جامـــــعـة المـــــسـتـقـبـل
AL MUSTAQBAL UNIVERSITY

كلية العلوم

قســـم الانظمة الطبية الذكية

Lecture: (3)

Information Security in Healthcare

Subject: Methods of Defense & Cryptographic Techniques
Level: Fourth
Lecturer: Prof. Dr. Mehdi Ebady Manaa

1. Introduction: Why Healthcare Needs Strong Cyber Defense

Healthcare organizations are among the most targeted sectors in cybersecurity. Hospitals manage extremely sensitive data (patient identity, medical history, lab results) and operate life-critical systems such as ventilators, infusion pumps, and diagnostic equipment. A cyberattack in a hospital does not only cause financial loss it can result in delayed treatment, wrong diagnosis, or even patient death.

According to Brooks & Craig, in critical systems such as healthcare and industrial environments, availability and integrity are often more important than confidentiality because systems must function in real time and without interruption This means hospitals must build security mechanisms that keep systems operational, accurate, and trustworthy even during attacks.

2. Security Objectives in Healthcare Systems

In healthcare, these services are interpreted as follows:

Security Goal	**Meaning in Healthcare**
Confidentiality	Patient records must not be disclosed to unauthorized people
Integrity	Lab results, diagnoses, and prescriptions must not be altered
Authentication	Only real doctors, nurses, and staff can access systems
Non-repudiation	Doctors cannot deny issuing a prescription or report
Availability	Medical systems must always be online for patient care

3. Defense-in-Depth in Hospital Networks

Modern hospitals use a Defense-in-Depth strategy, meaning that security is applied in multiple layers, not in one single control. This model is strongly emphasized in Brooks & Craig's secure system architecture for critical systems

In healthcare, these layers include:

1. **Physical Security** – Server rooms, data centers, restricted wards
2. **Network Security** – Firewalls, VLANs, medical device segmentation
3. **System Security** – Windows and Linux hardening
4. **Application Security** – EHR and PACS access control
5. **Data Security** – Encryption and digital signatures

Even if one layer fails, others still protect the patient data and systems.

4. Role of Cryptography in Healthcare Defense

In healthcare, cryptography is used to protect:

- Electronic Health Records (EHR)
- Medical images (MRI, CT scans)

- Prescriptions
- Telemedicine communication
- Insurance transactions

Without cryptography, any attacker who accesses the network could read or modify patient data.

5. Symmetric Encryption in Medical Systems

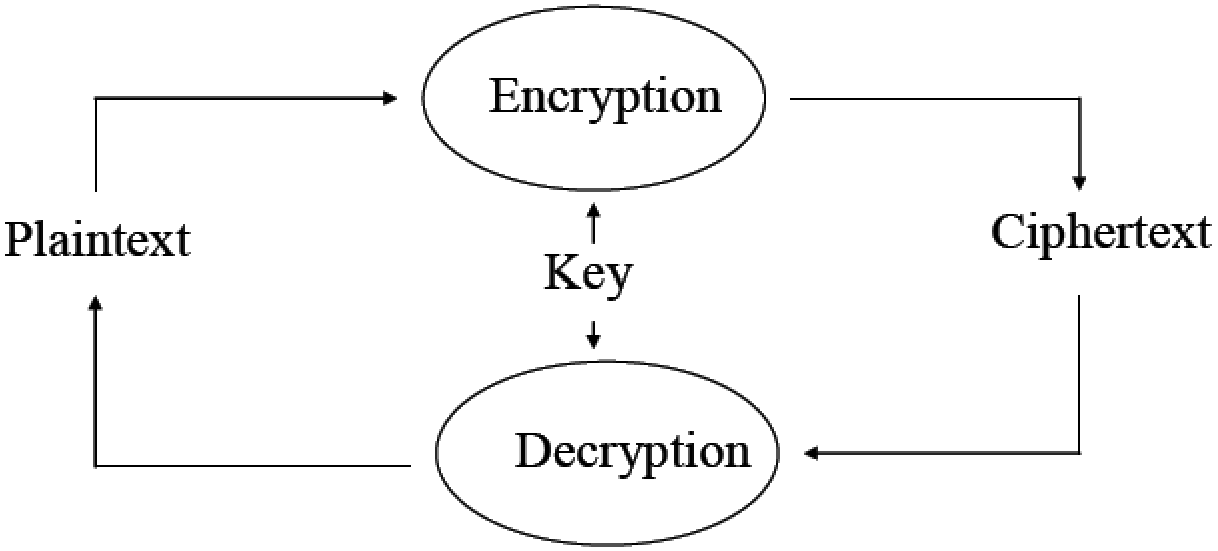
Hospitals typically use **AES (Advanced Encryption Standard)** for:

- Database encryption
- Disk encryption
- Backup encryption

For example, when a patient's MRI scan is stored in the hospital database, it is encrypted using AES. If someone steals the disk, they cannot read the medical images without the secret key.

6. Cryptographic Techniques

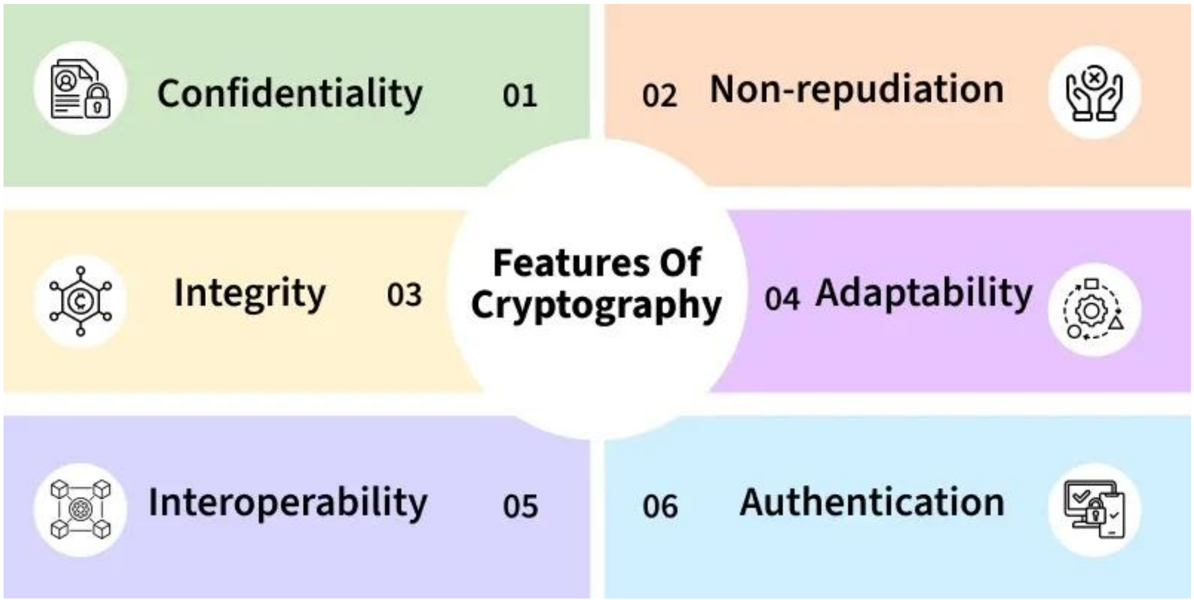
- Cryptography, a word with Greek origins, means "secret writing" However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks and to preserve confidentiality .
- Cryptography is a collection of mathematical techniques for protecting information.
- Converts plaintext into ciphertext using algorithms and keys
- Ensures confidentiality, integrity, authentication, and non-repudiation
- Used in secure communication, digital signatures, passwords, and online transactions



These algorithms are used for cryptographic key generation, digital signing, and verification to protect data privacy, web browsing on the internet and to protect confidential transactions such as credit card and debit card transactions.

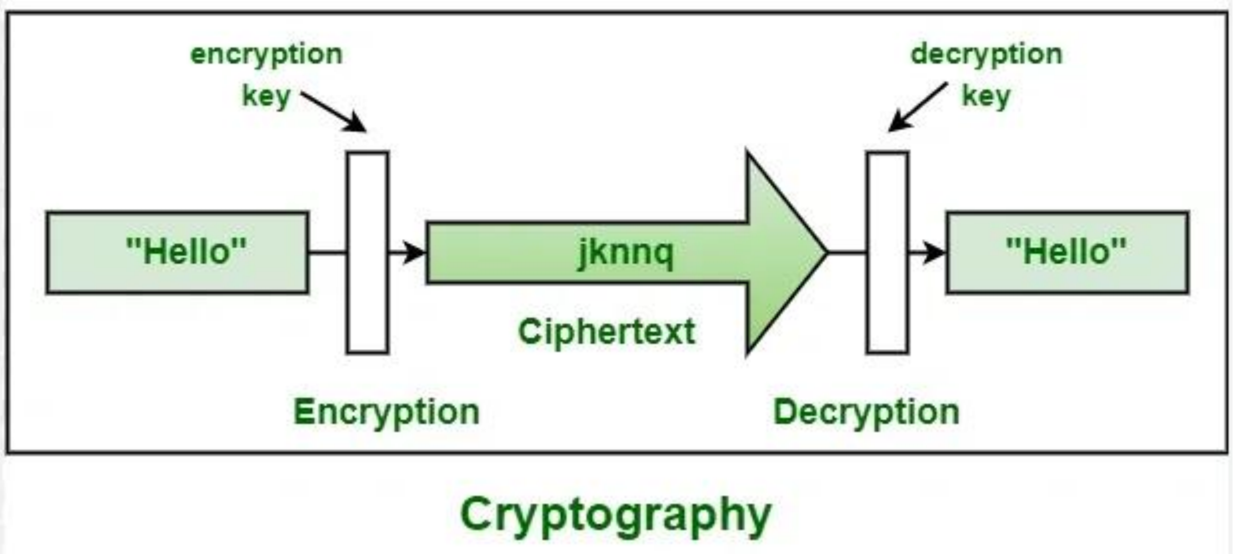
Features Of Cryptography

The features of cryptography that makes it a popular choice in various applications could be listed down as



Working in Cryptography

As we all know that cryptography technique is use to convert plain text into ciphertext. This technique is done by cryptographic key. Basically cryptographic key is a string of characters which is used to encrypts the data and decrypt the data.



"Hello" is a plaintext and convert into ciphertext "jknnq" with the help of cryptographic key and then decrypt into "Hello".

- **Plaintext is created**
  The original readable message or data.
- **A cryptographic algorithm is chosen**
  Example: AES, RSA, SHA-256, etc.
- **A key is applied**
  This key controls how the encryption or hashing is performed.
- **Encryption converts plaintext → ciphertext**
  The data becomes unreadable to unauthorized users.
- **Ciphertext is transmitted or stored securely**
  Even if intercepted, it cannot be understood without the correct key.
- **Decryption converts ciphertext → plaintext**

The receiver uses the correct key (same key for symmetric, different for asymmetric).

- **Integrity checks may be used**
  Hashing ensures the message has not been altered.