UNIVERSITY OF RAJSHAHI

Rajshahi, BANGLADESH.

Course Code:

ICE-4221

Course Title :

Fundamentals of Cryptography

Introductory Class

Course Details

Course Code: ICE 4221
Course Title: Fundamentals of Cryptography
Total Credit: 3 , Total Marks: 75
Total Lecture: 33 (Section A and B)
Exam Duration: 3 H

Section-A

Introduction to Classical Encryption
Block Cipher
Advanced & Contemporary Symmetric Cipher
Confidentiality Using Symmetric Encryption

Section-B

Public Key Encryption
Key Management and Elliptic Curve Cryptography
MAC and Hash Function
Hash Algorithm, Digital Signatures ad Authentication

Section – A

Introduction of Classical Encryption Techniques: Computer Security concepts, The OSI security architecture, A model for network security, Symmetric cipher model, Substitution cipher and Transposition cipher.

DES & Number Theory: Block cipher principles, The Data Encryption Standard, The strength of DES, Differential and linear cryptanalysis, Modular arithmetic, Euclid's algorithm, Finite fields, Polynomial arithmetic.

AES & Block Cipher Operation: The Origins of AES, AES structure, AES Round function, AES key expansion, AES cipher, Avalanche Effect, multiple encryption and triple DES, Block cipher modes of operation, Stream ciphers and RC4.

Key Management and Distribution: Symmetric key distribution using symmetric encryption and asymmetric encryption, Distribution of public key, public key infrastructure.

Section – B

Public-Key Encryption: Introduction to number theory, Principles of public-key cryptosystems, Applications for public-key cryptosystems, Requirements for public-key cryptography, the RSA algorithm.

Key Management and Elliptic Curve Cryptography (ECC): Key management, Diffie-Hellman key exchange, Elliptic curve arithmetic, ECC-key exchange using ECC, Elliptic curve encryption/decryption.

MAC and Hash Function: Authentication requirement, Authentication functions, Message authentication code, Hash functions, Security of hash functions and MACs, MD5 message digest algorithm, Secure hash algorithm, RIPEMD-160, HMAC.

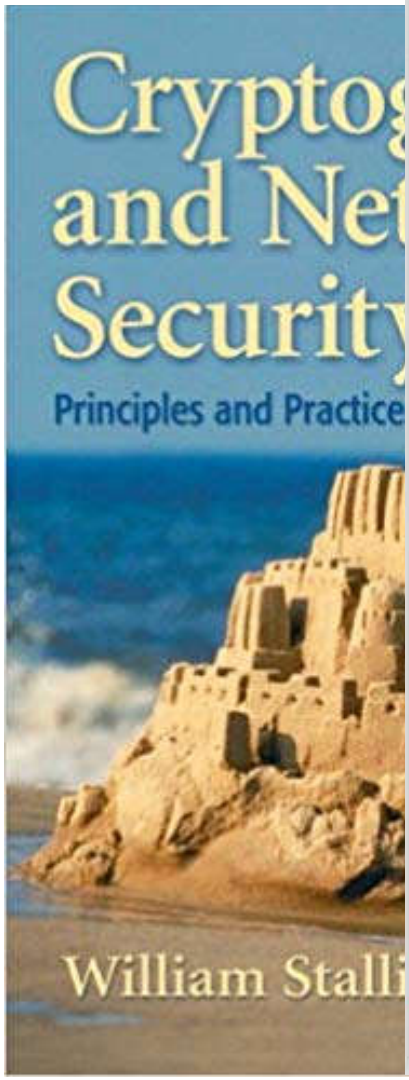
Hash Algorithm, Digital Signatures and Authentication Protocols: Secure hash algorithm, HMAC, HMAC design objectives, Digital signature, Authentication protocols, Digital signature standard, Mutual authentication, One-way authentication, Digital signature standard.

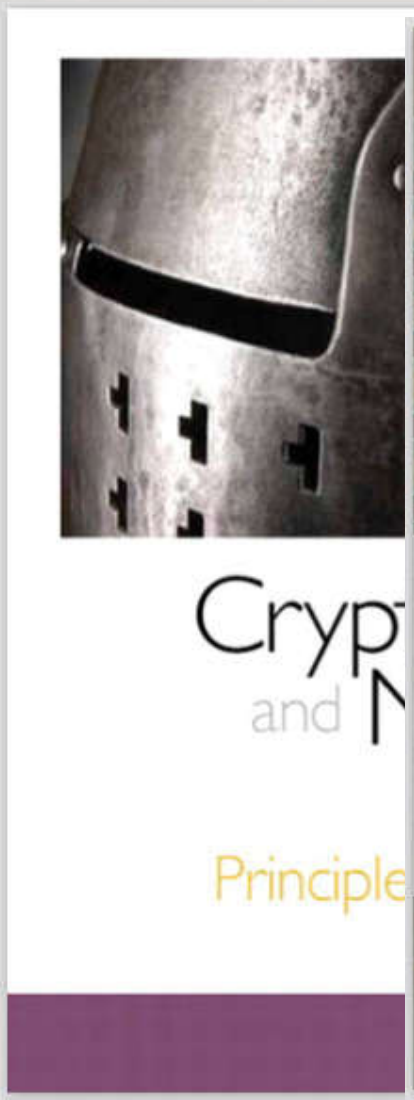
Text Books

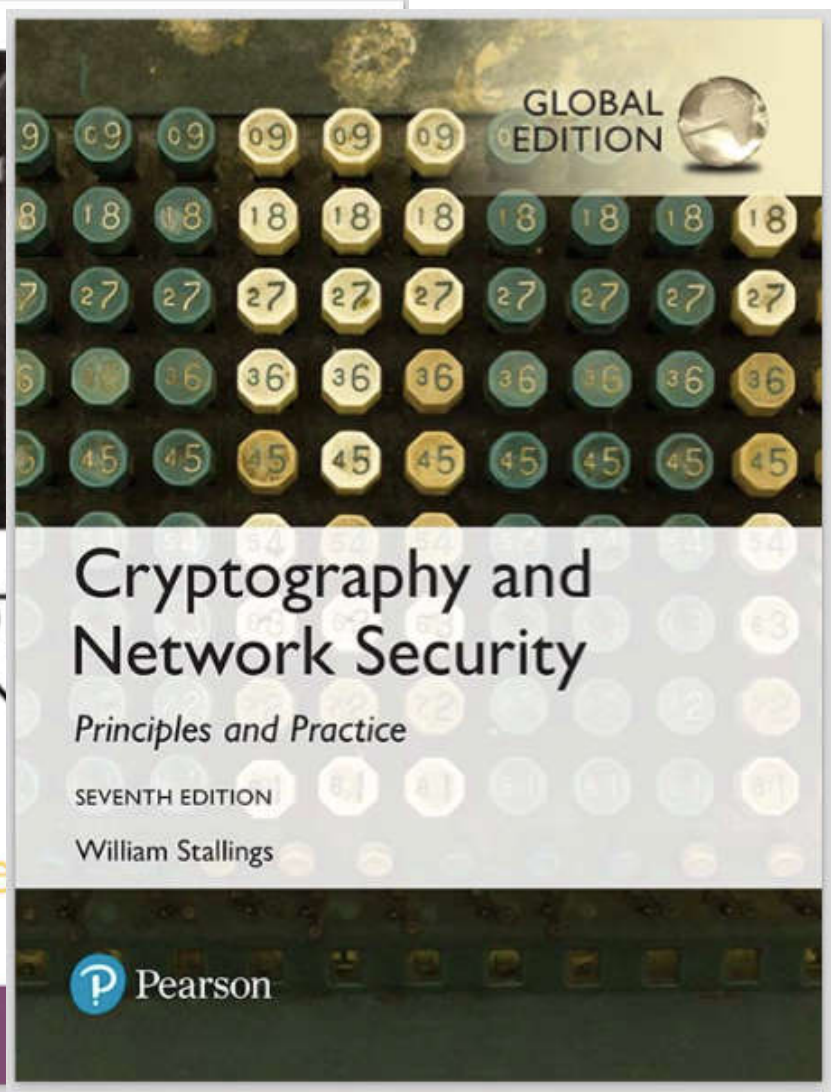
1. William Stallings : Cryptography and Network Security

Reference Books

2. Bruce Schneier : Applied Cryptography
3. Charles P. Pfleeger : Security in Computing

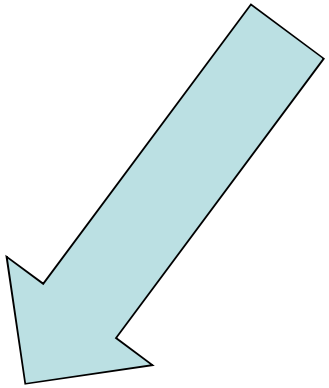


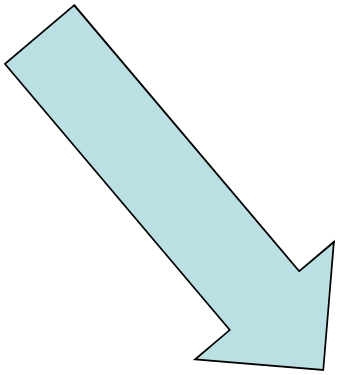




Cryptology

(Studying the techniques for ensuring the secrecy and/or authenticity of information)





Cryptography

(Studying of the design of such techniques for ensuring the secrecy and/or authenticity of information)

Cryptanalysis

(Dealing with the defeating such techniques, to recover information, or forging information that will be accepted as authentic)

Network Security

(Study to cover the use of cryptographic algorithms in network protocols and network applications)

Computer Security

(Study to covers the use of collection of tools (cryptographic algorithms) design to protect data and the thwart hackers)

Security Attacks

(Any actions that compromises the security of information owned by any organization)

- Can be happened in Network and/or Computers

A useful way to classifying security attacks is …

- Passive attacks, and
- Active attacks

✓ A Passive attacks attempts to learn or make use of Information from the system but does not affect system resources.

✓ An Active attacks, on the other hand, attempts to alter system resources or affect their operation.

Security Attacks (Cont')

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.

TWO types of passive attacks are …

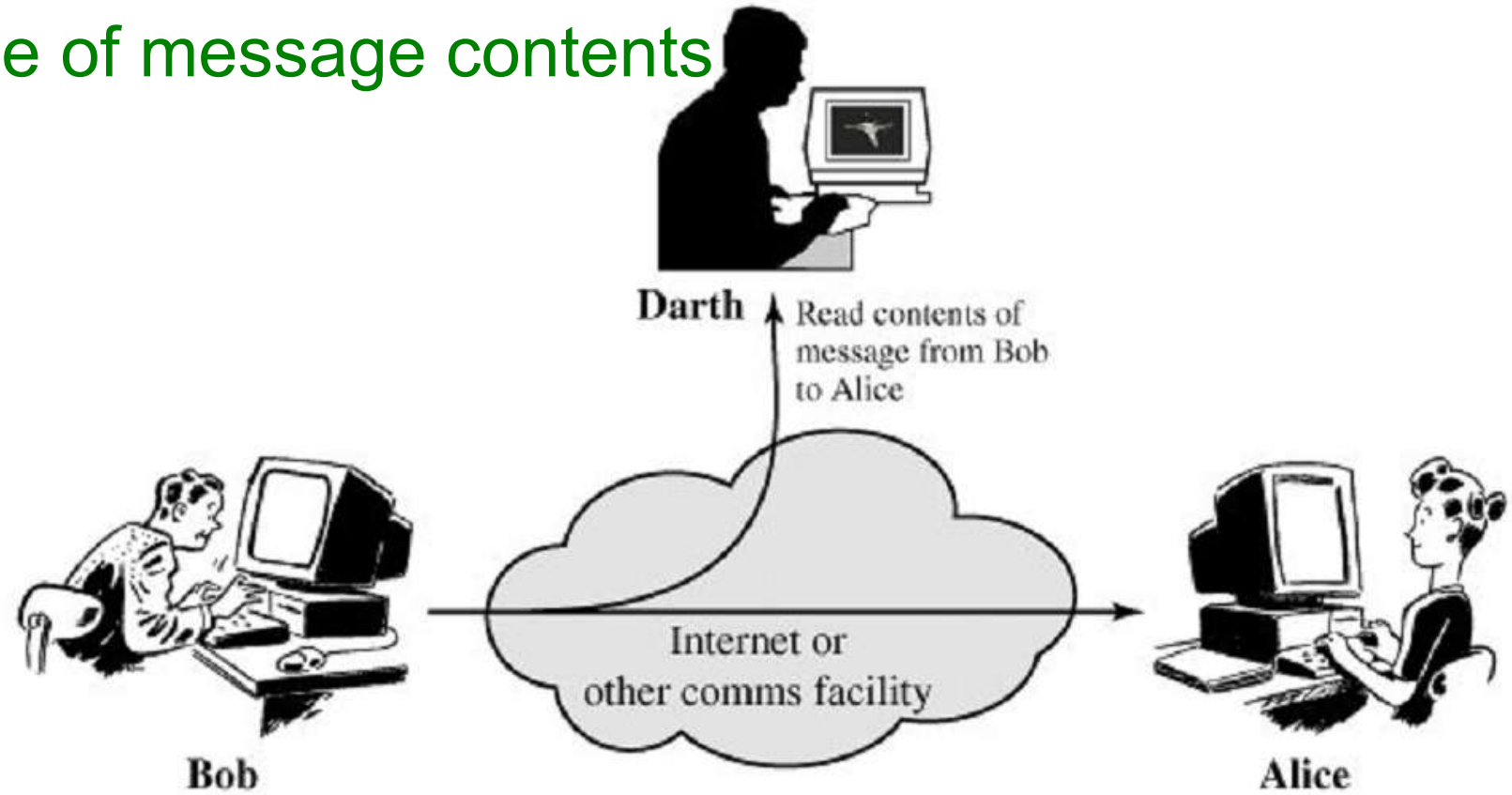
✓Release of message contents and

✓Traffic analysis.

Security Attacks (Cont')

Passive Attacks

Release of message contents

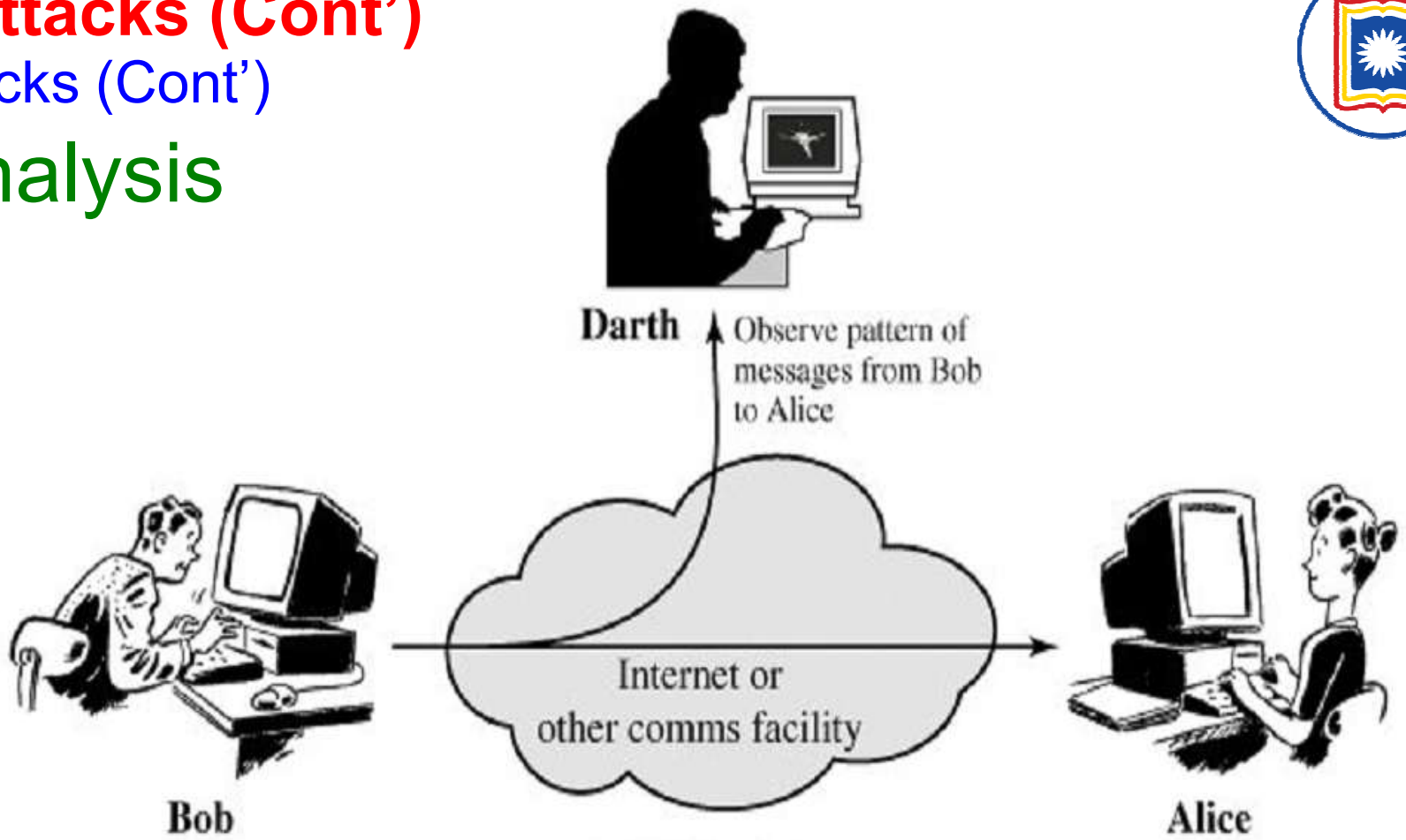


A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

Security Attacks (Cont')

Passive Attacks (Cont')

Traffic analysis

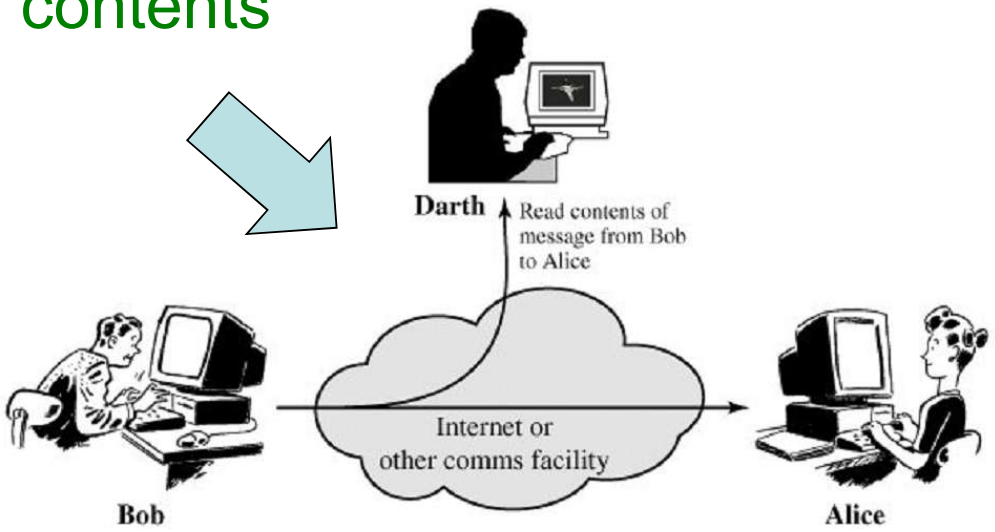


The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

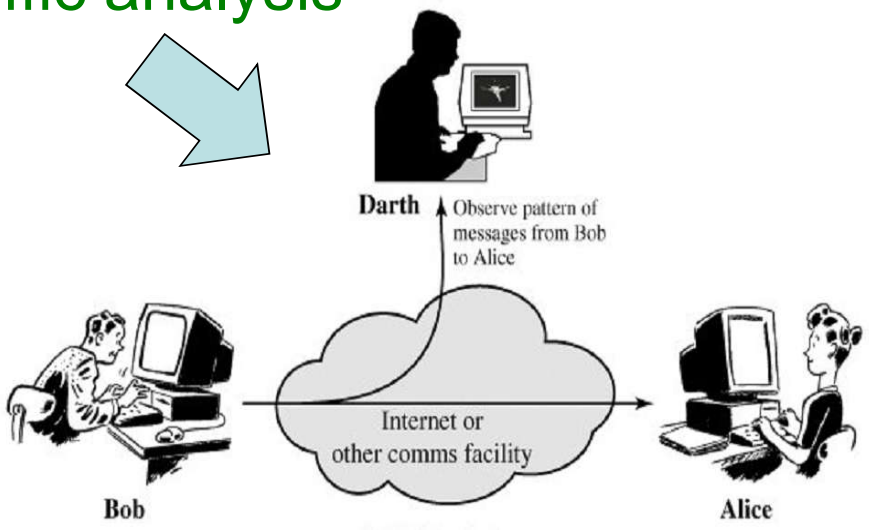
Security Attacks (Cont')

Passive Attacks (Cont')

Release of message contents



Traffic analysis



✓Passive attacks are very difficult to detect because they do not involve any alteration of the data.

✓Typically, the message traffic is sent and received in an apparently normal fashion and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.

✓However, it is feasible to prevent the success of these attacks

Security Attacks (Cont')

Active Attacks

Active attacks involve some modification of the data stream or the creation of a false stream.

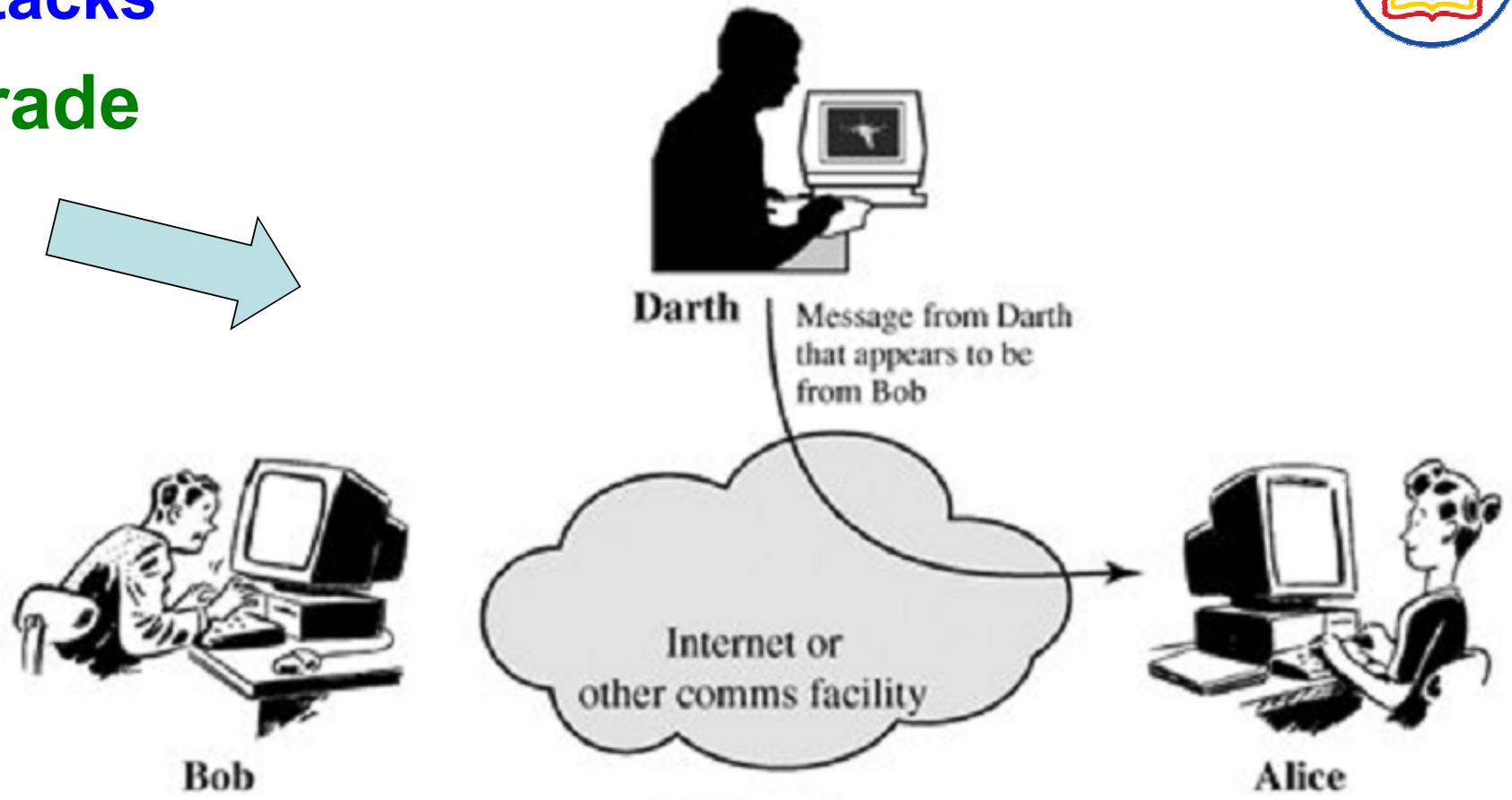
Active Attacks can be FOUR categories:

- ✓Masquerade,
- ✓Replay,
- ✓Modification of messages, and
- ✓Denial of service.

Security Attacks (Cont')

Active Attacks

Masquerade

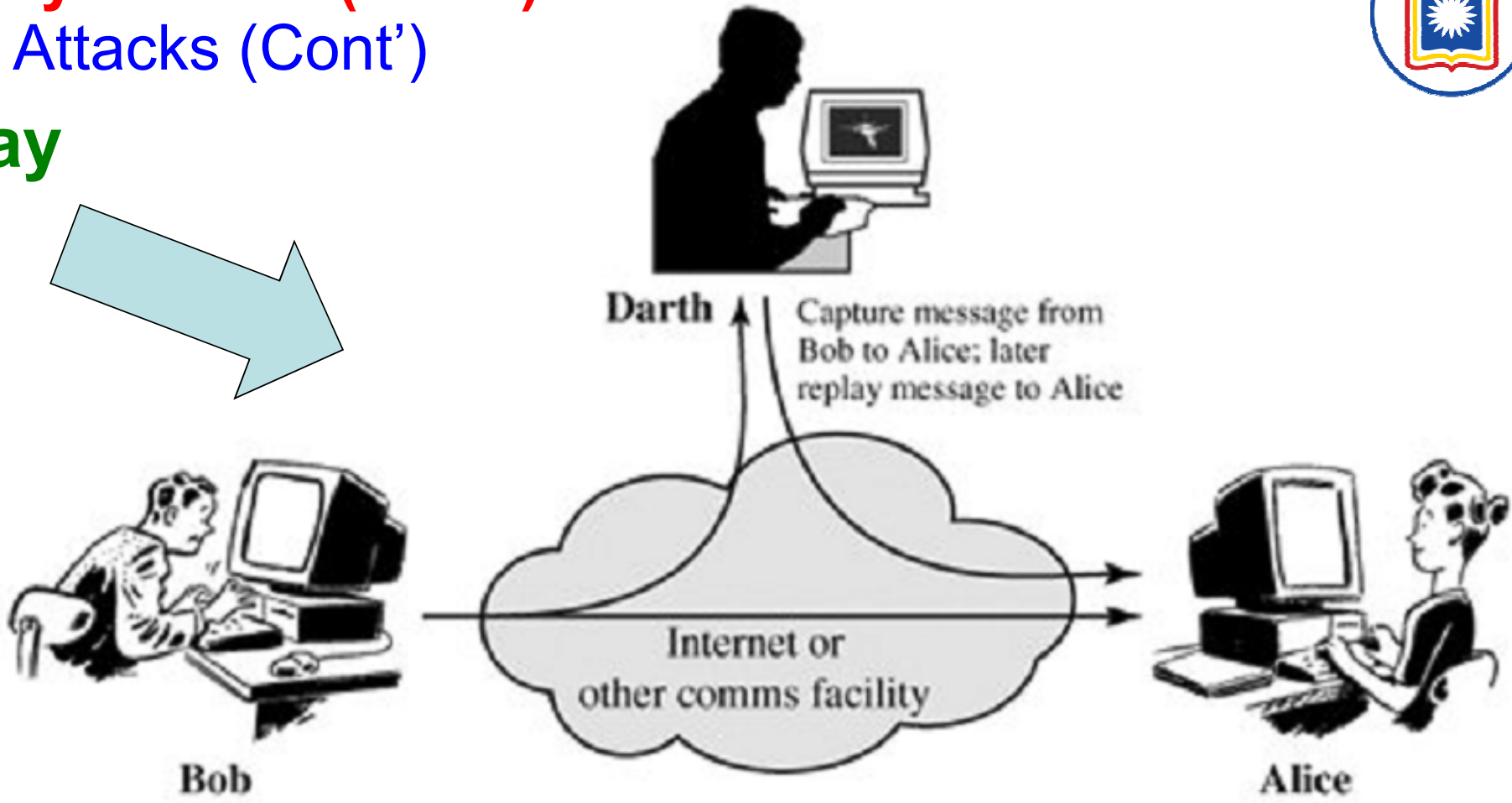


A **masquerade** takes place when one entity pretends to be a different entity . A masquerade attack usually includes one of the other forms of active attack.

Security Attacks (Cont')

Active Attacks (Cont')

Replay

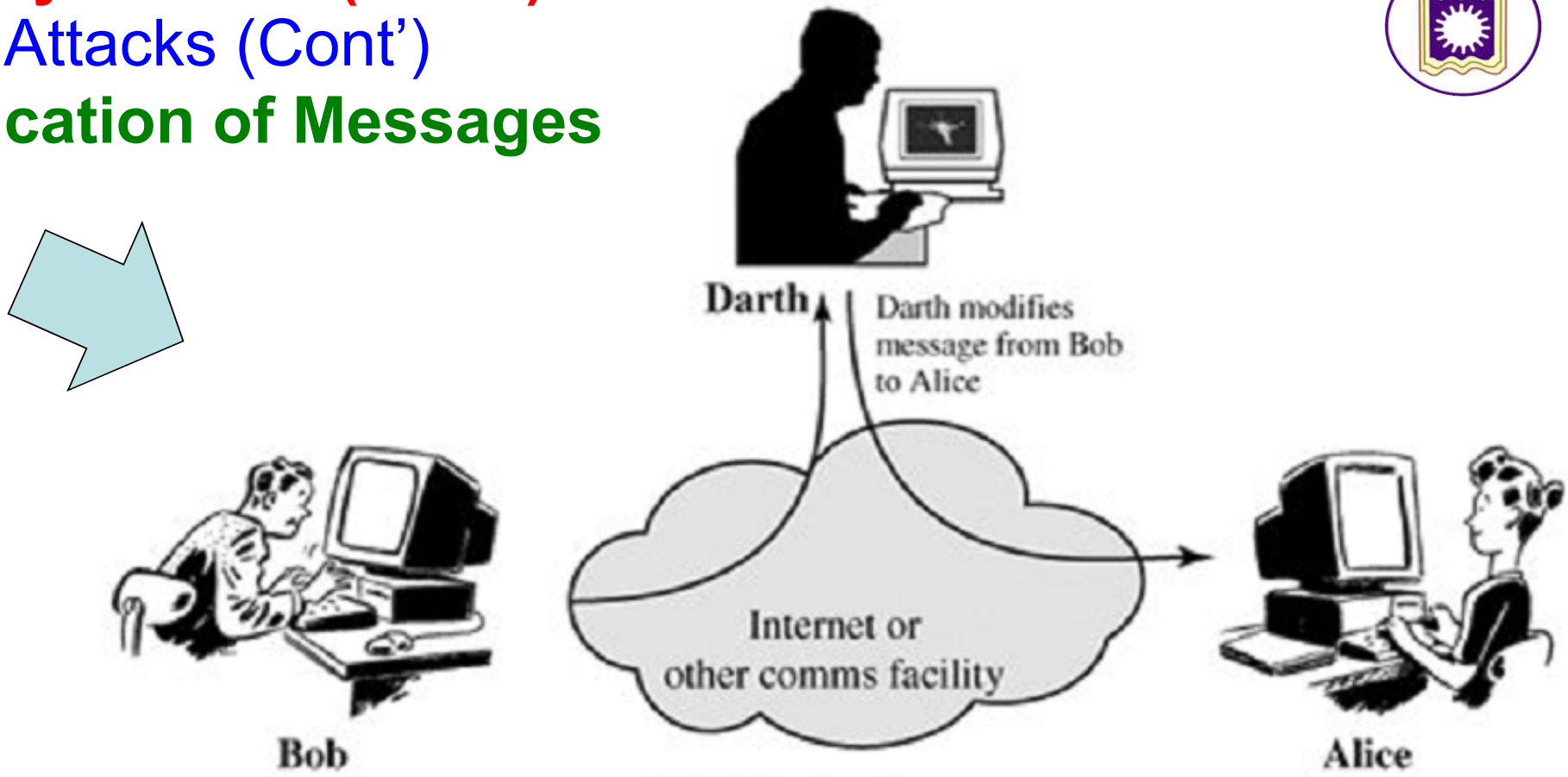


Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

Security Attacks (Cont')

Active Attacks (Cont')

Modification of Messages

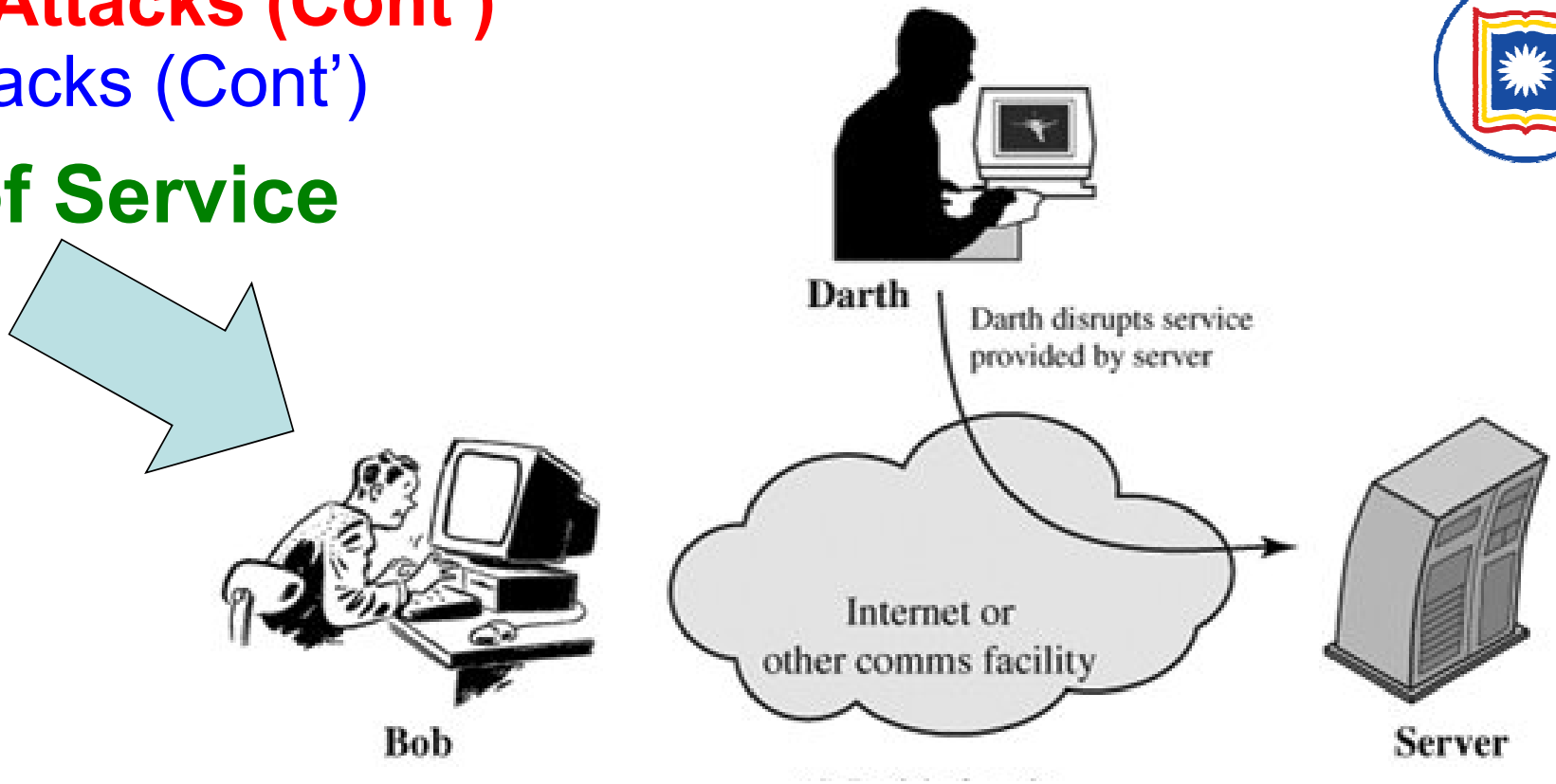


Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.

Security Attacks (Cont')

Active Attacks (Cont')

Denial of Service



The **denial of service** prevents or inhibits the normal use or management of communications facilities

Security Attacks (Cont')

Comparative Study of Active Attack and Passive Attack

(Active attacks present the opposite characteristics of passive attacks)

- **Passive attacks are difficult to detect, measures are available to PREVENT their success.**
- On the other hand, **it is quite difficult to prevent active attacks absolutely**, because of the wide variety of potential physical, software, and network vulnerabilities.
- **Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them.**

Security Services?

A processing or communication service that enhances the security of the data processing system and the information transfers of an organization.

- The services are intended to counter security attacks, and
- They make use of one or more **SECURITY MECHANISMS** to provide the services.

Security Services (Cont)

- **Security Services includes:**
  - **Authentication**
  - **Data Confidentiality**
  - **Data Integrity**
  - **Access Control**(access control is the ability to limit and control the access to host systems and applications via communications links.)
  - **Nonrepudiation, and**
  - **Availability** (availability to be the property of a system or a system resource being accessible and usable upon demand by an authorized system entity

Security Mechanisms ?

A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

- **Examples of security mechanisms are:**
  - **Encryption Algorithm**
  - **Digital Signature**
  - **Digital Envelope**
  - **Authentication Protocols**

Computer and Network Security

Computer and Network Security address FOUR requirements:

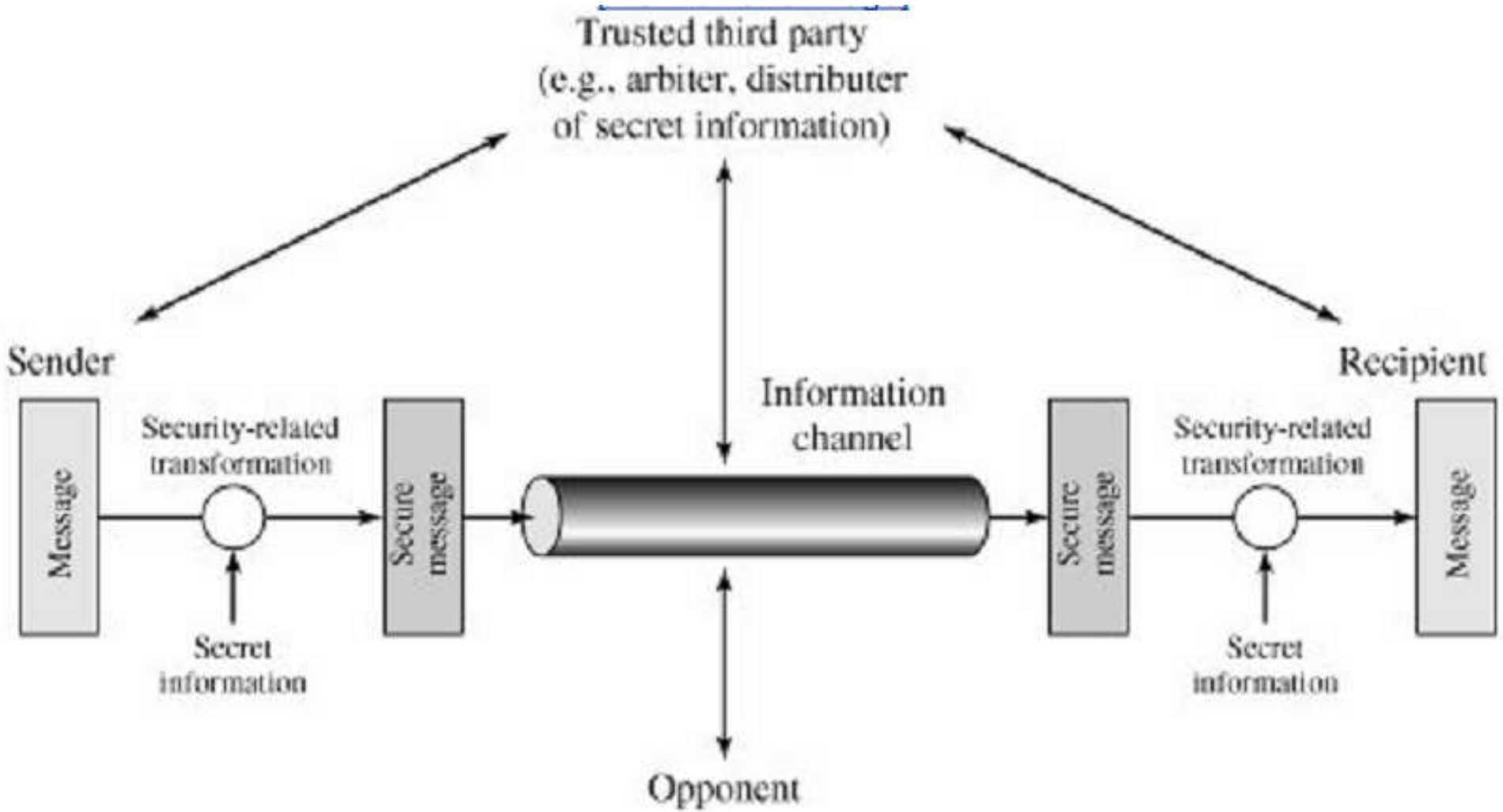
✓ **Confidentiality-** Requires that data only be accessible by authorized parties. This types of access including printing, displaying, and other forms of disclosure.

✓ **Integrity-** Requires that data can be modified only by authorized parties. Modification includes writing, changing, changing status, deleting, and creating.

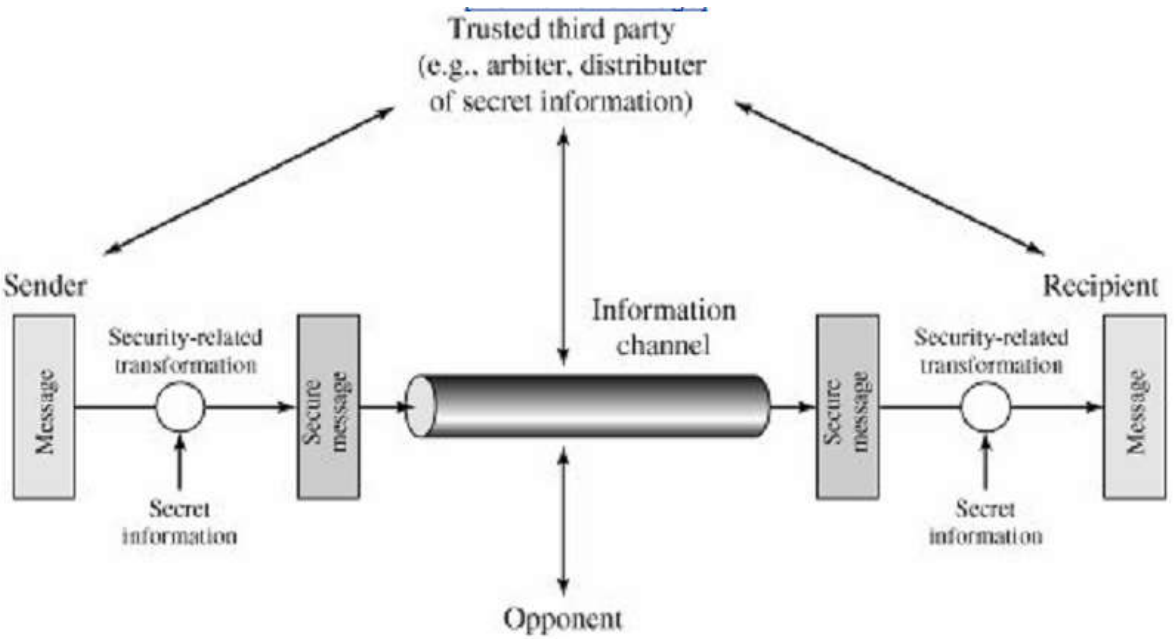
✓ **Availability-** Requires that data are available to authorized parties.

✓ **Authenticity-** Requires that a host or services be able to verify the identity of a user.

A Model for Network Security



A Model for Network Security (Cont')



All Security mechanisms/techniques for providing security have TWO components:

- ✓ A security-related transformation on the information to be sent.
- ✓ Some secret information shared by the two principals and, it is hoped, unknown to the opponent.

Tasks in Designing a Particular Security Services

- **Design an algorithm** for performing the security-related transformation.
- **Generate the secret information (Key)** to be used with the algorithm
- **Develop methods for the distribution and sharing** of the secret information (key).
- **Specify a protocol to be used** by the two principals that makes use of the security algorithm and the secret information.

Network Access Security Model