WIFI Training Program

Module 6 – Assignment Questions

1. What are the pillars of Wi-Fi security?
2. Explain the difference between authentication and encryption in WIFI security.
3. Explain the differences between WEP, WPA, WPA2, and WPA3.
4. Why is WEP considered insecure compared to WPA2 or WPA3?
5. Why was WPA2 introduced?
6. What is the role of the Pairwise Master Key (PMK) in the 4-way handshake?
7. How does the 4-way handshake ensure mutual authentication between the client and the access point?
8. What will happen if we put a wrong passphrase during a 4Way handshake?
9. What problem does 802.1X solve in a network?
10. How does 802.1X enhance security over wireless networks?

Q1) What are the pillars of Wi-Fi security?

The pillars of Wi-Fi security refer to the fundamental principles and mechanisms that ensure the confidentiality, integrity, and availability of data transmitted over wireless networks. These pillars help protect wireless communication from unauthorized access, data breaches, and other security threats. The main pillars of Wi-Fi security include:

1. Authentication
    - Ensures that only authorized users and devices can access the Wi-Fi network.
    - Common methods include Pre-Shared Key (PSK) and Enterprise authentication (802.1X using RADIUS servers).
    - Prevents unauthorized access and impersonation attacks.
2. Encryption
    - Protects the confidentiality of data by converting it into a secure format that is unreadable to unauthorized users.
    - Common encryption protocols include:
        - WEP (Wired Equivalent Privacy) – outdated and insecure
        - WPA (Wi-Fi Protected Access) – improved but still vulnerable
        - WPA2 – widely used and more secure (uses AES)
        - WPA3 – latest standard with enhanced encryption and protection against brute-force attacks
3. Integrity Protection
    - Ensures that data is not tampered with during transmission.
    - Uses cryptographic checksums and message integrity codes (e.g., CCMP with AES in WPA2/WPA3).
    - Helps detect and prevent data modification or injection attacks.
4. Access Control
    - Manages and restricts what resources users can access once connected to the network.
    - Includes MAC address filtering, VLAN segmentation, and firewall rules.
    - Helps isolate devices and limit the spread of threats within the network.
5. Monitoring and Management
    - Involves continuous observation of network activity to detect and respond to suspicious behavior.
    - Includes intrusion detection systems (IDS), logging, and real-time alerts.
    - Enables network administrators to take prompt action against threats.

Q2) Explain the difference between authentication and encryption in WIFI security.

Authentication and encryption are two distinct but complementary components of Wi-Fi security. They serve different purposes in protecting wireless networks. The table below outlines their key differences:

Aspect	Authentication	Encryption
Purpose	Verifies the identity of users or devices	Protects data from being read by unauthorized parties
Function	Grants access only to authorized entities	Converts data into a coded format
Role in Security	Controls who can join the network	Ensures confidentiality of transmitted data
When applied	Before establishing a connection	During and after the connection is established
Common Protocols	WPA/WPA2/WPA3-PSK WPA/WPA2/WPA3-Enterprise	- WEP (insecure) - TKIP (used in WPA) - AES/CCMP (used in WPA2/WPA3)
Outcome	Device is allowed or denied network access	Data is scrambled so only authorized devices can read it
Example	A user entering a Wi-Fi password to connect	Data packets being encrypted with AES over Wi-Fi

Q3) Explain the differences between WEP, WPA, WPA2, and WPA3.

The evolution of Wi-Fi security standards—WEP, WPA, WPA2, and WPA3—reflects progressive improvements in wireless network protection. Below is a comparison that highlights the key differences between them:

Feature	WEP (Wired Equivalent Privacy)	WPA (Wi-Fi Protected Access)	WPA2	WPA3
Encryption Algorithm	RC4 (stream cipher)	TKIP (Temporal Key Integrity Protocol)	AES-CCMP (Advanced Encryption Standard)	AES-GCMP (Galois/Counter Mode Protocol)
Security Level	Low (easily breakable)	Moderate (transitional solution)	High (widely used and secure)	Very High (strongest available)
Key Management	Static key	Dynamic key (per session)	Dynamic key with robust protocol	Enhanced key management (SAE)
Authentication Methods	Pre-Shared Key (PSK) only	PSK and 802.1X (Enterprise)	PSK and 802.1X (Enterprise)	SAE (Simultaneous Authentication of Equals) for personal, 802.1X for enterprise
Protection Against Attacks	Poor	Improved over WEP	Strong protection, but vulnerable to some side-channel attacks	Resistant to offline dictionary and side-channel attacks
Backward Compatibility	N/A	Compatible with WEP	Compatible with WPA	Not backward compatible with WEP/WPA
Use Today	Deprecated	Obsolete	Still widely used	Emerging

Q4) Why is WEP considered insecure compared to WPA2 or WPA3?

WEP (Wired Equivalent Privacy) is considered insecure for several reasons when compared to more advanced standards like WPA2 and WPA3. The key weaknesses are outlined below:

1. Weak Encryption Algorithm (RC4)
    - WEP uses the RC4 stream cipher with short initialization vectors (IVs), typically 24 bits long.
    - These short IVs are reused frequently, making it easier for attackers to detect patterns and decrypt the data.
2. Static Key Usage
    - WEP relies on a single, manually configured static key shared among users.
    - This key never changes unless done manually, making it susceptible to key recovery through prolonged monitoring.
3. IV Collisions and Repetition
    - The limited number of IVs leads to frequent repetition (especially in busy networks), enabling attackers to perform statistical analysis and recover the encryption key.
4. Lack of Key Management
    - WEP does not support dynamic key generation or per-session keys.
    - WPA2 and WPA3 generate unique keys for each session, which significantly improves security.
5. No Strong Integrity Check
    - WEP uses a weak CRC-32 checksum for integrity, which can be altered without detection.
    - WPA2 and WPA3 use cryptographic integrity checks like CCMP (AES-based), which are resistant to tampering.
6. Vulnerable to Passive and Active Attacks
    - Tools such as Aircrack-ng can break WEP encryption in minutes using captured packets.
    - WPA2 and WPA3 are resistant to such attacks due to stronger encryption and handshake mechanisms.
7. No Protection Against Replay Attacks
    - WEP lacks replay protection, allowing attackers to reuse captured packets to interfere with or impersonate network communication.

Q5) Why was WPA2 introduced?

WPA2 (Wi-Fi Protected Access 2) was introduced in 2004 by the Wi-Fi Alliance as a significant improvement over WPA (Wi-Fi Protected Access) and WEP (Wired Equivalent Privacy). The primary reasons for its introduction are outlined below:

1. To Address Security Flaws in WEP and WPA
    - WEP was highly vulnerable to attacks due to weak encryption (RC4) and static key usage.
    - WPA was an interim solution that still relied on RC4 and TKIP, which had known limitations.
    - WPA2 introduced AES (Advanced Encryption Standard) and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), providing a much higher level of security.
2. To Comply with IEEE 802.11i Standard
    - WPA2 fully implements the IEEE 802.11i security specification, which was developed to standardize robust Wi-Fi security practices.
    - WPA, in contrast, was only a partial implementation of the standard and was designed as a temporary fix.
3. To Improve Data Confidentiality and Integrity
    - WPA2 replaced TKIP with AES-CCMP, offering better encryption and stronger data integrity checks.
    - This reduced the risk of data tampering, eavesdropping, and replay attacks.
4. To Support Enterprise-Grade Security
    - WPA2 includes support for 802.1X authentication and RADIUS servers, enabling secure and scalable enterprise deployments.
    - It supports both Personal Mode (WPA2-PSK) and Enterprise Mode (WPA2-Enterprise).
5. To Future-Proof Wi-Fi Security
    - With the growing use of wireless networks for sensitive applications, there was a need for a security protocol that could scale and resist evolving threats.
    - WPA2 was designed to remain effective for many years with minimal vulnerabilities.

Q6) What is the role of the Pairwise Master Key (PMK) in the 4-way handshake?

The Pairwise Master Key (PMK) plays a crucial role in the 4-way handshake process, which is part of the authentication and key management process in WPA2 and WPA3. The purpose of the 4-way handshake is to establish a secure, encrypted communication channel between the client (supplicant) and the access point (authenticator). Here's the role of PMK within this process:

Role of the Pairwise Master Key (PMK) in the 4-Way Handshake

1. PMK Derivation
   The PMK is derived during the initial authentication phase and is a product of the Pre-Shared Key (PSK) or 802.1X (in enterprise networks) along with a unique SSID (network name). The PMK serves as the basis for generating session keys that will be used for encryption and integrity protection during the communication session.
   - For WPA2-PSK, the PMK is generated by applying a hash function to the SSID and the pre-shared key (password).
   - For WPA2-Enterprise, the PMK is derived from the 802.1X authentication process, which involves interaction with a RADIUS server.
2. Usage in the 4-Way Handshake
   The 4-way handshake involves the exchange of four messages between the client and the access point to establish a secure communication channel. The PMK is used in these steps to derive the Pairwise Transient Key (PTK), which is then used for encryption.
   - Message 1 (AP → Client): The access point sends a nonce (a random value) to the client, along with the AP's MAC address.
   - Message 2 (Client → AP): The client responds with its own nonce and a message integrity code (MIC), proving it has the same PMK.
   - Message 3 (AP → Client): The AP sends a confirmation message, including a key encryption identifier (KEK) and the final MIC. This step ensures that both parties have successfully derived the same PTK from the PMK.
   - Message 4 (Client → AP): The client sends a final confirmation, and now the session keys are established.
3. Derivation of Session Keys (PTK)
   The PMK is used to derive the Pairwise Transient Key (PTK). The PTK is a set of keys that will be used for encryption and integrity protection of the data being transmitted. The PTK is derived from:
   - The PMK
   - The nonces (random values) exchanged during the 4-way handshake
   - The MAC addresses of the client and access point

Q7) How does the 4-way handshake ensure mutual authentication between the client and the access point?

1. Initial Setup

Before the 4-way handshake begins, the PMK is already derived. This can be done via a Pre-Shared Key (PSK) (in WPA2-Personal) or through 802.1X authentication (in WPA2-Enterprise), which involves communication with a RADIUS server. The PMK serves as the shared secret that both the client and the AP will use during the handshake.

2. Message Exchange in the 4-Way Handshake

Message 1: AP → Client

- The access point (AP) sends a nonce (ANonce), which is a random number generated by the AP.
- This nonce is used to ensure that the session keys are unique and are not repeated during subsequent sessions.
- The AP also sends its MAC address as part of the message, confirming its identity.

Message 2: Client → AP

- The client generates its own nonce (SNonce), another random number, to be used in the generation of the session keys.
- The client sends this nonce and its MAC address back to the AP.
- The client also calculates a Message Integrity Code (MIC) for both the nonce and the AP's nonce (ANonce). This MIC proves that the client possesses the correct PMK, as only a valid PMK can produce a correct MIC based on the nonces exchanged.

At this point, the client has proven to the AP that it knows the shared PMK because it could generate the correct MIC. This establishes one-way authentication (client to AP).

Message 3: AP → Client

- The AP responds by confirming that it has successfully received the client's nonce and MAC address.
- The AP also sends a Message Integrity Code (MIC) that covers both the AP's and client's nonces (ANonce and SNonce), proving that the AP has the correct PMK and can derive the same session keys.
- This step proves to the client that the AP is legitimate and that it knows the correct PMK.

Message 4: Client → AP

- The client sends a final message to confirm that both sides (client and AP) have successfully established the same session keys.
- This is the final confirmation of the secure communication channel being established.

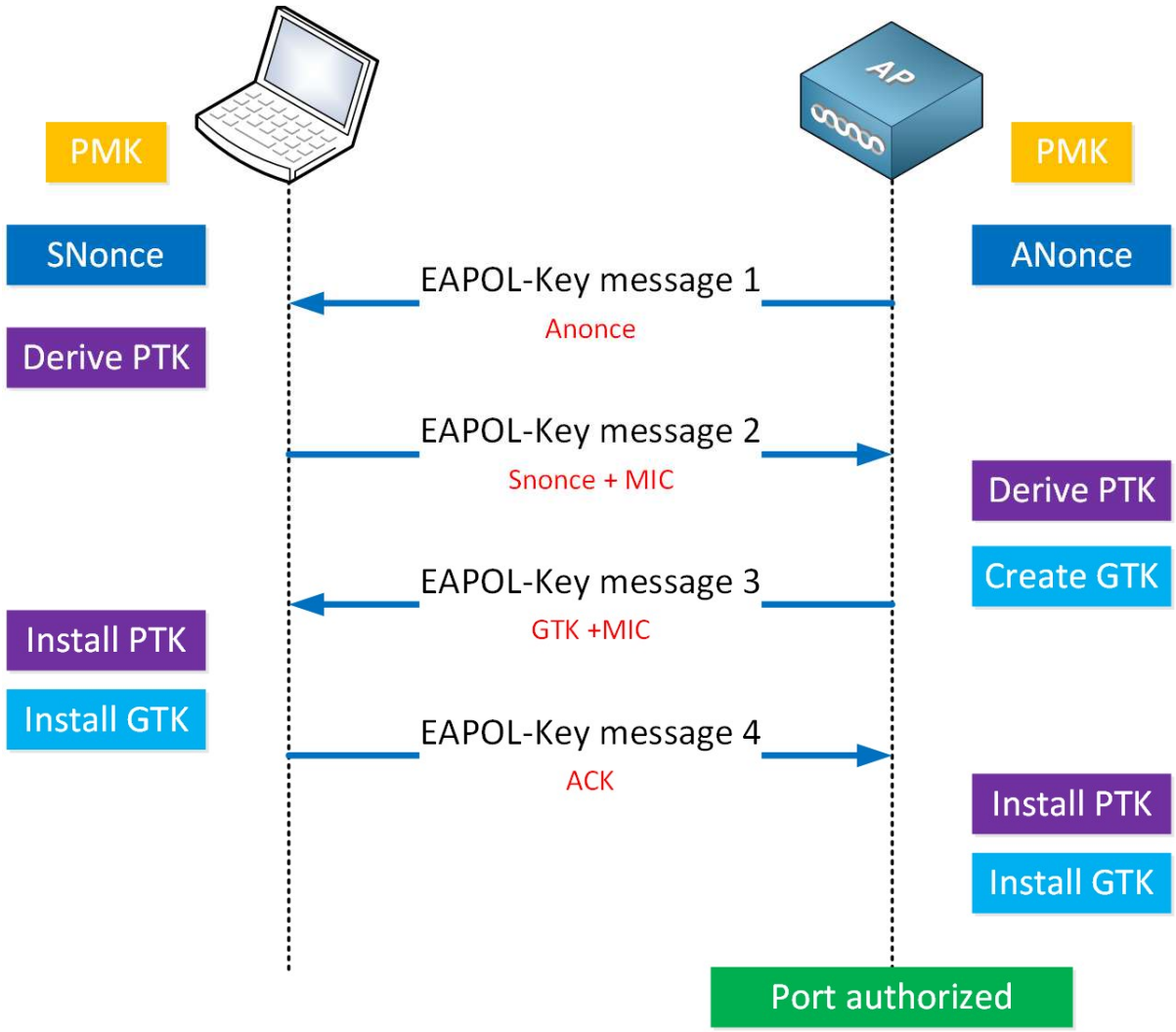
3. Mutual Authentication

- Client → AP Authentication: The client demonstrates it knows the shared secret (PMK) by generating the MICs based on the nonces. This proves its identity to the AP.
- AP → Client Authentication: The AP proves its identity to the client by providing a MIC for both nonces, which only an AP that knows the shared PMK could generate. Thus, the AP is authenticated to the client.

4. Key Derivation

At the end of the 4-way handshake:

- Both the client and AP have independently derived the same Pairwise Transient Key (PTK) from the PMK, the nonces, and their MAC addresses.
- The PTK will be used for encrypting data and ensuring the integrity of communications between the client and AP.



Q8) What will happen if we put a wrong passphrase during a 4Way handshake?

If a wrong passphrase is provided during the 4-way handshake, the authentication and key establishment process will fail. Here's what specifically happens in this case:

1. Incorrect PMK Derivation

- The Pairwise Master Key (PMK) is derived from the passphrase (in WPA2-Personal) or from the 802.1X authentication process (in WPA2-Enterprise).
- If the passphrase is incorrect, the PMK derived from it will be different from the correct PMK that both the client and access point (AP) should share.

2. Failure in MIC Verification

- During the 4-way handshake, both the client and the AP exchange Message Integrity Codes (MICs), which are based on the nonces and the PMK.
- If the PMK is incorrect, the client will generate a MIC that does not match the expected MIC from the AP, and vice versa.
- When the client and AP exchange the MICs (as part of the verification process), they will fail to match because the MIC is directly dependent on the correct PMK.

3. Handshake Termination

- As a result of the MIC mismatch, the 4-way handshake will not complete successfully.
- The AP or the client will detect the mismatch, and the handshake process will be terminated.
- The AP may simply reject the connection attempt or drop the connection without completing the secure key exchange.

4. No Encryption Established

- Since the Pairwise Transient Key (PTK) cannot be successfully derived (because the wrong PMK was used), there will be no session keys established for encryption or integrity protection.
- Without the PTK, the communication cannot be encrypted, and the network remains insecure.

5. Error Feedback

- Typically, the client (in WPA2-PSK mode) will display an error indicating an incorrect passphrase.
- The user will be prompted to enter the correct passphrase to attempt the connection again.

Q9 & Q10) What problem does 802.1X solve in a network? How does 802.1X enhance security over wireless networks?

802.1X is a network access control protocol that solves several key security issues in wired and wireless networks, primarily addressing the challenges of authentication, authorization, and accounting (AAA). The protocol is widely used in enterprise environments to provide strong, scalable security for both wired and wireless networks. Here's an overview of the key problems it solves:

1. Lack of Centralized Authentication

- Problem: In traditional networks (such as those using WEP or WPA-PSK), the authentication process is often static and based on shared secrets like pre-shared keys (PSK). This approach doesn't scale well for large networks and offers weak security.
- Solution: 802.1X uses a centralized authentication model through the use of an Authentication Server (typically a RADIUS server). This enables the centralized management of credentials and policies, making it easier to enforce security and manage access.

2. Weak Security in Shared Secret Models

- Problem: Shared secret authentication methods (e.g., WPA-PSK) are vulnerable because the same passphrase is used across many devices, making it susceptible to exposure or brute-force attacks.
- Solution: 802.1X implements dynamic, per-session authentication. Each device must be authenticated using strong credentials (e.g., usernames, passwords, certificates) before gaining network access. The authentication process is much more secure than a shared passphrase.

3. Limited Device Access Control

- Problem: Without 802.1X, it's difficult to differentiate between users, devices, or locations accessing the network, leading to uncontrolled access.
- Solution: With 802.1X, administrators can enforce granular control over who can connect to the network. It provides the ability to authenticate users based on username and password, certificates, or other credentials, allowing administrators to control who can access the network.

4. Lack of Guest and Temporary Access Management

- Problem: Traditional Wi-Fi security (e.g., WPA2-PSK) doesn’t offer a secure way to manage guest access or temporary users without compromising network security.
- Solution: 802.1X allows the implementation of dynamic guest access through a portal or captive portal, where guests can authenticate via temporary credentials. This ensures that guests are isolated from sensitive network resources.

5. Insecure Network Access for Devices

- Problem: Devices, especially IoT (Internet of Things) devices, may not be secure or properly configured for traditional network security methods, which exposes the network to potential vulnerabilities.
- Solution: 802.1X allows the use of device certificates or authentication methods tailored to ensure that only compliant and secure devices can join the network, increasing overall network security.

6. Non-Scalable Management of Network Access

- Problem: Managing network access individually for each device or user becomes complex and difficult to scale, especially in large enterprise environments.
- Solution: 802.1X enables automated network access control. The use of a centralized RADIUS server allows for easier management and enforcement of authentication policies across a large number of devices.

7. Post-Authentication Access Control

- Problem: In traditional networks, once a user gains access, there is little control over what network resources they can access, leading to potential unauthorized access.
- Solution: 802.1X works in conjunction with network access policies to ensure that users and devices are only granted access to appropriate resources after successful authentication. Once authenticated, network policies can be applied to control access based on user roles or device characteristics.

8. Integration with Other Security Services

- Problem: Without a proper access control mechanism, integrating security measures like VPNs, firewalls, and intrusion detection systems (IDS) becomes more challenging.
- Solution: 802.1X integrates with other AAA services (Authentication, Authorization, Accounting) and can trigger actions such as VPN access or restricted network access based on user identity and device security posture.

How 802.1X Works:

The 802.1X protocol involves three key components:

- Supplicant: The device seeking access to the network (e.g., a laptop, smartphone, or IoT device).
- Authenticator: The network device (usually a switch or wireless access point) that controls access to the network.
- Authentication Server: Typically a RADIUS server that validates the credentials of the supplicant and makes the decision on whether to allow or deny network access.