**Week 3: Encryption, VPNs & Security Protocols**

**Objective:** Study encryption standards and secure communication protocols.

**Task#03: Research common security protocols: HTTPS, SSL/TLS, SSH, IPSec — document their purpose.**

**Solution:**

**1. HTTPS (Hypertext Transfer Protocol Secure)**

* **Purpose:** HTTPS is an extension of the Hypertext Transfer Protocol (HTTP) that adds a layer of security. Its primary purpose is to **provide secure communication over a computer network**, most notably on the Internet. It ensures:
  + **Data Encryption:** All data exchanged between your browser and the website is encrypted, protecting it from eavesdropping by malicious actors.
  + **Data Integrity:** It verifies that the data has not been tampered with or altered during transit.
  + **Authentication:** It authenticates the server (and sometimes the client), ensuring you are communicating with the intended website and not an imposter. This is typically achieved through SSL/TLS certificates.

**2. SSL/TLS (Secure Sockets Layer / Transport Layer Security)**

* **Purpose:** SSL and its successor, TLS, are cryptographic protocols designed to **provide communication security over a computer network**. They are foundational technologies used by HTTPS.
  + **Encryption:** They encrypt the data exchanged between applications and servers.
  + **Authentication:** They verify the identity of the communicating parties (typically the server, but sometimes the client too) using digital certificates.
  + **Integrity:** They ensure that the data has not been altered during transmission.
  + **Relationship to HTTPS:** TLS is the underlying protocol that HTTPS uses to achieve its security goals. While "SSL" is still commonly used, all modern secure communication uses TLS.

**3. SSH (Secure Shell)**

* **Purpose:** SSH is a cryptographic network protocol for **operating network services securely over an unsecured network**. Its main purposes are:
  + **Secure Remote Access:** It provides a secure channel over an unsecured network by using strong cryptography. This is widely used by system administrators to log into remote servers and execute commands.
  + **Secure File Transfer:** It enables secure file transfers using protocols like SFTP (SSH File Transfer Protocol) and SCP (Secure Copy Protocol).
  + **Port Forwarding/Tunneling:** It can create secure tunnels for other network services, allowing insecure traffic to be securely encapsulated.

**4. IPSec (Internet Protocol Security)**

* **Purpose:** IPSec is a suite of protocols for **securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session**. Its primary purposes are:
  + **Virtual Private Networks (VPNs):** It is widely used to implement VPNs, allowing secure remote access to private networks over the public internet.
  + **Data Confidentiality:** Encrypts data to prevent unauthorized disclosure.
  + **Data Integrity:** Ensures that data has not been modified in transit.
  + **Data Authentication:** Verifies the identity of the senders and receivers.
  + **Anti-Replay Protection:** Prevents attackers from capturing and retransmitting packets.
  + IPSec can operate in two modes: **Transport Mode** (secures communication between two hosts) and **Tunnel Mode** (secures entire IP packets, often used for VPNs between networks).