Module 5: Cryptography & Network Security:

---

1. Explain Mitigation in reference to Cyber Security.

Mitigation refers to techniques and actions used to **reduce the impact of cyber threats**.
It does not remove the threat completely but **minimizes damage**, such as:

- Using firewalls, antivirus, IDS/IPS
- Patching software
- Creating backups
- Applying access control and encryption

---

2. Difference between IDS & IPS

Feature	IDS (Intrusion Detection System)	IPS (Intrusion Prevention System)
Action	Detects attacks	Detects + blocks attacks
Mode	Passive	Active
Placement	Outside traffic flow	Inline with traffic
Example	Alerts admin	Drops malicious packets

---

3. Explain Network-based IDS

A Network-based IDS (NIDS):

- Monitors **network traffic** in real-time
- Detects suspicious activity, attacks, or policy violations
- Uses signatures and anomaly detection
- Placed at strategic locations (e.g., near firewall)
- Examples: Snort, Suricata

---

4. Explain How SSL & TLS Work

SSL/TLS is used to secure communication over the internet.

How it works (simple steps):

1. Client sends a connection request to the server.
2. Server sends its **digital certificate**.
3. Client verifies certificate using CA.

4. Both generate a **session key** (symmetric key).
5. All further communication is **encrypted** using session key.

TLS is the upgraded version of SSL.

---

5. Symmetric vs Asymmetric Key Cryptography

Symmetric Key

- Uses **one key** for encryption and decryption
- Fast but less secure
- Example: AES, DES

Asymmetric Key

- Uses **two keys** (public + private)
- More secure but slower
- Example: RSA, ECC

---

6. How to Secure Server and Personal Computers

Secure Server

- Use firewalls & antivirus
- Apply OS and software updates
- Enable encryption (SSL/TLS)
- Disable unnecessary services and ports
- Use strong passwords and multi-factor authentication
- Take regular backups

Secure Personal Computer

- Install antivirus
- Keep OS updated
- Use firewall
- Avoid suspicious downloads
- Use strong passwords
- Enable disk encryption
- Backup important files

---

7. Explain Suricata and SolarWinds

Suricata

- Open-source IDS/IPS and network security monitoring tool
- Detects threats using signatures + anomalies
- Used for real-time traffic analysis

SolarWinds

- Network monitoring and management tool
- Helps track performance, detect failures, and manage devices
- Known for tools like Orion Platform, Network Performance Monitor

---

8. Describe VPN and IPSec

VPN (Virtual Private Network)

A secure tunnel that encrypts internet traffic, allowing safe communication over public networks. Used for remote access and privacy.

IPSec (Internet Protocol Security)

- A protocol suite used to secure IP communication
- Provides confidentiality, integrity, and authentication
- Works in **Tunnel Mode** (entire packet encrypted)
- Used commonly in **VPNs**