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

1. Confidentiality:

- Ensures that sensitive information is only accessible to those who are authorized to view it.
- Methods to achieve confidentiality include encryption, access control, authentication, and data classification.

2. Integrity:

- Ensures that data remains accurate, consistent, and unmodified during storage, transmission, and processing.
- Methods to ensure integrity include hashing, checksums, digital signatures, and data validation mechanisms.

3. Authentication:

- Authentication is the process of verifying the identity of a user, device, or system before granting access to resources.
- It's essentially about making sure that the entity trying to access a system or data is who they claim to be.

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

1. Authentication:

- **Purpose:** Ensures that only authorized users or devices can access the Wi-Fi network.
- **What it does:**
  - Authentication is the process of verifying the identity of users or devices before granting access to the network.
  - It confirms that the device or user trying to connect is legitimate.
  - In Wi-Fi security, WPA2 and WPA3 are common standards that use passwords or security keys for authentication. These methods prevent unauthorized access to the network.
- **Example:**
  When you try to connect to a Wi-Fi network, your device must provide the correct **password** (or other credentials) to **authenticate** itself. If the credentials are valid, the device is allowed access.

2. Encryption:

- **Purpose:** Ensures that the data transmitted over the Wi-Fi network is **protected from eavesdropping** and tampering.
- **What it does:**
  - Encryption is the process of **scrambling** the data so that it can only be understood by authorized parties who have the correct decryption key.

    - It prevents anyone who intercepts the wireless signals from reading or modifying the data being transferred between devices and the access point.
    - Wi-Fi security protocols like WPA2 and WPA3 use AES (Advanced Encryption Standard) for strong encryption of transmitted data.
- **Example:**
  Once your device is authenticated and connects to the Wi-Fi network, all the data you send (like browsing information, emails, etc.) is encrypted, making it unreadable to attackers who might be intercepting the signal.

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

1. WEP (Wired Equivalent Privacy):

- **Introduced:** 1997, as part of the IEEE 802.11 standard.
- **Encryption Type: RC4 stream cipher**.
- **Key Size:** Typically 64-bit or 128-bit keys (the security of WEP is weak even with 128-bit keys).
- **Authentication:** Uses **shared key authentication**.
- **Security Vulnerabilities:**
    - **Weak encryption**: WEP's RC4 encryption can be easily cracked due to flaws in its key management and the use of weak initialization vectors (IVs).
    - **Easily cracked**: Tools to crack WEP encryption (such as aircrack-ng) are widely available, making it extremely insecure.
- **Status: Deprecated**. WEP is no longer considered secure and is not recommended for use.

2. WPA (Wi-Fi Protected Access):

- **Introduced:** 2003, as an interim solution to replace WEP.
- **Encryption Type: TKIP (Temporal Key Integrity Protocol)**.
- **Key Size:** Dynamic 128-bit keys (with TKIP).
- **Authentication:** Supports **802.1X authentication** for enterprise networks or **Pre-Shared Key (PSK)** for home networks.
- **Security Improvements:**
    - TKIP was designed to fix some WEP vulnerabilities by dynamically changing keys for each packet.
    - WPA is more secure than WEP but still has weaknesses.
- **Security Vulnerabilities:**
    - TKIP encryption is still vulnerable to attacks like **packet injection** and **key reuse**.

- **Status: Deprecated**. WPA is no longer widely used and has been replaced by WPA2 and WPA3.

3. WPA2 (Wi-Fi Protected Access 2):

- **Introduced:** 2004, as the successor to WPA.
- **Encryption Type: AES (Advanced Encryption Standard)**.
- **Key Size:** 128-bit AES keys (considered secure).
- **Authentication:** Uses **802.1X** for enterprise networks (RADIUS) and **PSK** for home networks.
- **Security Improvements:**
    - **AES encryption** is far stronger than TKIP, offering robust protection against attacks.
    - **CCMP (Counter Mode with CBC-MAC Protocol)** is the encryption protocol used with WPA2, providing better security and integrity than TKIP.
- **Security Vulnerabilities:**
    - While WPA2 is much more secure than WEP and WPA, it's vulnerable to attacks like **KRACK** (Key Reinstallation Attack) that can exploit the 4-way handshake in WPA2.
    - Weak passwords or poor configurations can still leave the network vulnerable.
- **Status:** Still widely used but is considered less secure than WPA3, especially in light of newer vulnerabilities like KRACK.

4. WPA3 (Wi-Fi Protected Access 3):

- **Introduced:** 2018, as the latest and most secure Wi-Fi standard.
- **Encryption Type: AES encryption** with improved **Suite B** cryptography for higher levels of security.
- **Key Size:** 128-bit AES (with additional improvements).
- **Authentication:** Uses **Simultaneous Authentication of Equals (SAE)** for stronger authentication, particularly in personal networks.
- **Security Improvements:**
    - **Stronger encryption**: WPA3 uses stronger cryptographic methods like 192-bit security for enterprise-grade networks and **256-bit encryption**.
    - **Forward secrecy**: Even if the password is compromised, previously encrypted data remains secure.
    - **Protection against offline dictionary attacks**: WPA3's **SAE** handshake prevents attackers from using offline methods to guess the password.
    - **Improved public Wi-Fi security**: WPA3 introduces **Opportunistic Wireless Encryption (OWE)**, which provides encryption even on open networks.
- **Security Vulnerabilities:**

    - WPA3 is much more resistant to attacks, but early implementation may have some bugs in certain devices.

- **Status: Recommended** for all Wi-Fi networks, especially as it provides better protection against modern attacks and improves user privacy.

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

1. Weak Encryption (RC4 Cipher):

- WEP uses the **RC4** stream cipher, which has inherent weaknesses.
- The RC4 algorithm is **vulnerable to various attacks** like **known-plaintext attacks**, **fluency attacks**, and **key recovery**.
- The encryption used in WEP is easily cracked with modern computing power, making it **very easy to decrypt** WEP-protected traffic.

2. Short Initialization Vector (IV):

- WEP uses a **24-bit initialization vector (IV)**, which is relatively short.
- This short IV leads to **IV collisions** (repeated use of the same IV), making it easier for attackers to **break the encryption** by gathering enough packets.
- In contrast, WPA2 uses a much stronger 128-bit IV, providing better security.

3. Static Key Management:

- WEP relies on a **static key** (shared secret) for encryption. The same key is used for a long period, which makes it **vulnerable to key reuse** and **brute force attacks**.
- In WPA2, **dynamic key management** (using protocols like **802.1X**) ensures that encryption keys change frequently, making it harder to intercept and crack the keys.

4. Lack of Integrity Checking:

- WEP does not include proper integrity checks or mechanisms to verify that the data has not been tampered with. While it uses a **CRC-32 checksum** for error detection, this method is **not strong enough** to protect against attacks like **bit-flipping** (where an attacker changes the data being transmitted).
- WPA2 includes **Message Integrity Check (MIC)**, which helps detect tampering with the data during transmission, providing an extra layer of security.

5. Easily Cracked with Modern Tools:

- Tools like **aircrack-ng** and others can easily **crack WEP keys** in minutes or hours with relatively low amounts of traffic or by exploiting weaknesses in the WEP protocol.
- WPA2 and WPA3, on the other hand, are designed with stronger encryption methods (such as **AES**), making them much more resistant to brute-force and other attacks.

6. Lack of Protection Against Dictionary Attacks:

- WEP is vulnerable to **dictionary attacks**, where an attacker can guess the key by testing a large number of possibilities.
- WPA2, with its **802.1X-based authentication** and **stronger encryption**, significantly reduces the risk of these attacks.
- WPA3 further strengthens protection by incorporating **Simultaneous Authentication of Equals (SAE)**, making it resistant to offline dictionary attacks.

5. Why was WPA2 introduced?

1. Weaknesses in WEP (Wired Equivalent Privacy):

- **WEP** was the original security protocol used in Wi-Fi networks, but it was found to be **easily crackable** due to fundamental flaws in its design.
- WEP used the **RC4 stream cipher**, which was vulnerable to **key-recovery attacks**, and it used a **short 24-bit initialization vector (IV)**, which resulted in **IV collisions** that could be exploited by attackers.
- **Weak encryption** and **static key management** made WEP easily breakable with tools that could decrypt the data in a short time.

2. Stronger Encryption with AES (Advanced Encryption Standard):

- WPA2 introduced **AES encryption**, which is a much stronger and more secure encryption method than the RC4 stream cipher used in WEP.
- AES is a **symmetric block cipher** that is resistant to a wide range of cryptographic attacks, making it much more secure and less vulnerable to cracking attempts.
- WPA2, by mandating AES for encryption, provided **better protection** for the confidentiality of data transmitted over wireless networks.

3. Improved Key Management:

- WPA2 uses **dynamic key management** as opposed to WEP's static key system.
- WPA2 implements the **4-way handshake** to securely exchange encryption keys between devices and the access point. This ensures that the encryption keys are **changed periodically**, which helps prevent **key reuse** and **brute-force attacks**.
- WEP's reliance on a single static key made it easier for attackers to decrypt the traffic once they obtained the key.

4. Message Integrity:

- WPA2 introduces **Message Integrity Check (MIC)**, also known as **CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)**. MIC helps ensure that the data transmitted over the network is not tampered with.
- In contrast, WEP only used a simple **CRC-32 checksum**, which could be easily manipulated by attackers, allowing them to alter the data without detection.

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

1. **Generation of the PMK:**
   - The **Pairwise Master Key (PMK)** is generated during the **authentication process** (either via a pre-shared key (PSK) for personal mode or through 802.1X-based authentication for enterprise mode).
   - In WPA2-Personal (PSK), the PMK is derived from the **pre-shared key (PSK)** (a password or passphrase) and the **SSID** (Service Set Identifier) of the network.
   - In WPA2-Enterprise, the PMK is derived from the **authentication server** (usually via RADIUS) after the client is successfully authenticated using methods like **EAP (Extensible Authentication Protocol)**.
2. **Use of PMK in the 4-Way Handshake:**
   - The **4-way handshake** is a process where the PMK is used to derive a **fresh session key** that both the access point and client can use to encrypt data traffic. This ensures that the session keys are unique and that communication is secure.
   - The handshake involves both the client and access point proving to each other that they have the same PMK without actually sending the PMK over the air. Instead, the PMK is used to **generate temporary keys** that are exchanged during the handshake.

Steps in the 4-Way Handshake Involving the PMK:

1. **Message 1 (AP → Client):**
   - The access point (AP) sends a message to the client containing a **nonce** (a random number used once) and an **ANonce** (Access Point Nonce). This is used to start the process of deriving fresh keys.
2. **Message 2 (Client → AP):**
   - The client responds with its own **nonce** (SNonce) and also proves that it has the same PMK by encrypting its response with the PMK. This ensures mutual authentication between the client and the AP without revealing the PMK.
   - The client also includes the **Pairwise Transient Key (PTK)**, derived from the PMK, which will be used for encrypting data during the session.
3. **Message 3 (AP → Client):**
   - The AP sends a confirmation to the client, which includes a **key confirmation** message (encrypted with the PTK). It also includes the **Group Temporal Key (GTK)**, which is used for broadcast/multicast communication.
4. **Message 4 (Client → AP):**
   - The client responds, confirming that it has successfully received and installed the keys (PTK, GTK), and the handshake is complete.

7. How does the 4-way handshake ensure mutual authentication between the client

and the access point?

1. Initial Setup:

- **Pairwise Master Key (PMK)**: Both the client and the AP have a shared **Pairwise Master Key (PMK)**. This key is derived either from a pre-shared key (PSK) in WPA2-Personal mode or from a RADIUS server in WPA2-Enterprise mode during the initial authentication process. This PMK is not sent over the air.
- The **PMK** is used to generate session keys for encrypting data during the connection.

2. Message 1 (AP → Client):

- The AP sends a message that contains a **random number** (ANonce, Access Point Nonce) to the client.
- This message also indicates that the AP is ready to establish a secure connection.

3. Message 2 (Client → AP):

- In response, the client generates its own **random number** (SNonce, Station Nonce) and sends it to the AP.
- At this point, the client proves that it knows the **PMK** by using it to generate a message that is encrypted with the **PMK-derived key**. The client sends this encrypted message along with its SNonce to the AP.
- By encrypting its response with the PMK, the client proves to the AP that it is indeed the intended client and that it possesses the correct PMK. This is **mutual authentication** in action—only the client with the correct PMK could have produced this valid encrypted response.

4. Message 3 (AP → Client):

- The AP responds with an encrypted message confirming that it also has the correct PMK. This message is encrypted using the **PMK-derived key**, and it essentially proves that the AP has authenticated itself as well.
- In addition, the AP sends the **Group Temporal Key (GTK)**, which is used to encrypt multicast and broadcast traffic.

5. Message 4 (Client → AP):

- The client responds to the AP’s confirmation, indicating that it has successfully received and installed the encryption keys (Pairwise Transient Key or PTK, and GTK).
- At this point, both parties have confirmed each other’s identity and have established secure encryption keys for the session.

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

- The AP will **not be able to complete the handshake** because the client's encrypted message cannot be validated.
- The client will not receive the expected response from the AP in the third message of the handshake.
- The AP may drop the connection attempt, and the client will fail to authenticate.
- The client will typically receive an **authentication failure** message or a timeout error, indicating that the 4-way handshake could not be completed.

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

1. Unauthorized Network Access:

- In traditional network access setups (especially in **open** networks or networks without strong authentication), **any device** can connect to the network without verifying its legitimacy.
- 802.1X solves this by **requiring authentication** before granting access to the network. It ensures that only devices and users with valid credentials can access the network.

2. Lack of Strong Authentication:

- Many networks (especially legacy ones) might rely on weaker authentication methods or even no authentication at all, making it easy for unauthorized users to gain access.
- 802.1X uses **strong authentication protocols**, such as **EAP (Extensible Authentication Protocol)**, to authenticate users or devices securely. It allows a range of authentication methods (like **username/password**, **certificates**, or **biometrics**) to be used.

3. Man-in-the-Middle (MitM) Attacks:

- Without proper access control, attackers could potentially intercept network traffic or masquerade as legitimate devices.
- 802.1X helps protect against such attacks by ensuring **mutual authentication** (both the client and the network device (access point or switch) authenticate each other), thus preventing attackers from impersonating legitimate network devices.

4. Dynamic and Scalable Authentication:

- In large networks, especially enterprise environments, manually managing user access or using static credentials can be cumbersome and insecure.
- 802.1X integrates with **RADIUS (Remote Authentication Dial-In User Service)**, which allows **centralized authentication**, making it easier to scale and manage authentication across large networks. This centralized approach enables **single sign-on (SSO)** capabilities and simplifies management.

5. Unencrypted Network Traffic:

- Before 802.1X, once a device was connected to the network, the device often had access to unencrypted traffic. Attackers could potentially **eavesdrop** on the network if the device wasn't properly authenticated.
- 802.1X establishes a **secure channel** for communication before access is granted, ensuring that all communications between the device and the network infrastructure are encrypted.

6. Device and User Differentiation:

- 802.1X can authenticate not only **users** but also **devices**. It ensures that specific devices (such as computers, smartphones, or IoT devices) are permitted to join the network, which adds an extra layer of security beyond just user authentication.

10. How does 802. IX enhance security over wireless networks?

1. Prevents Unauthorized Access:

- **802.1X** enforces **port-based network access control** (PNAC), meaning that a device attempting to connect to the network must first authenticate before being allowed access to the network's resources.
- This means unauthorized devices cannot just connect to the network by being in range, making it more difficult for attackers to gain network access without proper credentials.

2. Strong Authentication:

- **802.1X** uses **Extensible Authentication Protocol (EAP)**, which supports a variety of authentication methods, including:
    - **EAP-TLS (Transport Layer Security)** for certificate-based authentication.
    - **EAP-PEAP** or **EAP-TTLS** for encrypted username/password authentication.
    - **EAP-MD5**, **EAP-SIM**, and others, depending on the specific use case.
- This flexibility allows for strong, enterprise-grade authentication mechanisms to be used, such as digital certificates or smartcards, which are much harder to compromise than traditional static credentials (like WEP keys or PSK).

3. Mutual Authentication:

- **802.1X** supports **mutual authentication**, where both the client (supplicant) and the network (authenticator) authenticate each other. This ensures that the client is connecting to a legitimate access point (AP), and the AP is allowing only authenticated clients to connect.
- This is especially critical in **wireless environments** where an attacker might set up rogue access points (evil twins) to trick users into connecting and intercepting their data. Mutual authentication prevents such attacks.

4. Dynamic Key Generation:

- After the **successful authentication** of the client, **802.1X** facilitates the generation of **dynamic encryption keys** between the client and the access point. These keys are unique for each session, ensuring that each communication is encrypted and protected from eavesdropping.

- In Wi-Fi networks using WPA2/WPA3, the **Pairwise Master Key (PMK)** is used to generate these session keys during the 4-way handshake. This dynamic key generation ensures that each connection is secure and isolated from previous sessions.