LEC2

Detailed explanation of concepts in Cryptography

2025-2026

Second semester

2026-2-11

Alaa Y. Taqa

1. Data Security

Data Security is the practice of protecting digital information from unauthorized access, modification, or destruction. It ensures that data remains safe whether it is **stored, processed, or transmitted** across networks.

Objectives of Data Security

The main objectives are:

1.1 Confidentiality

Confidentiality ensures that sensitive information is only accessible to authorized users.

Example:

- Encryption of passwords
- Secure banking transactions

Techniques used:

- Encryption
- Access control
- Authentication

1.2 Integrity

Integrity ensures that data is **accurate and has not been altered** by unauthorized persons.

Example:

- A hacker modifying bank account balances
- Changing information in a database

Techniques used:

- Hash functions
- Digital signatures
- Checksums

1.3 Availability

Availability ensures that authorized users can **access information whenever they need it**.

Example:

- A website must be accessible to users 24/7
- Cloud servers storing data must be available

Threats to availability:

- Hardware failures
- Denial-of-Service attacks

Network failures

2. Security Attacks

A **Security Attack** is any action that attempts to **compromise the confidentiality, integrity, or availability of information**.

Security attacks try to:

- Steal information
- Modify data
- Interrupt communication
- Gain unauthorized system access

Types of Security Attacks

2.1. Passive Attacks

The attacker only **monitors communication** but does not modify the data.

Example:

- Eavesdropping on network traffic
- Intercepting emails

2.2 Active Attacks

The attacker **modifies or disrupts data**.

Example:

- Changing messages
- Destroying files
- Injecting malicious data

3. Security Services

Security Services are mechanisms designed to **protect information systems and communications from security attacks**.

They ensure that communication between users is secure.

Main Security Services

3.1. Authentication

Authentication verifies the **identity of users or devices** before granting access.

Example:

- Username and password login
- Biometric verification (fingerprint, face recognition)

Types:

- User authentication
- Data authentication

3.2. Access Control

Access control limits who can **access certain resources**.

Example:

- Only administrators can modify system settings
- Employees can access only specific company files

Methods:

- Password protection
- Role-based access control

3.3 Data Confidentiality

This service ensures that **information is protected from unauthorized disclosure**.

Example:

- Encryption of messages
- Secure online payments

Tools used:

- Encryption algorithms
- Secure communication protocols

3.4. Data Integrity

Data integrity ensures that **data remains accurate and unchanged during transmission**.

Example:

- Detecting if someone modifies a message during transmission.

Techniques:

- Hashing
- Digital signatures

3.5. Non-Repudiation

Non-repudiation ensures that a sender **cannot deny sending a message**.

Example:

- Digital signatures in electronic transactions
- Email verification

This is important in:

- Online contracts
- Financial transactions

4. Passive Attack

A **Passive Attack** occurs when an attacker **monitors communication channels to obtain information** without modifying the data.

The attacker remains **hidden and undetected**.

Characteristics

- Does not affect system resources
- Difficult to detect
- Used mainly for gathering information

Types of Passive Attacks

4.1. Release of Message Contents

The attacker reads private communication.

Example:

- Reading emails
- Intercepting phone calls
- Monitoring network messages

4.2. Traffic Analysis

Even if the data is encrypted, the attacker can analyze **communication patterns**.

Example:

- Identifying who communicates with whom
- Monitoring message frequency

Example scenario:
A military communication network may reveal important information by analyzing traffic patterns even if the messages are encrypted.

5. Basic Principles of Information Security

The **Basic Principles of Security** are commonly known as the **CIA Triad**.

These principles form the foundation of cryptography and cybersecurity.

5.1. Confidentiality

Confidentiality ensures that **only authorized users can access sensitive information**.

Example:

- Encrypted emails
- Password-protected files

Methods used:

- Encryption
- Authentication
- Access control

Example scenario:
If a hacker intercepts encrypted data, they cannot read it without the encryption key.

5.2. Integrity

Integrity ensures that **data is not altered or modified without authorization**.

Example:

- A bank transaction should not be changed during transfer.

Techniques used:

- Hash functions
- Message Authentication Codes (MAC)
- Digital signatures

Example scenario:
If someone modifies a file during transmission, integrity mechanisms will detect the change.

5.3. Availability

Availability ensures that **information systems and data are accessible when needed**.

Example:

- Websites should remain operational
- Databases should be accessible to users

Threats:

- Denial-of-Service (DoS) attacks
- Server crashes
- Power failures

Solutions:

- Backup systems
- Redundant servers
- Disaster recovery plans


Questions


THANK
YOU