**Q1)**  **PILLARS OF Wi-Fi SECURITY:**

**1. Encryption (Protecting Data in Transit)**

Encryption ensures that data transmitted over Wi-Fi is unreadable to unauthorized parties.

**Key Protocols:**

* **WPA3 (Wi-Fi Protected Access 3)** – The strongest standard today:
* Uses **AES-256 encryption** (military-grade).
* Introduces **Simultaneous Authentication of Equals (SAE)** to prevent brute-force attacks.
* Provides **forward secrecy**, meaning past sessions remain secure even if the password is compromised.
* **WPA2 (Wi-Fi Protected Access 2)** – Still widely used but has known vulnerabilities (e.g., KRACK attack).
* **Avoid WEP (Wired Equivalent Privacy)** – Easily cracked in minutes using tools like Aircrack-ng.

**Best Practices:**

* Always use **WPA3** if supported by devices.
* For backward compatibility, use **WPA2/WPA3 mixed mode**.
* Ensure **AES encryption** (not TKIP, which is weak).

**2. Authentication (Verifying User/Device Identity)**

Authentication ensures only authorized users or devices can join the network.

**Methods:**

* **Personal Mode (PSK - Pre-Shared Key):**
* Uses a single password for all users (common in homes/small offices).
* Vulnerable to brute-force attacks if the password is weak.
* **Enterprise Mode (802.1X/EAP):**
* Requires a **RADIUS server** for authentication (used in businesses).
* Supports **individual user logins** (e.g., via usernames/passwords or certificates).
* Protocols: **EAP-TLS (most secure, uses certificates), PEAP, EAP-TTLS**.

**Best Practices:**

* For businesses, use **WPA3-Enterprise with EAP-TLS** (certificate-based auth).
* For home networks, use a **strong, unique Wi-Fi password** (12+ characters, mix of letters, numbers, symbols).

**3. Access Control (Restricting Network Access)**

Limits who or what can connect to the network.

**Techniques:**

* **MAC Address Filtering:**
* Only allows devices with pre-approved MAC addresses.
* **Weakness:** MAC addresses can be spoofed.
* **Network Segmentation:**
* **Guest Network:** Isolates visitors from the main network.
* **VLANs (Virtual LANs):** Separates devices (e.g., IoT devices from workstations).
* **Client Isolation:** Prevents devices on the same network from communicating with each other.

**Best Practices:**

* Use **VLANs + Firewall Rules** for better security than MAC filtering.
* Enable **AP Isolation** in public hotspots.

**4. Monitoring & Intrusion Detection**

Detects and prevents unauthorized access or attacks.

**Tools & Methods:**

* **Wireless Intrusion Detection System (WIDS):**
* Monitors for rogue access points, unauthorized devices, and attacks (e.g., deauthentication floods).
* **Log Analysis:**
* Checks for unusual login attempts or traffic patterns.
* **Automated Alerts:**
* Notifies admins of suspicious activity (e.g., multiple failed login attempts).

**Best Practices:**

* Use tools like **Kismet, Wireshark, or enterprise solutions (Cisco ISE, Aruba ClearPass)**.
* Regularly audit connected devices.

**5. Firmware & Patch Management**

Outdated router firmware is a common attack vector.

**Key Actions:**

* **Regularly update router firmware** to fix security flaws.
* Disable **remote administration** (to prevent external attacks).
* Replace **end-of-life (EOL) hardware** that no longer receives updates.

**Best Practices:**

* Enable **auto-updates** if available.
* Check manufacturer websites for security bulletins.

**6. Physical Security**

If an attacker gains physical access to a router, they can reset it or extract passwords.

**Prevention Measures:**

* Place routers in **locked cabinets** in offices.
* Use **rack-mounted equipment** in server rooms.
* Enable **BIOS/UEFI passwords** on network devices.