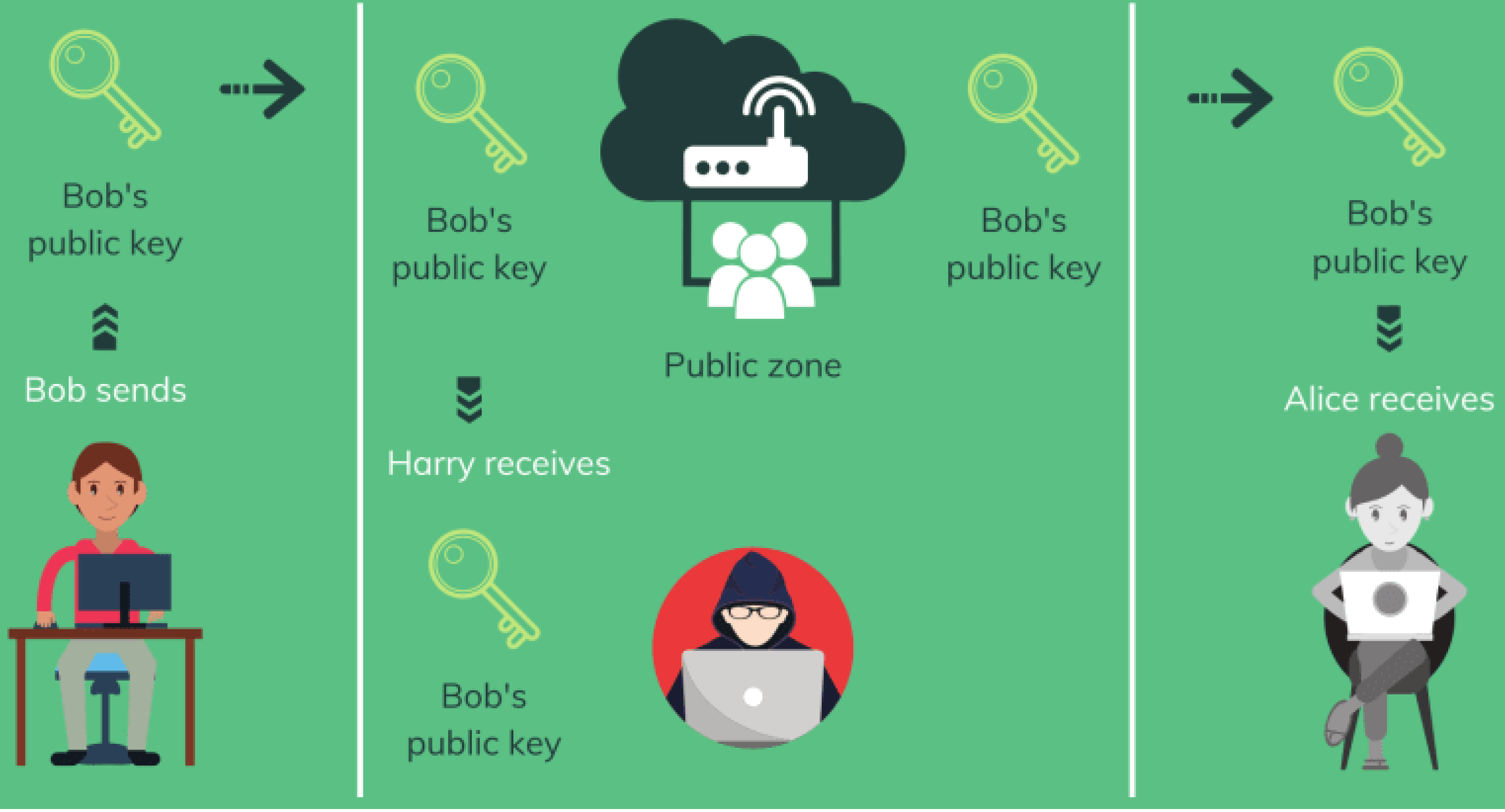
Encrypt

Encrypted message

ae6f21b

Encrypted message with MAC

PUBLIC KEY SHARING



Bob's public key

Bob sends

Bob's public key

Harry receives

Bob's public key

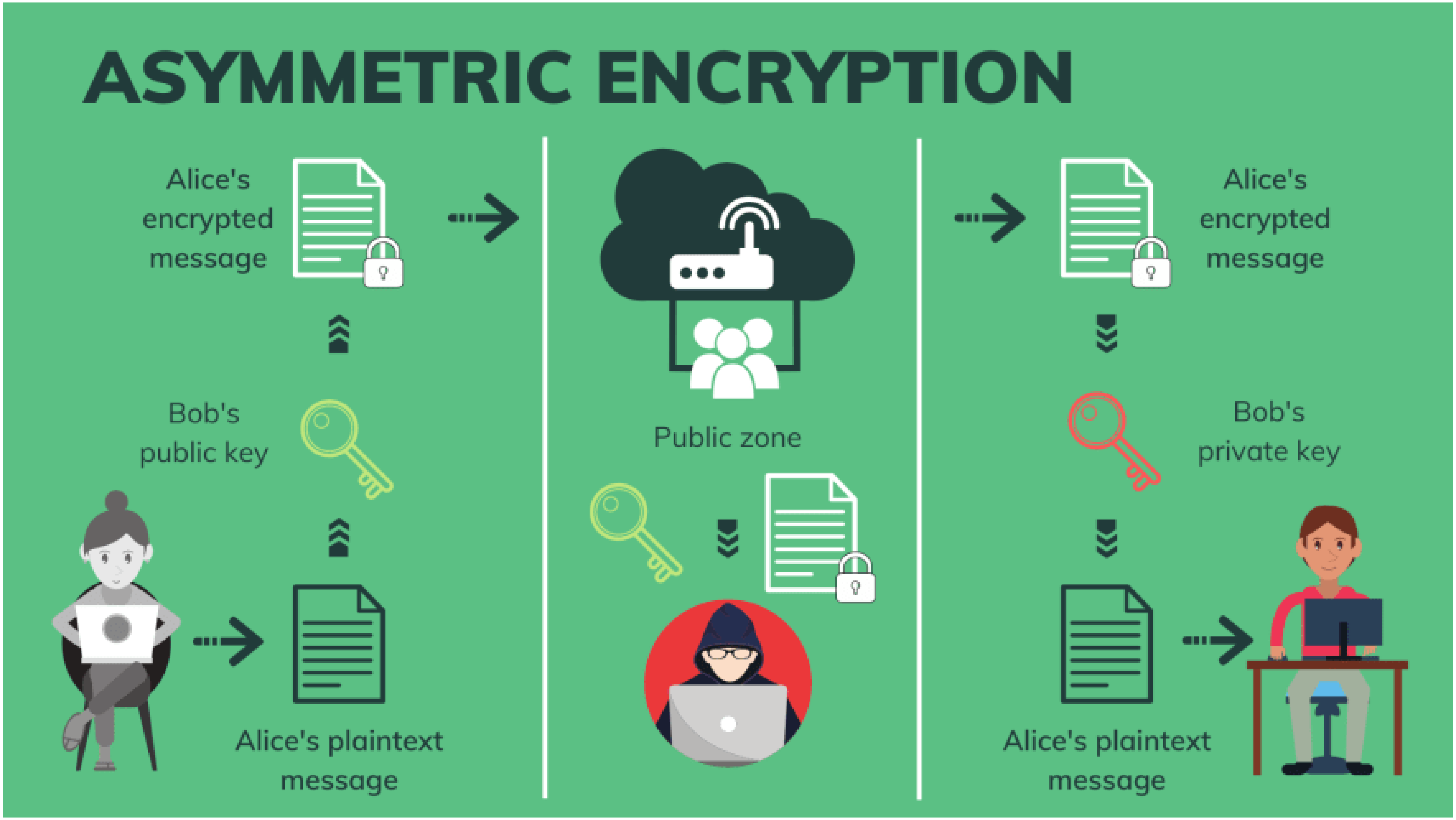
Public zone

Bob's public key

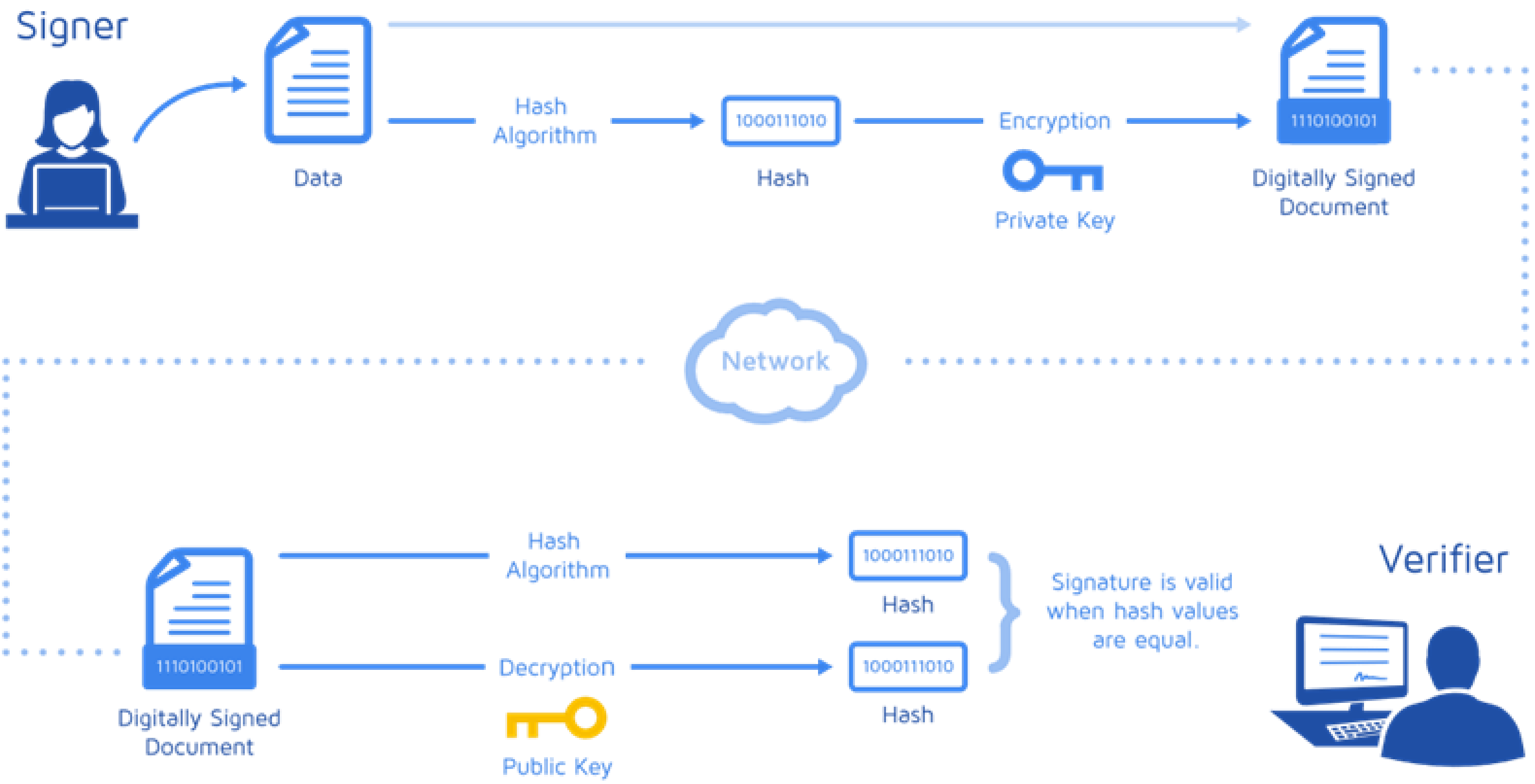
Bob's public key

Alice receives

Asymmetric encryption

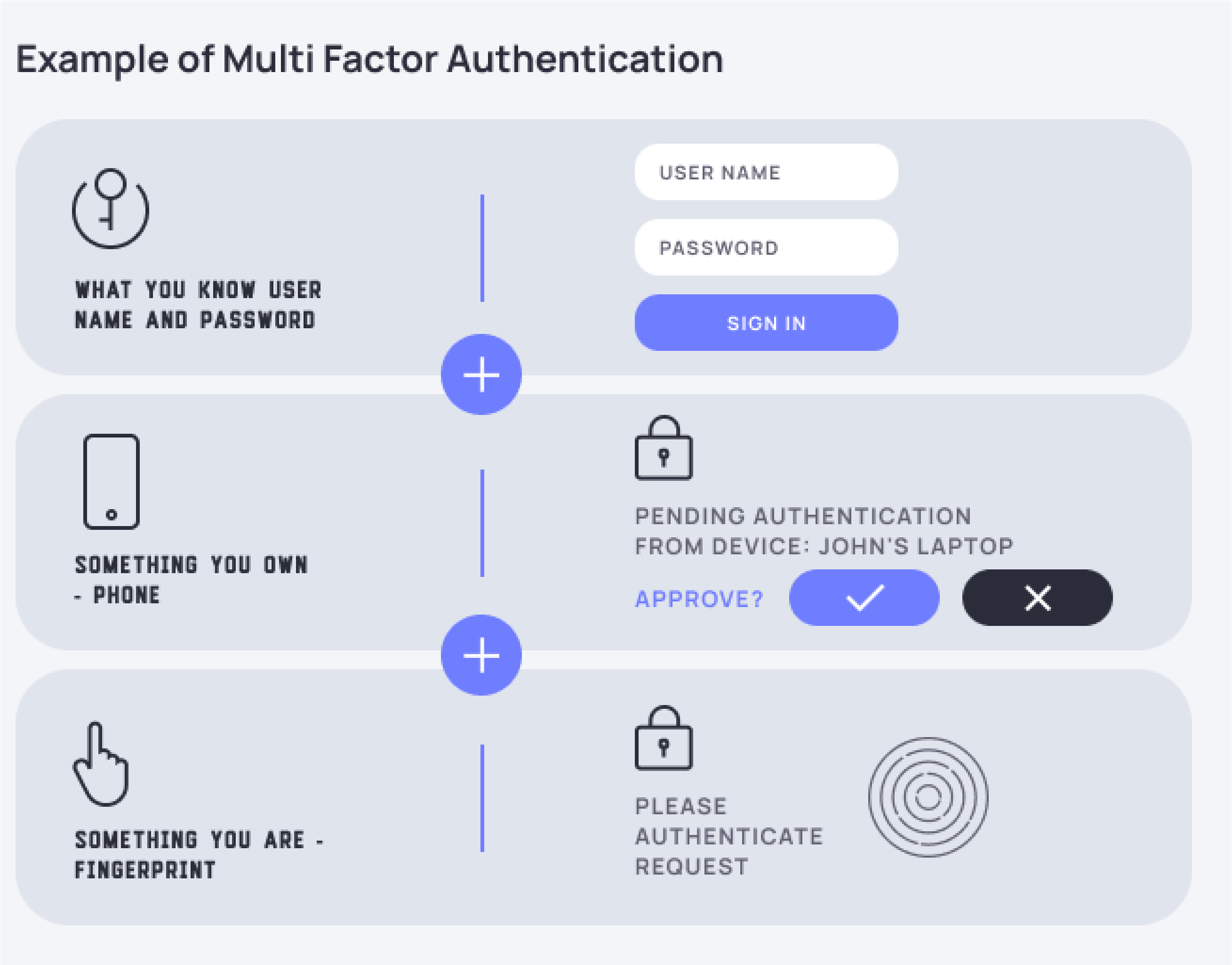

ASYMMETRIC ENCRYPTION
Alice's encrypted message
Bob's public key
Alice's plaintext message
Public zone
Alice's encrypted message
Bob's private key
Alice's plaintext message

Digital Signature



User/Device Authentication

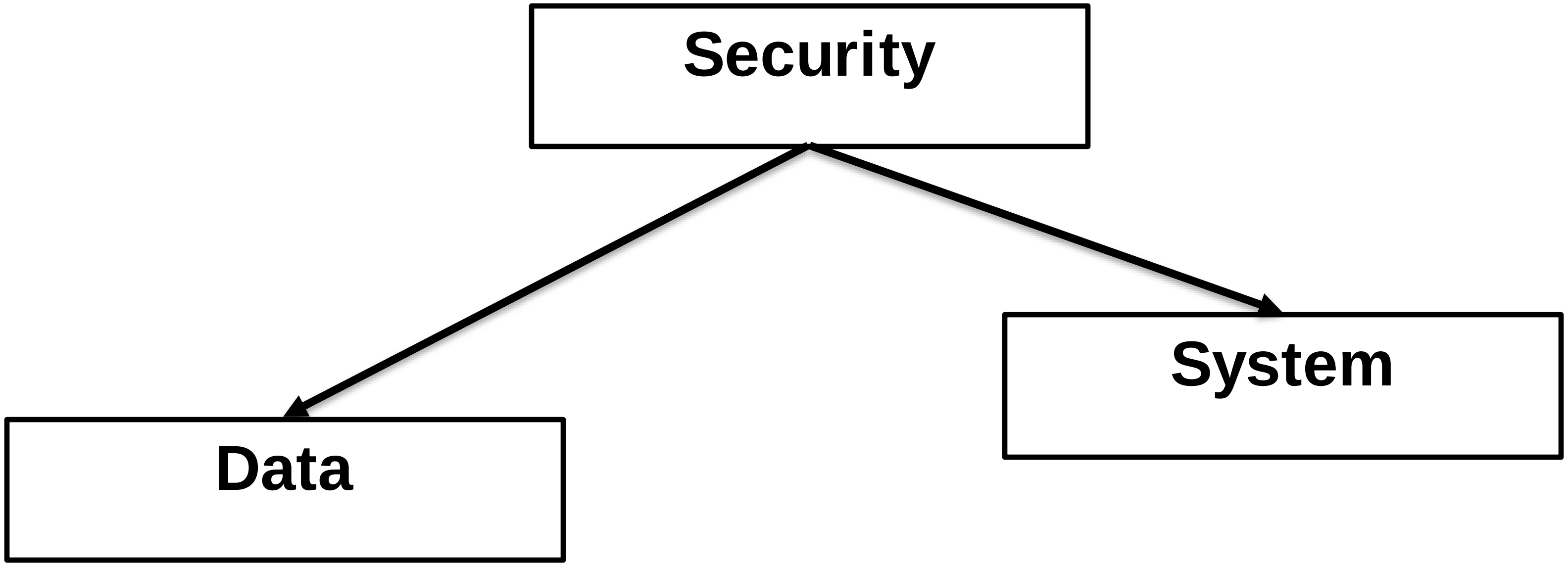
Example of Multi Factor Authentication


WHAT YOU KNOW USER NAME AND PASSWORD
USER NAME
PASSWORD
SIGN IN
SOMETHING YOU OWN - PHONE
PENDING AUTHENTICATION FROM DEVICE: JOHN'S LAPTOP
APPROVE?
SOMETHING YOU ARE - FINGERPRINT
PLEASE AUTHENTICATE REQUEST

Examples of Security Requirements

- Confidentiality – student grades
- Integrity – patient information
- Availability – any online service

Information Security

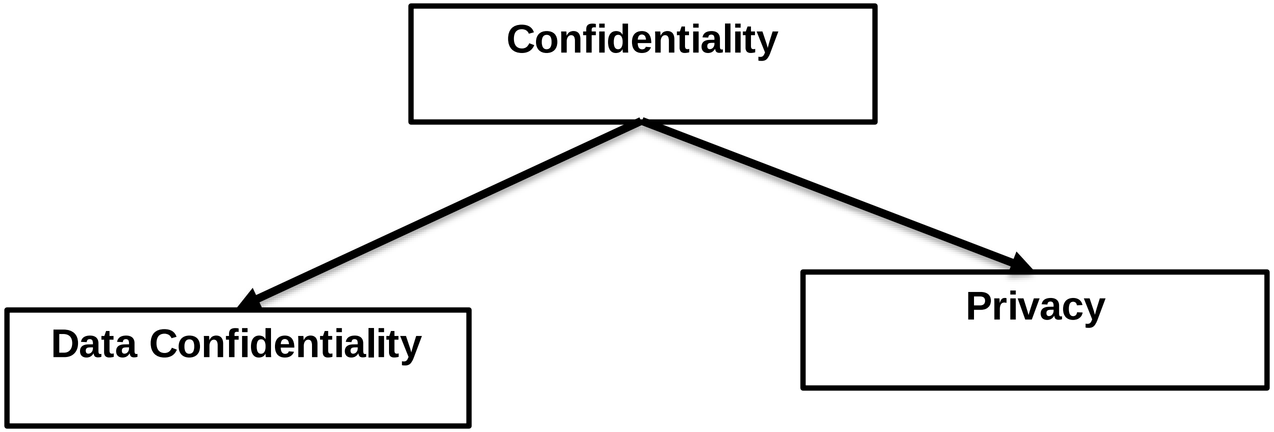


Security

Data

System

Confidentiality

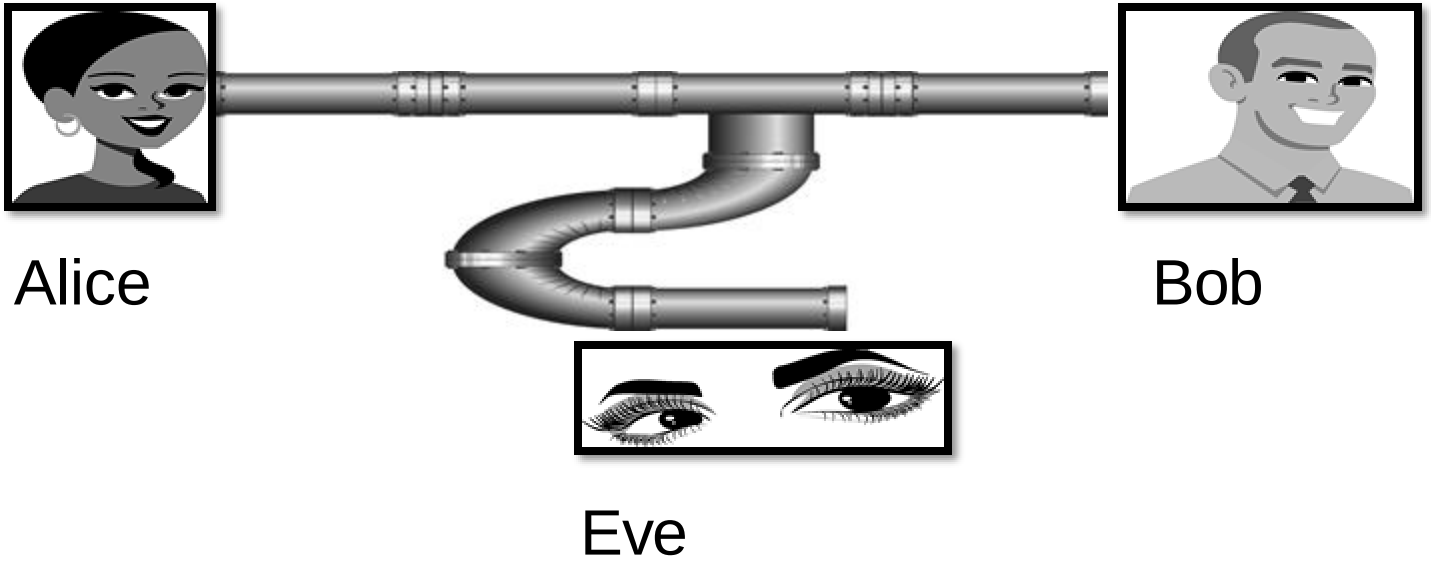


This term covers two related concepts:

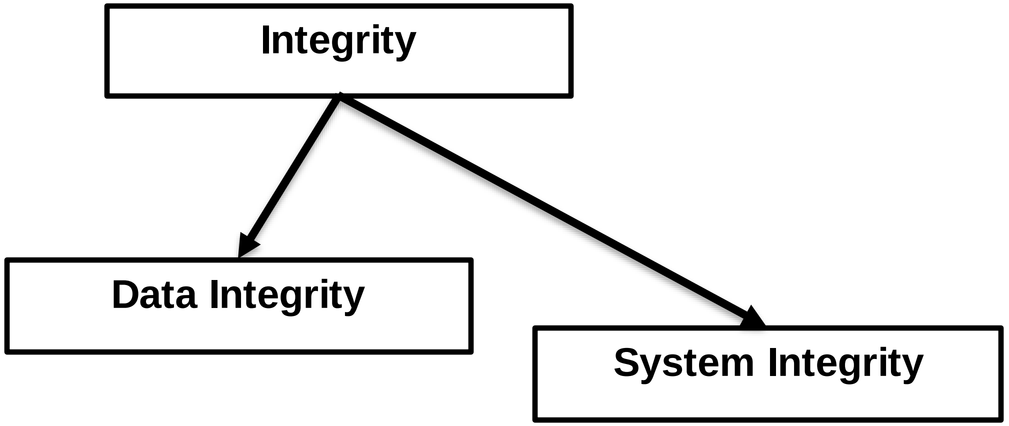
- **Data confidentiality**: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
- **Privacy**: protecting personal privacy and proprietary information.

Eavesdropping

The interception of information intended for someone else during its transmission over a communication channel.



Integrity



This term covers two related concepts:

- **Data integrity**:

  Assures that information (both stored and in transmitted) are changed only in a specified and authorized manner.

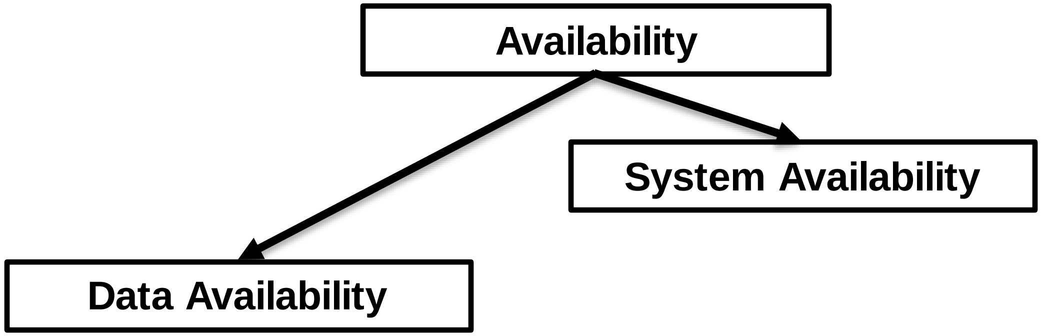
- **System integrity**:

  Assures that a system **performs its intended function** in an unimpaired manner towards preventing any unauthorized manipulation of the system.

Availability

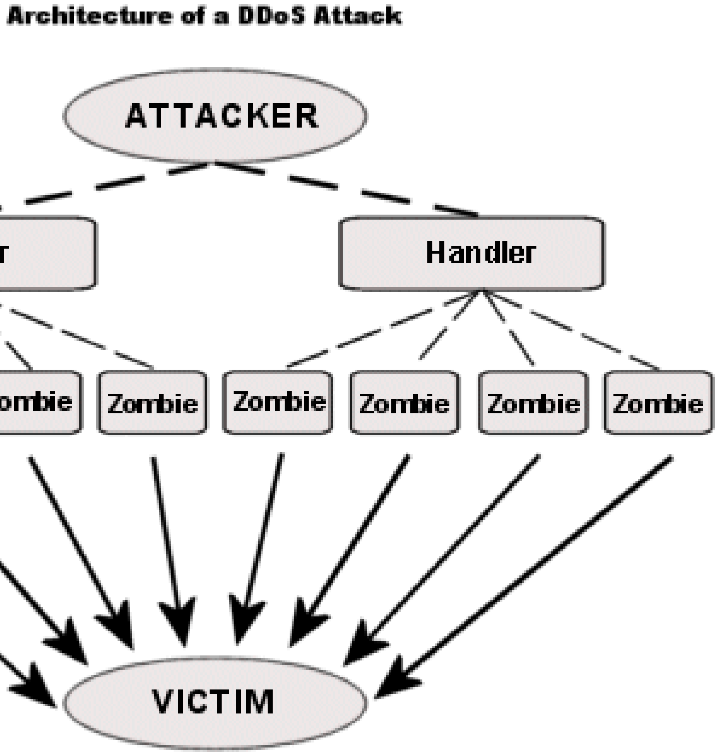
Assures that systems work promptly and service/data is not denied to authorized users.
This term covers two related concepts:

- ➢System Availability
- ➢Data Availability



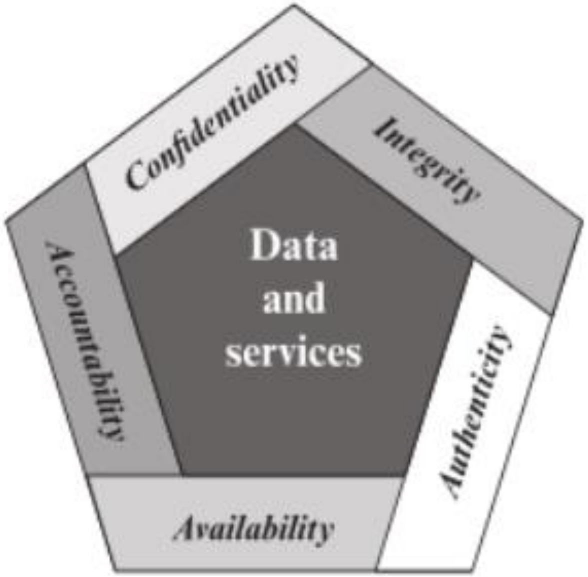
Denial of Service (DoS)

- In computing, a denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users.
- Distributed denial-of-service attacks are sent by two or more persons, or **bots**, and DoS attacks are sent by one person or system.



Other Security Concepts

Additional concepts are needed to present a complete picture.



- **Authenticity**:
  - **Entity Authentication**: verifying that users (or devices) are **who they say they are**.
  - **Data origin authentication**: and that each input arriving at the **system came from a trusted source**.

- **Accountability**: To be able **to trace a security breach to a responsible party**. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

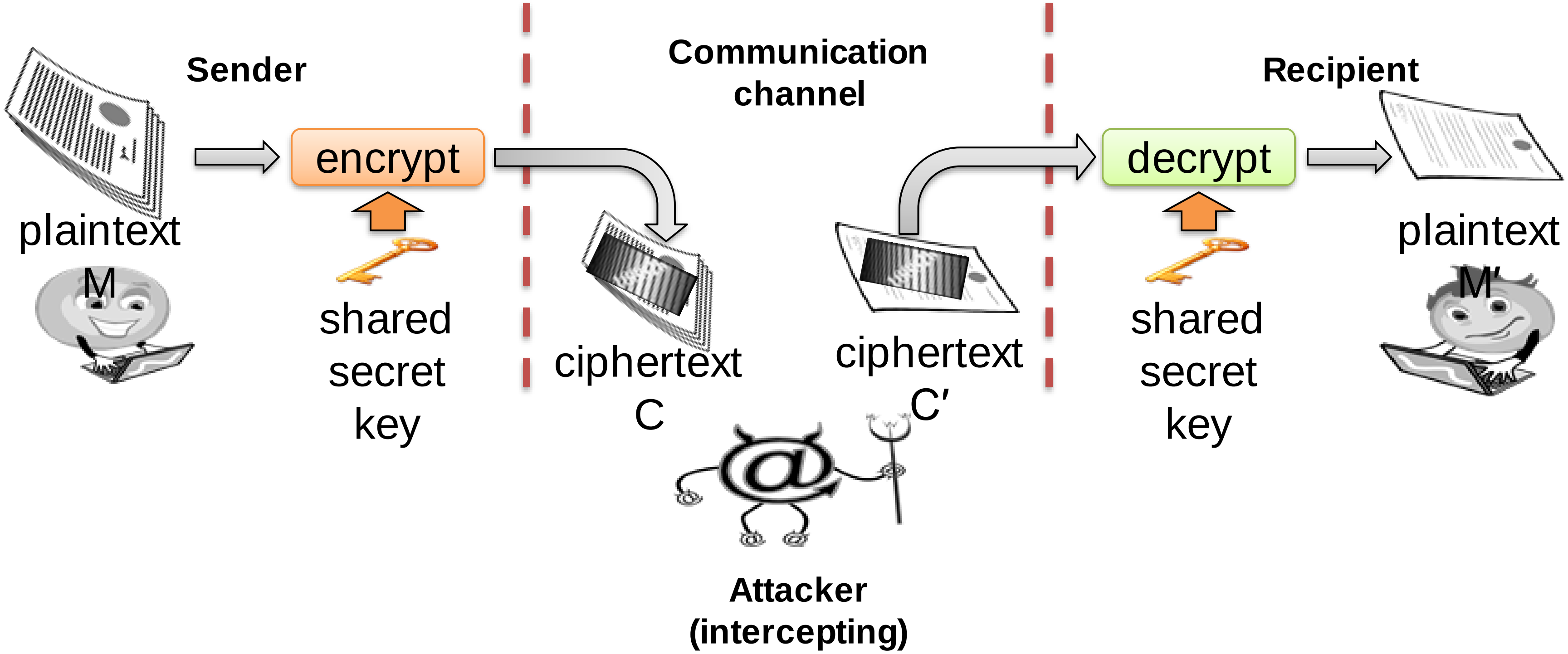
Masquerading:

- The fabrication of information that is purported to be from someone who is not actually the author.

“From: Alice”
(really is from Eve)

The **man-in-the-middle attack**

- **Example:** the **man-in-the-middle attack,** where a network stream is intercepted, modified, and retransmitted.



Repudiation

- The denial of a commitment or data receipt.

    - This involves an attempt to back out of a contract or a protocol that requires the different parties to provide receipts acknowledging that data has been received.

Public domain image from http://commons.wikimedia.org/wiki/File:Plastic_eraser.jpeg

Security Attacks

- **any action that compromises the security of information owned by an organization**
- We can classify attacks generically as:
  - Passive
  - Active

- information security is about how **to prevent attacks**, or failing that, **to detect attacks** on information-based systems
- **have a wide range of attacks**

Threat vs attack

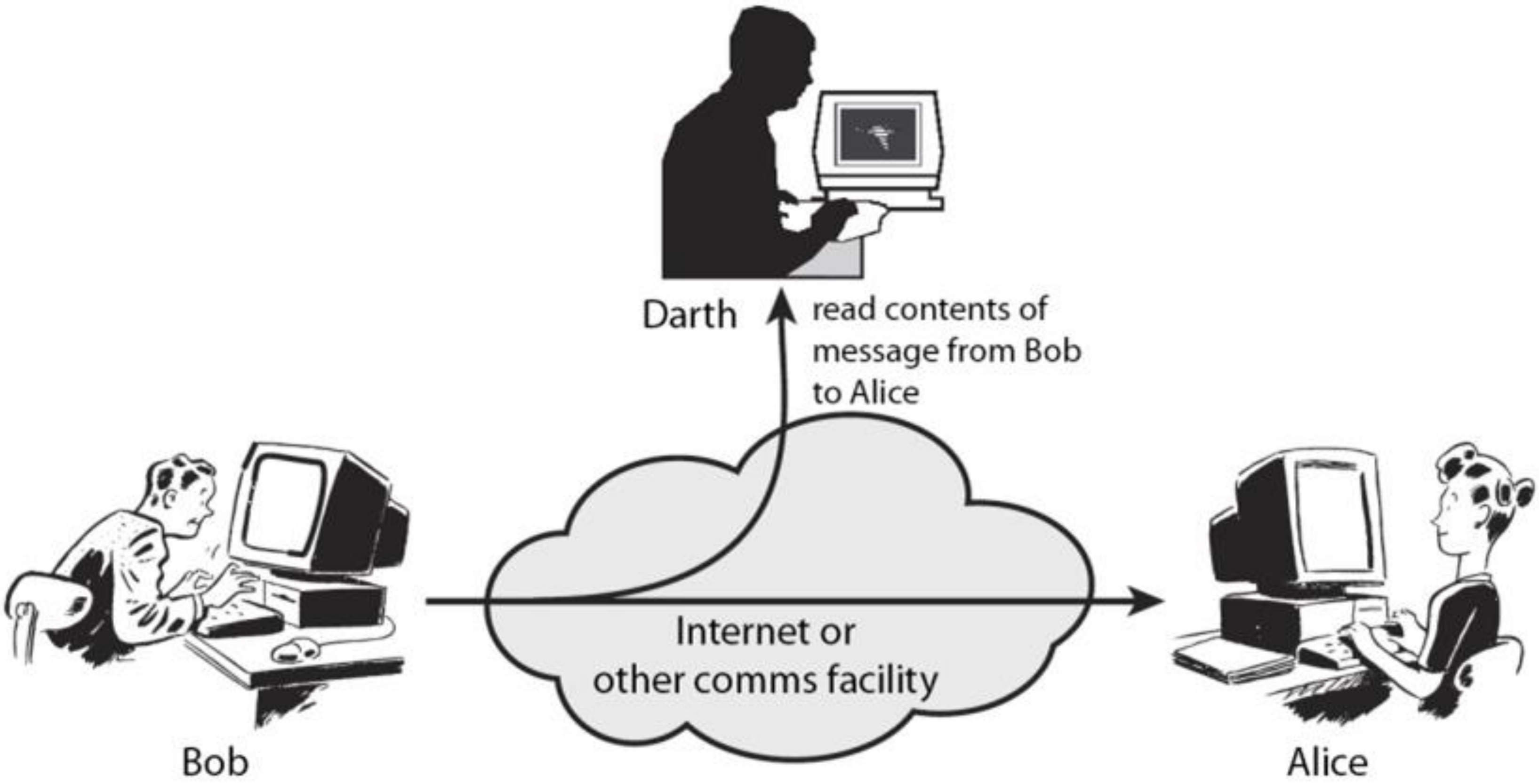
- Often threat & attack used to mean same thing
  - Threat is a potential for violation of security
  - Attack is an offensive on system security that derives from an intelligent threat.

    - **Attack=Threat + Vulnerability**

Passive Attacks

- They are in the nature of **eavesdropping** on or **monitoring of transmissions**
- Two types of passive attacks:
  - are release of message
  - and traffic analysis
- Passive attacks **are difficult to detect** because they do not alter the data.

Passive Attacks


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

- **To prevent the success of such attacks, usually encryption is used**.

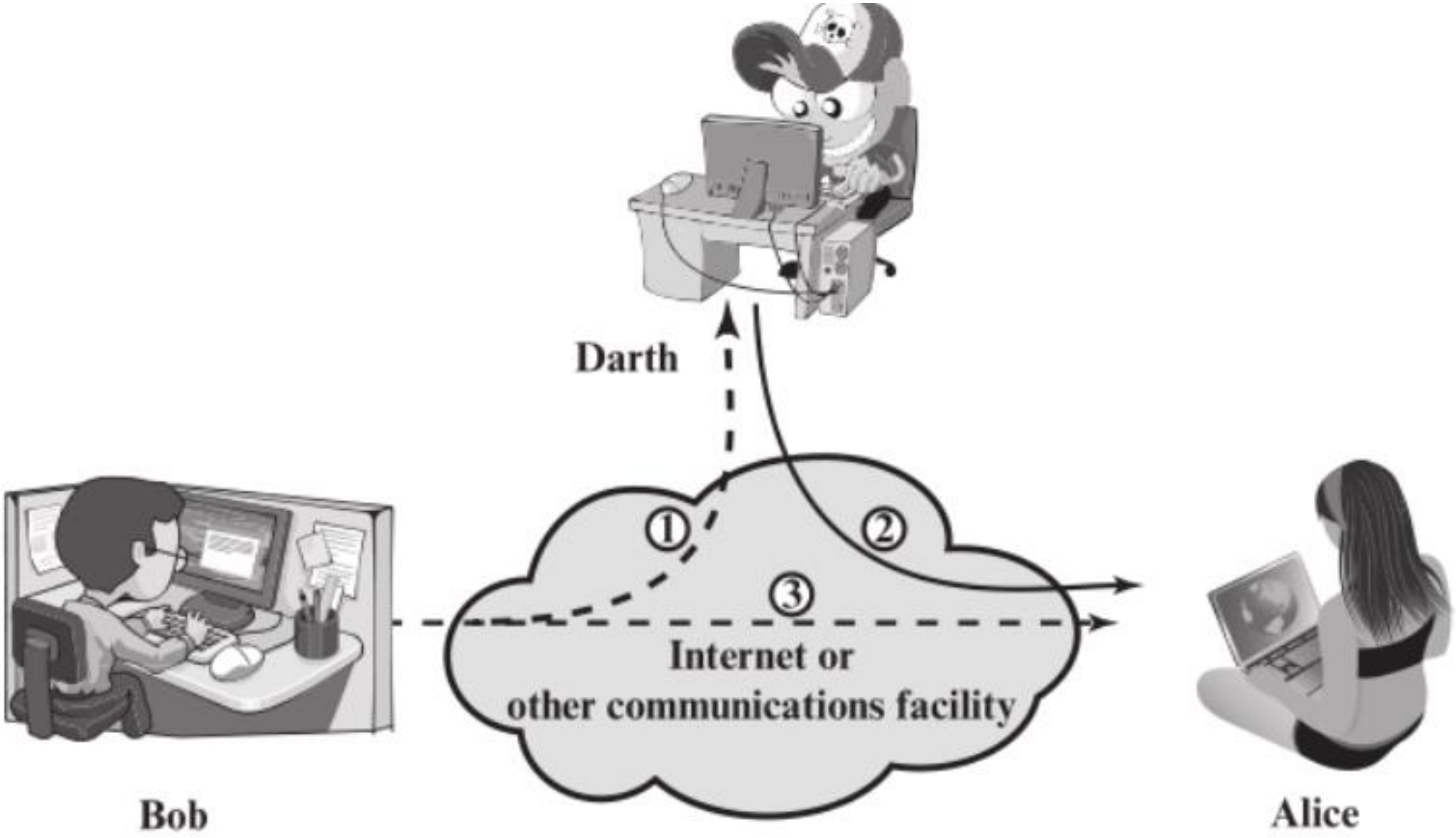
Active Attacks

- They involve alteration of the data stream or the creation of a false stream.
- They can be subdivided into 4 categories:
  - **Masquerade** takes place when one entity pretends to be a different entity
  - **Replay** is the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
  - Modification of messages
  - **Denial of service** prevents the normal use or management of communications facilities
    - Suppress all messages directed to a destination
    - Overloading the network with messages to degrade its performance

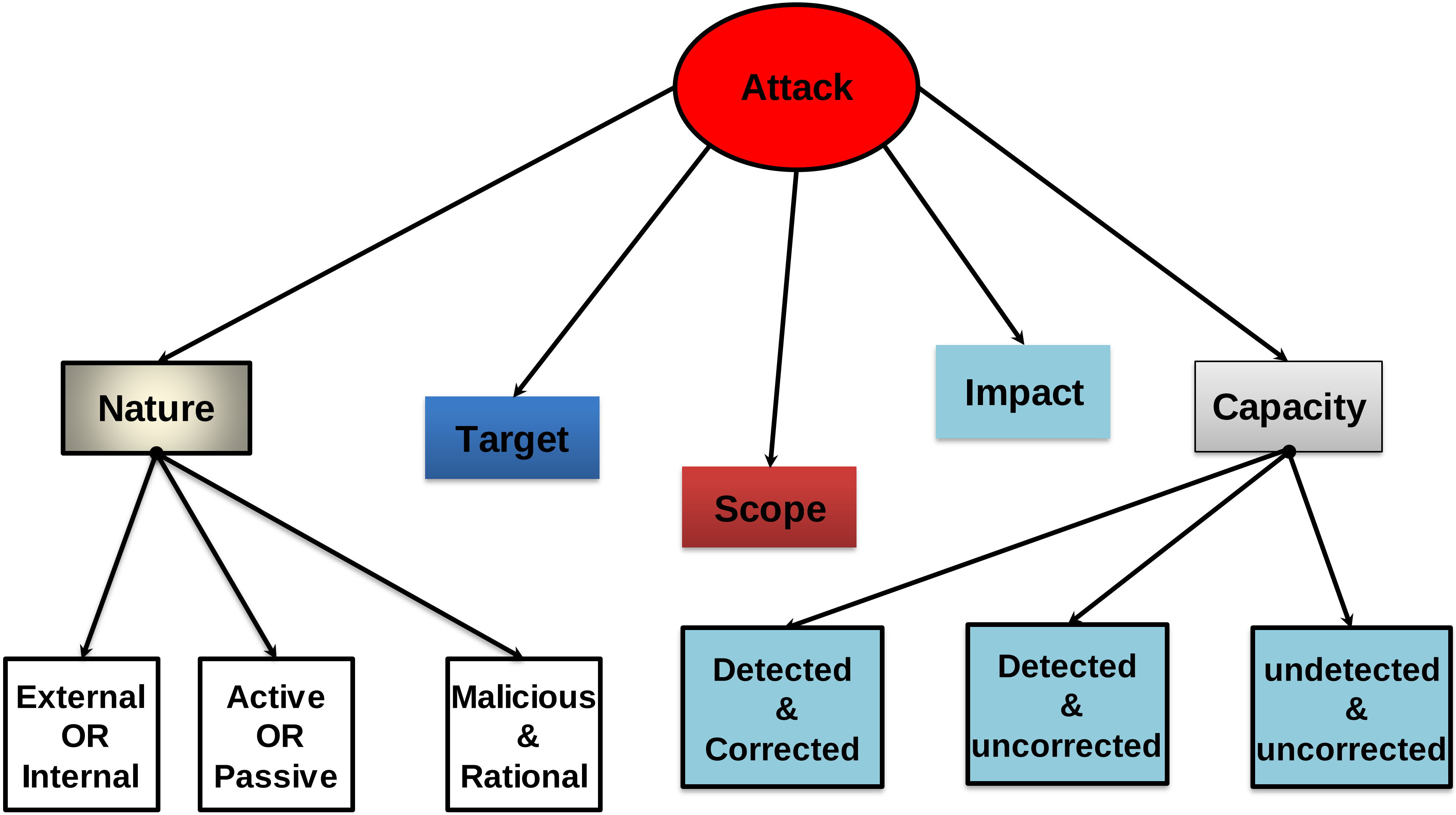
Active Attacks

- **It is difficult to prevent active attacks absolutely because of the wide variety of potential physical, software, and network vulnerabilities.**
- It is important to detect active attacks and to recover from them.

Active Attacks



Attacks profile and characteristics



Impact of security violations

- Three levels of impact on organizations or individuals can be quantified after a breach of security (i.e., a loss of confidentiality, integrity, or availability) :

1) **Low**:

The loss could be expected to have a limited effect on:

a) operations;
b) assets;
c) or Individuals.

2) Moderate:

The loss could be expected to have a serious effect.

3) **High**:

The loss could be expected to have a catastrophic effect.

Tools for Peer Entity Authentication

- **Peer Entity Authentication:** the determination of the identity or role that someone has.
- This determination can be done in a number of different ways, but it is usually based on a combination of
  - something **the person has** (like a smart card or a radio key fob storing secret keys),
  - something **the person knows** (like a password),
  - something **the person is** (like a human with a fingerprint).

human with fingers and eyes

Something you are

password=uclb()w1V
mother=Jones
father=Caesar

Something you know

radio token with secret keys

Something you have

Tools for Data-Origin Authenticity

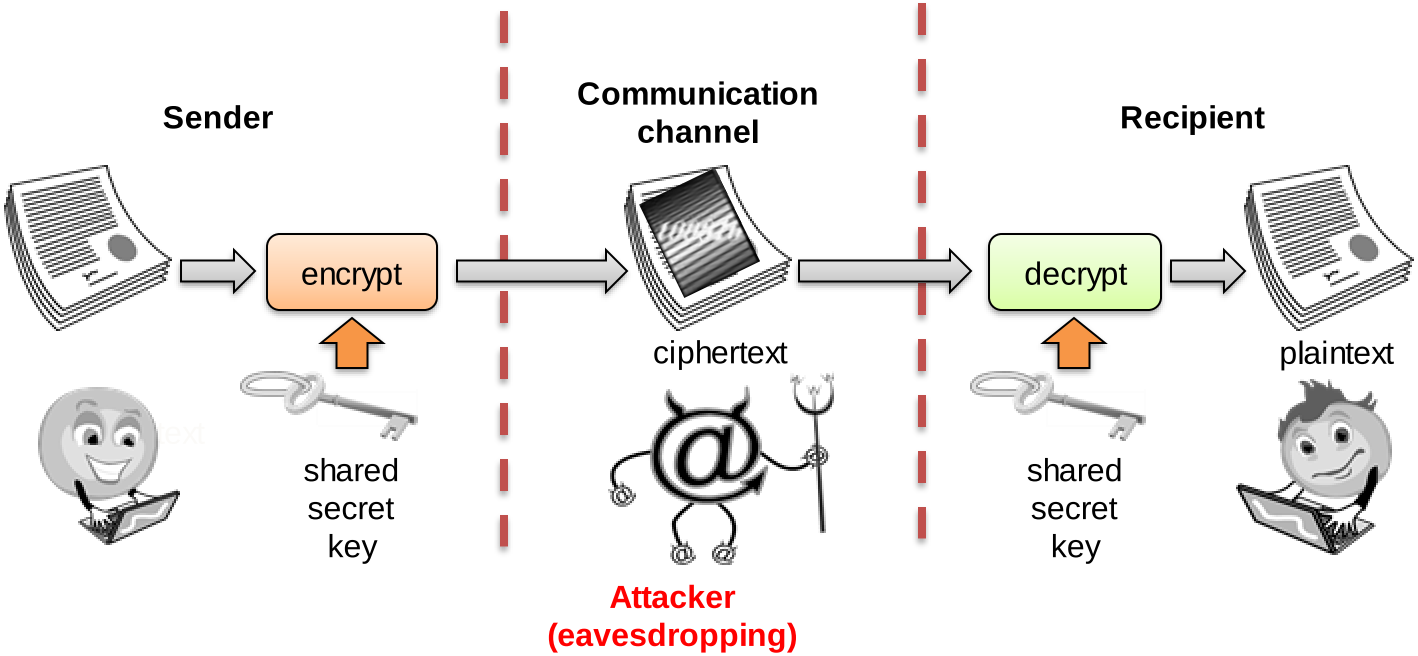
- **Data-Origin Authentication**
  - In a connectionless transfer, provides assurance that the source of received data is as claimed.
  - **Tools : Keyed hash function and Digital signatures**.

Authorization

- **Authorization:** the determination if a person or system is allowed access to resources, **based on an access control scheme**.
  - **Access control:** rules and policies that limit access to confidential information to those people and/or systems with a “need to know.”
  - This need to know may be **determined by identity (authentication)**, such as a person’s name or a computer’s serial number, or by a role that a person has, such as being a manager or a computer security specialist.
  - Such **authorizations should prevent an attacker from tricking the system into letting him have access to protected resources**.

Tools for Confidentiality

- **Encryption:** the transformation of information using a secret, called an encryption key, so that the transformed information can only be read using another secret, called the decryption key (which may, in some cases, be the same as the encryption key).



Sender

Communication channel

Recipient

encrypt

decrypt

ciphertext

plaintext

shared secret key

shared secret key

Attacker (eavesdropping)

Tools for Data Integrity

- **Integrity:** the property that information has not be altered in an unauthorized way.

- **Tools:**

  - **Checksums:** the computation of a function that maps the contents of a file to a numerical value. A checksum function depends on the entire contents of a file and is designed in a way that even a small change to the input file (such as flipping a single bit) is highly likely to result in a different output value.

  - **Data correcting codes:** methods for storing data in such a way that small changes can be easily detected and automatically corrected.

  - **Cryptographic Hash function (secure one)**

Tools for Availability

- **Availability:** the property that information is accessible and modifiable in a timely fashion by those authorized to do so.

- **Tools:**

  - **Backups:** the periodic archiving of data.

  - **Physical protections:** infrastructure meant to keep information available even in the event of physical challenges.

  - **Computational redundancies:** computers and storage devices that serve as fallbacks in the case of failures.