**Wi-Fi Training Program**

**Assignment Solutions – Module 6**

**1. What are the pillars of Wi-Fi security?**  
The three main pillars are:

* **Authentication** – Verifies who can access the network.
* **Encryption** – Protects data during transmission.
* **Integrity** – Ensures data hasn’t been tampered with.

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

* **Authentication**: Confirms a user or device is allowed to connect.
* **Encryption**: Scrambles the data so only authorized parties can read it.

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

| **Security Protocol** | **Introduced** | **Encryption Used** | **Key Features** | **Security Level** |
| --- | --- | --- | --- | --- |
| **WEP** | 1997 | RC4 (static key) | Easy to break, short keys | Weak |
| **WPA** | 2003 | TKIP + RC4 | Temporary fix for WEP flaws | Moderate |
| **WPA2** | 2004 | AES-CCMP | Strong encryption + 4-way handshake | Strong |
| **WPA3** | 2018 | AES + SAE | Resistant to brute force, better for open networks | Very Strong |

**4. Why is WEP considered insecure compared to WPA2 or WPA3?**  
WEP uses weak encryption (RC4) and static keys, making it **vulnerable to cracking in minutes** using freely available tools. WPA2 and WPA3 use **stronger encryption** (AES) and better key management.

**5. Why was WPA2 introduced?**  
WPA2 was introduced to **replace WPA and WEP**, offering:

* Strong AES-based encryption.
* Better security protocols like CCMP.
* Compliance with IEEE 802.11i security standard.

**6. What is the role of the Pairwise Master Key (PMK) in the 4-way handshake?**  
PMK is a **secret key** derived from the passphrase.  
It’s used to generate the **Pairwise Transient Key (PTK)**, which encrypts communication between the client and access point.

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

* Both sides prove they know the **PMK** without sending it.
* If either party fails to validate the keys, the connection fails.
* This ensures **both the client and AP are legitimate**.

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

* The client and AP derive **different PMKs**.
* As a result, the handshake **fails** and the device **can’t connect**.

**9. What problem does 802.1X solve in a network?**  
802.1X provides **port-based access control**, solving:

* **Unauthorized access**.
* Enables centralized **authentication** (usually with a RADIUS server).

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

* It supports **dynamic key generation** per session.
* Allows **user-based** authentication (not just device).
* Enables **enterprise-level security** using certificates or credentials.