**1. What are the pillars of Wi-Fi security?**

The three main pillars of Wi-Fi security are:

* **Authentication**: Ensures that only authorized users can access the network.
* **Encryption**: Protects the data being transmitted over the network from eavesdropping.
* **Integrity**: Ensures that the data has not been altered during transmission.

**2. Explain the difference between authentication and encryption in Wi-Fi security.**

* **Authentication**: Verifies the identity of the device or user attempting to join the network (e.g., using a password or certificate).
* **Encryption**: Secures the actual data transmitted across the network so that even if it is intercepted, it cannot be read without the encryption keys.

**Summary**: Authentication controls *who* can access, while encryption protects *what* is sent.

**3. Explain the differences between WEP, WPA, WPA2, and WPA3.**

| **Standard** | **Key Features** | **Security Level** |
| --- | --- | --- |
| **WEP** | Static keys, RC4 encryption | Very low (easily hackable) |
| **WPA** | TKIP (Temporal Key Integrity Protocol) over RC4 | Improved but still weak |
| **WPA2** | AES encryption with CCMP protocol | Strong and widely used |
| **WPA3** | SAE (Simultaneous Authentication of Equals), stronger encryption | Very strong, resistant to offline attacks |

**4. Why is WEP considered insecure compared to WPA2 or WPA3?**

**WEP** is insecure because:

* It uses a **static key** for encryption, making it easy to crack with tools.
* **Weak initialization vectors (IVs)** make repeated patterns detectable.
* Modern computers can break WEP encryption in **minutes**.

In contrast, **WPA2** and **WPA3** use dynamic keys and strong encryption algorithms like **AES**, making them far more secure.

**5. Why was WPA2 introduced?**

WPA2 was introduced because WPA (which was only a temporary fix over WEP) still had vulnerabilities.  
WPA2 mandated the use of **AES encryption with CCMP** for strong data protection, addressing both security flaws and performance issues from previous standards.

**6. What is the role of the Pairwise Master Key (PMK) in the 4-way handshake?**

The **PMK** is the **master key** derived from the passphrase (or received via 802.1X authentication).  
During the 4-way handshake:

* The PMK is used to generate the **Pairwise Transient Key (PTK)**, which encrypts communication between the client and AP.
* It ensures both sides share a common secret without transmitting it directly.

**7. How does the 4-way handshake ensure mutual authentication between the client and the access point?**

The 4-way handshake ensures mutual authentication by:

* Exchanging **nonces** (random numbers) between client and AP.
* Both sides independently derive the **same PTK** from the PMK and the nonces.
* If the derived PTKs match, both client and AP are authenticated to each other without sending passwords over the air.

**8. What will happen if we put a wrong passphrase during a 4-way handshake?**

If a wrong passphrase is entered:

* The client and AP will derive **different PMKs** and hence different PTKs.
* The Message Integrity Check (MIC) during the handshake will **fail**.
* As a result, the connection attempt will **fail**, and the client won't be able to join the network.

**9. What problem does 802.1X solve in a network?**

**802.1X** addresses the problem of **secure access control** in networks.  
It ensures that **only authenticated users** can access the network resources by integrating with an **authentication server (RADIUS)**.  
It enables **per-user authentication** instead of relying only on shared passwords.

**10. How does 802.1X enhance security over wireless networks?**

802.1X enhances wireless security by:

* Using **EAP (Extensible Authentication Protocol)** methods for strong authentication.
* Generating **dynamic, session-specific encryption keys** for every connection.
* Preventing unauthorized access even if the network is visible, because authentication must be completed before network access is allowed.

Thus, 802.1X provides **enterprise-level protection**, supporting features like per-user credentials, certificates, and integration with corporate directories.