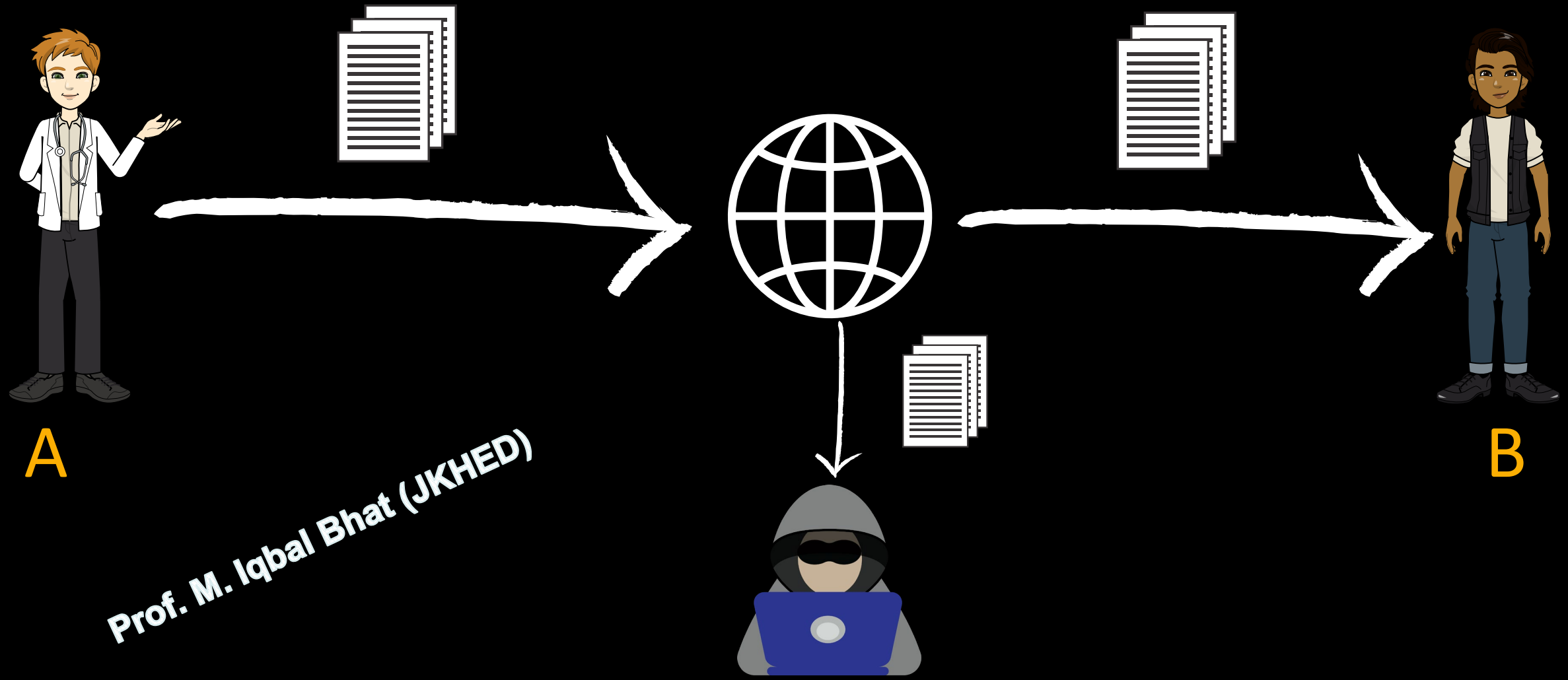
Network Security

By
Prof. Muhammad Iqbal Bhat
Government Degree College Beerwah

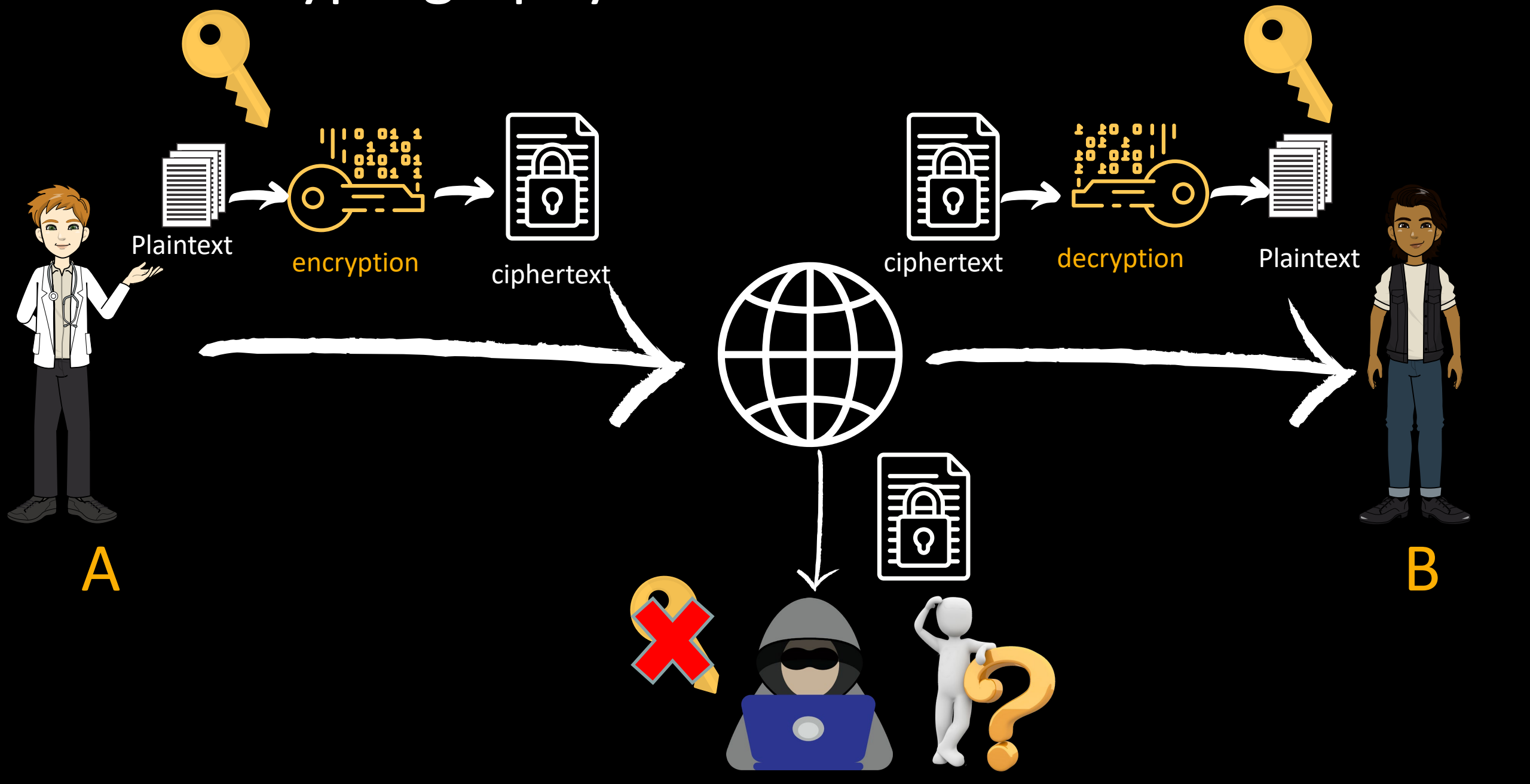
Outline

- Network Security
- Attacks, services and mechanisms
- Security attacks
- Security services
- Methods of Defense
- A model for Internetwork Security
- Internet standards and RFCs

What is Cryptography?



What is Cryptography?



What is Network Security?

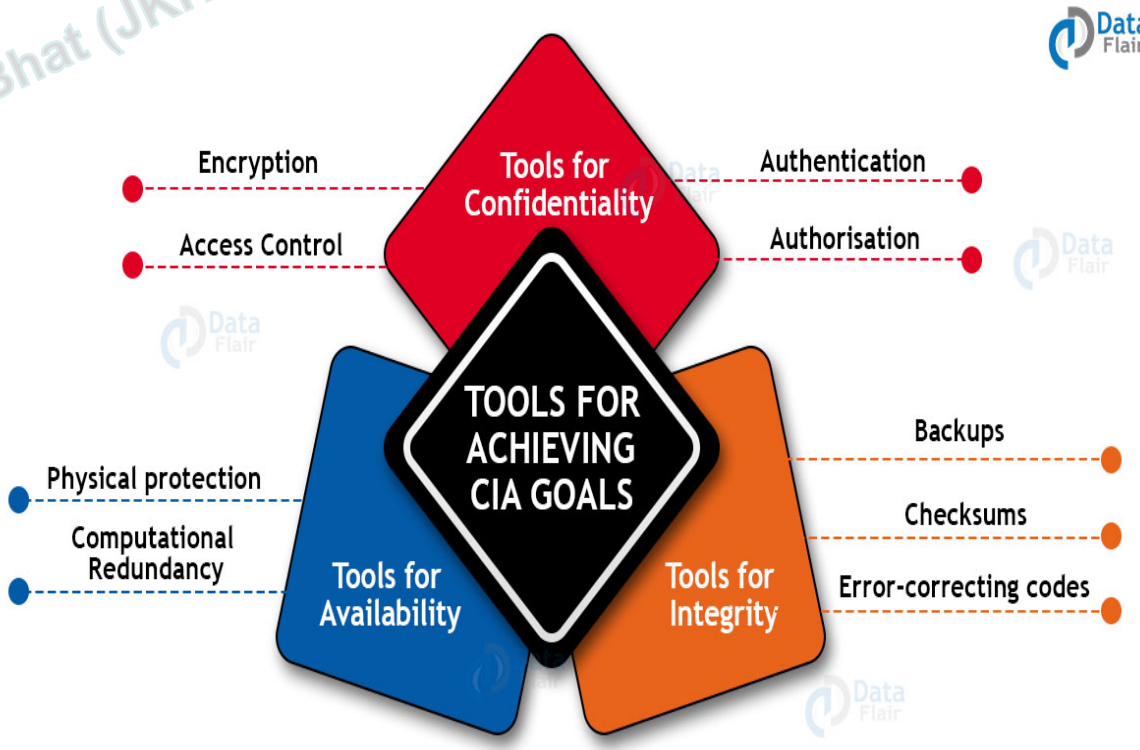
Network security is any activity designed to protect the usability and integrity of your network and data.

What it includes:

- It includes both hardware and software technologies
- It targets a variety of threats
- It stops them from entering or spreading on your network
- Effective network security manages access to the network

Security goals?

- What does it refer to?
- Three Fundamental goals:
  - Confidentiality
    - Authorized users get entry
    - Inspection of information, printing of information and knowledge of resource existence
  - Availability
    - Legitimate user be able to access resources and service should be provided at anytime
  - Integrity
    - Changed in adequate way
    - Modification done by authorized people



Confidentiality (C)

The central idea behind the term confidentiality in the CIA Triad. The CIA Triad ensures that the data is only accessible by genuine authorized users. It helps in preventing disclosure to unintended parties who might exploit the privacy of the user.

Methods to ensure Confidentiality:

- Encryption of raw data
- Using biometrics for authentication
- Two way or multifactor authentication

Confidentiality (C)

Tools for Confidentiality:

- Encryption – It is the process of transforming plain data into unreadable cipher data using an encryption key.
- Access Control – It has rules and policies to limit access to the resources by checking the credentials of users.
- Authentication – It is the confirmation of the user's identity for providing access to the resources.
- Authorization – Verifies the user's access level and either grant or refuses resource access.
- Physical Security – It is required to keep the information available and improve the robustness of the system during hardware failures. It secures business-sensitive information, trade secrets, and customer information.

Integrity (I)

Integrity is making sure the data is unaltered during the time of transmission and ensuring it reaches the end-user in the correct form. It maintains the consistency and reliability of data.

Methods to ensure Integrity:

- Making use of user access control to restrict unauthorized modification of files.
- Setting up backups to restore data during any system failure.
- Version control systems help to identify any modification by tracing the logs.

Integrity (I)

Tools for Integrity:

- Backups – These are duplicate archives of original data.
- Checksums – It is a computational function that maps the contents of the data to a numerical value to check whether the data is the same before and after the transaction.
- Error-correcting codes – Method for controlling errors during and unreliable data transfer over noisy channels.

Availability (A)

The last component of the CIA Triad – Availability helps in delivering resources as and when requested by the user without any intervention like Denial of Service warnings.

Methods to ensure Integrity:

- Installing firewalls, proxy servers during downtime.
- Locating backups at geographically isolated locations.

Availability (A)

Tools for Availability:

- Physical protection - Safeguarding the data against physical challenges like fire or theft.
- Computational Redundancy - Makes the system fault-tolerant and protects against accidental modification.

Threat vs Attack vs Vulnerability

- **Threat** – Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
- **Attack** – Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.
- **Vulnerability**: A weakness or gap in your protection.

Threat: Something that can damage or destroy an asset

Vulnerability: A weakness or gap in your protection

Risk: Where assets, threats, and vulnerabilities intersect

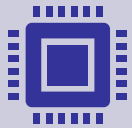
Stages of Attacks

- Three stages called MOM
  - Method
    - Ability, information, tools
  - Opportunity
    - Time and Access
  - Motive
    - Testing system reliability
    - Competition between attackers or testing their own skills
    - Breaking into well-secured systems like law enforcement, government agencies
    - To gain popularity, financial gain, information gain
    - Just for fun
    - No motive at all

Aspects of Security

Security Attack: Any action that compromises the security of information.

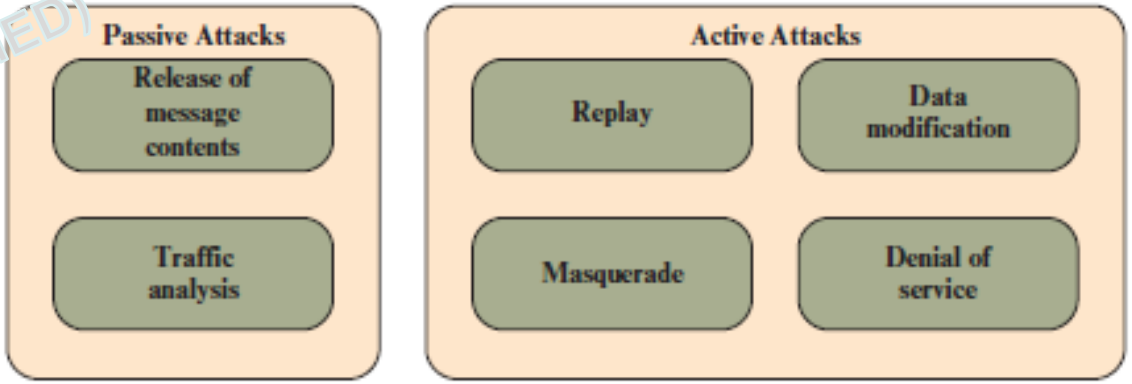
Security Mechanism: A mechanism that is designed to detect, prevent, or recover from a security attack.



Security Service: A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.

Active vs Passive Attacks

- Passive Attack
  - Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted
  - attempts to learn or make use of information from the system but does not affect system resources
- Active Attack
  - attempts to alter system resources or affect their operation
  - Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories



Active vs Passive Attacks

Active Attack	Passive Attack
In an active attack, Modification in information takes place.	While in passive attack, Modification in the information does not take place.
Active Attack is a danger to **Integrity** as well as **availability**.	Passive Attack is a danger to **Confidentiality**.
In an active attack, attention is on prevention.	While in passive attack attention is on detection.
Due to active attacks, the execution system is always damaged.	While due to passive attack, there is no harm to the system.
In an active attack, Victim gets informed about the attack.	While in a passive attack, Victim does not get informed about the attack.
In an active attack, System resources can be changed.	While in passive attack, System resources are not changing.
Active attack influences the services of the system.	While in passive attack, information and messages in the system or network are acquired.
In an active attack, information collected through passive attacks are used during executing.	While passive attacks are performed by collecting information such as passwords, and messages by themselves.
Active attack is tough to restrict from entering systems or networks.	Passive Attack is easy to prohibited in comparison to active attack.
Can be easily detected.	Very difficult to detect.

Types of Security Attacks

Interruption: This is an attack on availability

Interception: This is an attack on confidentiality

Modification: This is an attack on integrity

Fabrication: This is an attack on authenticity

Types of Security Attacks

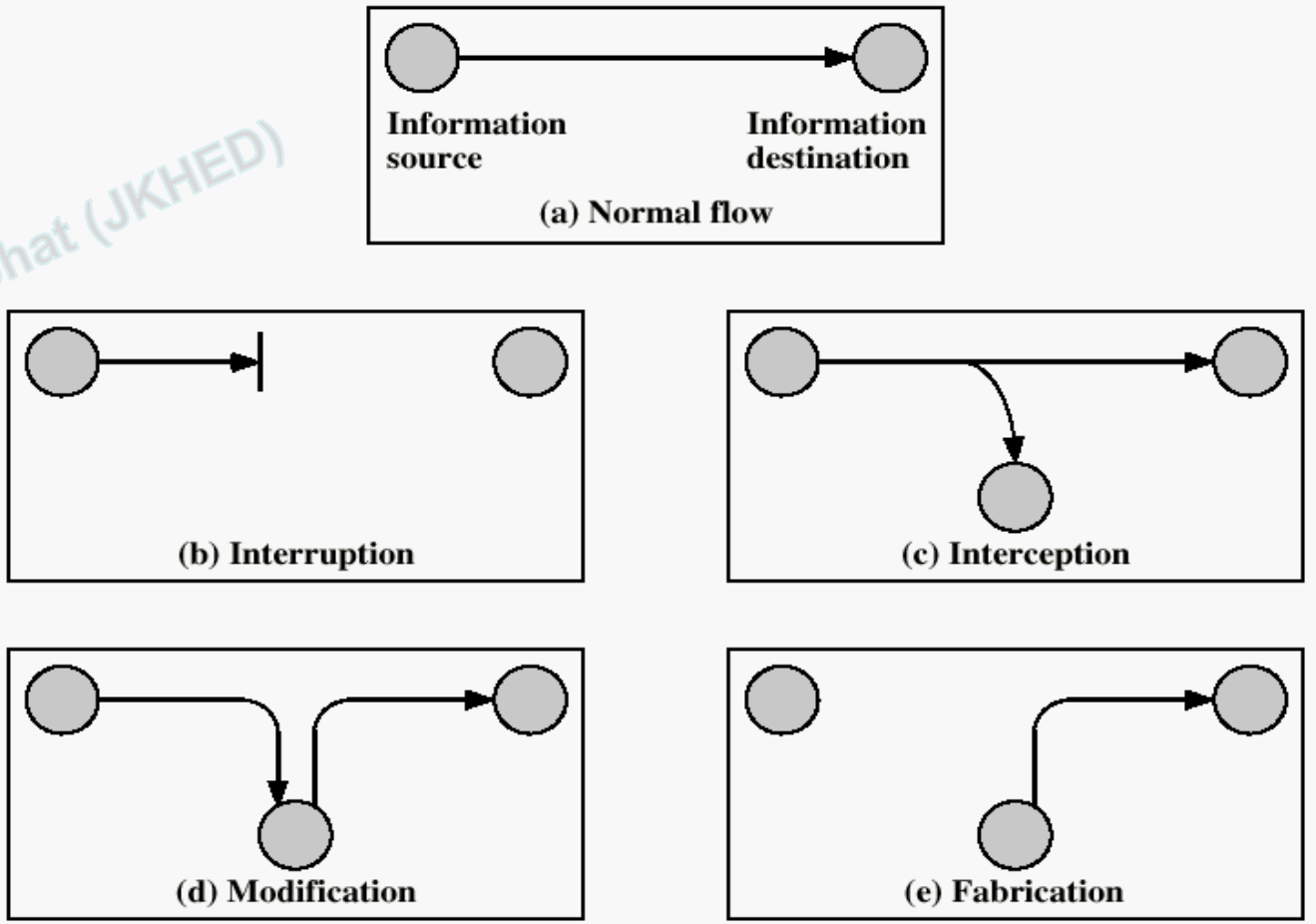
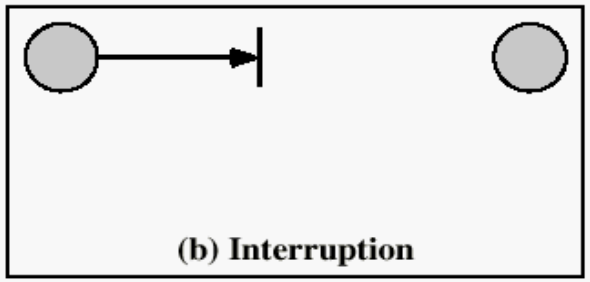


Figure 1.1 Security Threats

Interruption

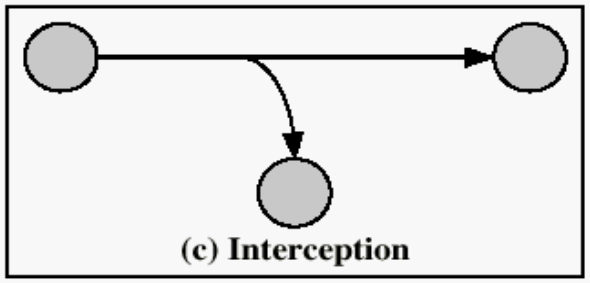
- In an interruption attack, a network service is made degraded or unavailable for legitimate use. They are the attacks against the availability of the network.
- Examples of Interruption attacks:
  - Overloading a server host so that it cannot respond.
  - Cutting a communication line.
  - Blocking access to a service by overloading an intermediate r
  - Redirecting requests to invalid destinations.
  - Theft or destruction of software or hardware involved.



- Mitigate the attack :
- Use Firewalls - Firewalls have simple rules such as to allow or deny protocols, ports or IP addresses. Modern stateful firewalls like Check Point FW1 NGX and Cisco PIX have a built-in capability to differentiate good traffic from DoS attack traffic.
- Keeping backups of system configuration data properly.
- Replication

Interception

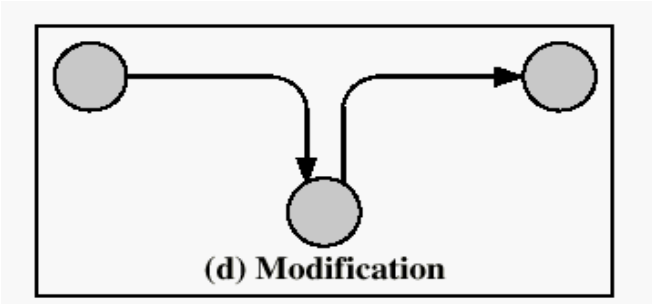
- An interception is where an unauthorized individual gains access to confidential or private information. Interception attacks are attacks against network the confidentiality objective of the CIA Triad.
- Examples of Interception attacks:
  - Eavesdropping on communication.
  - Wiretapping telecommunications networks.
  - Illicit copying of files or programs.
  - Obtaining copies of messages for later replay.
  - Packet sniffing and key logging to capture data from a computer system or network.



- Mitigate the attack :
- Using Encryption - SSL, VPN, 3DES, BPI+ are deployed to encrypts the flow of information from source to destination so that if someone is able to snoop in on the flow of traffic, all the person will see is ciphered text.
- Traffic Padding - It is a function that produces cipher text output continuously, even in the absence of plain text. A continuous random data stream is generated. When plaintext is available, it is encrypted and transmitted. When input plaintext is not present, the random data are encrypted and transmitted. This makes it impossible for an attacker to distinguish between tree data flow and noise and therefore impossible to deduce the amount of traffic.

Modification

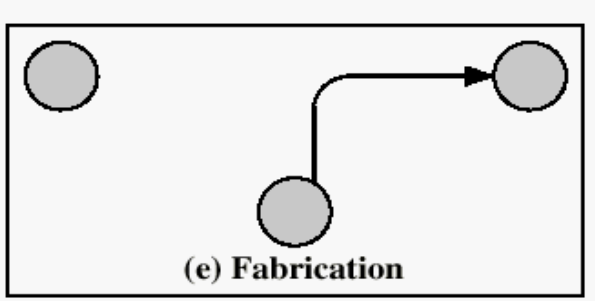
- Modification is an attack against the integrity of the information. Basically there is three types of modifications. (change, Insertion, Deletion)
- Examples of Modification attacks:
  - Modifying the contents of messages in the network.
  - Changing information stored in data files.
  - Altering programs so they perform differently.
  - Reconfiguring system hardware or network topologies.



- Mitigate the attack :
- Introduction of intrusion detection systems (IDS) which could look for different signatures which represent an attack.
- Using Encryption mechanisms
- Traffic padding
- Keeping backups
- Use messaging techniques such as checksums, sequence numbers, digests, authentication codes

Fabrication

- fabrication is one of the four broad-based categories used to classify attacks and threats. A fabrication attack creates illegitimate information, processes, communications or other data within a system.
- Examples of Modification attacks:
  - SQL Injection
  - Route Injection
  - User / Credential Counterfeiting
  - Log / Audit Trail Falsification
  - Email Spoofing

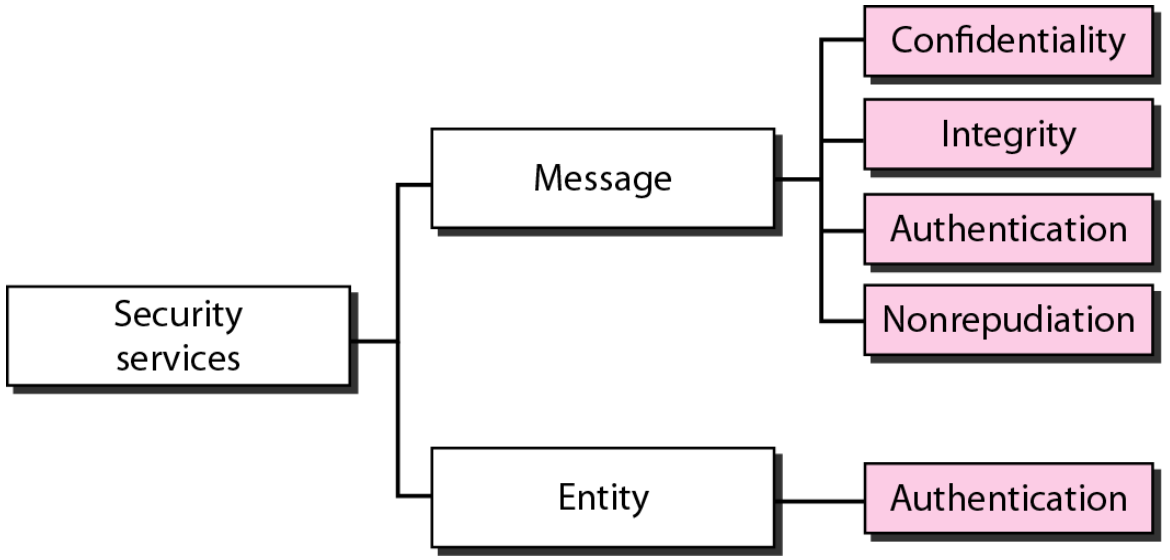


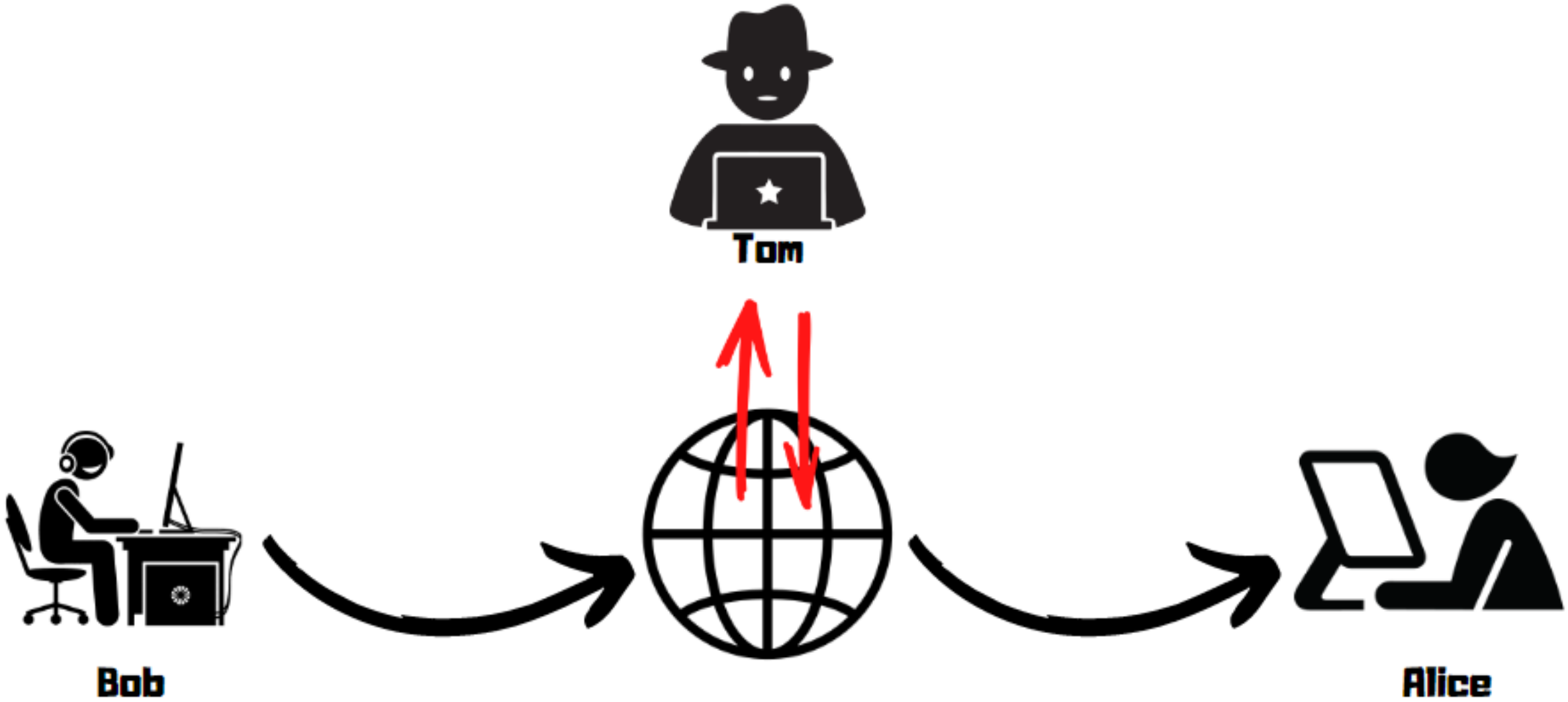
- Mitigate the attack :
- Use of Authentication and authorization mechanisms
- Using Firewalls
- Use Digital Signatures - Digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document.

Security Services

A security service is a capability that supports one or more of the security requirements (confidentiality, integrity, availability, authenticity, and accountability). Security services implement security policies and are implemented by security mechanisms.

- Processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms
  - Confidentiality (protect data from unauthorized disclosure)
  - Authentication (who created or sent the data)
  - Data Integrity (has not been altered)
  - Non-repudiation (the order is final)
  - Access control (prevent misuse of resources)
  - Availability (property of a system or a system resource being accessible and usable upon demand by an authorized system entity)
    - Denial of Service Attacks

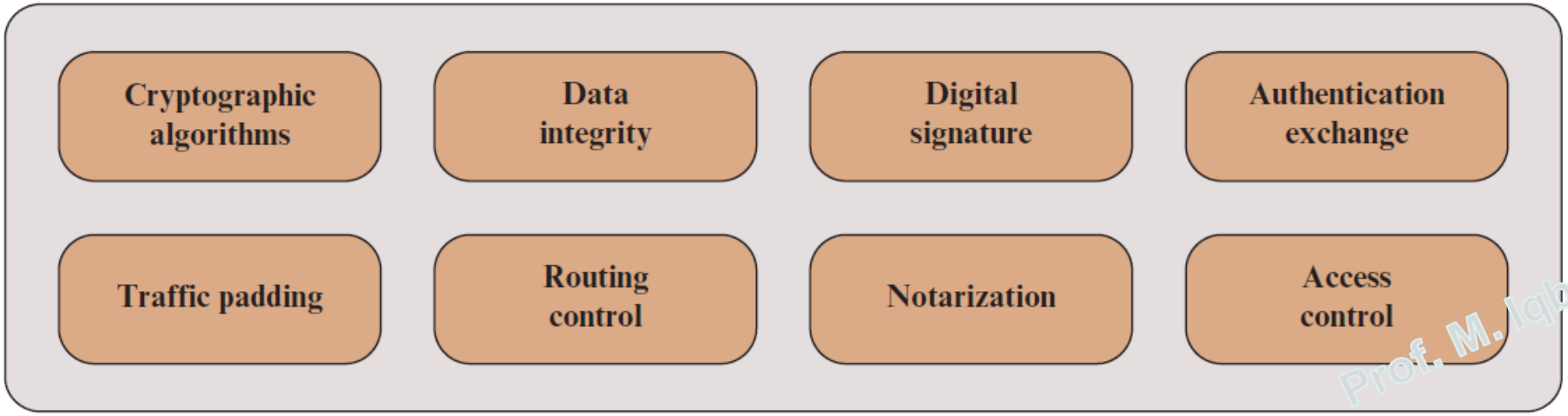



Tom
Bob
Alice

Security Mechanism

A mechanism that is designed to detect, prevent, or recover from a security attack

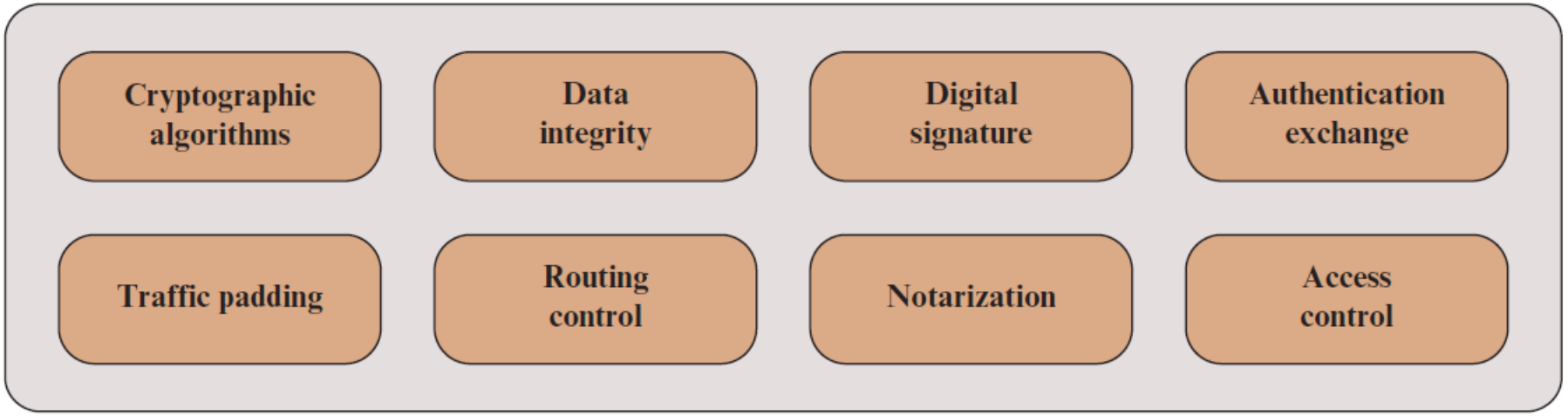
- **Cryptographic algorithms**: We can distinguish between reversible cryptographic mechanisms and irreversible cryptographic mechanisms. A reversible cryptographic mechanism is simply an encryption algorithm that allows data to be encrypted and subsequently decrypted. Irreversible cryptographic mechanisms include hash algorithms and message authentication codes, which are used in digital signature and message authentication applications.



Security Mechanism

A mechanism that is designed to detect, prevent, or recover from a security attack

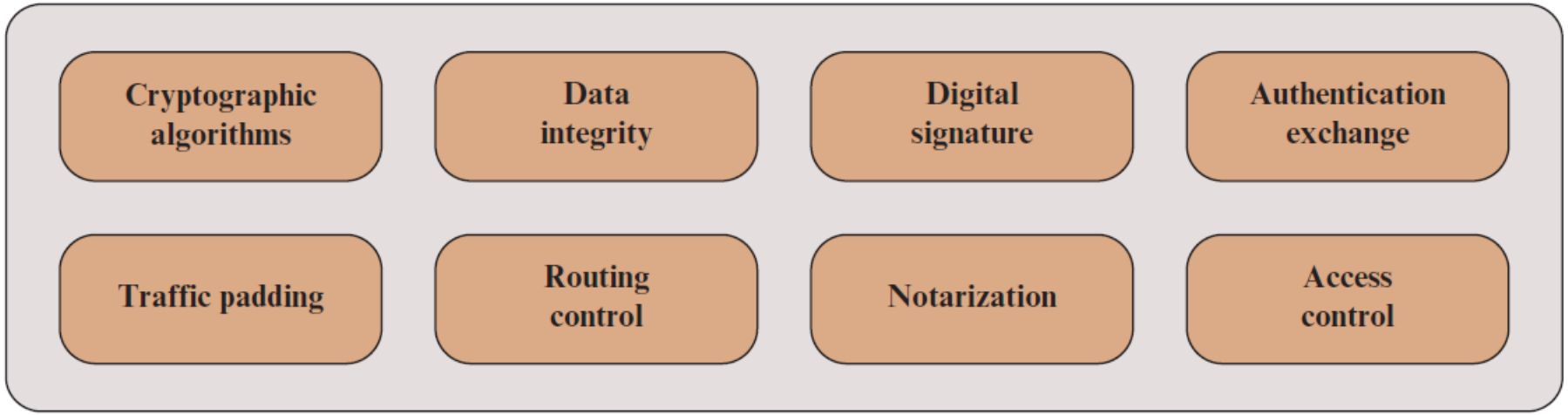
- **Data integrity:** This category covers a variety of mechanisms used to assure the integrity of a data unit or stream of data units.
- **Digital signature**: Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.



Security Mechanism

A mechanism that is designed to detect, prevent, or recover from a security attack

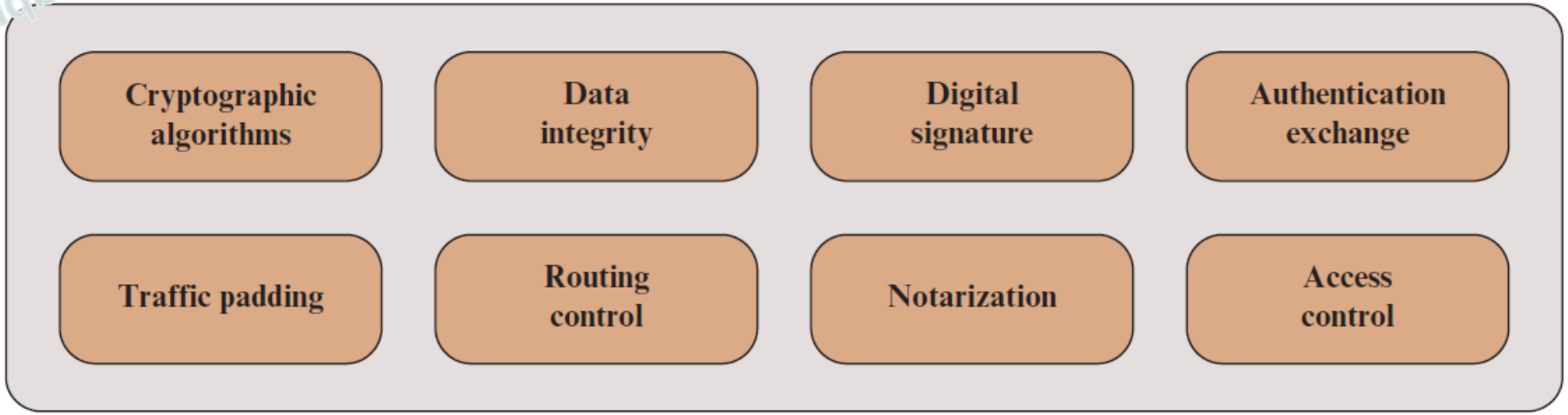
- **Authentication exchange:** A mechanism intended to ensure the identity of an entity by means of information exchange.
- **Traffic padding**: The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
- **Routing control**: Enables selection of particular physically or logically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.



Security Mechanism

A mechanism that is designed to detect, prevent, or recover from a security attack

- **Notarization:** The use of a trusted third party to assure certain properties of a data exchange.
- **Access control**: A variety of mechanisms that enforce access rights to resources.



Relation between security and services mechanism

Security Service	Security Mechanism
Data Confidentiality	Encipherment and routing control
Data Integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism