Wi-Fi Module 6

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

- Encryption
- Authentication
- Integrity

2. Explain the Difference between authentication and encryption in Wi-Fi security?

Authentication ensures that **only authorized users or devices** can **connect** to a Wi-Fi network.

Encryption ensures that **data transmitted over the Wi-Fi network** is **confidential** and **protected from eavesdropping**.

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

1. WEP (Wired Equivalent Privacy)

Encryption: Uses the **RC4 stream cipher** with a **40-bit or 104-bit key**.

Authentication: Supports **Open System** (no authentication) or **Shared Key** (pre-shared key-based authentication).

2. WPA (Wi-Fi Protected Access)

Encryption: Uses **RC4 with TKIP** (though still based on RC4), which improved upon WEP by **changing keys dynamically** during communication.

Authentication:

- Supports **PSK** (Pre-Shared Key) for home networks and **802.1X/EAP** for enterprise networks.

3. WPA2 (Wi-Fi Protected Access II)

Encryption: Uses **AES (Advanced Encryption Standard)**, which is much stronger and more secure than TKIP or WEP's RC4.

Authentication:

- Supports **PSK (Pre-Shared Key)** for home networks and **802.1X/EAP** for enterprise networks.
- Also includes **PMK (Pairwise Master Key)** and **TKIP fallback** for compatibility.

4. WPA3 (Wi-Fi Protected Access III)

Encryption:

- **AES** encryption with **GCMP (Galois/Counter Mode Protocol)** for **stronger data integrity**.
- **192-bit encryption** in WPA3-Enterprise for **high-level security**.

Authentication:

- **Simultaneous Authentication of Equals (SAE)** replaces PSK in WPA3-Personal, providing **stronger protection against offline dictionary attacks**.
- **Forward secrecy** ensures that even if a key is compromised in the future, past communications remain **secure**.

Improved Security for Public Networks:

- **Enhanced Open** (no password) uses **Opportunistic Wireless Encryption (OWE)** to encrypt data even on open networks, preventing eavesdropping.

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

- Weak Encryption
- Short IV
- Static keys

5.Why was WPA2 introduced?

WPA2 was introduced to address the shortcomings of WEP

It introduced stronger AES encryption algorithm

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

The **Pairwise Master Key (PMK)** plays a **central role in the WPA/WPA2 4-way handshake**, serving as the **foundation for deriving all encryption keys** used between a Wi-Fi client (supplicant) and an access point (authenticator). It ensures **mutual authentication** and enables the creation of **unique session keys** for secure communication.

- It ensures both the AP and the supplicant derive the same PTK without the need for sharing the PTK.

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

- The authentication is ensured because the PTK generated will be same for both the devices.
- It consists of Anonce Snonce AP MAC client Mac therefore it is unique.
- This ensures mutual authentication.

8. What will happen if we put a wrong passphrase during a 4Way handshake?

- Wrong passphrase means wrong PMK then the MIC fails.
- Therefore the 4 way handshake will fail.

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

It ensures that only authenticated users can access the networks.

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

Each client is authenticated using **unique credentials** (username/password, certificate, smartcard, etc.).

Replaces shared passphrases (like in WPA2-Personal) with **per-user identities**.

Prevents unauthorized devices from joining the network.