Weak Encryption Algorithm (RC4):

- WEP: Uses the RC4 stream cipher with a small 24-bit Initialization Vector (IV) and static keys (64-bit or 128-bit, including the IV). RC4 has known cryptographic weaknesses, and the short IV leads to frequent reuse, enabling attackers to collect enough data to crack the key.
- WPA2: Replaces RC4 with AES (Advanced Encryption Standard) and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), which are far more robust and resistant to cryptographic attacks.
- WPA3: Also uses AES with CCMP and adds GCMP-256 (Galois/Counter Mode Protocol), providing even stronger encryption and forward secrecy, making it harder to decrypt past sessions even if a key is compromised.

Static Key Usage:

- **WEP:** Relies on static, manually configured keys that rarely change, making them easier to crack over time as more data is captured. There's no mechanism for automatic key rotation.
- **WPA2:** Uses dynamic key generation through TKIP (in older implementations) or CCMP, with keys derived per session via 802.1X/EAP (enterprise) or PSK (personal), reducing the risk of key compromise.
- **WPA3:** Implements SAE (Dragonfly Key Exchange), which generates unique session keys for each connection and supports forward secrecy, ensuring compromised keys don't expose past or future sessions.

Vulnerability to Specific Attacks:

- **WEP:** Highly susceptible to attacks like:
    - IV reuse attacks: Tools exploit repeated IVs to decrypt data.
    - FMS attack: Exploits RC4 weaknesses to recover the key.
    - Chopchop attack: Decrypts packets without knowing the key. These attacks are practical and require minimal effort, often breaking WEP in under 10 minutes.
- **WPA2:** More secure but vulnerable to the KRACK (Key Reinstallation Attack) in 2017, which exploits handshake flaws, and offline dictionary attacks if weak PSK passwords are used. However, these are harder to execute than WEP attacks.
- **WPA3:** Patches KRACK vulnerabilities and resists offline dictionary attacks through SAE, which uses a password-based key exchange that's computationally intensive for attackers, even with weak passwords.

Lack of Message Integrity:

- **WEP:** Uses a weak CRC-32 checksum for integrity, which can be manipulated by attackers to alter data without detection.
- **WPA2:** Employs CCMP with a Message Integrity Check (MIC) to ensure data hasn't been tampered with, providing strong integrity protection.

- **WPA3:** Enhances integrity with GCMP and SAE, ensuring robust protection against tampering and replay attacks.

Authentication Weaknesses:

- **WEP:** Supports Open System (no real authentication) or Shared Key authentication, which is insecure because it exposes key information during the authentication process, aiding attackers.
- **WPA2:** Uses stronger authentication via 802.1X/EAP for enterprise networks or PSK for personal networks, though weak PSKs can be brute-forced.
- **WPA3:** Introduces SAE, which provides mutual authentication and resists offline brute-force attacks, even with weaker passwords, making authentication far more secure.

Ease of Exploitation:

- **WEP: T**ools like Aircrack-ng, Wireshark, or Kali Linux make WEP cracking accessible to novices, requiring only a few packets to break encryption.
- **WPA2:** Requires more sophisticated attacks, like capturing a 4-way handshake and brute-forcing a weak PSK, which is time-consuming and less reliable.
- **WPA3:** Resists handshake-based attacks and brute-forcing due to SAE's design, making it significantly harder to crack, even for advanced attackers.