**FUNDAMENTALS OF CRYPTOGRAPHY LEC 02**

**CIA** – Same as Fundamentals of Data Security. However mainly talk about C and I.

**OSI Architecture**

**Security Attack**: An action compromising security of information.

Passive or active attacks.

**Security Mechanism:** Process that detect, prevents or recover from an attack.

**Security Services:** Service to counter attacks using mechanisms.

**Security Services**

* Authentication – Main concern
* Access control
* Data confidentiality
* Data Integrity
* Nonrepudiation

**Techniques for Cyber Security**

* Encryption
* Digital Signature
* Hash functions for integrity check
* Authentication exchange protocol
* Packet Filters
* Intrusion Detection

**Architecture model**

**Information Channel:** TCP/IP Connection

**A:** Sender – encryption, authentication

**B:** Receiver – decryption, verification

**Third party:** in charge of key distribution or arbitrator for disputes

**Opponent:** can be hackers or any threats

**Packet Filters**

**Route Filter:** verifies sources and destination of IP addressed

**Packet Filter:** Scans headers of packets and discards if rule set failed

**Content Filter:** Scans content of packets and discards if rule set failed

**Dematerialised zone**

A sub-network that separates an internal network from other untrusted networks (like internet). This sub network can access the internet but cannot reach the main internal LAN.