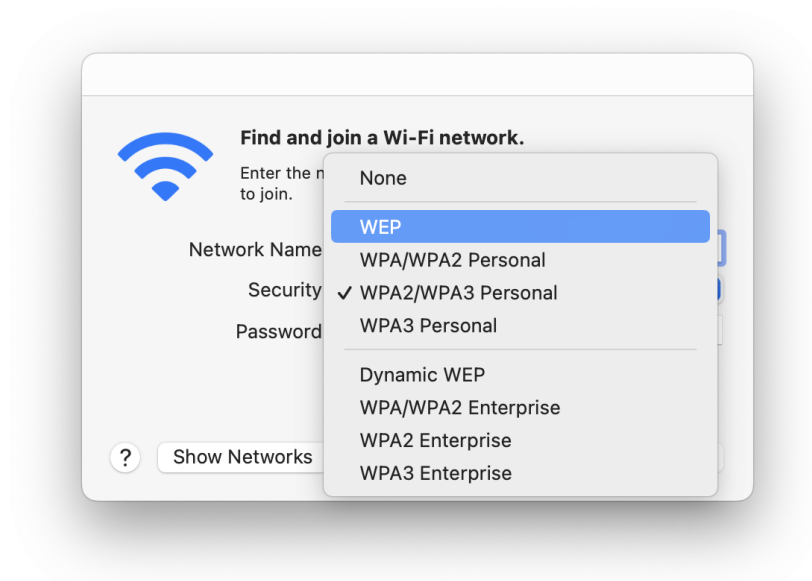


Wi-Fi Security



WEP is original and weak

WPA variants are new and good

Wi-Fi Security



Wi-Fi security encrypts frames that your machine broadcasts


But in motivating SSL, IPsec, and similar, we have assumed that packets are public, anyway...

Reasons to care about Wi-Fi security:

- security in depth
- proximity of attacker
- ease of identifying a specific Wi-Fi user

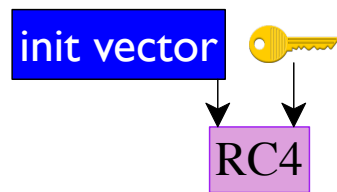
WEP

Wired Equivalency Privacy (WEP) is the original 802.11 standard

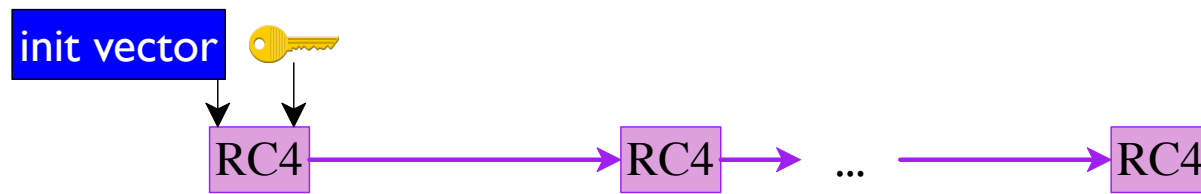
- Based on a 40-bit password/key 
- Same key for all users
- Typically entered manually as 10 hex digits!

 plus a per-frame init vector seeds RC4 for a stream cipher

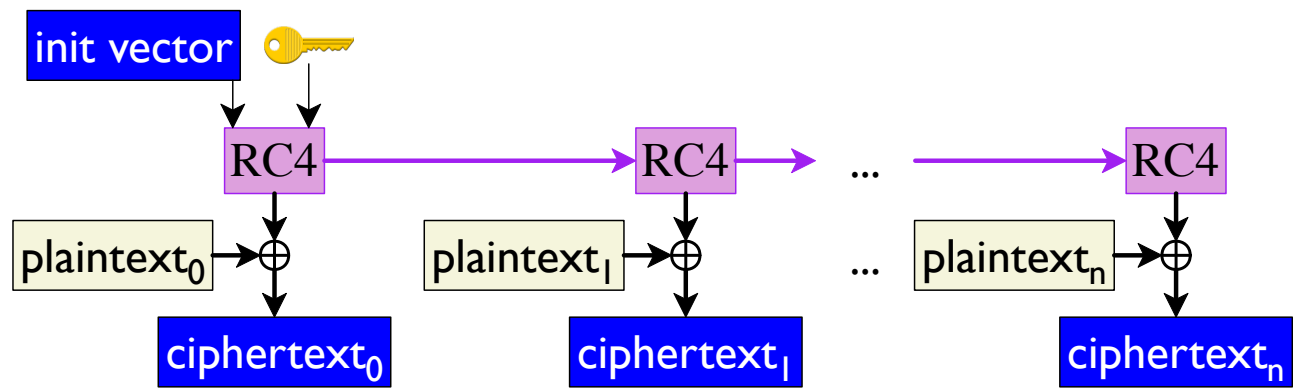
WEP



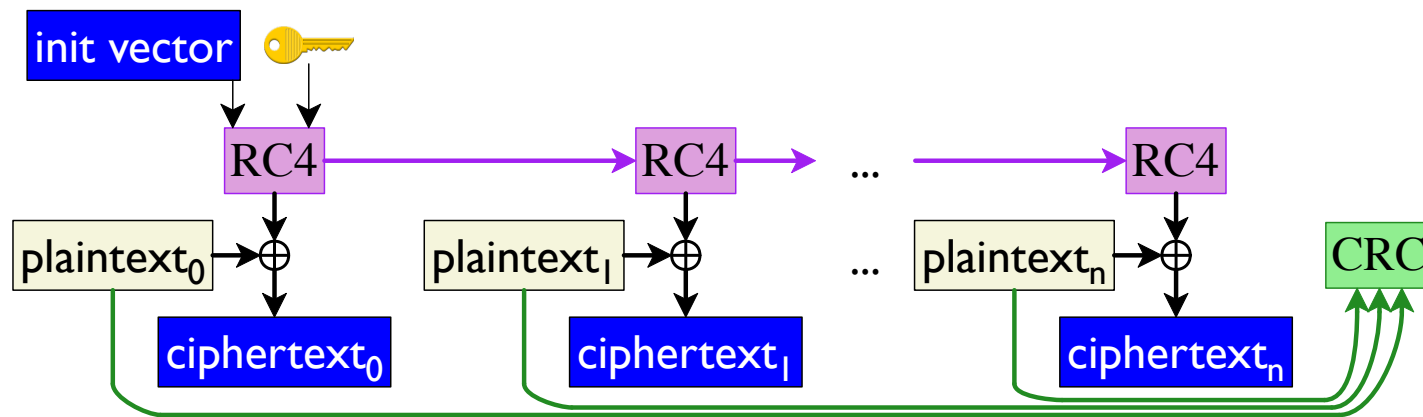
WEP



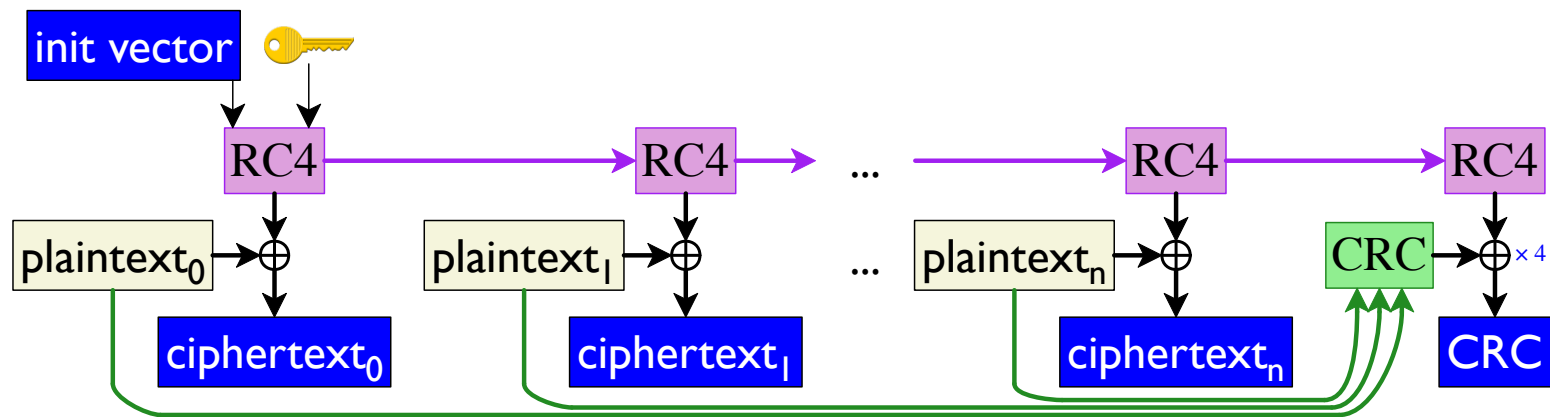
WEP



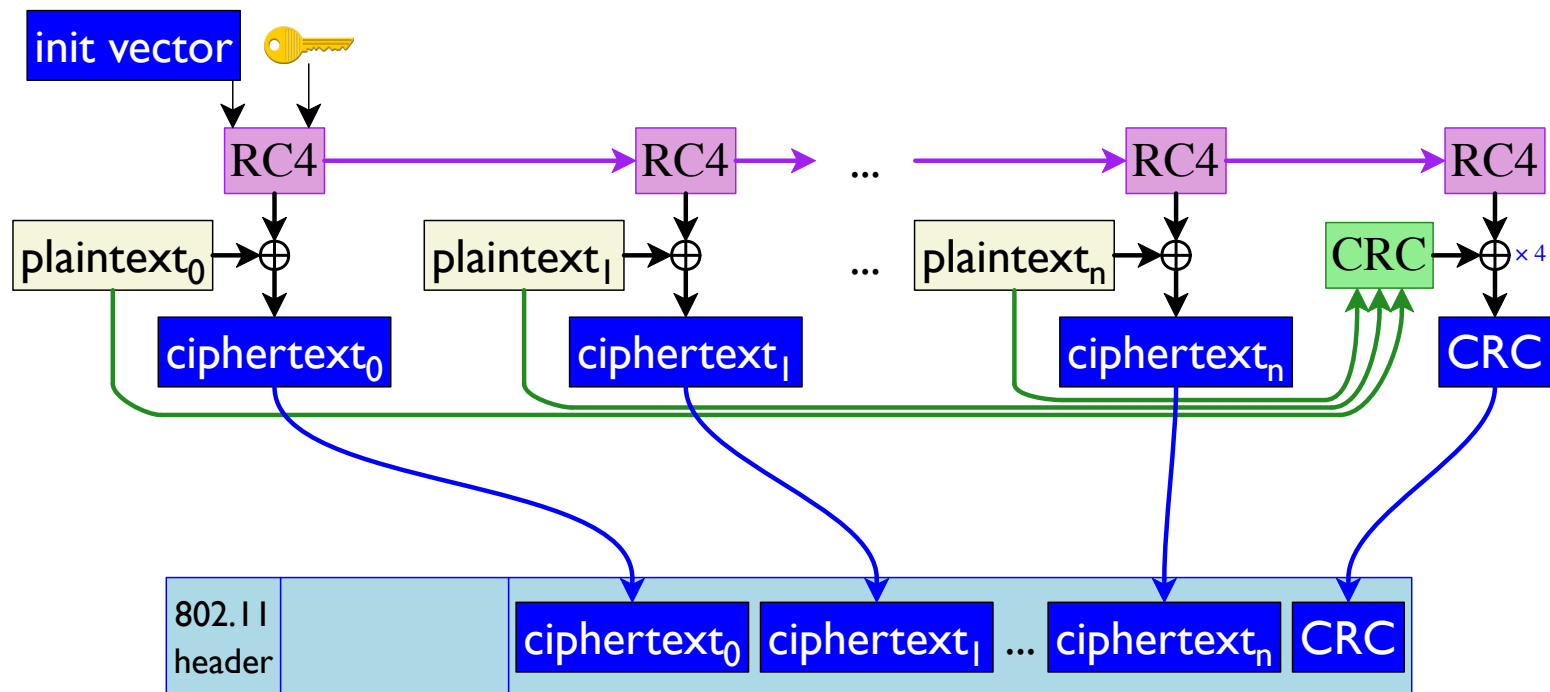
WEP



WEP

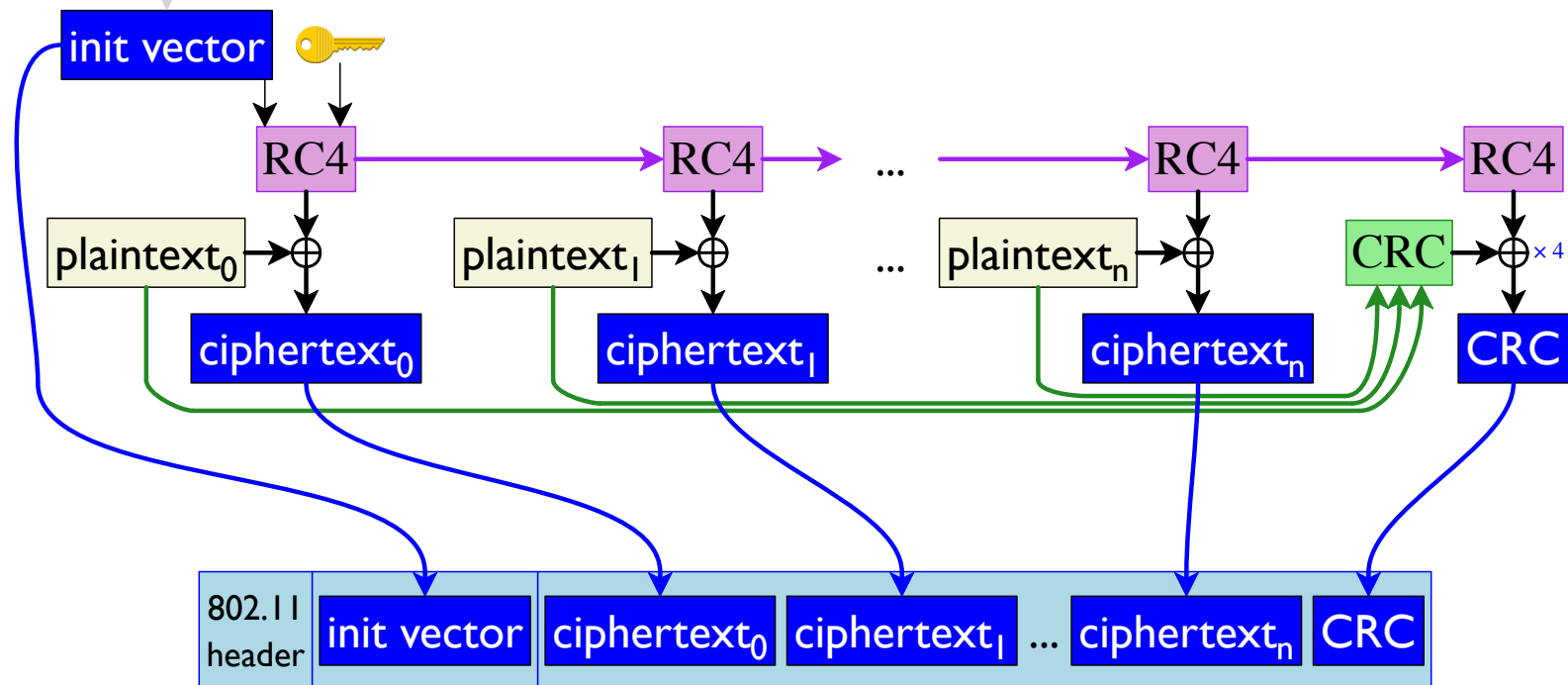


WEP

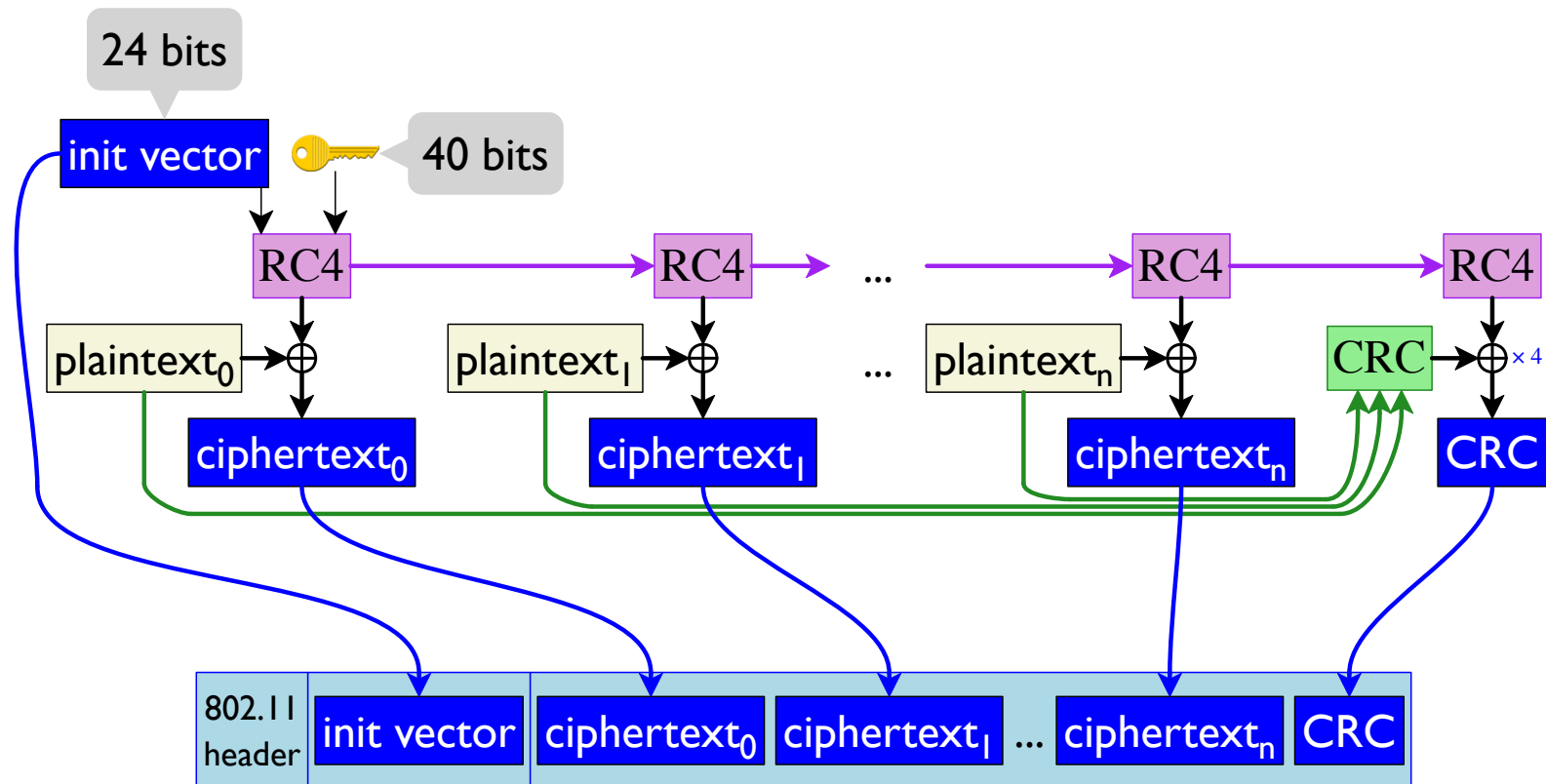


WEP

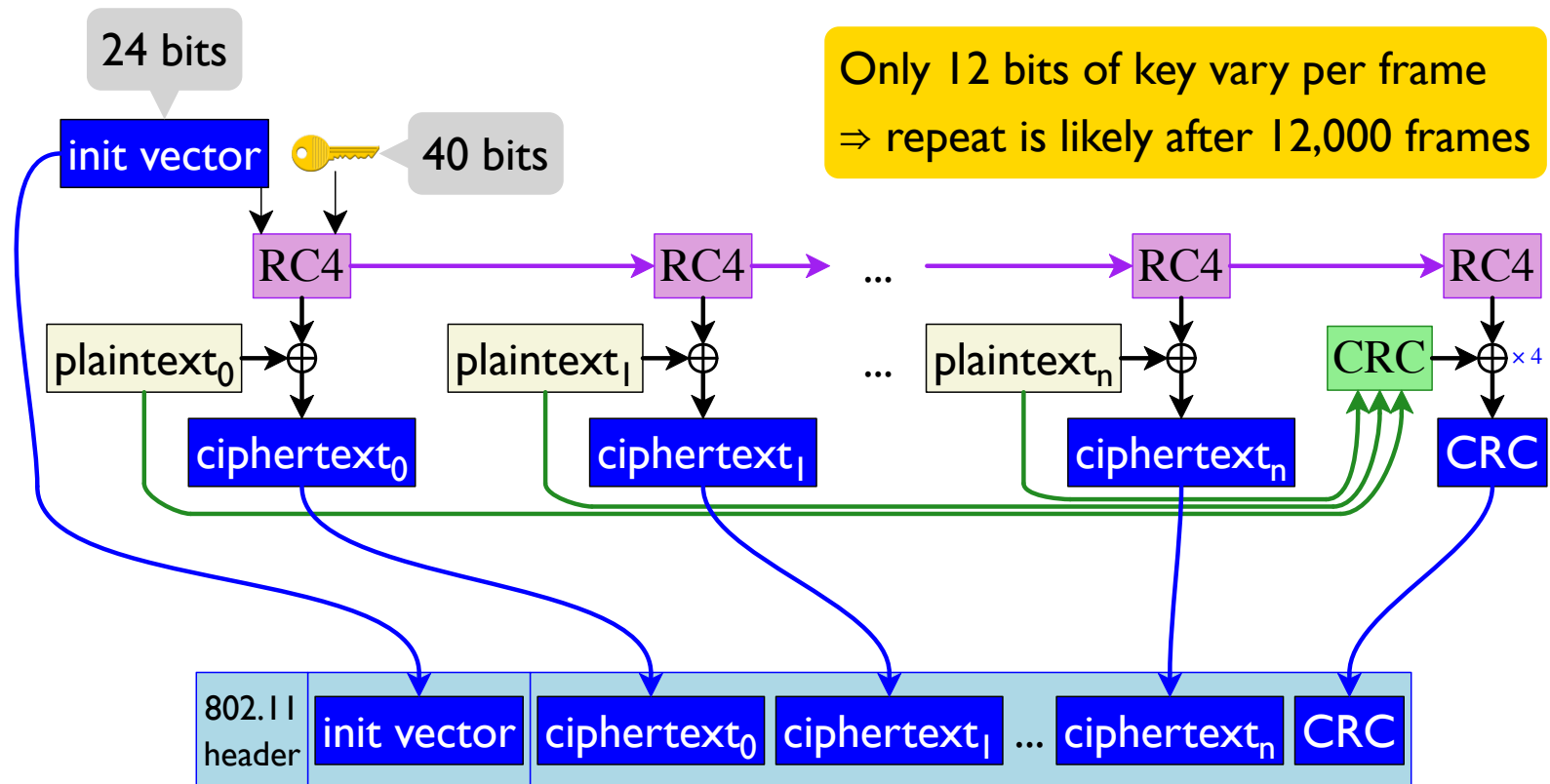
Fresh random for each frame



WEP

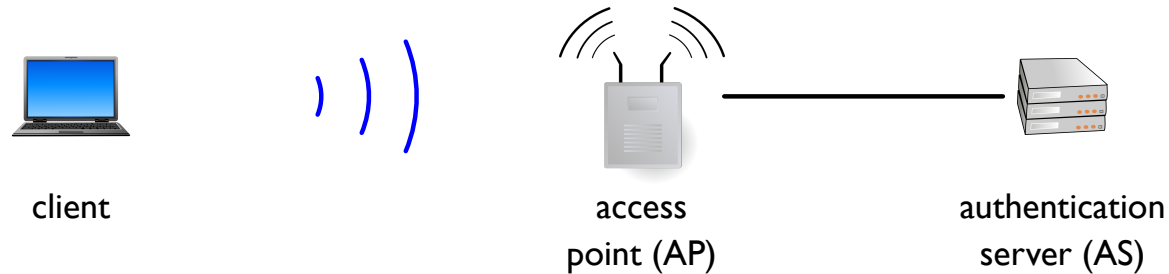


WEP



WPA

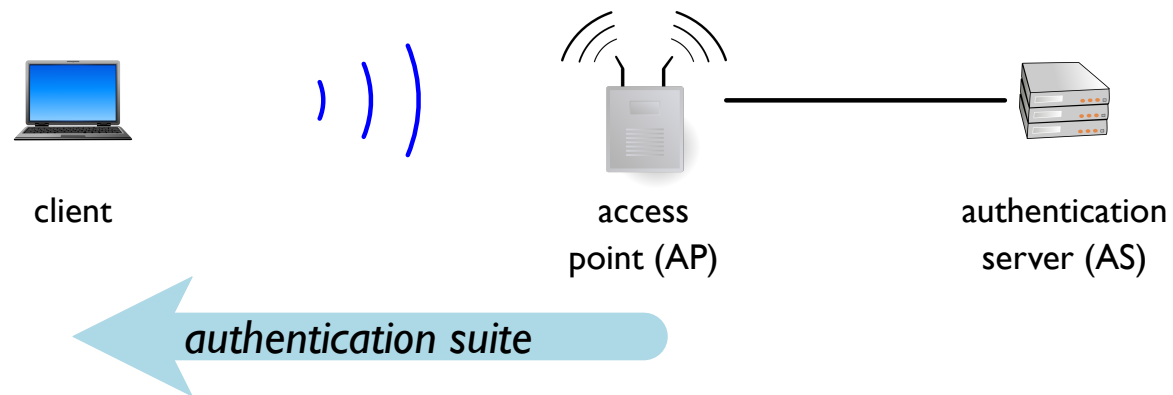
Wi-Fi Protected Access (WPA) is the successor to WEP



Supports an **authentication server (AS)** that is separate from the Wi-Fi **access point (AP)**

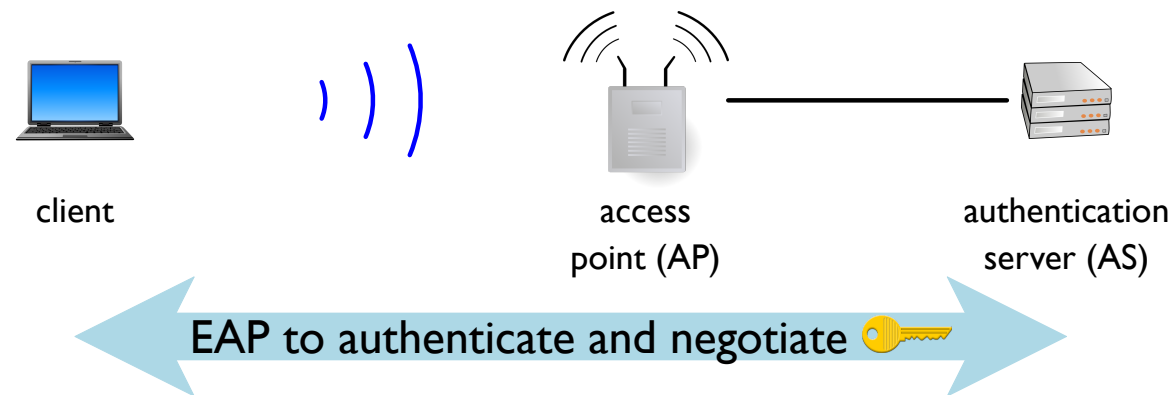
which reduces AP configuration for a large network
with **WPA Enterprise** user-specific authentication

WPA Enterprise



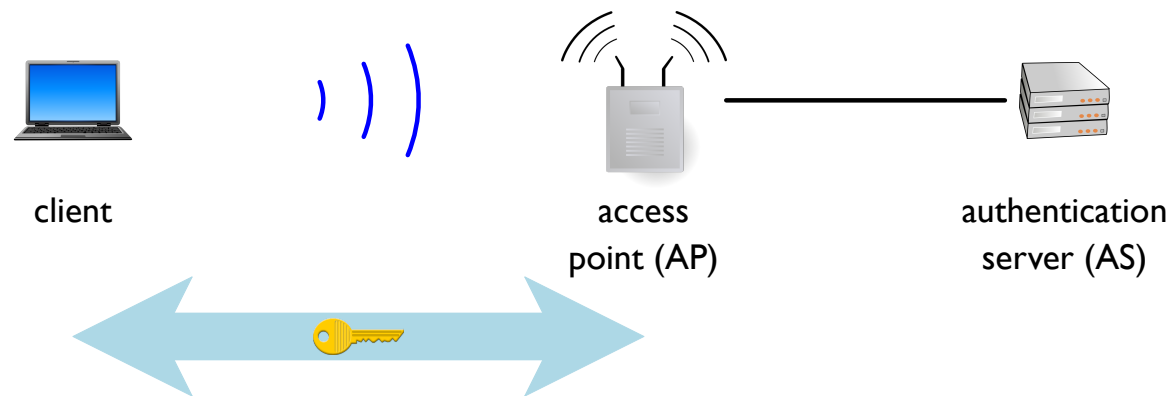
Initially, the AP advertises authentication protocols to clients

WPA Enterprise



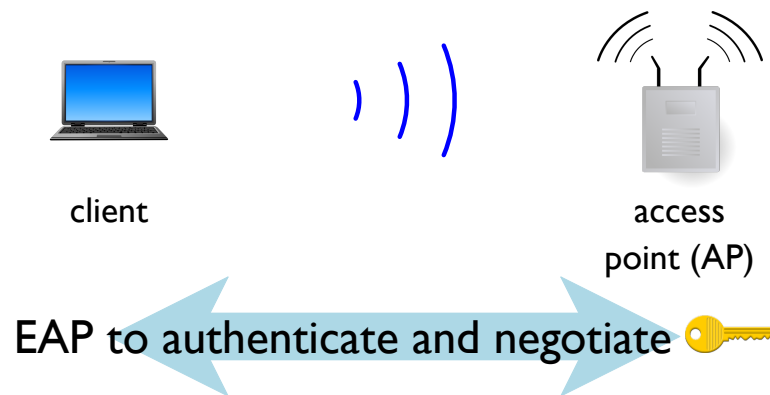
The AP then acts as a bridge for client and AS to pick a master key 🗝️ using the **Extensible Authentication Protocol (EAP)**

WPA Enterprise



Client and AP communicate with session keys from 🗝️

WPA Personal



WPA Personal is a simplified organization where the AP acts as AS with a single password for all users

Cryptography and Government

The NSA's mission is in part to

- ensure good encryption for U.S. entities
- be able to defeat encryption for everyone else

Some ways this has played out:

- DES and the ensuing controversy, leading to AES
- The **Clipper chip** design of 1993-1996
- The Snowden revelations of 2013

Cryptography and Export

Export of cryptographic technology is controlled by law:

- Before 1996: on the *Munition List* managed by the State Department
- After 1996: on the *Commerce Control List* managed by the Commerce Department

Until 1999, export limited to 512-byte RSA and 40-bit RC, roughly

Netscape Navigator had a “U.S. Edition” and “International Edition”

WEP had to be weak to enable export

Cryptography and Export



Cryptography and Quantum Computing

Existing public-key cryptography relies on just three hard problems:

- integer factorization
- discrete logarithm
- elliptic-curve discrete logarithm

Shor's algorithm can solve these on a large enough quantum computer

For now:

- *large enough* seems far away
- Noise in quantum circuits may be a further obstacle
- Symmetric-key algorithms and hash functions are not affected

Summary

WPA is TLS again, this time at the physical layer

Weaknesses of the original **WEP** protocol relate to larger questions about cryptography and government