CRYPTOGRAPHY AND SYSTEM SECURITY

MODULE 1 – Introduction and Number Theory

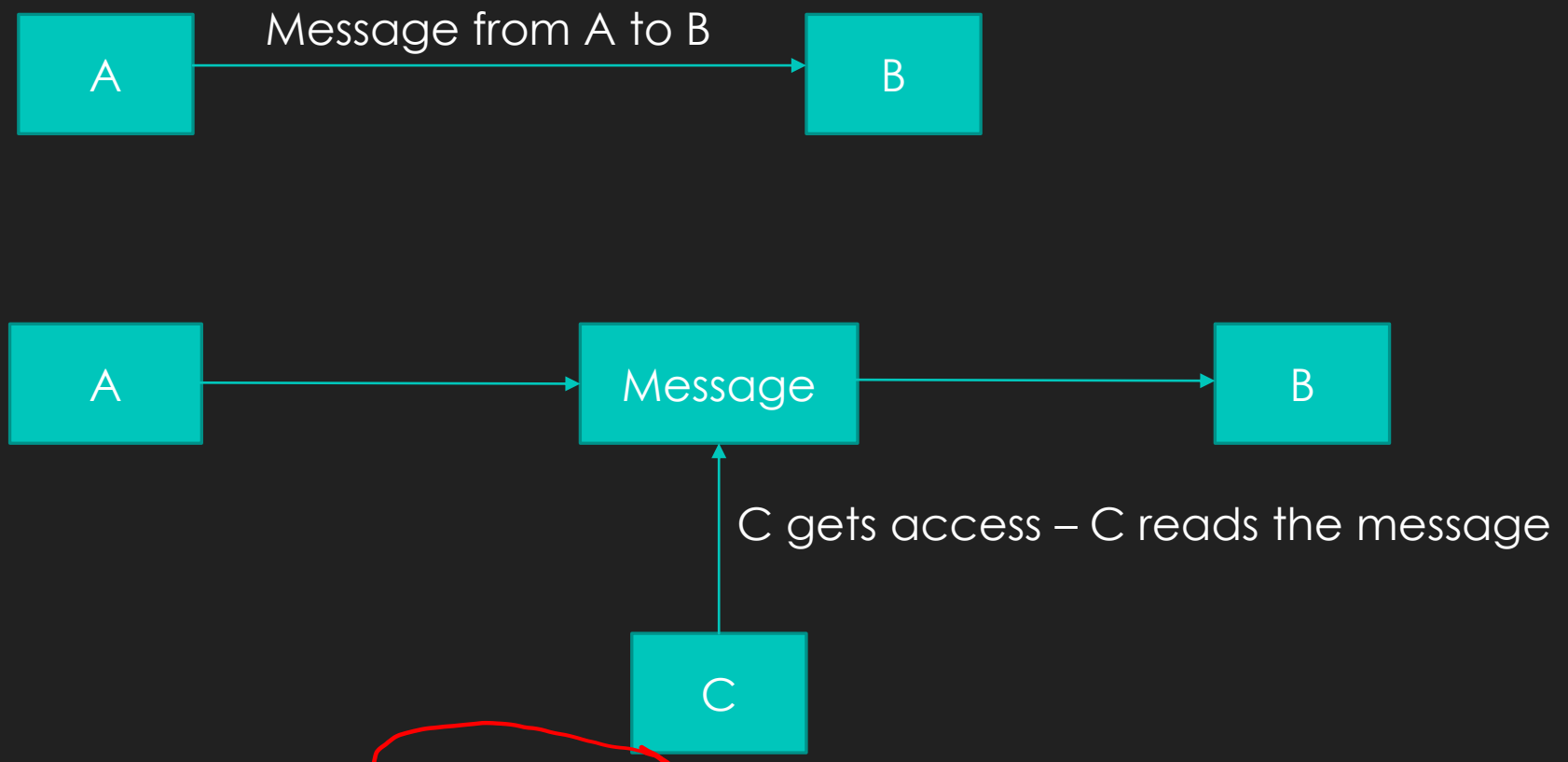
Prof. Sarala Mary – APSIT – Department of CSE – Data Science

Principles/Services of Security

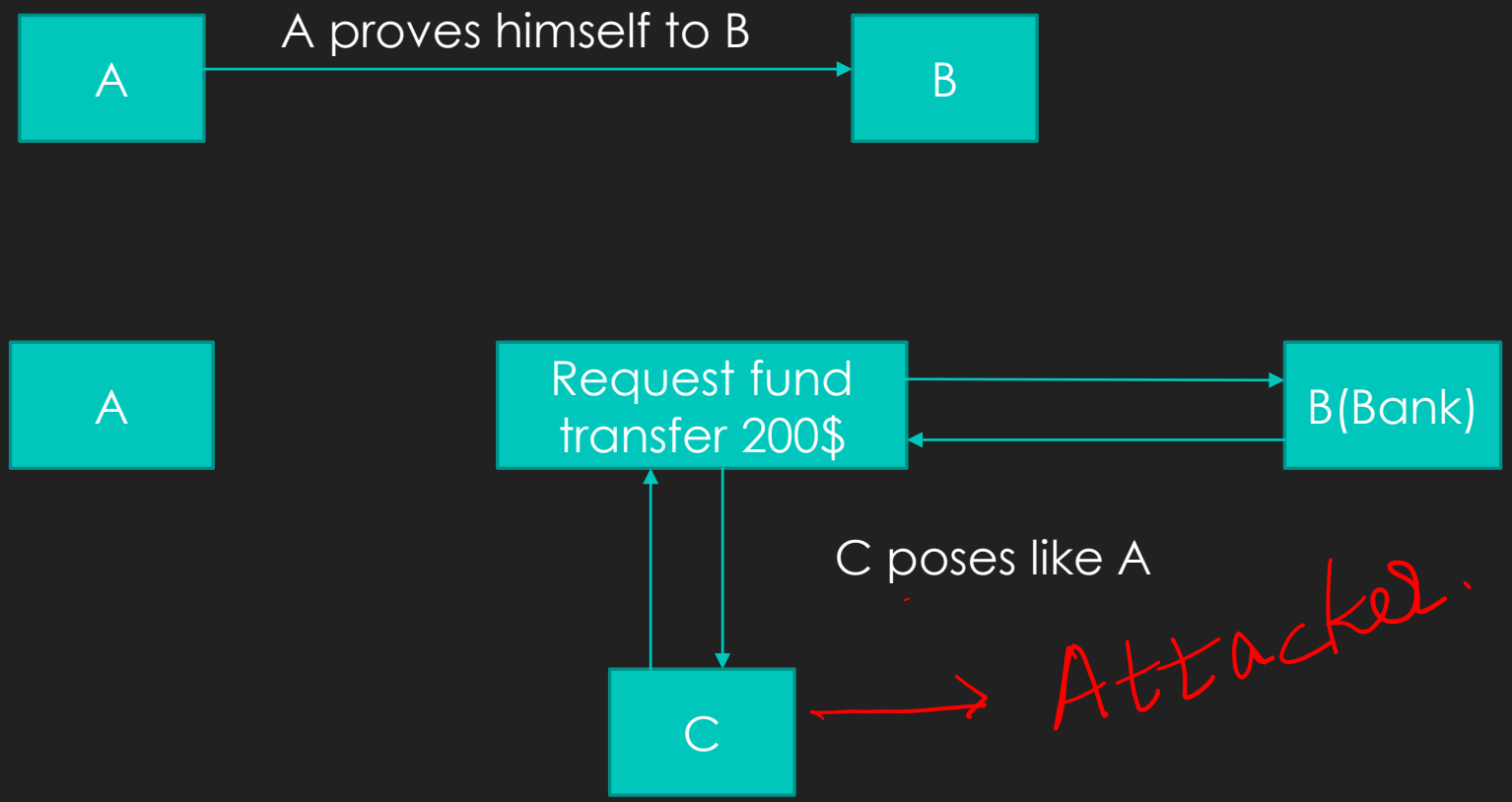
PRINCIPLES/SERVICES OF SECURITY

- Confidentiality → Cryptography
- Authentication
- Integrity → Digital Signature
- Non – Repudiation
- Access Control
- Availability

Confidentiality

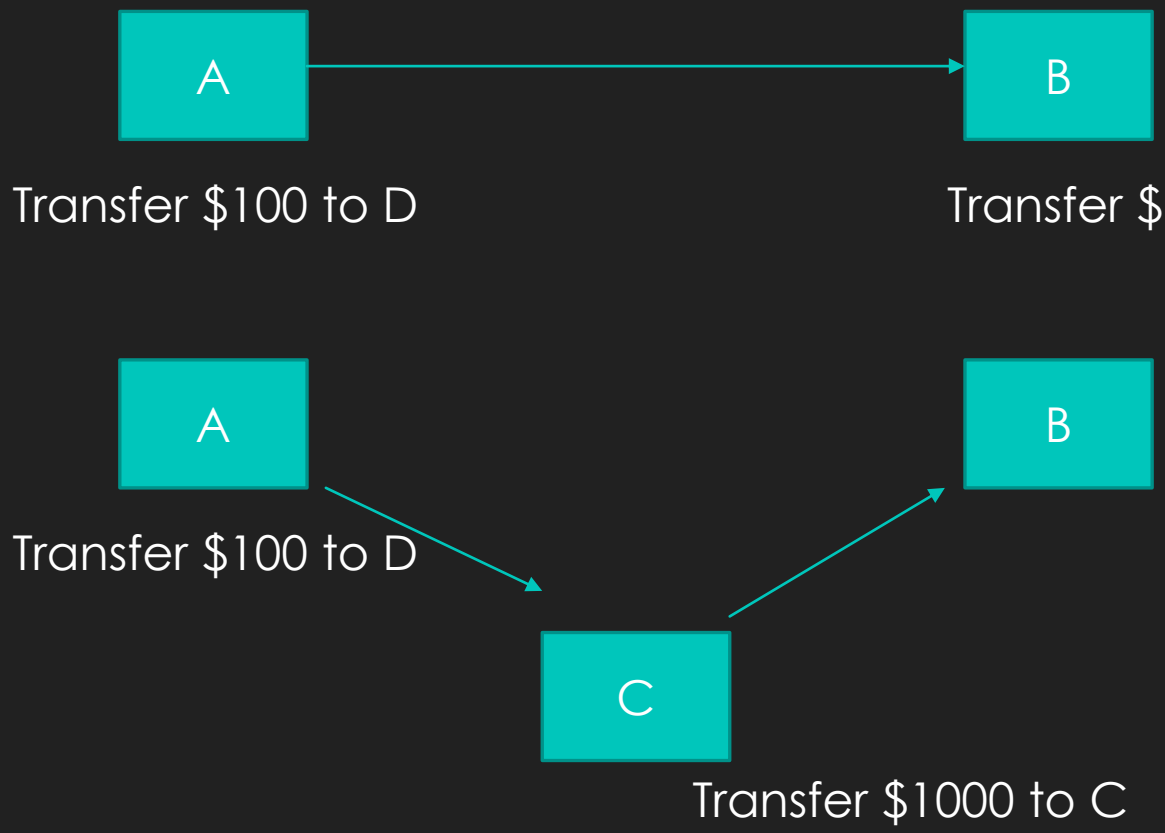


Authentication



Fabrication – It is possible in absence of proper authentication

Integrity



Everyone can read msg But nobody should modify the msg

Modification – Loss of Integrity

Quiz 1

The principle of only sender and receiver should be able to read the message is known as

a) Confidentiality
b) Integrity
c) Authentication

Answer: a

Quiz 2

The attack against confidentiality is known as

a) Fabrication
b) Interception
c) Modification

Answer: b

Quiz 3

The data must arrive at receiver exactly as they were sent, its called

a) Message Confidentiality.
b) Message Integrity.
c) Message Sending.

Answer: b

Quiz 4

Lack of Authentication is known as

a) Confidentiality
b) Modification
c) Fabrication

Answer: b

Quiz 5

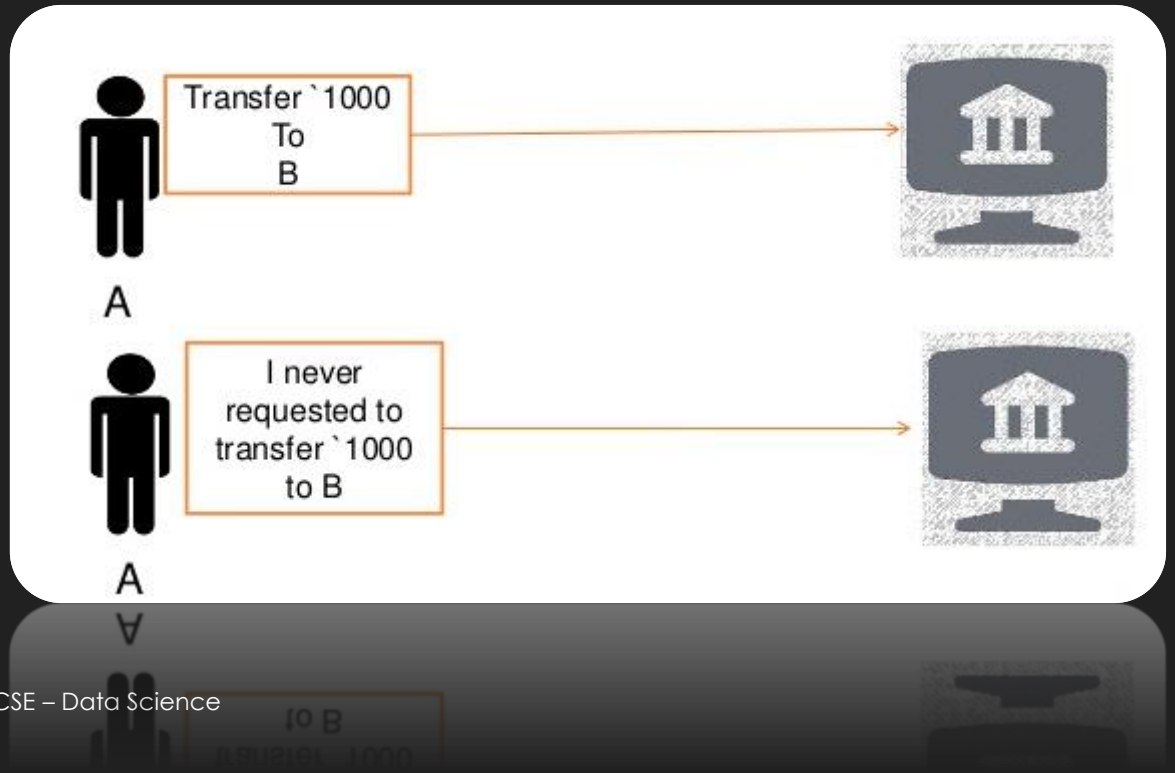
Modification is caused due to

a) Lack of Confidentiality
b) Lack of Authentication
c) Lack of Integrity

Answer: c

Non - Repudiation

User sends a message and later on denies that he or she has not send that message.



Access Control

Access Control determines who should be able to do what.

- Role Management
- Rule Management

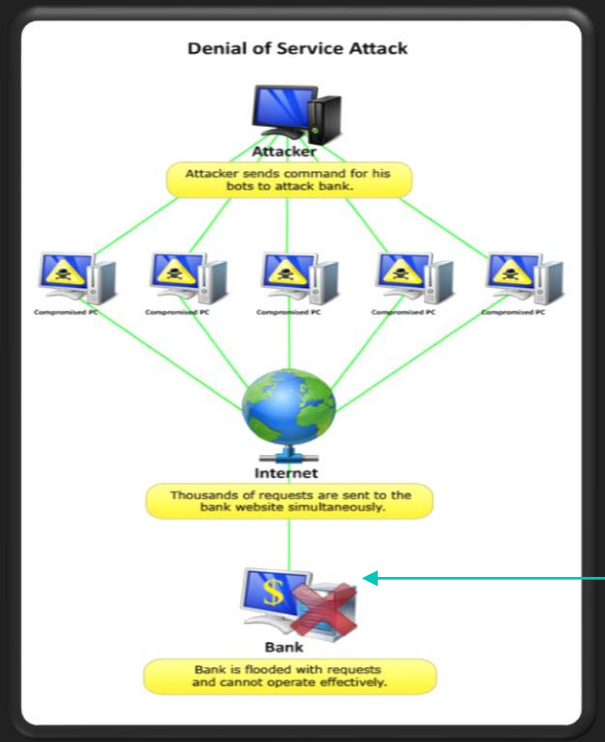
Example

chmod → used to change the file permissions

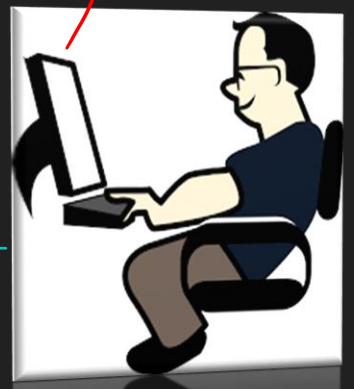
Role of faculty and student with different rule.

Availability

- Resources should be available to authorized person at all time.



Access Denied



Authorized user!

Interruption - exploit against Availability

Principles/Services/Mechanism

Sr.No.	Services	Attacks and Example	Mechanism
1.	**Confidentiality**	Interception – Packet sniffing	Encipherment – Symmetric and Asymmetric key Cryptography
2.	**Authentication**	Fabrication – Phishing/Password Hacking	Authentication Protocol, Hashing algorithm
3.	**Integrity**	Modification - Man in the middle attack, Data Didling	Digital Signature
4.	**Non – Repudiation**	Denial by Sender	Digital Signature
5.	**Access Control**	Exploiting sudo rights	Access Control List
6.	**Availability**	Interruption – Denial of Service, Distributed Denial Of System	Intrusion Detection System, Firewall Honey pots

Quiz 1

Which is not an objective of network security?

a) Non - Repudiation
b) Authentication
c) Access control
d) Lock mechanism

Answer: d

Quiz 2

DOS attack exploits _____ service.

a) Confidentiality
b) Non – Repudiation
c) Availability
d) Integrity

Answer: c

Quiz 3

In confidentiality, the transmitted message must make sense to only

a) Receiver
b) Sender
c) Modular
d) Translator

Answer: a

Quiz 4

A sender must not be able to deny sending a message that was sent, is known as

a) Non – Repudiation
b) Integrity
c) Confidentiality

Answer: a

Quiz 5

Digital Signature is a mechanism used to achieve

a) Confidentiality
b) Integrity
c) Access Control
d) Availability

Answer: b