WEP (Wired Equivalent Privacy):

- **Introduced**: 1997
- **Encryption**: Uses RC4 stream cipher with 64-bit or 128-bit keys (40-bit or 104-bit plus 24-bit IV).
- **Authentication**: Supports Open System or Shared Key authentication.
- **Security**: Weak due to small initialization vector (IV) and key management flaws, making it vulnerable to attacks like IV reuse and key cracking (e.g., Aircrack-ng).
- **Key Features**: Static keys, no dynamic key exchange, easily compromised.
- **Status**: Obsolete, not recommended since 2004

WPA (Wi-Fi Protected Access):

- **Introduced**: 2003
- **Encryption**: Still uses RC4 but introduces TKIP (Temporal Key Integrity Protocol) for dynamic key encryption.
- **Authentication**: Supports 802.1X/EAP for enterprise or PSK (Pre-Shared Key) for personal use.
- **Security**: Stronger than WEP, with per-packet key mixing and message integrity checks, but TKIP is still vulnerable to some attacks (e.g., Beck-Tews attack).
- **Key Features**: Temporary solution to address WEP's flaws, backward-compatible with older hardware.
- **Status**: Deprecated due to vulnerabilities in TKIP.

WPA2:

- **Introduced**: 2004
- **Encryption**: Uses AES (Advanced Encryption Standard) with CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), replacing TKIP.
- **Authentication**: Same as WPA (802.1X/EAP for enterprise, PSK for personal).
- **Security**: Much stronger than WPA, but vulnerable to KRACK (Key Reinstallation Attack) in 2017 and offline dictionary attacks on weak PSK passwords.
- **Key Features**: Mandatory AES encryption, robust for its time, widely adopted.
- **Status**: Still in use but being phased out in favor of WPA3.

WPA3:

- **Introduced**: 2018
- **Encryption**: Continues AES with CCMP, adds GCMP-256 (Galois/Counter Mode Protocol) for enhanced security.
- **Authentication**: Introduces SAE (Simultaneous Authentication of Equals), replacing PSK with a more secure handshake (Dragonfly Key Exchange).
- **Security**: Resists offline dictionary attacks, protects against KRACK, offers forward secrecy, and includes 192-bit security mode for enterprise.

    - **Key Features**: Easier secure setup for IoT devices via Easy Connect (DPP), stronger encryption for open networks (Opportunistic Wireless Encryption).
    - **Status**: Current standard, gradually replacing WPA2, but requires compatible hardware.

Key Differences:

- **Encryption Strength**:
    - WEP (weak RC4) < WPA (RC4+TKIP) < WPA2 (AES+CCMP) < WPA3 (AES+GCMP, enhanced protections).

- **Vulnerability**:
    - WEP is easily cracked; WPA has TKIP flaws; WPA2 is susceptible to specific attacks; WPA3 is the most secure with modern defenses.

- **Authentication**:
    - WEP uses basic methods; WPA/WPA2 use PSK or 802.1X; WPA3 uses SAE for stronger protection.

- **Use Case**:
    - WEP is obsolete; WPA is outdated; WPA2 is still common but aging; WPA3 is the future-proof choice but needs newer devices.