**Q2) Difference Between Authentication and Encryption in Wi-Fi Security**

|  |  |  |
| --- | --- | --- |
| Feature | Authentication | Encryption |
| Purpose | Verifies the identity of users/devices trying to connect. | Secures data transmitted over the network to prevent eavesdropping. |
| How It Works | Checks credentials (e.g., passwords, certificates) before granting access. | Scrambles data using cryptographic algorithms so only authorized parties can read it. |
| Examples | - WPA2-PSK (Pre-Shared Key) - WPA3-Enterprise (802.1X/EAP) - MAC Filtering (weak) | - WPA3 (AES-256) - WPA2 (AES) - WEP (insecure, deprecated) |
| Weaknesses | - Weak passwords can be brute-forced. - MAC addresses can be spoofed. | - Outdated protocols (WEP, TKIP) can be cracked. - Key reuse risks (e.g., KRACK attack on WPA2). |
| Real-World Analogy | Like a bouncer checking IDs at a club. | Like a locked envelope—only |

1. **Authentication = "Who are you?"**

* Ensures only authorized users/devices join the network.
* Critical for preventing unauthorized access (e.g., rogue devices).

1. **Encryption = "Protect what you say."**

* Ensures data (e.g., emails, passwords) can't be read by hackers sniffing Wi-Fi signals.
* Critical for privacy and compliance (e.g., GDPR, HIPAA).

### ****Why Both Are Needed:****

* **Without authentication**, anyone could connect to your Wi-Fi.
* **Without encryption**, attackers could read all transmitted data (e.g., credit card details).

**Example:**

* A coffee shop’s **open Wi-Fi (no authentication, no encryption)** lets anyone connect but exposes all traffic.
* A corporate network using **WPA3-Enterprise (strong authentication) + AES-256 (encryption)** ensures only employees access data securely.

### ****Best Practices:****

* **For Authentication:**
* Use **WPA3-Enterprise (802.1X/EAP)** for businesses.
* For home networks, use **WPA3-PSK with a strong password**.
* **For Encryption:**
* Always prefer **WPA3 (AES-256)** or **WPA2 (AES)**.
* Never use **WEP or TKIP**.