Below is a **professionally formatted, sentence-by-sentence study breakdown** of your document **"202. Wireless Encryption Notes"**, preserving every essential point while keeping the formatting **clear, minimalistic, and ideal for pasting into Microsoft Word**. It’s designed for serious exam review and technical understanding — not overly spaced, not too dense, and logically segmented.

**CompTIA A+ 1102 — Wireless Encryption (Section 202) Professional Study Notes**

**1. Introduction to Wireless Encryption**

* Wireless encryption ensures that **data transmitted over Wi-Fi** is protected from **unauthorized access**.
* Over time, protocols like **WEP**, **WPA**, **WPA2**, and **WPA3** have been developed to improve wireless security.
* This lesson focuses **only on WPA2 and WPA3**, which are the **current standards**.
* Older protocols (**WEP** and original **WPA**) are now considered **insecure and deprecated**.

**2. WPA2 – Wi-Fi Protected Access 2**

* **WPA2** was introduced in **2004** and became the **standard** for wireless encryption.
* It replaced WPA and offers **stronger encryption** using **AES (Advanced Encryption Standard)**.
* **AES** is a **symmetric encryption algorithm**, known for its **strength and efficiency**.

**2.1 AES and CCMP in WPA2**

* WPA2 typically uses **AES** paired with **CCMP** (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol).
  + To help secure wireless communications.
* This combination ensures **confidentiality** and **data integrity**.

**2.2 Hardware Compatibility**

* Devices must **support AES** to use WPA2 securely.
* **Older devices** may not support AES and require **WPA2-TKIP**, which falls back to the **less secure TKIP encryption**.
* TKIP is a legacy protocol and should be **avoided when possible**.

**2.3 Known Vulnerability: KRACK**

* **KRACK (Key Reinstallation Attack)** is a known vulnerability in WPA2.
* It exploits flaws in WPA2’s **four-way handshake** to intercept/manipulate encrypted data.
* To mitigate this:
  + Use **strong passwords**
  + Disable outdated protocols (WEP/WPA)
  + Due to its vulnerability a new variant known as WPA3 was released.

**3. WPA3 – Wi-Fi Protected Access 3**

* **WPA3** was introduced in **2018** to address WPA2’s vulnerabilities and enhance usability.

**3.1 Encryption Improvements**

* WPA3 uses **AES-GCMP (Galois/Counter Mode Protocol)** instead of AES-CCMP.
* GCMP offers **stronger encryption** and **authentication mechanisms**.

**3.2 Simultaneous Authentication of Equals (SAE)**

* SAE replaces the **Pre-Shared Key (PSK)** model from WPA2-Personal.
* SAE provides **stronger protection against brute-force attacks by making password cracking more difficult**, even with **weaker passwords**.

**3.3 Forward Secrecy**

* WPA3 implements **forward secrecy** — even if a key is compromised, **previous sessions remain protected**.
* This helps prevent **decryption of historical data** from stored network captures.

**3.4 Enterprise Enhancements**

* In enterprise networks, WPA3 enhances **802.1X authentication** and supports **stronger protocols** for sensitive environments.

**3.5 Wi-Fi Easy Connect**

* Simplifies connection of **IoT (Internet of Things) devices** that lack interfaces.
* Uses **QR codes** or **NFC (Near-Field Communication)** to connect securely.

**4. Compatibility and Deployment Considerations**

* **Legacy devices** may not support WPA3, so many networks operate in **WPA2/WPA3 mixed mode**.
* **Mixed mode** allows backward compatibility but **compromises some WPA3 security features**.
* Organizations are encouraged to **fully adopt WPA3** wherever feasible.

**5. Summary and Key Takeaways**

* **WPA2**:
  + Uses **AES + CCMP**
  + Widely deployed and secure, but vulnerable to **KRACK**
  + Falls back to **TKIP** on older hardware (not recommended)
* **WPA3**:
  + Introduces **SAE**, **AES-GCMP**, and **forward secrecy**
  + More resilient against **brute-force attacks**
  + Supports **IoT connectivity** and **enterprise-grade security**
* Wireless encryption is **critical** for securing Wi-Fi networks.
* By understanding and implementing **WPA2 and WPA3**, technicians can ensure the **safety and reliability** of modern wireless environments.