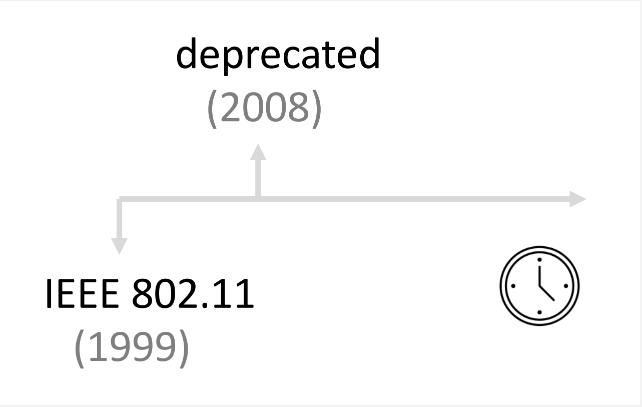
Wired Equivalent Privacy (WEP) -

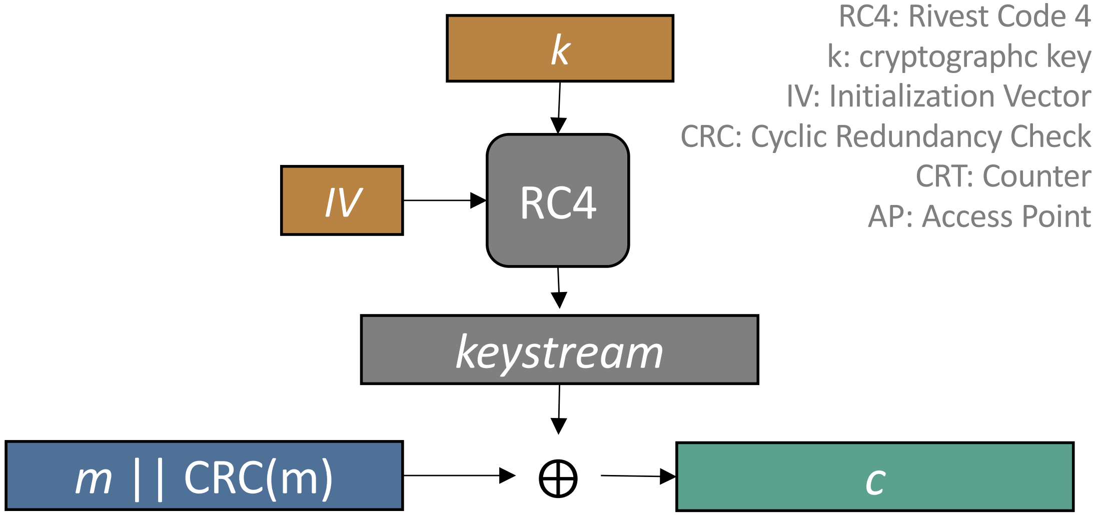


Sizes

k: 104 bits (40 bits export)

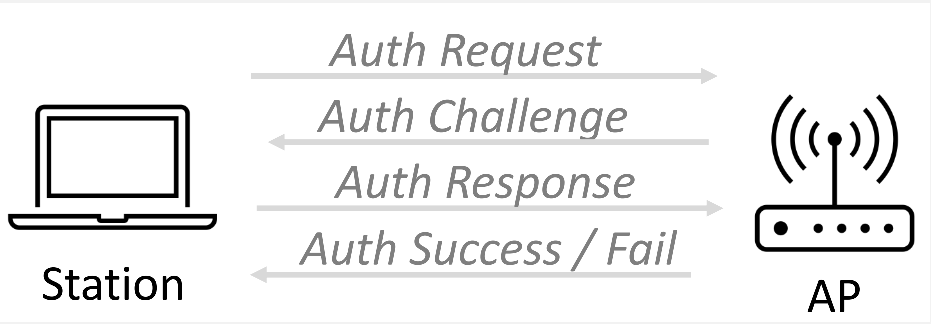
IV: 24 bits (used in CTR mode)

- − *Confidentiality:* short k, short IV, linearity / bit flipping, …
- − *Integrity:* CRC is not a MAC/MIC
- − *Key management:* a single key for all devices
- − *Authentication:* not mutual, $\mathcal{A}$ can passively find the keystream for used IV
- + *Open standard*

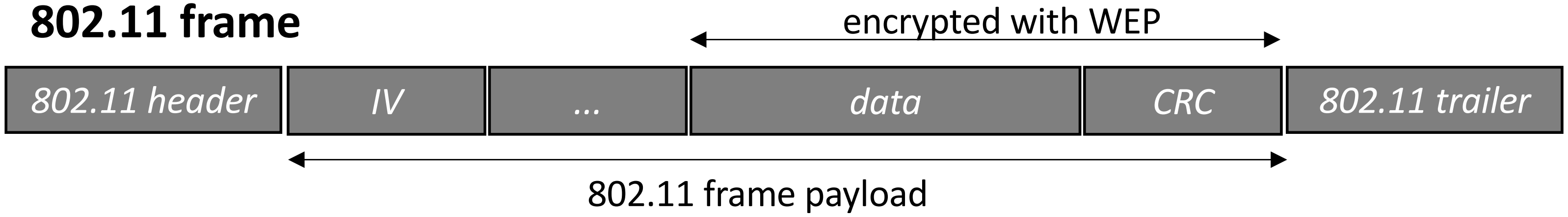


RC4: Rivest Code 4
k: cryptographc key
IV: Initialization Vector
CRC: Cyclic Redundancy Check
CRT: Counter
AP: Access Point

Encryption: $c = (IV, RC4(k,IV) \oplus m||CRC(m))$
Decryption: $m\,||CRC(m) = RC4(k,IV) \oplus c$



802.11 frame


encrypted with WEP
802.11 header
IV
…
data
CRC
802.11 trailer
802.11 frame payload