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

* **Confidentiality:**

Confidentiality ensures that sensitive information is accessible only to authorized individuals or systems and prevents unauthorized access. The goal is to protect private data from being viewed, accessed, or used by unauthorized persons.

* **Integrity**

Integrity ensures that data remains unaltered during transmission or storage. If the data is modified in any way, its integrity is compromised.

* **Authentication:** Authentication ensures that messages are sent to the right user and not any other user.

**2. Explain the difference between authentication and encryption in WiFi security.**

**Authentication: -It verifies the identity**

Confirms that the parties involved in communication (e.g., a user and a network) are who they claim to be.

In Wi-Fi: Ensures only authorized devices/users can join the network (e.g., via 802.1X or WPA2-PSK).

**Encryption-It protects the data**

Changes data so that only auth parties can read it by decrypting it .Even if someone intercept they can only see the encrypted data and cant read it

Encrypts data packets transmitted over the air (e.g., using AES), so attackers can't see what you're sending or receiving.

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

**WEP :**

* Stands for Wireless Equivalent Privacy which was introduced to provide same level of security to Wi-Fi as given for Wired Communication and hence the name.
* It used RC4 encryption which was a very weak encryption protocol
* Used 24 bit random Initialization Vector along with 40 or 104 bit Key(constant key)
* Since it used the same base key for all communication, larger sample spaces can lead to the base key to be exposed. Hence this Wi-Fi security protocol was considered to be weak.

**WPA :**

* Stands for Wireless Protected Access
* It was introduced to overcome the shortcomings of WEP by introducing unique per packet encryption keys.
* It uses receiver’s MAC address to generate the keys and uses MIC to check the message's integrity.
* Uses TKIP (Temporal Key Integrity Protocol) for stronger encryption than WEP. But they are still prone to Brute Force Attacks.

**WPA 2:**

* This was enhanced version of the WPA protocol which uses advanced encryption methods like AES algorithm.
* Packet Number is used to prevent replay attacks and CCM ensures user of new temporal key for each session.
* APs can support WPA+WPA2 modes for backward compatibility.
* However unlike WPA, WPA2 needs hardware supports and weaker passwords were prone to attacks.

**WPA 3:**

* This was an enhancement to WPA2 where 128/192/256-bit keys are used for data encryption.
* One main improvement was to encrypt Management Frames in addition to encrypting Data Frames.
* Replaces use of Pre Shared Keys with Simultaneous Authentication of Equals.

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

WEP is considered insecure to WPA2 and WPA3 as the encryption methods and security promised in WEP is very low in comparison to WPA2 or WPA3. Since it was the very first standard to be introduced in Wi-Fi security, it main goal was to ensure security to messages and it did not use the most complex methods to ensure security. It used a weak encryption mechanism like RC4 and used the same base key along with a random 24 bit Initialization Vector. WPA2 and WPA3 by using much stronger encryption mechanisms like AES, Secure Hash Algorithm etc ensure that messages sent over the wireless medium cannot be easily sniffed by others.

**5. Why was WPA2 introduced?**

WPA2 was introduced to address the shortcomings of WPA. While WPA promised better security than WEP, it still had its shortcomings. It still used RC4 cipher as its encryption algorithm and had Message Integrity Check as its hashing algorithm. By providing a much stronger and complex encryption algorithm like AES, WPA2 promised better security than WPA. It also replaced Cipher Block Chaining Message Authentication Code as its Hashing Algorithm and moved away from MIC.

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

The Pairwise Master Key (PMK) is crucial in the 4-way handshake process. Although it is derived from the Pre-Shared Key (PSK) or an authentication server, it doesn't directly participate in the handshake itself. Instead, it is used to generate keys that are involved in the handshake. The PMK is used to create the Pairwise Transient Key (PTK) on the client side, which is then used to generate the Group Temporal Key (GTK). By ensuring that keys are not transmitted over the air, the PMK helps securely generate session keys, enabling secure communication between the authenticator and the supplicant.

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

The 4-way handshake ensures mutual authentication between the client (supplicant) and the access point (authenticator) by verifying that both sides possess the same Pairwise Master Key (PMK) without ever transmitting it over the air.

Here’s how it works:

1. Message 1 (AP → Client):  
   The access point sends a random number (ANonce) to the client.
2. Message 2 (Client → AP):  
   The client uses the ANonce, its own random number (SNonce), and the PMK to generate the Pairwise Transient Key (PTK). It then sends the SNonce and a Message Integrity Code (MIC) (calculated using the PTK) to the AP.
3. Message 3 (AP → Client):  
   The AP uses both nonces and the PMK to compute its own version of the PTK. It then sends the Group Temporal Key (GTK) encrypted with the PTK and includes a MIC.
4. Message 4 (Client → AP):  
   The client confirms the receipt of the GTK by replying with a MIC using the PTK.

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

* The access point (AP) and the client independently generate the Pairwise Master Key (PMK)—the AP from its stored passphrase and the client from the one the user entered.
* During the 4-way handshake, both sides use the PMK to derive a Pairwise Transient Key (PTK).
* When the client sends its response (Message 2), it includes a Message Integrity Code (MIC) computed using the PTK.
* The AP checks this MIC using its own PTK.
* If the passphrase is incorrect, the PMKs (and therefore PTKs) will not match, and the MIC validation will fail.
* As a result, the AP will terminate the handshake, and the device will fail to connect to the network.

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

802.1X solves the problem of unauthorized network access by providing port-based network access control. It ensures that only authenticated users or devices can connect to a network—whether it's wired or wireless. Without 802.1X, anyone can plug into a network port or connect to a wireless access point and potentially access sensitive resources, leading to security risks.

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

802.1X enhances security over wireless networks by enforcing user and device authentication before allowing access to the network. It acts as a gatekeeper that ensures only authorized users or devices can connect.It enhances by

* Authenticating devices/users before granting access.
* Using an authentication server (typically RADIUS) to verify credentials.
* Preventing access to the internal network until the user or device is authenticated.