CRYPTOGRAPHY

LECTURE ONE

Introduction

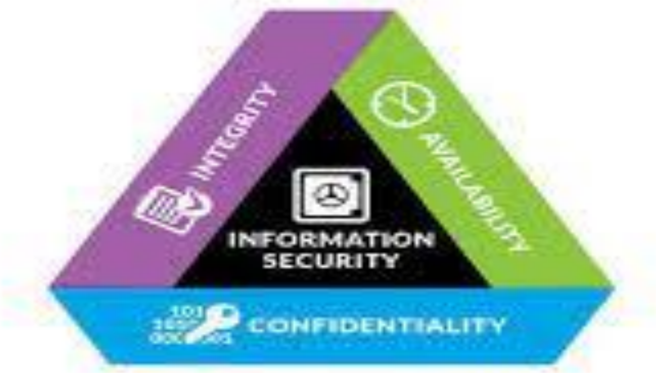
Assist prof. Dr. Saja J.Mohammed

2024-2025

uefqbro

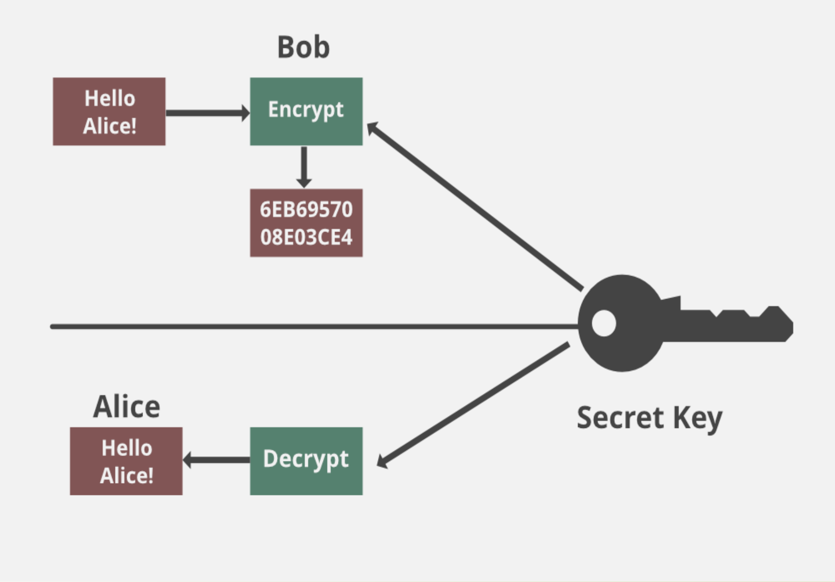
CIA TRIANGLE

Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization. The model is also sometimes referred to as the AIC triad (availability, integrity and confidentiality) to avoid confusion.
Although elements of the triad are three of the most foundational of cybersecurity needs, experts believe the CIA triad needs an upgrade to stay effective.



CONFIDENTIALITY

- Confidentiality means that only authorized individuals/systems can view sensitive or classified information. The data being sent over the network should not be accessed by unauthorized individuals. The attacker may try to capture the data using different tools available on the Internet and gain access to your information. A primary way to avoid this is to use encryption techniques to safeguard your data so that even if the attacker gains access to your data, he/she will not be able to decrypt it.



- ## INTEGRITY

Is the assurance that the information is trustworthy and accurate(make sure that data has not been modified).

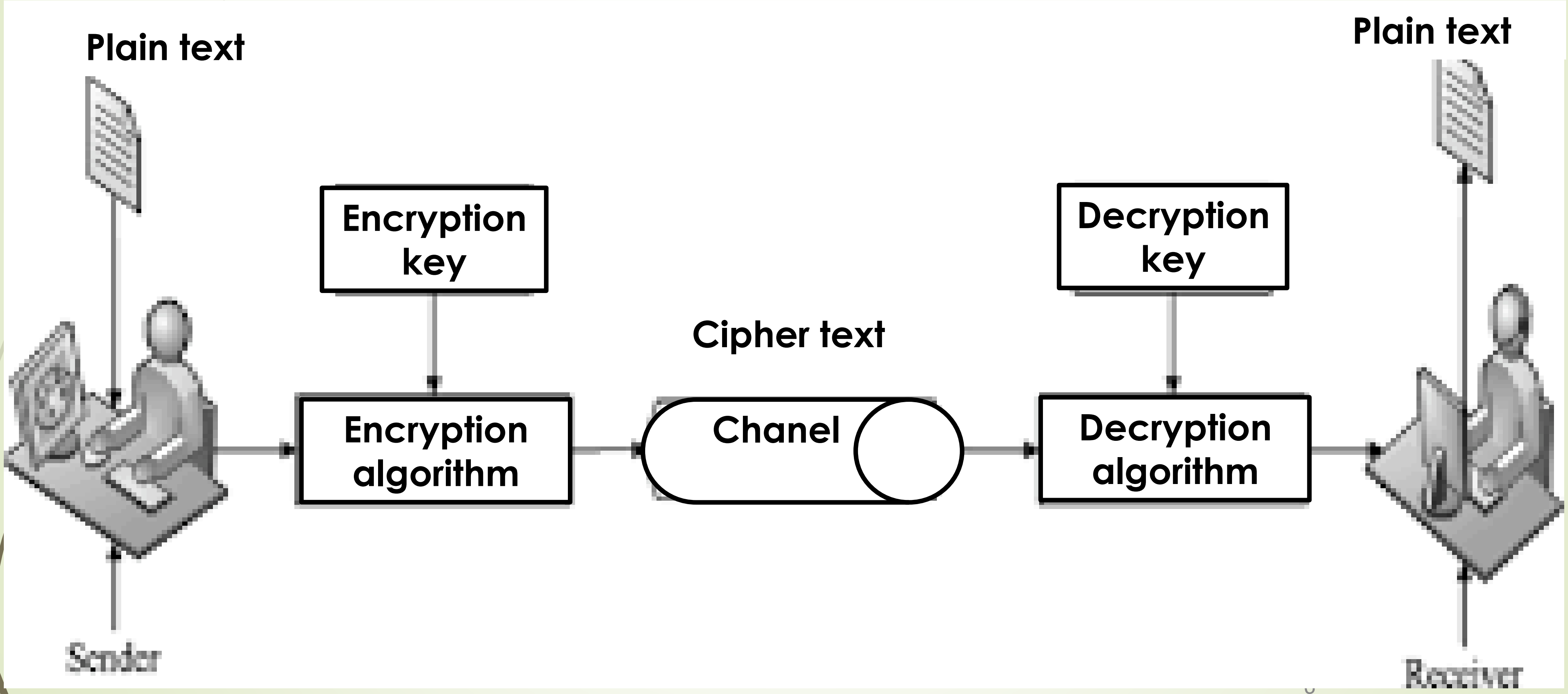
- ## AVAILABILITY

Means information should be accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information.

BASIC IMPORTANT TERMS

- **Plaintext:** Original message to be encrypted
- **Ciphertext:** The encrypted message.
- **Enciphering or encryption:** The process of converting plaintext into ciphertext
- **Encryption algorithm:** An algorithm which performs encryption (Two inputs: a plaintext and a secret key)
- **Deciphering or decryption:** Recovering plaintext from ciphertext
- **Decryption algorithm:** An algorithm which performs decryption (Two inputs: ciphertext and secret key)
- **Key:** key used for encryption and decryption.
- **Cryptography:** Science of studying ciphers (encryption and decryption)
- **Cryptanalysis:** Science of studying attacks against cryptographic systems
- **Cryptology:** Cryptography + cryptanalysis

BLOCK DIAGRAM OF CRYPTOSYSTEMS



MATHEMATICALLY:

Any encryption/ decryption algorithm can be written as follows:

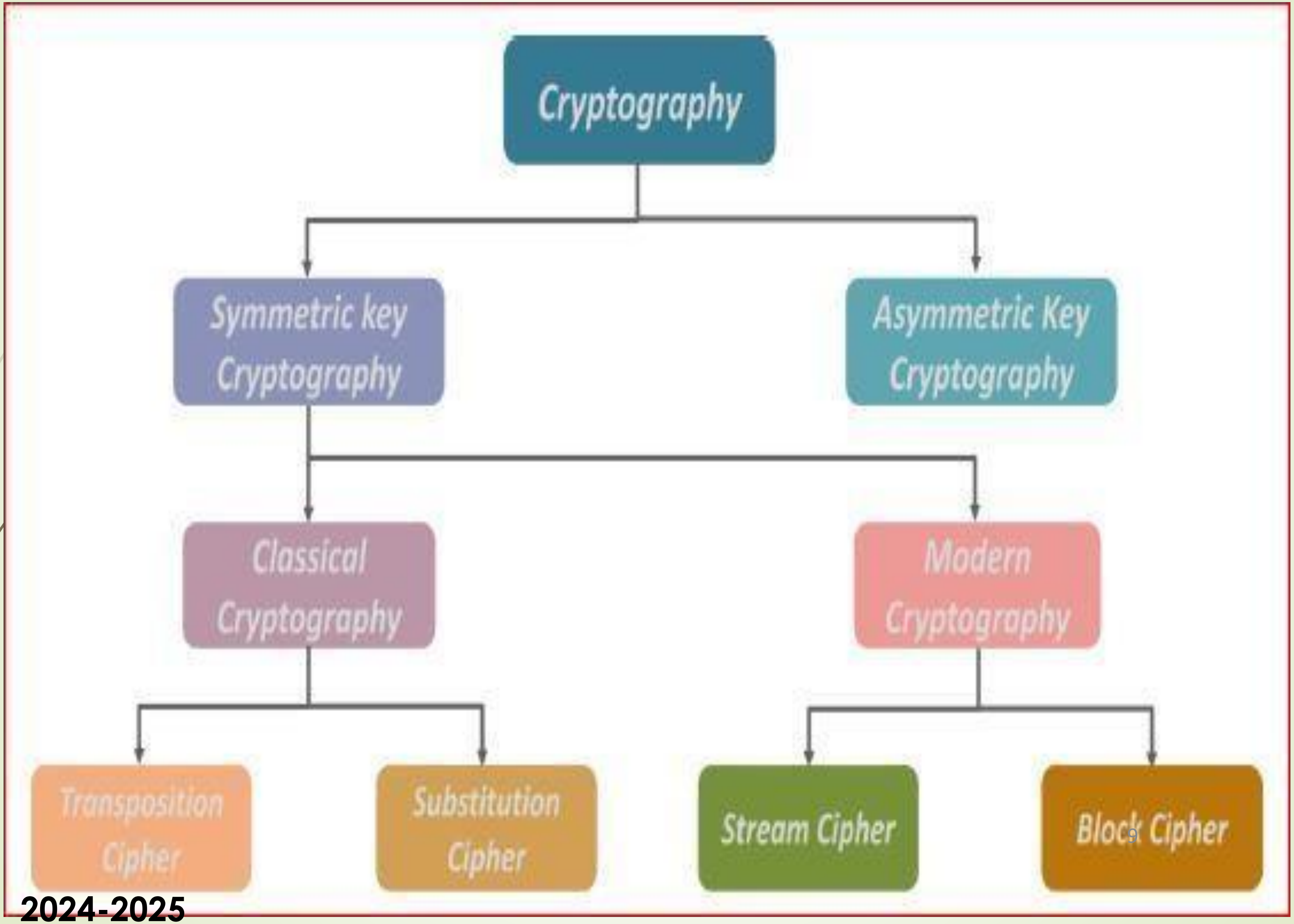
$$C = E_K(P) \text{ or } C = E(P, K)$$
$$P = D_K(C) \text{ or } P = D(C, K)$$

Where:

- P = plaintext
- C = ciphertext
- K = The used key
- E = Encryption algorithm
- D = Decryption algorithm

Cryptography can be used to ensure these security properties:

1. **Confidentiality :** Ensures that data is read only by authorized users.
2. **Integrity:** Ensure that data is not changed from source to destination.
3. **Non-repudiation** : Refer to a service, which provides proof of the origin and integrity of data.
4. **Authentication :** the process or action of verifying the identity of a user or process.


Cryptography
Symmetric key Cryptography
Asymmetric Key Cryptography
Classical Cryptography
Modern Cryptography
Transposition Cipher
Substitution Cipher
Stream Cipher
Block Cipher