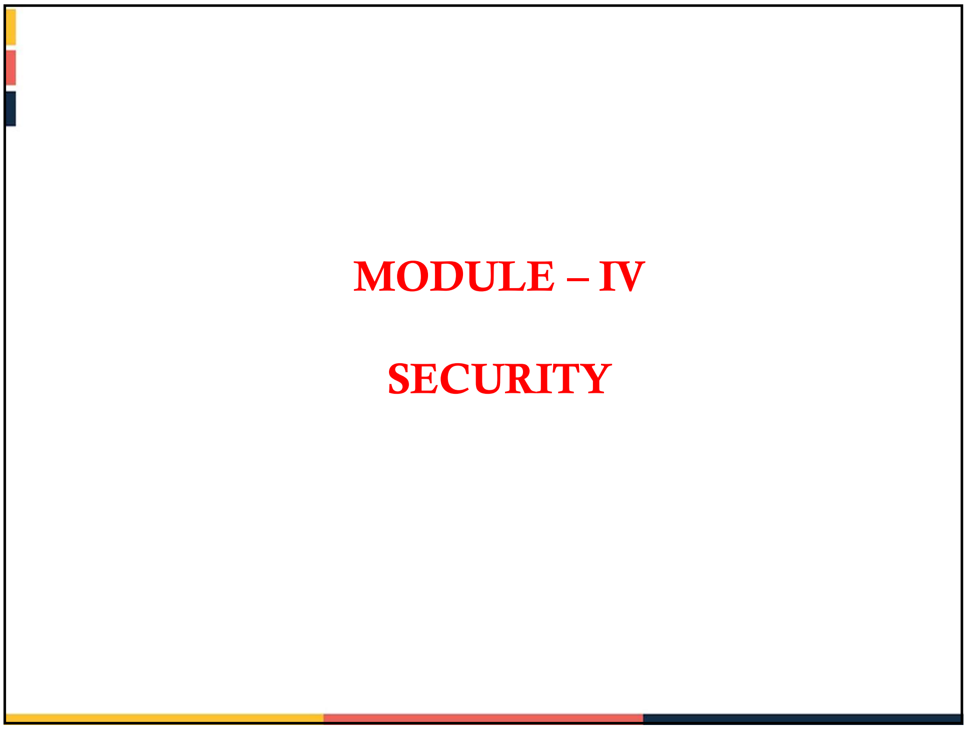
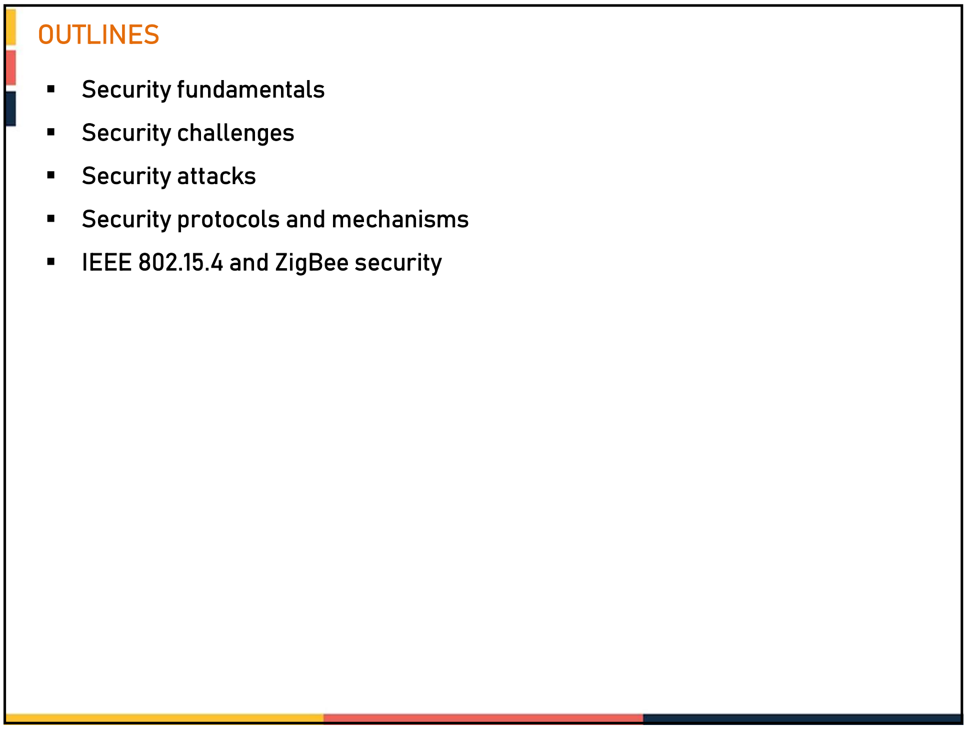


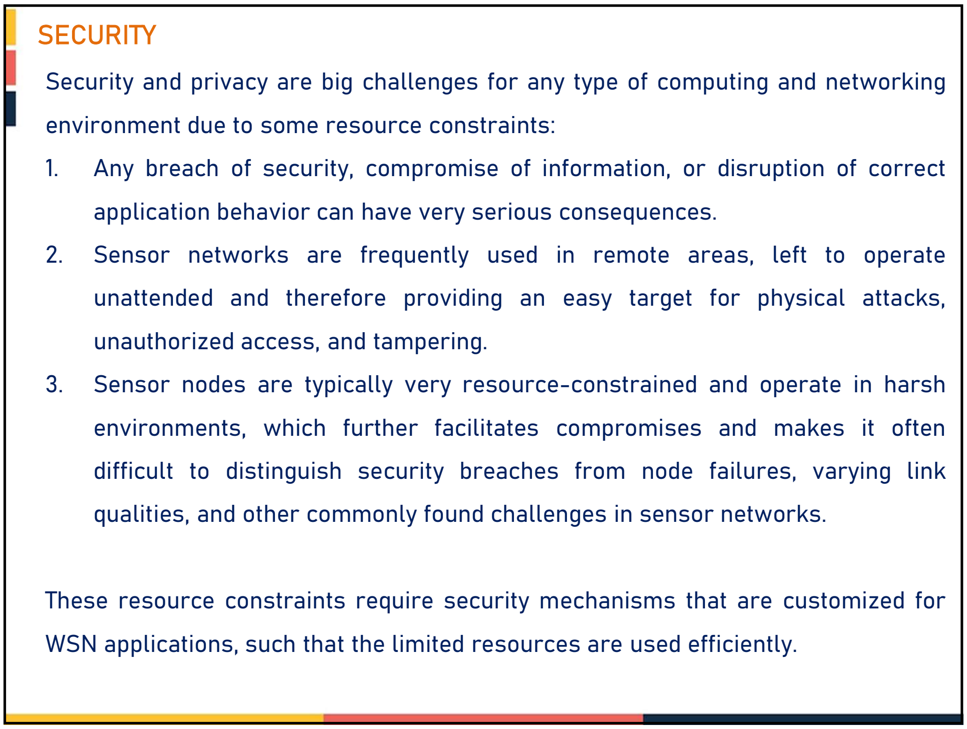
MODULE – IV

SECURITY



OUTLINES

- Security fundamentals
- Security challenges
- Security attacks
- Security protocols and mechanisms
- IEEE 802.15.4 and ZigBee security

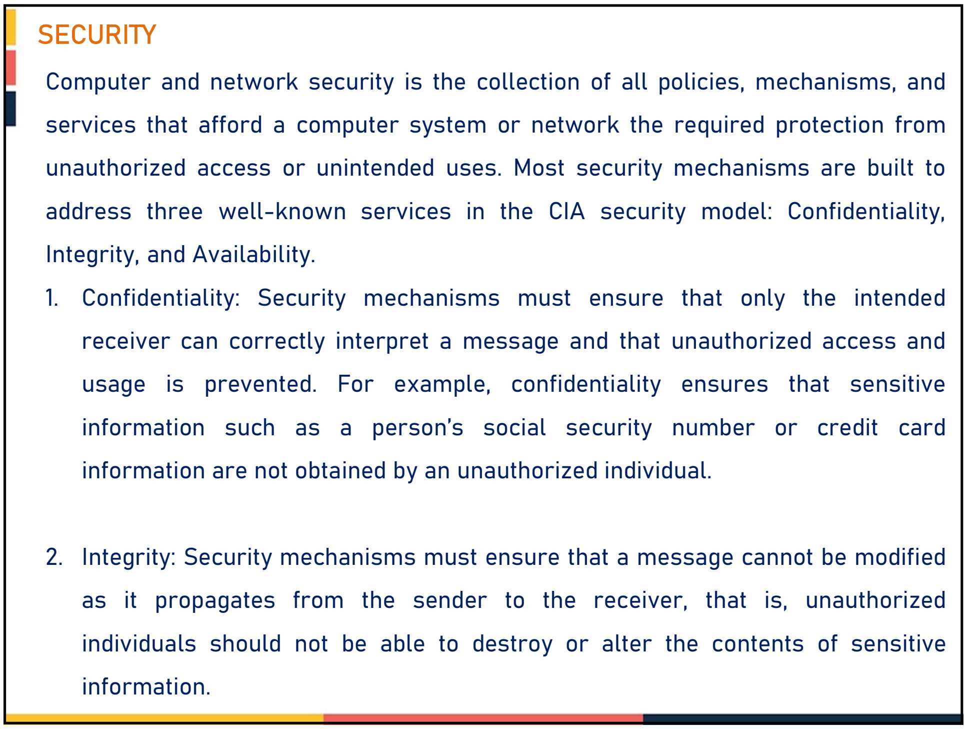


SECURITY

Security and privacy are big challenges for any type of computing and networking environment due to some resource constraints:

1. Any breach of security, compromise of information, or disruption of correct application behavior can have very serious consequences.
2. Sensor networks are frequently used in remote areas, left to operate unattended and therefore providing an easy target for physical attacks, unauthorized access, and tampering.
3. Sensor nodes are typically very resource-constrained and operate in harsh environments, which further facilitates compromises and makes it often difficult to distinguish security breaches from node failures, varying link qualities, and other commonly found challenges in sensor networks.

These resource constraints require security mechanisms that are customized for WSN applications, such that the limited resources are used efficiently.



SECURITY

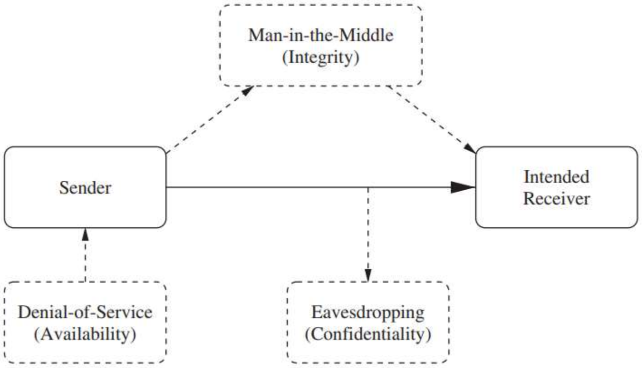
Computer and network security is the collection of all policies, mechanisms, and services that afford a computer system or network the required protection from unauthorized access or unintended uses. Most security mechanisms are built to address three well-known services in the CIA security model: Confidentiality, Integrity, and Availability.

1. Confidentiality: Security mechanisms must ensure that only the intended receiver can correctly interpret a message and that unauthorized access and usage is prevented. For example, confidentiality ensures that sensitive information such as a person’s social security number or credit card information are not obtained by an unauthorized individual.

2. Integrity: Security mechanisms must ensure that a message cannot be modified as it propagates from the sender to the receiver, that is, unauthorized individuals should not be able to destroy or alter the contents of sensitive information.

SECURITY

Integrity: Security mechanisms must ensure that a message cannot be modified as it propagates from the sender to the receiver, that is, unauthorized individuals should not be able to destroy or alter the contents of sensitive information.


Man-in-the-Middle (Integrity)
Sender
Intended Receiver
Denial-of-Service (Availability)
Eavesdropping (Confidentiality)

Examples of attacks and the CIA model.

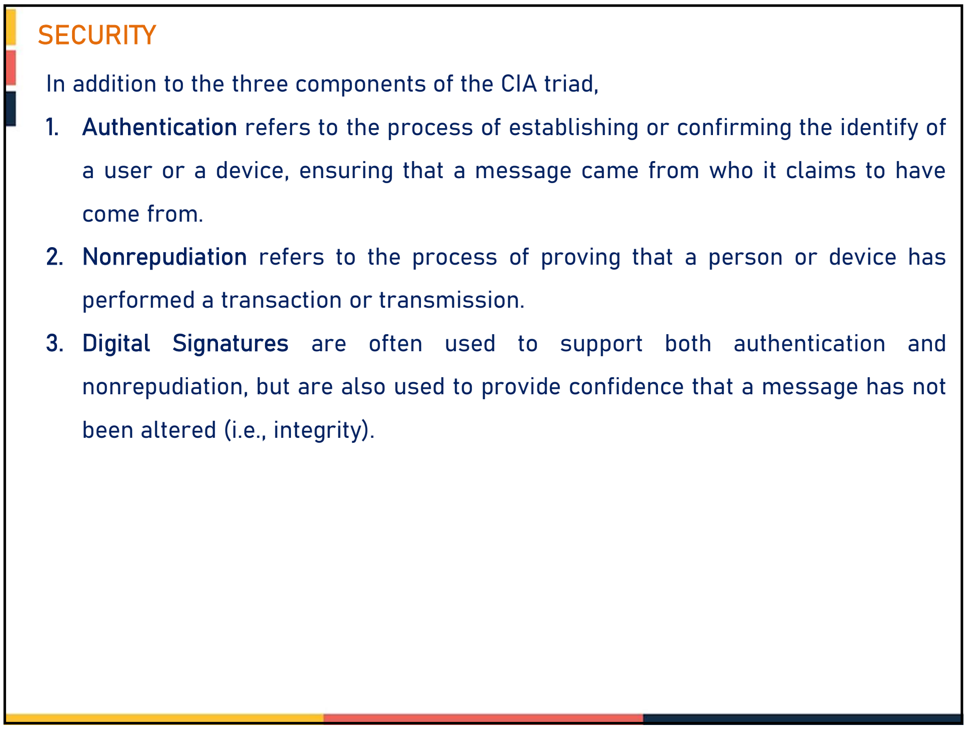
SECURITY

Figure shows attacks on a transmission between a sender and its intended receiver.

1. **Eavesdropping** refers to the reception of a message by an unauthorized individual, which can be prevented using confidentiality measures.

2. A **man-in-the-middle** attack refers to a situation where an unauthorized individual or system positions itself between the sender and receiver such that the sender’s messages are intercepted, modified, and retransmitted to the receiver (where the receiver believes the received message came directly from the original sender). This illustrates the need for integrity mechanisms.

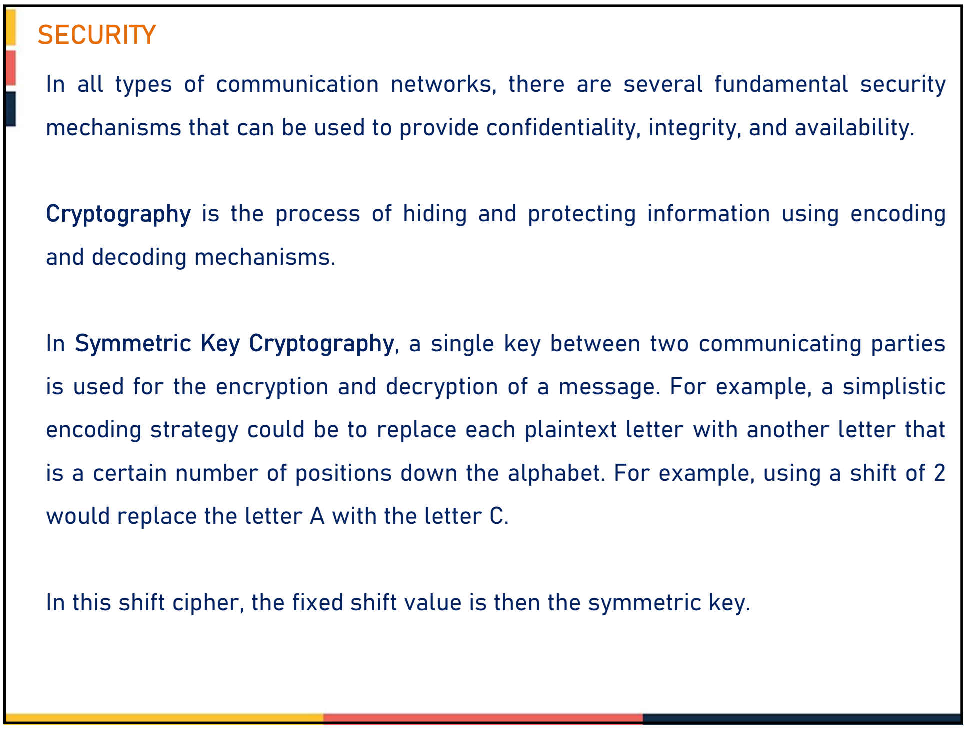
3. Finally, a **denial-of-service attack** refers to an adversary’s attempt to disrupt the transmission or service provided by the sender. For example, the adversary can overload the sender with requests and tasks such that the sender is not able to transmit its message (in a timely fashion) to the receiver. This type of attack necessitates security mechanisms that ensure availability.



SECURITY

In addition to the three components of the CIA triad,

1. **Authentication** refers to the process of establishing or confirming the identify of a user or a device, ensuring that a message came from who it claims to have come from.
2. **Nonrepudiation** refers to the process of proving that a person or device has performed a transaction or transmission.
3. **Digital Signatures** are often used to support both authentication and nonrepudiation, but are also used to provide confidence that a message has not been altered (i.e., integrity).



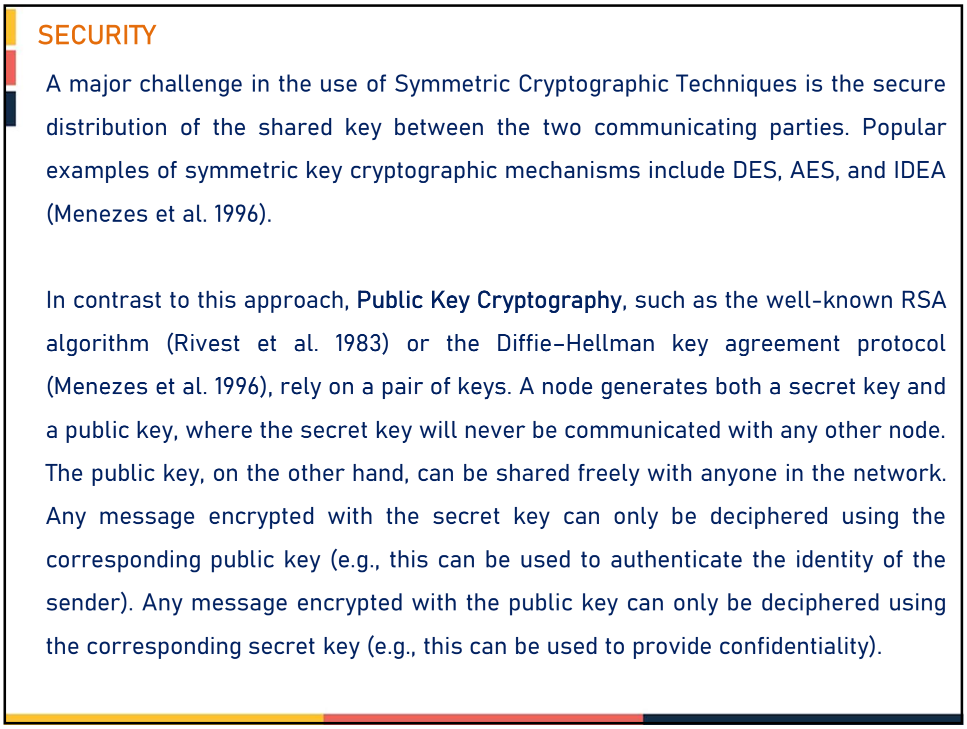
SECURITY

In all types of communication networks, there are several fundamental security mechanisms that can be used to provide confidentiality, integrity, and availability.

Cryptography is the process of hiding and protecting information using encoding and decoding mechanisms.

In **Symmetric Key Cryptography**, a single key between two communicating parties is used for the encryption and decryption of a message. For example, a simplistic encoding strategy could be to replace each plaintext letter with another letter that is a certain number of positions down the alphabet. For example, using a shift of 2 would replace the letter A with the letter C.

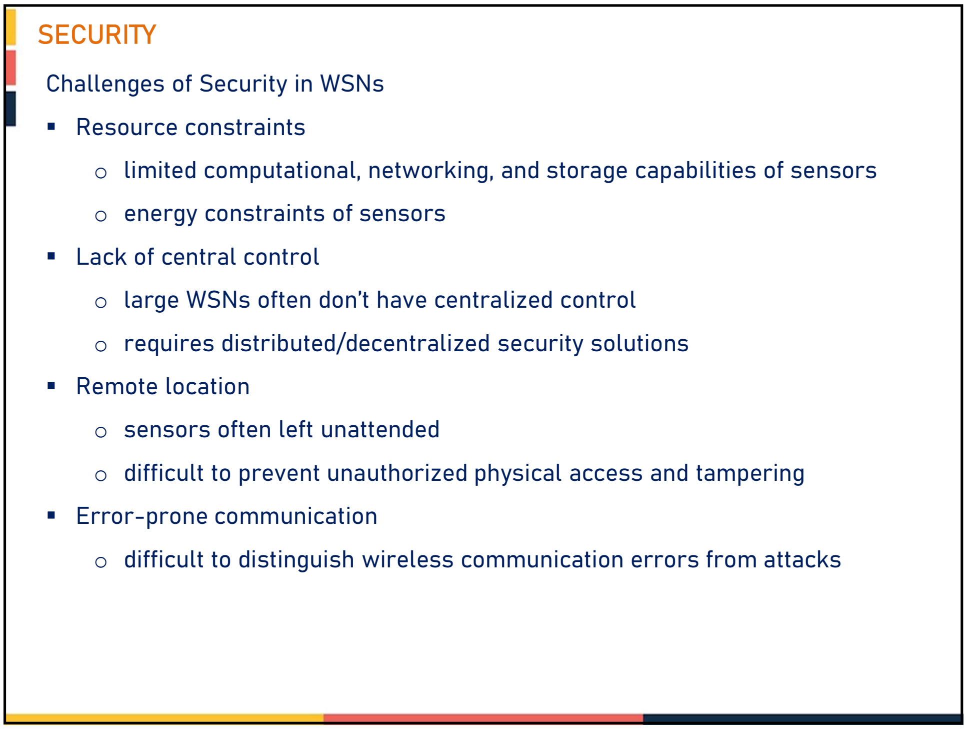
In this shift cipher, the fixed shift value is then the symmetric key.



SECURITY

A major challenge in the use of Symmetric Cryptographic Techniques is the secure distribution of the shared key between the two communicating parties. Popular examples of symmetric key cryptographic mechanisms include DES, AES, and IDEA (Menezes et al. 1996).

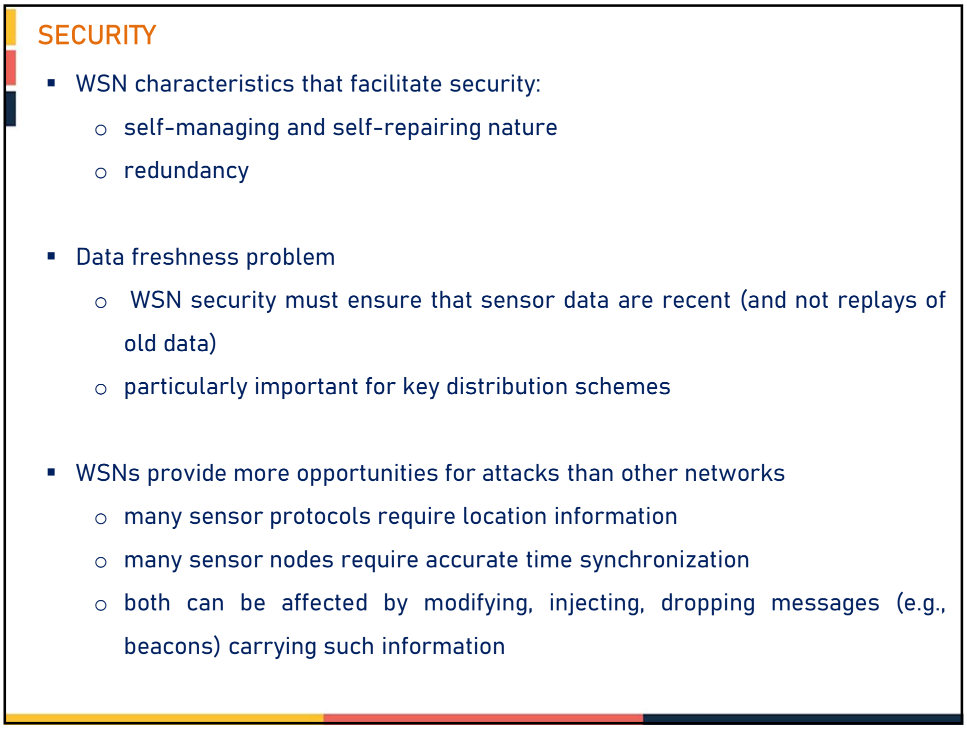
In contrast to this approach, **Public Key Cryptography**, such as the well-known RSA algorithm (Rivest et al. 1983) or the Diffie–Hellman key agreement protocol (Menezes et al. 1996), rely on a pair of keys. A node generates both a secret key and a public key, where the secret key will never be communicated with any other node. The public key, on the other hand, can be shared freely with anyone in the network. Any message encrypted with the secret key can only be deciphered using the corresponding public key (e.g., this can be used to authenticate the identity of the sender). Any message encrypted with the public key can only be deciphered using the corresponding secret key (e.g., this can be used to provide confidentiality).



SECURITY

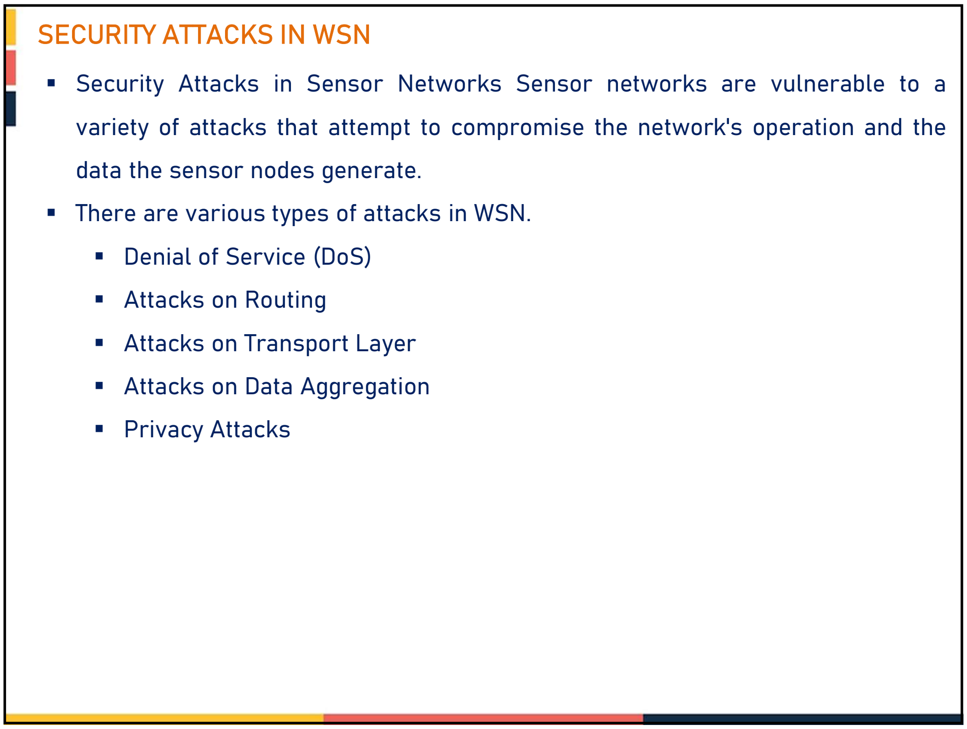
Challenges of Security in WSNs

- Resource constraints
  - limited computational, networking, and storage capabilities of sensors
  - energy constraints of sensors
- Lack of central control
  - large WSNs often don't have centralized control
  - requires distributed/decentralized security solutions
- Remote location
  - sensors often left unattended
  - difficult to prevent unauthorized physical access and tampering
- Error-prone communication
  - difficult to distinguish wireless communication errors from attacks



SECURITY

- WSN characteristics that facilitate security:
  - self-managing and self-repairing nature
  - redundancy
- Data freshness problem
  - WSN security must ensure that sensor data are recent (and not replays of old data)
  - particularly important for key distribution schemes
- WSNs provide more opportunities for attacks than other networks
  - many sensor protocols require location information
  - many sensor nodes require accurate time synchronization
  - both can be affected by modifying, injecting, dropping messages (e.g., beacons) carrying such information



SECURITY ATTACKS IN WSN

- Security Attacks in Sensor Networks Sensor networks are vulnerable to a variety of attacks that attempt to compromise the network's operation and the data the sensor nodes generate.
- There are various types of attacks in WSN.
  - Denial of Service (DoS)
  - Attacks on Routing
  - Attacks on Transport Layer
  - Attacks on Data Aggregation
  - Privacy Attacks