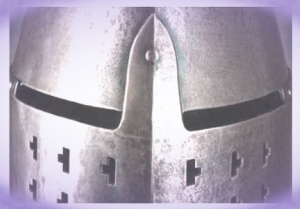
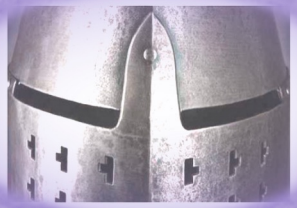


Cryptography and Network Security

Eighth Edition
by William Stallings



Chapter 1

Information and Network Security Concepts

Cybersecurity

Cybersecurity *is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyberspace environment and organization and users' assets. Organization and users' assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyberspace environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and users' assets against relevant security risks in the cyberspace environment. The general security objectives comprise the following: availability; integrity, which may include data authenticity and nonrepudiation; and confidentiality*

Cybersecurity

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

Network Security

- This term refers to protection of networks and their service from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side effects

Security Objectives (CIA Triad)

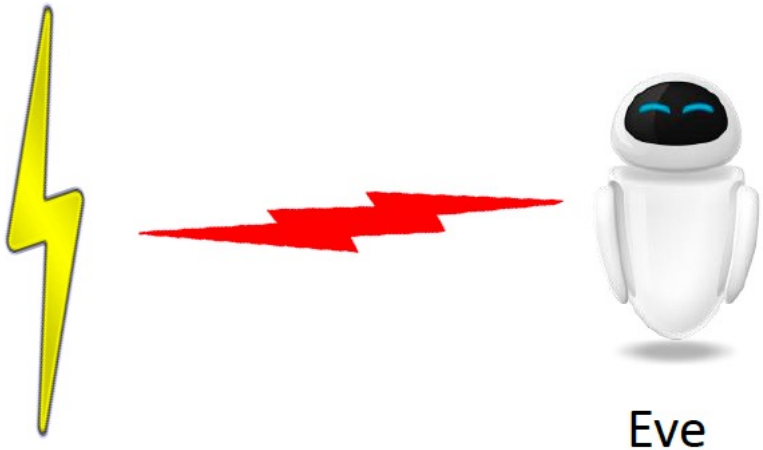
- The cybersecurity definition introduces three key objectives that are at the heart of information and network security:
  - **Confidentiality:** This term covers two related concepts:
    - **Data confidentiality:** Assures that private or confidential information is not made available or disclosed 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 and programs are changed only in a specified and authorized manner. This concept also encompasses data authenticity, which means that a digital object is indeed what it claims to be or what it is claimed to be, and nonrepudiation, which is assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information
  - **System integrity**: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system
- **Availability:** Assures that systems work promptly and service is not denied to authorized users

Confidentiality (example)

"JFK Airport Wifi"



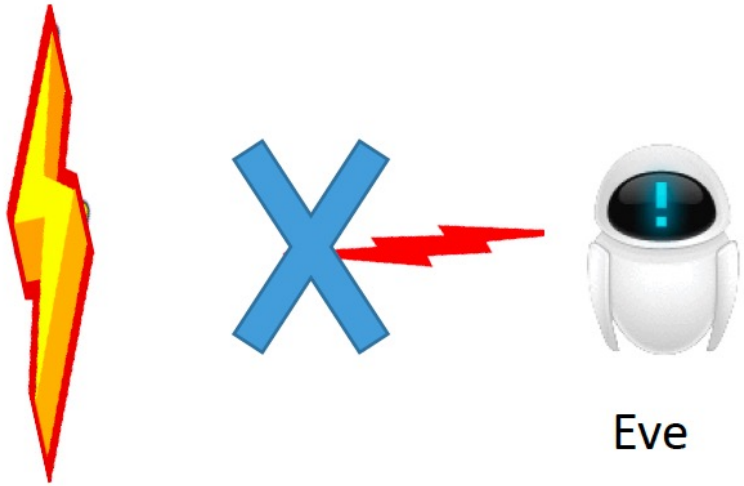
Eve

Alice's laptop

- If Alice's connection to "JFK Airport Wifi" is not secured, Eve can eavesdrop!
- How do we prevent this?

Confidentiality (example)

"JFK Airport Wifi"



Eve

Alice's laptop

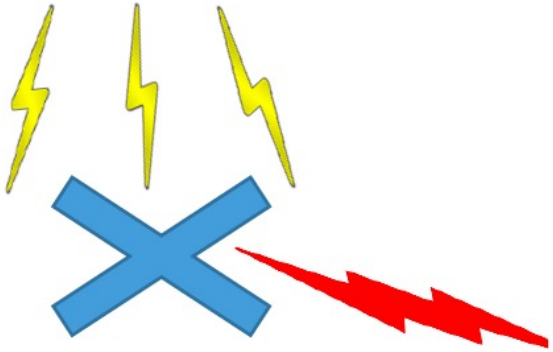
- Only use encrypted wireless channels!
- WPA2 is the current standard

Integrity (example)

- What if "JFK Airport Wifi" isn't who you think it is?
- How can this type of "man in the middle attack" be prevented?

Availability (example)

"JFK Airport Wifi"



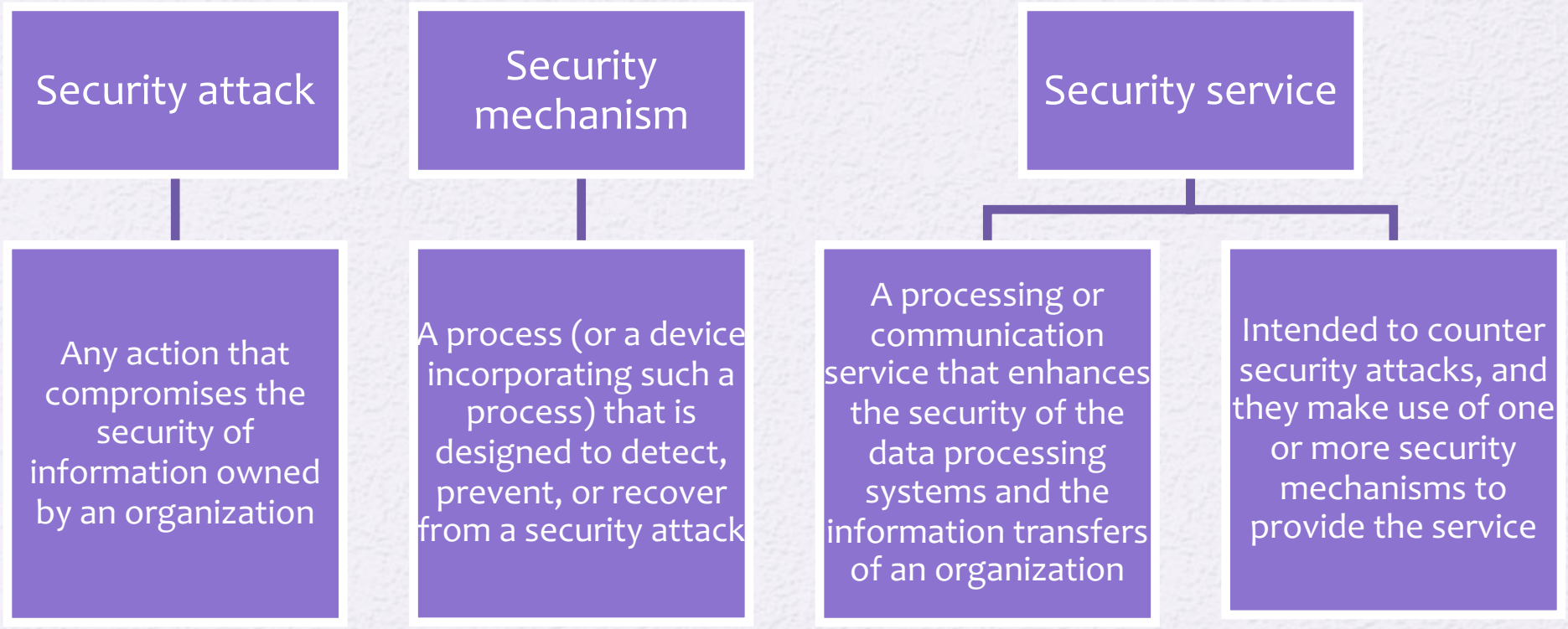
Eve

Alice's laptop

- With a strong wireless signal, Eve can jam legitimate signals in a denial of service (DoS) attack.
- How do we mitigate such an attack?

Eve image courtesy of the Disney Wiki: http://disney.wikia.com/wiki/The_Disney_Wiki

OSI Security Architecture



Threats and Attacks

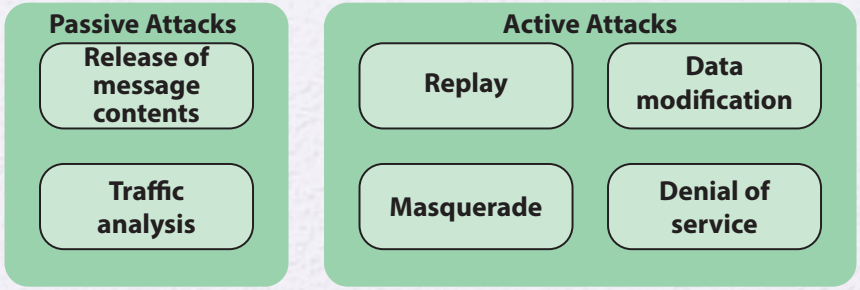
Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

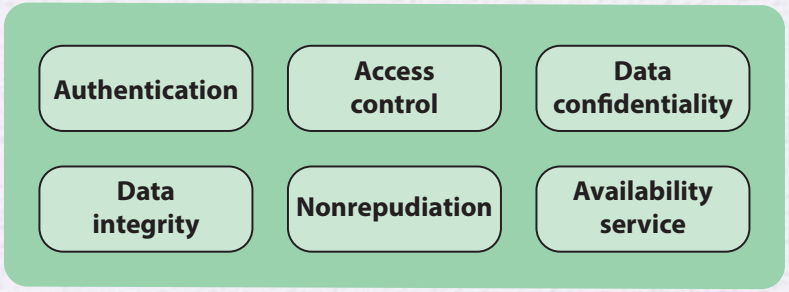
Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

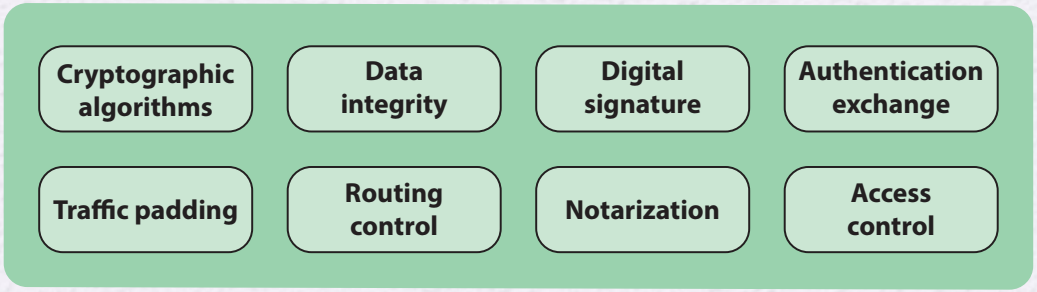
OSI security architecture



(a) Attacks



(b) Services



(c) Mechanisms

Figure 1.2 Key Concepts in Security

Security Attacks

- A means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of *passive attacks* and *active attacks*
- A *passive attack* attempts to learn or make use of information from the system but does not affect system resources
- An *active attack* attempts to alter system resources or affect their operation

Passive Attacks

- Are in the nature of eavesdropping on, or monitoring of, transmissions
- Goal of the opponent is to obtain information that is being transmitted

- Two types of passive attacks are:
  - The release of message contents
  - Traffic analysis

Active Attacks

- Involve some modification of the data stream or the creation of a false stream
- Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
- Goal is to detect attacks and to recover from any disruption or delays caused by them

Masquerade

- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack

Replay

- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

Data Modification

- Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect

Denial of service

- Prevents or inhibits the normal use or management of communications facilities

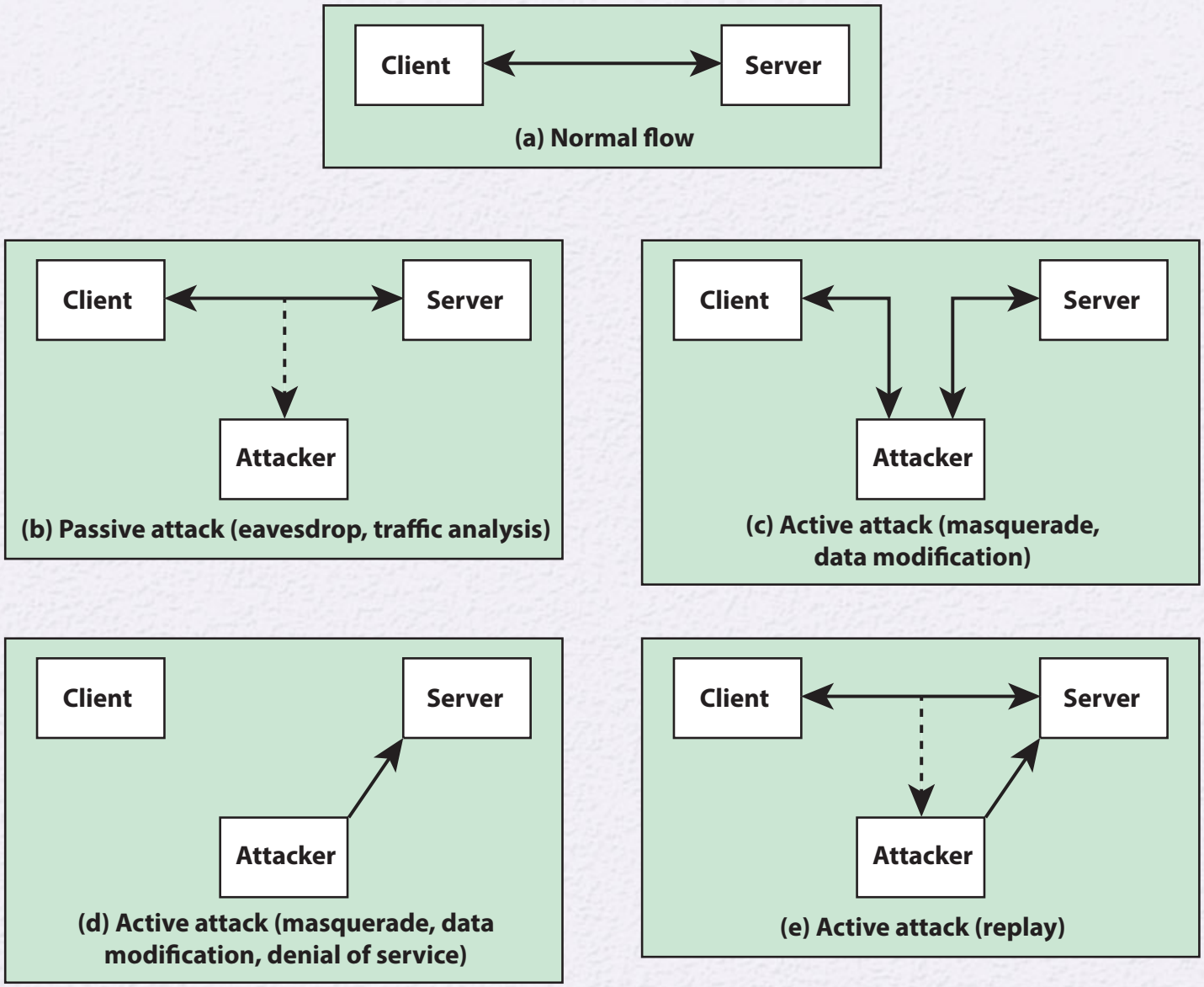


Figure 1.3 Security Attacks

Passive Attack

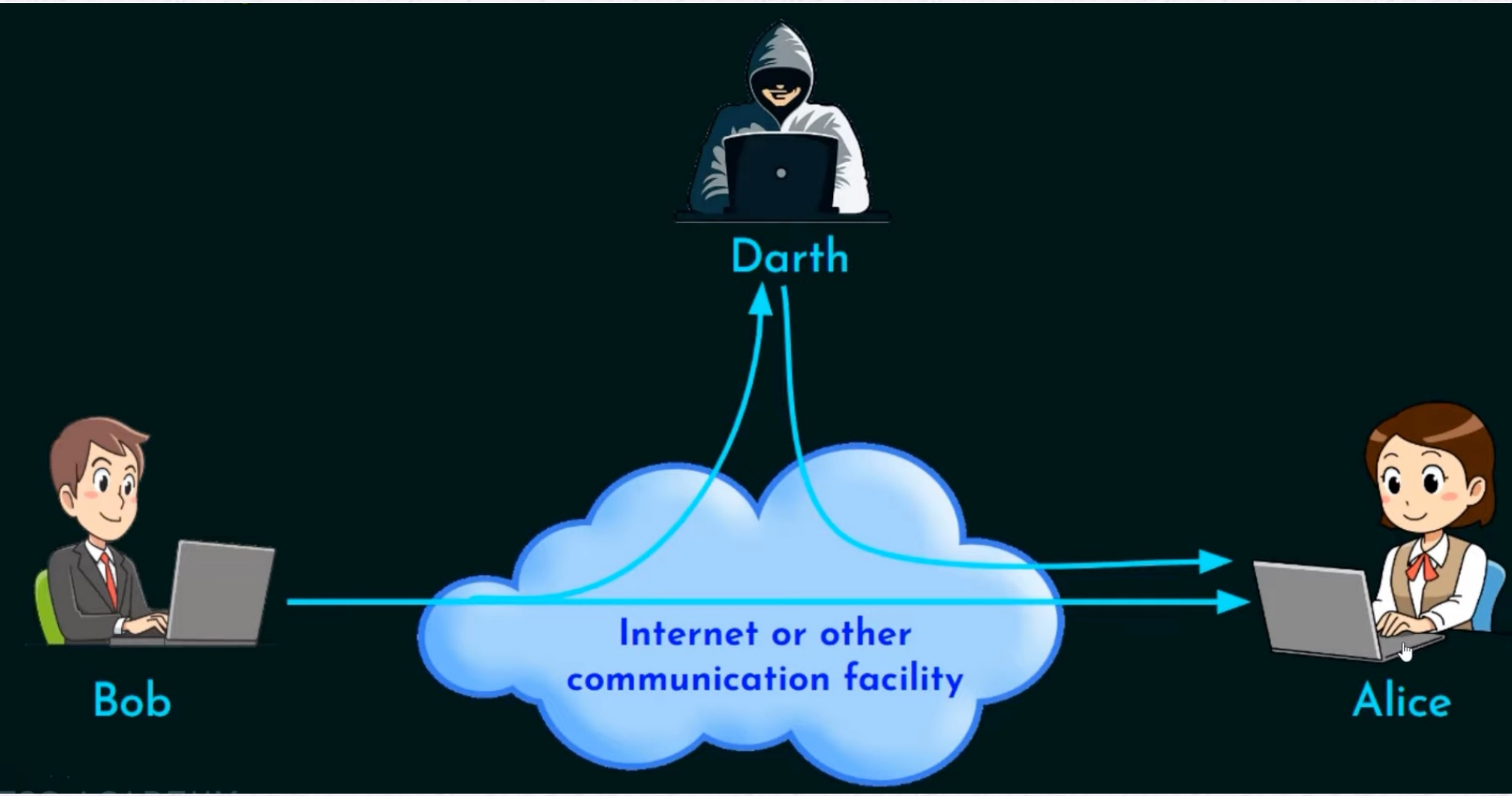
- ★ Hard to Detect.
- ★ Neither sender nor receiver is aware of the attack.
- ★ Encryption prevents the success of the passive attacks.
- ★ More emphasis is on prevention than detection.

Active Attack

- ★ Hard to Prevent.
- ★ Difficult to prevent - Physical, software and network vulnerabilities.
- ★ Detect and recover from any disruption or delays.
- ★ If the detection has a deterrent effect, it may also contribute to prevention.

What is Authentication?

- Authentication
  - Binding of identity to subject
- How do we do it?
  - Entity *knows* something (secret)
    - Passwords, id numbers
  - Entity *has* something
    - Duo mobile, smart card, hand-held tokens
  - Entity *is* something
    - Biometrics: fingerprints or retinal characteristics
  - Entity is in *someplace*
    - Source IP, restricted area terminal

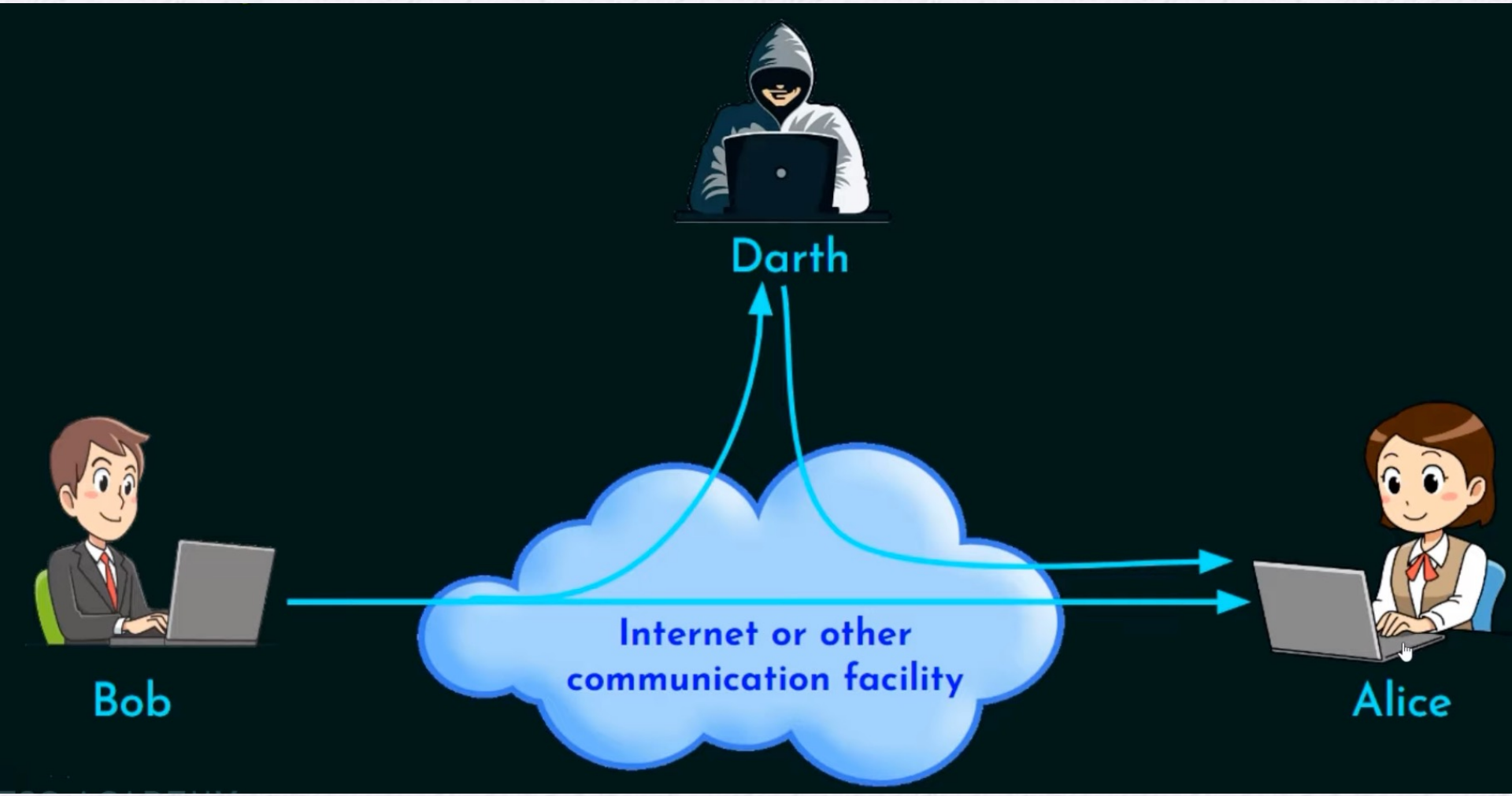


Access Control

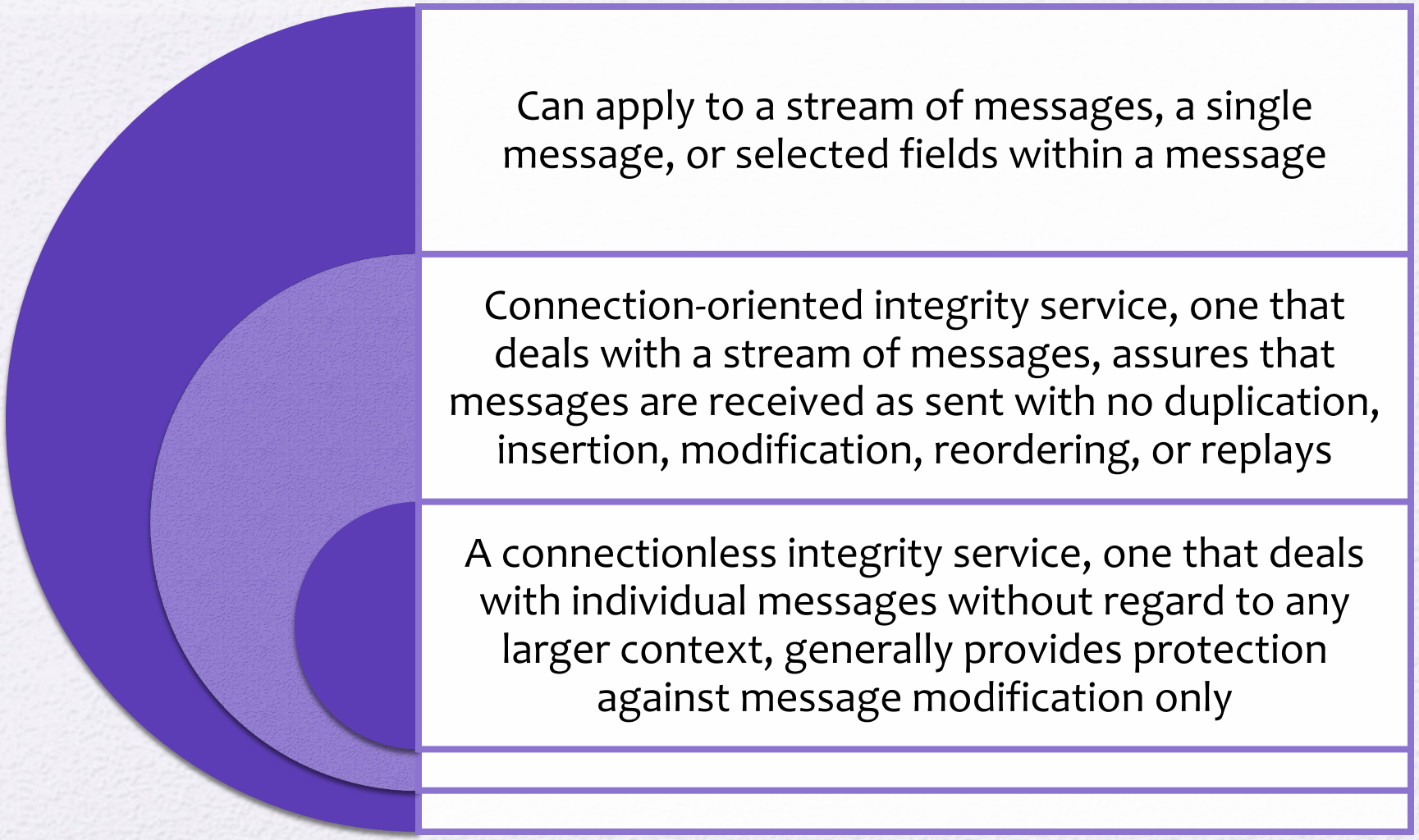
- Control access to data, executables, hardware
- Subjects [do-ers] and objects [do-ees]
  - Subjects often defined by user and group membership
  - Objects have owners and access control lists (ACL)
- Enforced by security kernel/reference monitor
  - Sometimes by an application (e.g. database system)
- Mandatory access controls (MAC)
- Discretionary access controls (DAC)
- Role-based access controls (RBAC)

Data Confidentiality

- The protection of transmitted data from passive attacks
  - Broadest service protects all user data transmitted between two users over a period of time
  - Narrower forms of service includes the protection of a single message or even specific fields within a message
- The protection of traffic flow from analysis
  - This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility



Data Integrity



Nonrepudiation

- Prevents either sender or receiver from denying a transmitted message

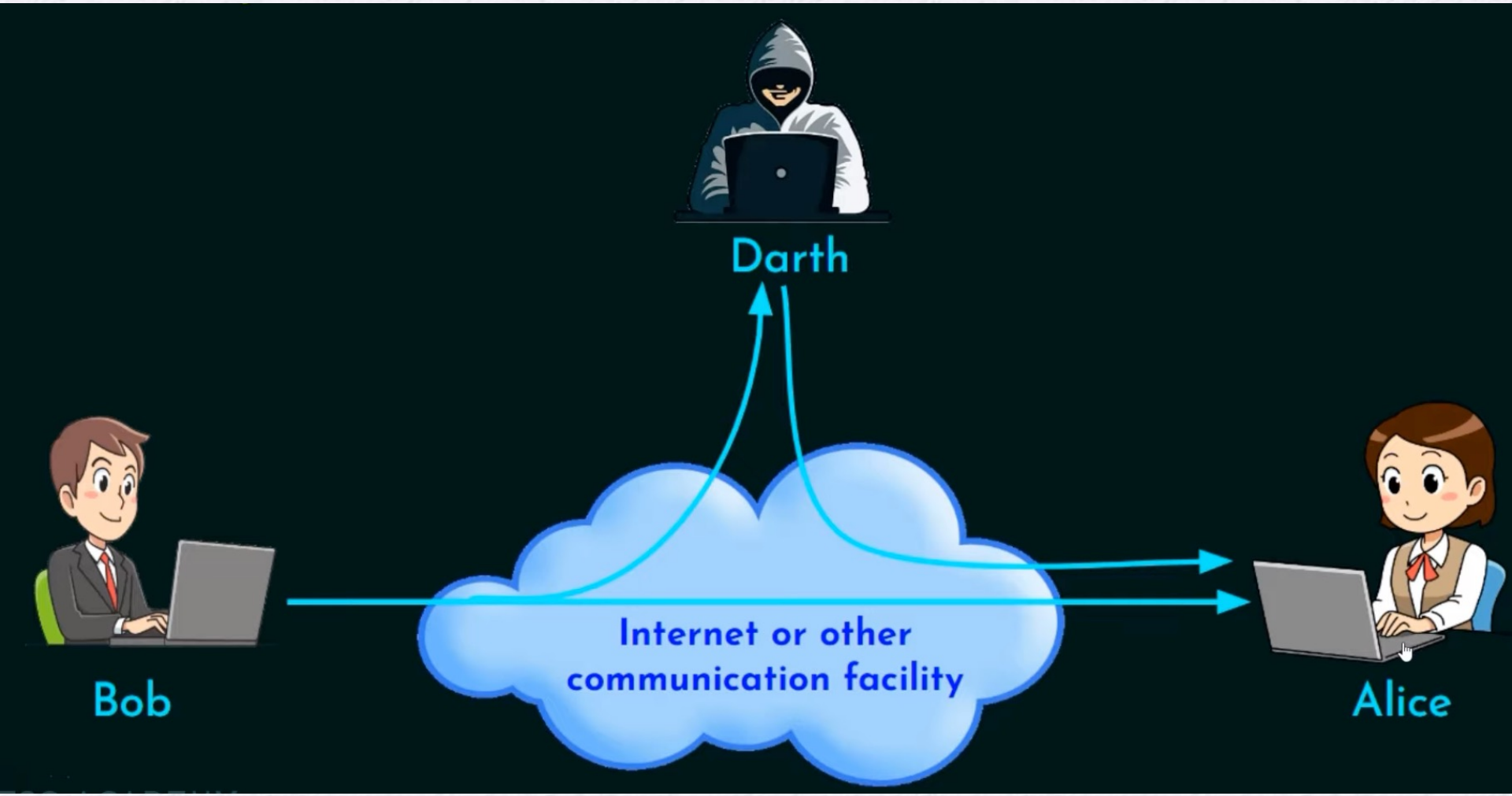
- When a message is sent, the receiver can prove that the alleged sender in fact sent the message
- When a message is received, the sender can prove that the alleged receiver in fact received the message

Availability Service

- Protects a system to ensure its availability
- This service addresses the security concerns raised by denial-of-service attacks
- It depends on proper management and control of system resources and thus depends on access control service and other security services

Security Mechanisms

- **Cryptographic algorithms:** We can distinguish between reversible cryptographic mechanisms and irreversible cryptographic mechanisms. A reversible cryptographic mechanism is simply an encryption algorithm that allows data to be encrypted and subsequently decrypted. Irreversible cryptographic mechanisms include hash algorithms and message authentication codes, which are used in digital signature and message authentication applications.
- **Digital signature:** Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.
- **Access control:** A variety of mechanisms that enforce access rights to resources.
- **Data integrity:** This category covers 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.
- **Routing control:** Enables selection of particular physically or logically 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



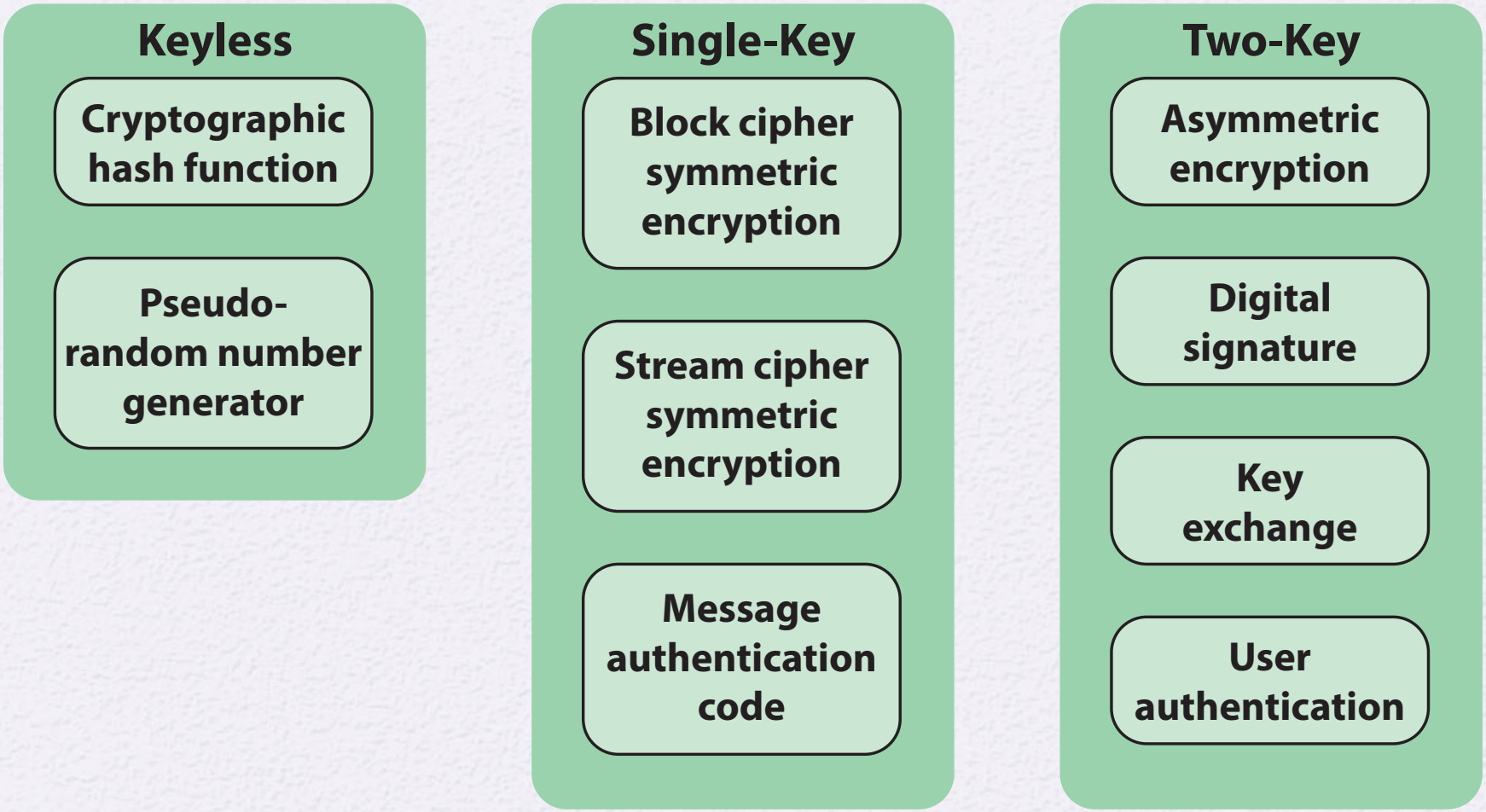
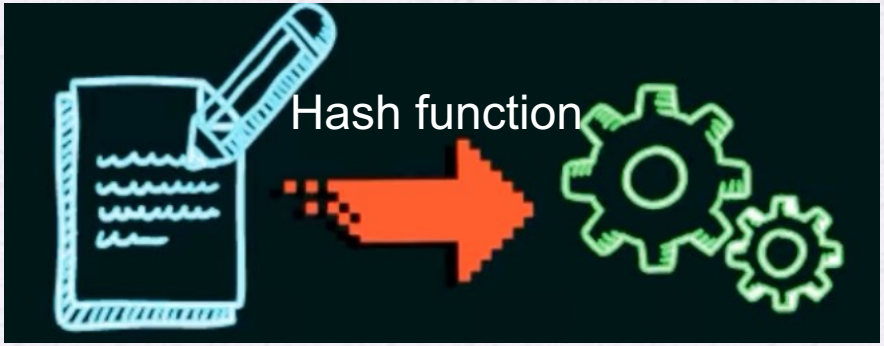


Figure 1.4 Cryptographic Algorithms

Keyless Algorithms

- Deterministic functions that have certain properties useful for cryptography
- One type of keyless algorithm is the cryptographic hash function
  - A hash function turns a variable amount of text into a small, fixed-length value called a *hash value, hash code, or digest*
  - 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

Keyless Algorithms



Plain text

Hash value, hash code, or digest: A small, fixed-length value called a

Single-Key Algorithms

Single-key cryptographic algorithms depend on the use of a secret key

Encryption algorithms that use a single key are referred to as *symmetric encryption algorithms*

With symmetric encryption, an encryption algorithm takes as input some data to be protected and a secret key and produces an unintelligible transformation on that data

A corresponding decryption algorithm takes the transformed data and the same secret key and recovers the original data

Symmetric encryption takes the following forms:

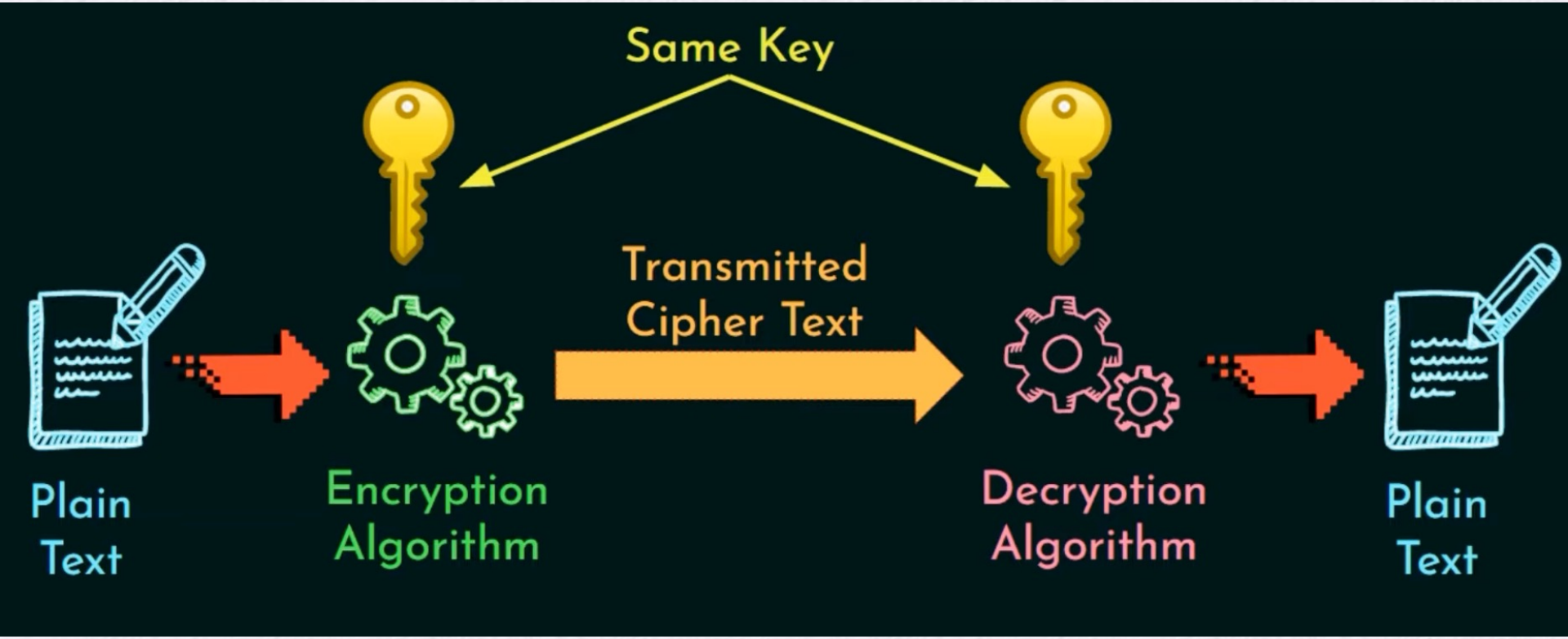
Block cipher

- A block cipher operates on data as a sequence of blocks
- In most versions of the block cipher, known as modes of operation, the transformation depends not only on the current data block and the secret key but also on the content of preceding blocks

Stream cipher

- A stream cipher operates on data as a sequence of bits
- As with the block cipher, the transformation depends on a secret key

Symmetric Encryption

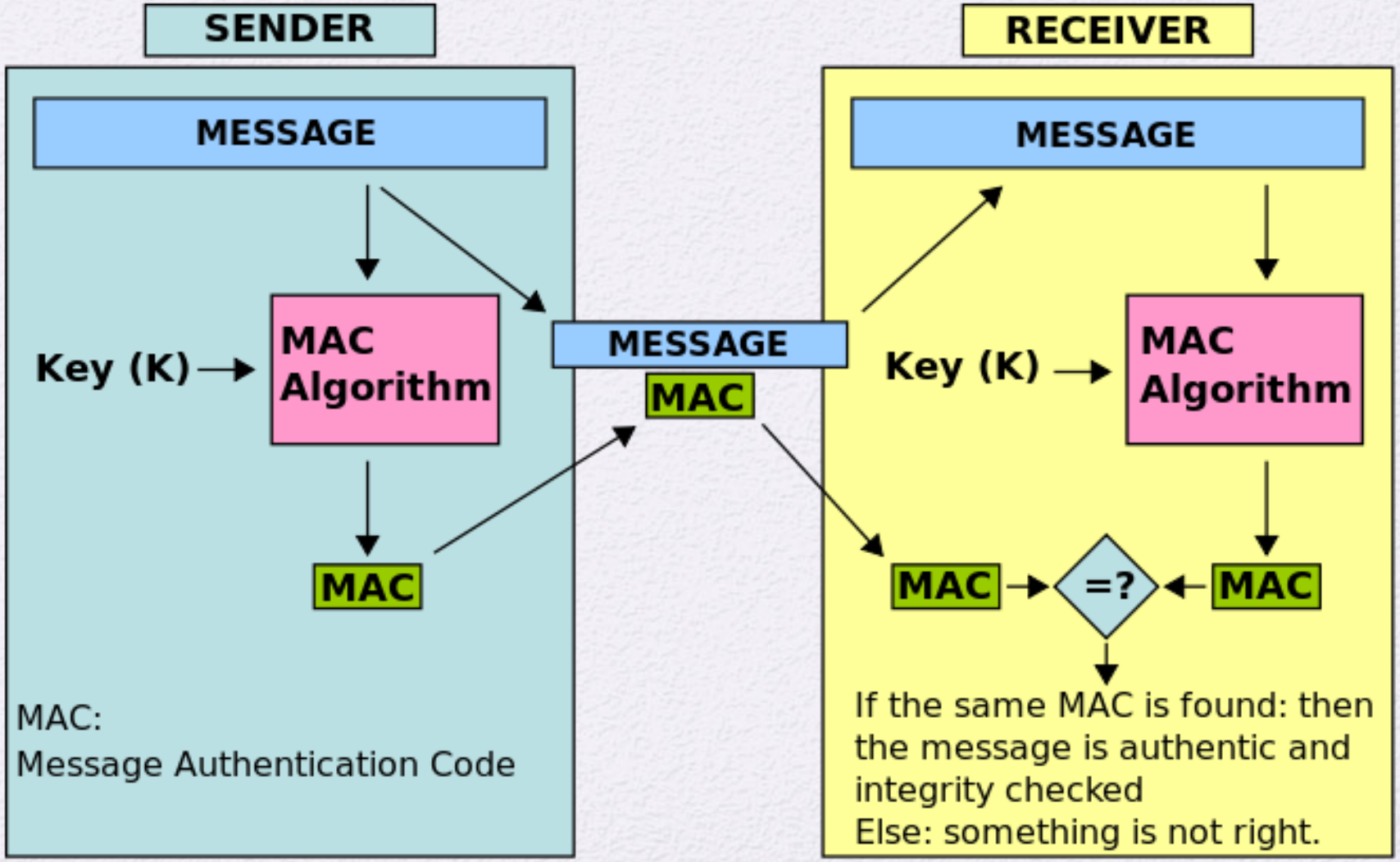


Single-Key Algorithms

Another form of single-key cryptographic algorithm is the *message authentication code (MAC)*

- A MAC is a data element associated with a data block or message
- The MAC is generated by a cryptographic transformation involving a secret key and, typically, a cryptographic hash function of the message
- The MAC is designed so that someone in possession of the secret key can verify the integrity of the message
- The recipient of the message plus the MAC can perform the same calculation on the message; if the calculated MAC matches the MAC accompanying the message, this provides assurance that the message has not been altered

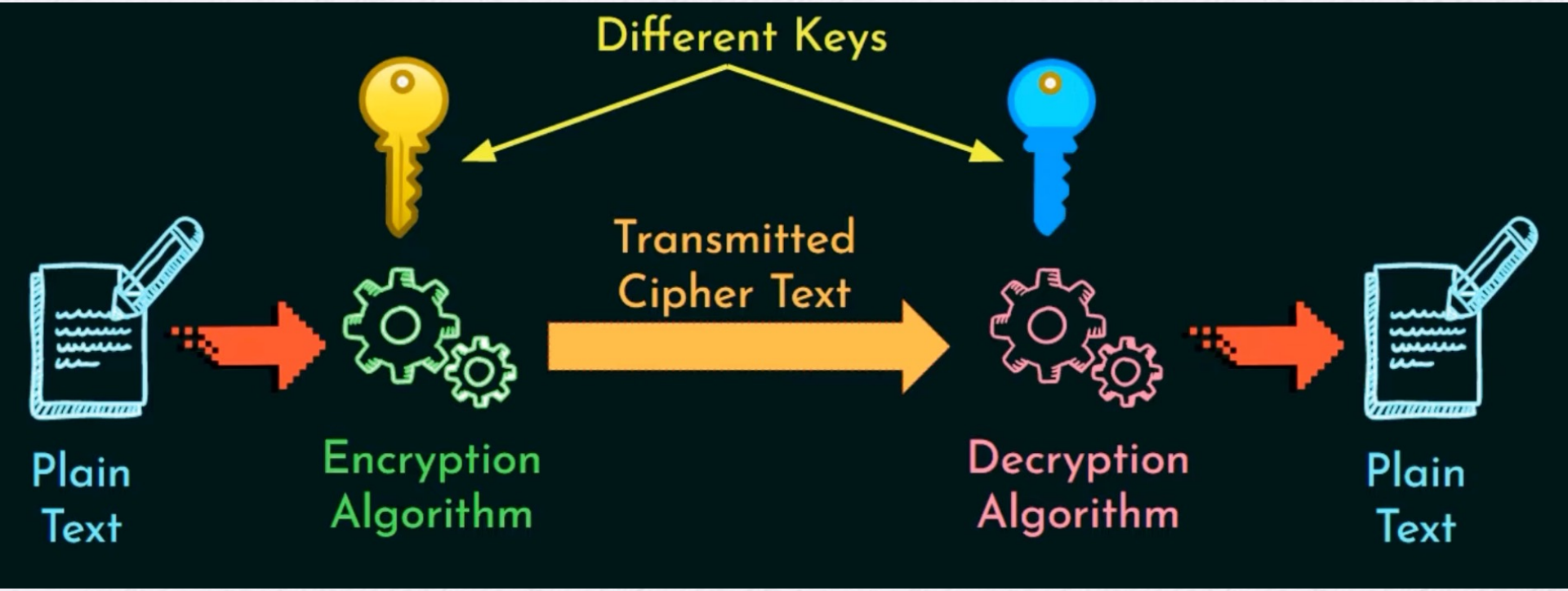
Message authentication code



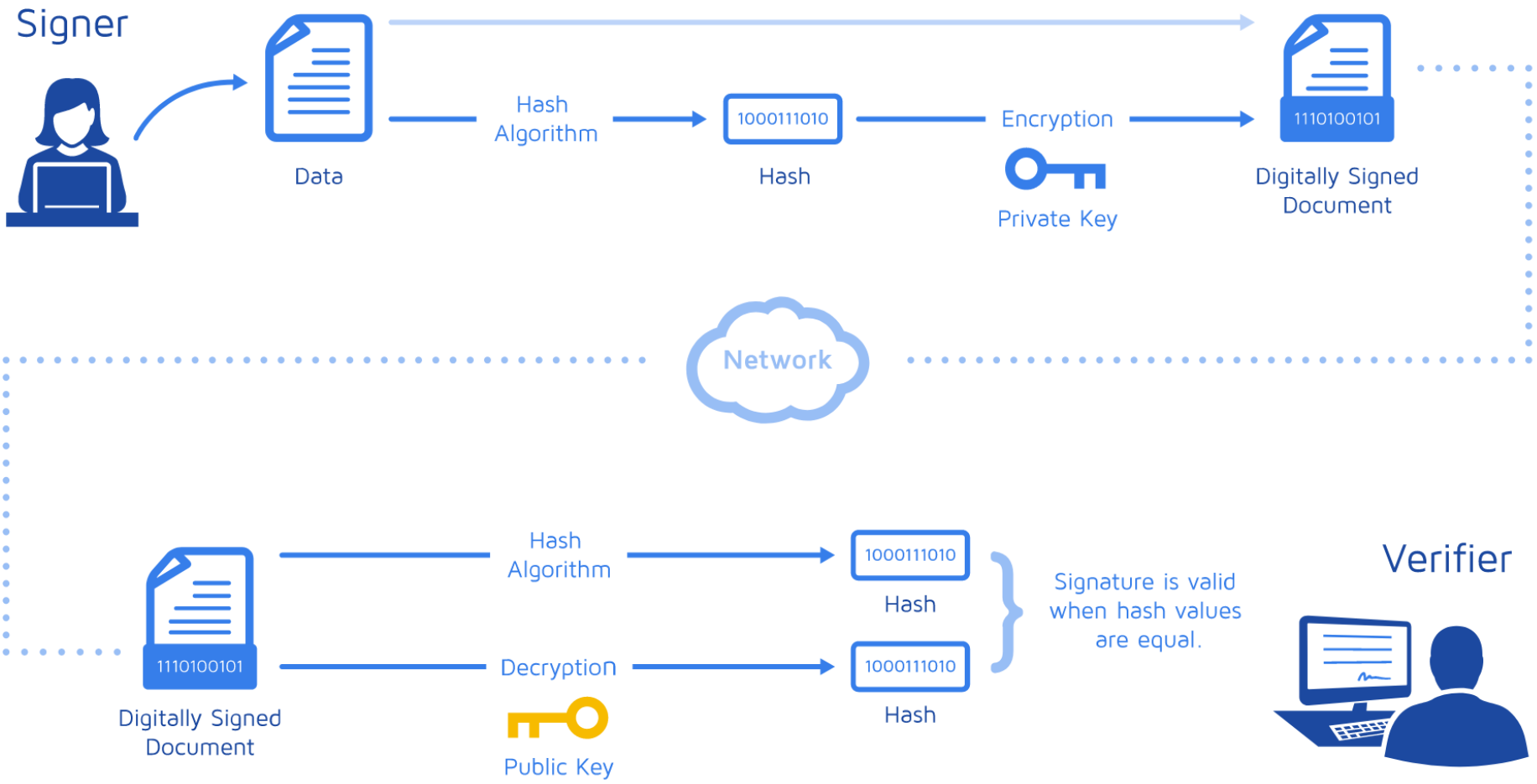
Two-key Algorithms

- Encryption algorithms that use two different keys are referred to as *asymmetric encryption algorithms*
- Digital signature algorithm
  - 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
  - The process of securely distributing a symmetric key to two or more parties
- User authentication
  - The process of authenticating that a user attempting to access an application or service is genuine and, similarly, that the application or service is genuine

Asymmetric Encryption



Digital Signature Algorithms



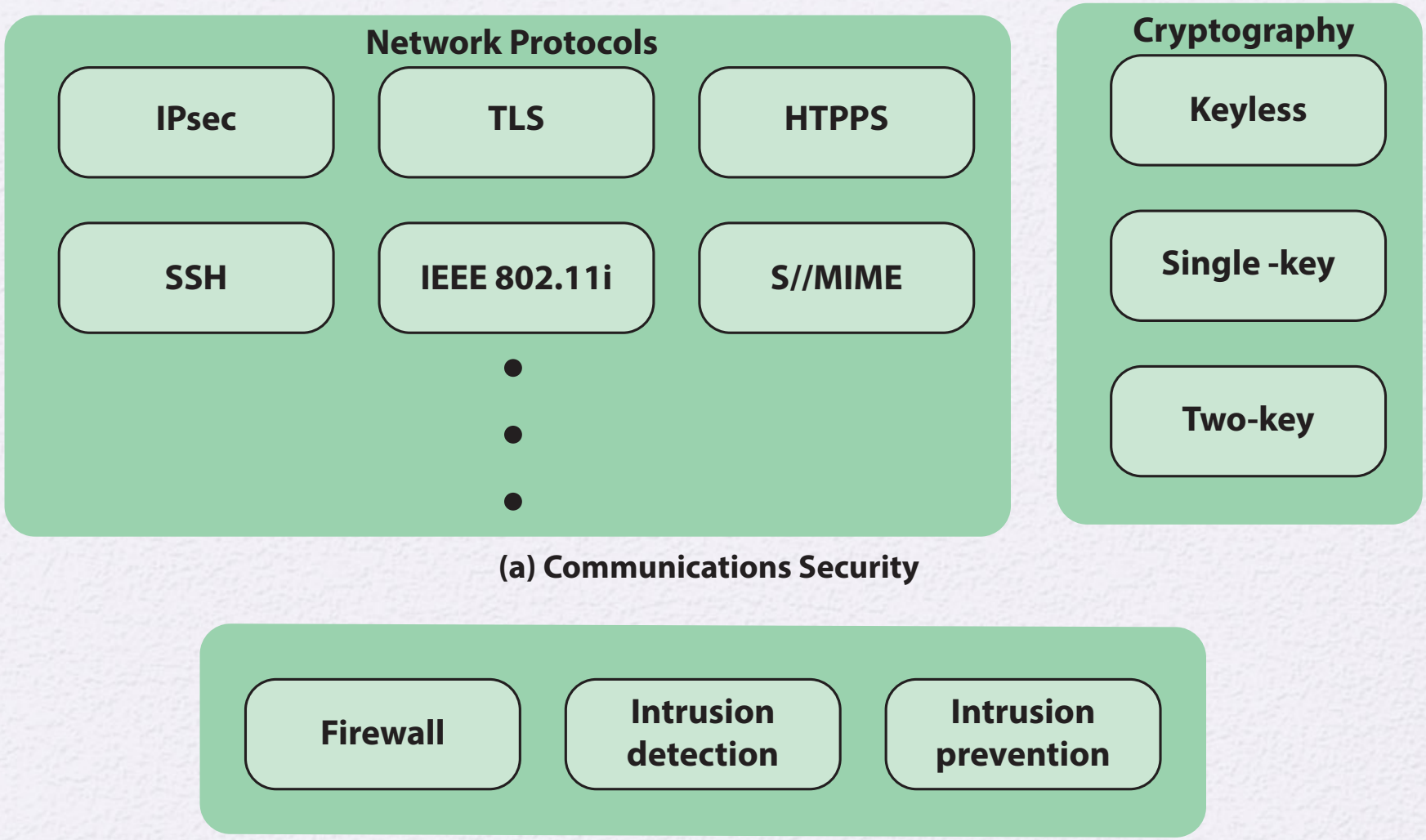


Figure 1.5 Key Elements of Network Security

Communications Security

- Deals with the protection of communications through the network, including measures to protect against both passive and active attacks
- Communications security is primarily implemented using network protocols
  - A network protocol consists of the format and procedures that governs the transmitting and receiving of data between points in a network
  - A protocol defines the structure of the individual data units and the control commands that manage the data transfer
- With respect to network security, a security protocol may be an enhancement that is part of an existing protocol or a standalone protocol

Device Security

- The other aspect of network security is the protection of network devices, such as routers and switches, and end systems connected to the network, such as client systems and servers
- The primary security concerns are intruders that gain access to the system to perform unauthorized actions, insert malicious software (malware), or overwhelm system resources to diminish availability
- Three types of device security are:
  - **Firewall**
    - A hardware and/or software capability that limits access between a network and device attached to the network, in accordance with a specific security policy. The firewall acts as a filter that permits or denies data traffic, both incoming and outgoing, based on a set of rules based on traffic content and/or traffic pattern
  - **Intrusion detection**
    - Hardware or software products that gather and analyze information from various areas within a computer or a network for the purpose of finding, and providing real-time or near-real-time warning of, attempts to access system resources in an unauthorized manner
  - **Intrusion prevention**
    - Hardware or software products designed to detect intrusive activity and attempt to stop the activity, ideally before it reaches its target

Summary

- Describe the key security requirements of confidentiality, integrity, and availability
- List and briefly describe key organizations involved in cryptography standards
- Provide an overview of keyless, single-key and two-key cryptographic algorithms

- Provide an overview of the main areas of network security
- Discuss the types of security threats and attacks that must be dealt with and give examples of the types of threats and attacks that apply to different categories of computer and network assets