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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Feature** | **WEP** | **WPA** | **WPA2** | **WPA3** |
| **Introduced** | 1997 | 2003 | 2004 | 2018 |
| **Encryption Type** | RC4 (Stream Cipher) | TKIP (Temporal Key Integrity Protocol) | AES + CCMP (Advanced Encryption Standard) | AES (Advanced Encryption Standard) |
| **Security Level** | Weak | Better than WEP, but insecure | Strong | Highest (most secure) |
| **Key Length** | 64-bit or 128-bit (with 24-bit IV) | 128-bit dynamic keys | 128-bit keys (AES) | 192-bit keys (AES) |
| **Data Integrity** | CRC - 32 | MIC | CBC - MAC | SHA |
| **Vulnerabilities** | Easily cracked, weak encryption | Vulnerable to dictionary and brute-force attacks | Vulnerable to KRACK attacks | Strong against offline attacks, includes forward secrecy |
| **Recommended Use** | Not recommended | Not recommended | Still widely used | Recommended for new networks |
| **Best For** | Legacy devices | Transition between WEP and WPA2 | Home and enterprise networks | New devices and high-security networks |
| **Additional Features** | None | None | KRACK vulnerability | SAE (Simultaneous Authentication of Equals), forward secrecy, enhanced public network protection |