**WPA/WPA2**

**Wired Equivalent Privacy (WEP)** the first encryption algorithm for the 802.11 standard -- with one main goal: prevent hackers from snooping on wireless data as it was transmitted between clients and APs. From its inception in the late 1990s, however, WEP lacked the strength necessary to accomplish this aim.

WEP uses the **RC4 (Rivest Cipher 4)** stream cipher for authentication and encryption. The standard originally specified a 40-bit, pre-shared encryption key; a 104-bit key later became available after the U.S. government lifted certain federal restrictions.

An administrator must manually enter and update the key, which combines with a 24-bit **initialization vector (IV)** in an effort to strengthen encryption. The small size of the IV increases the likelihood that users will recycle keys, however, making them easier to crack. This characteristic, along with several other security flaws and vulnerabilities (including problematic authentication mechanisms) makes WEP a **risky choice** for wireless security.

**Cracking flow:**

1. Use “airodump-ng” to monitor the wifi network.
2. Use “aireplay-ng --fakeauth” to establish communication with the wifi network.
3. Use “aireplay-ng --arpreplay” to catch ARP packet and resend it to increase number of packets.
4. Use “aircrack-ng” to scan packets for the password.
5. Use a password to enter the WEP network.