### Q3)Differences Between WEP, WPA, WPA2, and WPA3

**1. WEP (Wired Equivalent Privacy)**

* **Introduced:** 1997 (Original Wi-Fi security standard)
* **Encryption:** RC4 (weak, easily cracked)
* **Authentication:** Open System or Shared Key (both flawed)
* **Key Length:** 64-bit or 128-bit (both insecure)
* **Vulnerabilities:**
* **Static keys** (same key used for all traffic).
* **IV (Initialization Vector) reuse** allows packet injection.
* Can be cracked in **minutes** with tools like Aircrack-ng.
* **Status:** **Deprecated (never use it!)**

**2. WPA (Wi-Fi Protected Access)**

* **Introduced:** 2003 (Temporary fix for WEP flaws)
* **Encryption:** TKIP (Temporal Key Integrity Protocol) – better than WEP but still weak.
* **Authentication:**
* **WPA-Personal (PSK):** Uses a pre-shared key (password).
* **WPA-Enterprise (802.1X):** Uses a RADIUS server for individual logins.
* **Improvements over WEP:**
* Dynamic key generation (TKIP changes keys periodically).
* Message Integrity Check (MIC) to prevent packet forgery.
* **Vulnerabilities:**
* **TKIP is crackable** via brute-force or WPS attacks.
* Still uses RC4 (though with safeguards).
* **Status:** **Obsolete (avoid if possible)**

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

* **Introduced:** 2004
* **Encryption:** **AES-CCMP** (replaced TKIP, much stronger).
* **Authentication:**
* **WPA2-Personal (PSK):** Password-based.
* **WPA2-Enterprise (802.1X):** For businesses (uses EAP methods like PEAP, EAP-TLS).
* **Improvements over WPA:**
* Uses **AES encryption** (military-grade, secure if configured correctly).
* More resistant to attacks than TKIP.
* **Vulnerabilities:**
* **KRACK Attack (2017):** Exploits handshake flaws (fixed with patches).
* Weak passwords are still a risk (brute-force attacks).
* **Status:** **Widely used but being phased out for WPA3.**

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

* **Introduced:** 2018 (Current gold standard)
* **Encryption:** **AES-256 + GCMP** (stronger than WPA2).
* **Authentication:**
* **WPA3-Personal:** Uses **SAE (Simultaneous Authentication of Equals)** to prevent brute-force attacks.
* **WPA3-Enterprise:** Adds **192-bit cryptographic strength** (for governments/military).
* **Key Improvements:**
* **Forward Secrecy:** Past sessions remain secure even if the password is leaked.
* **Protection Against Offline Attacks:** SAE makes dictionary attacks harder.
* **Enhanced Open (OWE):** Encrypts public Wi-Fi (replaces open networks).
* **Vulnerabilities:**
* **Dragonblood Attack (2019):** Flaws in SAE implementation (patched in updates).
* Requires compatible hardware (not all old devices support it).
* **Status:** **Recommended for all new networks.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Feature | WEP | WPA | WPA2 | WPA3 |
| Encryption | RC4 (Weak) | TKIP (Weak) | AES (Strong) | AES-256 (Best) |
| Authentication | Shared Key | PSK/Enterprise | PSK/Enterprise | SAE/Enterprise |
| Key Management | Static | Dynamic (TKIP) | CCMP (AES) | SAE (No PSK reuse) |
| Security Level | Broken | Weak (Avoid) | Good (With Patches) | Best (Future-Proof) |
| Best For | **Never Use** | Legacy Devices | Older Devices | Modern Networks |