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

WEP uses RC4 encryption and static keys (which are easily cracked).

It has weak key management.

Tools can break WEP passwords in minutes.

WPA2 uses dynamic keys and strong AES encryption

5. Why was WPA2 introduced?

WPA (with TKIP) was only a temporary fix after WEP was broken.

WPA2 introduced AES encryption to provide real long-term security for Wi-Fi networks.

Also brought stronger key management and mandatory 802.1X support for enterprise.

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

PMK = Secret key derived from password (PSK) or from 802.1X server.

The 4-way handshake uses PMK to generate:

- PTK (Pairwise Transient Key) → for encrypting unicast traffic.
- GTK (Group Temporal Key) → for encrypting broadcast/multicast traffic.