Module 5 : CS - Cryptography and Network

Security

1. **Mitigation** in the context of **cybersecurity** refers to the strategies, practices, and tools used to **reduce or minimize the impact** of **cybersecurity threats, vulnerabilities,** and **risks.**

2. The primary role of an IDS is to **detect** malicious activity or violations of security policies within a network or system

An IPS has a similar role to an IDS, but its key difference is that it **actively prevents** detected threat.

3. A **Network-based Intrusion Detection System (NIDS)** is a type of Intrusion Detection System (IDS) that is deployed at various points within a **network** to monitor and analyze traffic for signs of malicious activities, policy violations, or attacks.

4. **SSL (Secure Sockets Layer)** and **TLS (Transport Layer Security)** are cryptographic protocols designed to secure communications over a computer network, such as the internet. They provide **data encryption, authentication**, and **integrity** to ensure that the information exchanged between clients (such as browsers) and servers (such as websites) remains private and secure.

5. In **symmetric key cryptography**, the **same key is** used for both **encryption** (transforming plaintext into ciphertext) and **decryption** (transforming ciphertext back to plaintext).

In **asymmetric key cryptography**, two **different keys** are used: a **public key** for encryption and a **private key** for decryption. The public key is shared openly, while the private key is kept secret.

6. A **VPN (Virtual Private Network)** is a technology that creates a secure, encrypted connection over a less secure network, such as the internet.

**IPSec (Internet Protocol Security)** is a suite of protocols designed to secure internet protocol (IP) communications by authenticating and encrypting each IP packet in a communication session.