### Q4)Why WEP is Considered Insecure (Compared to WPA2/WPA3)

WEP (Wired Equivalent Privacy) was the original Wi-Fi encryption standard introduced in **1997**, but it is now **completely broken** and deemed unsafe. Here’s why it fails compared to modern protocols like WPA2 and WPA3:

**1. Weak Encryption Algorithm (RC4)**

* **WEP uses RC4**, a stream cipher with known flaws.
* **No message integrity checks**, allowing attackers to tamper with data packets.
* **Fixed encryption keys** (same key for all traffic), making it easy to crack.

**WPA2/WPA3 Fix:**

* WPA2 uses **AES-CCMP** (strong block cipher).
* WPA3 upgrades to **AES-256-GCMP** (even more secure).

**2. Key Reuse & Small IV (Initialization Vector)**

* WEP’s **24-bit IV** (used to randomize encryption) is too short.
* IVs repeat frequently (after ~5,000 packets), enabling **statistical attacks**.
* Attackers can capture packets and recover the key in **minutes** (e.g., with tools like Aircrack-ng).

**WPA2/WPA3 Fix:**

* WPA2 uses **48-bit IVs** (far less repetition).
* WPA3’s **SAE (Simultaneous Authentication of Equals)** eliminates IV-based attacks entirely.

**3. No Protection Against Replay Attacks**

* WEP allows attackers to **re-send old packets** (e.g., fake authentication requests).
* No mechanism to detect duplicated or modified data.

**WPA2/WPA3 Fix:**

* WPA2/WPA3 use **sequence numbers** and **message integrity checks (MIC)** to block replay attacks.

**4. Authentication Flaws**

* **Open System Authentication**: No real authentication (anyone can join).
* **Shared Key Authentication**: Reveals key details during the handshake, making it easier to crack.

**WPA2/WPA3 Fix:**

* WPA2/WPA3 use **strong authentication**:
  + **WPA2-Personal**: Pre-shared key (PSK) with brute-force protections.
  + **WPA3-Personal**: SAE (resists offline dictionary attacks).
  + **Enterprise modes (802.1X)**: Certificates or RADIUS servers for per-user auth.

**5. No Forward Secrecy**

* Once a WEP key is cracked, **all past and future traffic** can be decrypted.

**WPA3 Fix:**

* WPA3 provides **forward secrecy**—each session uses a unique key.

**Real-World Exploit Example**

An attacker can:

1. Capture WEP traffic (~10,000–50,000 packets).
2. Use tools like **Aircrack-ng** to recover the key in **under 1 minute**.
3. Decrypt all data or inject malicious packets.

**WPA2/WPA3**: Requires significantly more effort (e.g., KRACK attack on WPA2 needs proximity and targeted exploitation; WPA3 is even tougher).

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | WEP | WPA2 | WPA3 |
| Encryption | RC4 (broken) | AES-CCMP (strong) | AES-256-GCMP (stronger) |
| Key Management | Static keys, reused IVs | Dynamic keys (per session) | SAE (no key reuse) |
| Authentication | Weak (Shared Key/Open System) | PSK or 802.1X (Enterprise) | SAE or 192-bit Enterprise |
| Forward Secrecy | ❌ No | ❌ No (except with patches) | ✅ Yes |
| Time to Crack | <1 minute | Years (with strong password) | Nearly impossible (with SAE |