|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Standard** | **Encryption** | **Authentication Method** | **Security** | **Vulnerabilities** | **Best For** | **Network Types** |
| **WEP** | RC4 (weak encryption) | Shared Key (Pre-shared key) | Very weak, easy to hack | Easily cracked using tools, vulnerable to attacks | **Avoid** – no longer secure. | Older networks, if any |
| **WPA** | TKIP (better than WEP but weak) | PSK (Pre-shared key) or 802.1X | Improved over WEP, but still insecure | Vulnerable to dictionary and brute-force attacks | Better than WEP, but outdated and vulnerable. | Small networks, older setups |
| **WPA2** | AES (Advanced Encryption Standard) | PSK (Pre-shared key) or 802.1X | Strong, reliable, widely used | Few known vulnerabilities, still secure if updated | Most common choice for home and business networks. | Home and business networks |
| **WPA3** | AES with 256-bit keys | Simultaneous Authentication of Equals (SAE) | Strongest encryption, better protection against attacks | Fewer vulnerabilities, more robust than WPA2 | Best choice for modern networks, offers the highest security. | Latest home, business, and public networks |

3. Explain the differences between WEP, WPA, WPA2, and WPA3 :