# MODULE 6 ASSIGNMENT

1. **What are the pillars of Wi-Fi security?**
   * **Authentication –** Verifies the identity of users/devices before granting access.
   * **Encryption –** Secures data during transmission, preventing eavesdropping.
   * **Integrity –** Ensures data is not tampered with during transit.
   * **Access Control –** Restricts network usage to authorized users only.
   * **Confidentiality –** Maintains the privacy of communication over the wireless medium.
2. **Explain the difference between authentication and encryption in Wi-Fi security.**

|  |  |  |
| --- | --- | --- |
| **Aspect** | **Authentication** | **Encryption** |
| **Purpose** | Validates identity of users/devices | Protects data from being read by  unauthorized parties |
| **Process** | Typically happens first during  connection | Happens once connection is established |
| **Examples** | PSK, 802.1X, certificate-based  login | TKIP, AES, CCMP |

1. **Explain the differences between WEP, WPA, WPA2, and WPA3.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Feature** | **WEP** | **WPA** | **WPA2** | **WPA3** |
| Encryption | RC4  (weak) | TKIP (interim  solution) | AES (stronger) | SAE, 192-bit security |
| Security | Very  weak | Moderate | Strong | Very strong |
| Key Mgmt | Static key | Dynamic key exchange | PMK + 4-way handshake | Forward secrecy +  Simultaneous Authentication of Equals (SAE) |
| Introduced | 1997 | 2003 | 2004 | 2018 |

1. **Why is WEP considered insecure compared to WPA2 or WPA3?**
   * Uses RC4 with weak IVs (Initialization Vectors).
   * Vulnerable to key reuse and packet sniffing.
   * Keys are statically configured and easy to crack.
   * WPA2/WPA3 use AES and dynamic key generation (much more secure).

# Why was WPA2 introduced?

* + To address vulnerabilities in WEP and WPA.
  + Required AES-based encryption (CCMP) for stronger security.
  + Enhanced key management via 4-way handshake.
  + Became a mandatory standard for Wi-Fi certification.

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

* + Derived during the authentication phase (e.g., from PSK or EAP).
  + Used to derive session-specific keys:
    - Pairwise Transient Key (PTK) for encrypting data.
  + Ensures both client and AP share a common secret.
  + Forms the backbone for secure key exchange in WPA/WPA2/WPA3.

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

* + Confirms both client and AP know the PMK.
  + Uses nonces (random numbers) to prevent replay attacks.
  + Establishes the PTK used for encryption and integrity.
  + Each party verifies the other's responses to ensure legitimacy.

# What will happen if we put a wrong passphrase during a 4-way handshake?

* + The derived PMK will not match between client and AP.
  + PTK generation will fail → handshake cannot be completed.
  + Connection will be rejected.
  + Logs may show “handshake timeout” or “authentication failed.”

# What problem does 802.1X solve in a network?

* + Provides port-based network access control.
  + Ensures only authorized users/devices can connect.
  + Supports dynamic key generation for encryption.
  + Centralized authentication using RADIUS or AAA servers.
  + Ideal for enterprise networks with many users.

# How does 802.1X enhance security over wireless networks?

* + Uses EAP (Extensible Authentication Protocol) for flexible authentication.
  + Allows certificate-based authentication → strong identity validation.
  + Dynamically generates session keys → no pre-shared keys required.
  + Works well with WPA2/WPA3-Enterprise modes.
  + Protects against rogue APs and MITM attacks.