Module 5 : CS - Cryptography and Network

1. Mitigation in Cyber Security
Mitigation means reducing risks and minimizing the impact of cyber threats by implementing measures like firewalls, patches, backups, and monitoring systems.

2. Difference Between IDS & IPS
IDS (Intrusion Detection System): Detects threats and alerts but doesn't act.
IPS (Intrusion Prevention System): Detects and actively blocks threats in real-time.

3. Network-Based IDS
A Network-Based IDS inspects network traffic to identify and alert on suspicious or malicious activities. It focuses on monitoring data packets across the network.

4. How SSL & TLS Work
SSL and TLS secure communication by encrypting data, authenticating servers/clients, and creating secure sessions through a handshake. TLS is the improved version of SSL.

5. Symmetric vs Asymmetric Key Cryptography
Symmetric: One key is used for both encryption and decryption (fast, less secure).
Asymmetric: Uses a public key for encryption and a private key for decryption (secure, slower).

6. How to Secure Servers and Personal Computers
Use firewalls and antivirus tools.
Enable regular updates and patches.
Apply strong passwords and multi-factor authentication.
Limit access and backup data regularly.

7. Suricata and SolarWinds
Suricata: An open-source tool for detecting and preventing intrusions, and analyzing network traffic.
SolarWinds: A commercial tool for monitoring networks, performance, and detecting security issues.

8. VPN and IPSec
VPN: Encrypts internet connections for private and secure browsing.
IPSec: A protocol for securing IP communications via encryption and authentication. Often used in VPNs.