Wireless LAN Security
- IEEE802.11i

Review

- **IEEE802.11b**
  - **CCK**
- **IEEE 802.11g**
  - **OFDM at 5GHz**

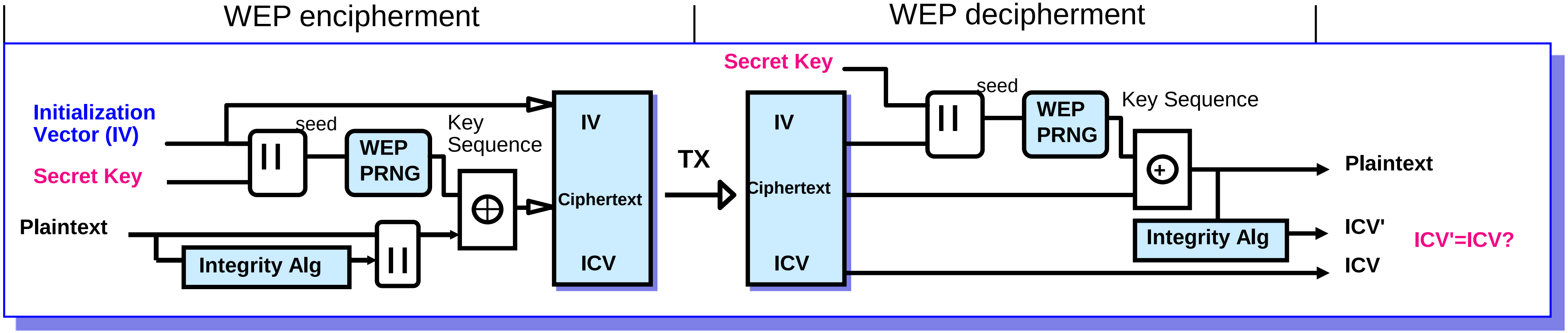
Introduction

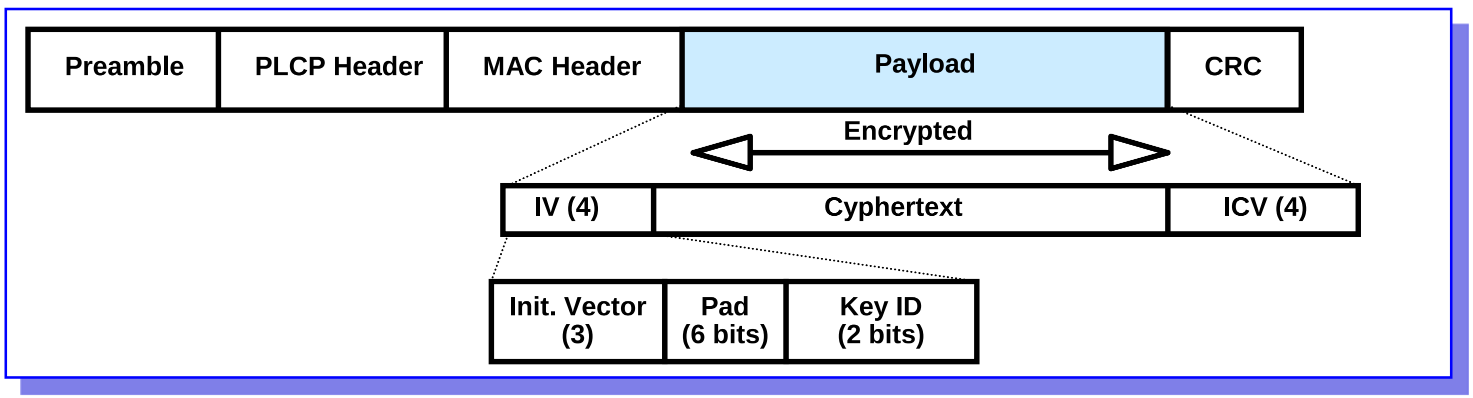
- 802.11 standard specifies the operating parameters of wireless local area networks (WLAN)
  - History: 802.11, b, a, g, i
- Minimal security in early versions
- Original architecture not well suited for modern security needs
- 802.11i attempts to address security issues with WLANs

WEP in 802.11b

- **Wired Equivalent Privacy (WEP)**
  - **Confidentiality**
    - » **Encryption**
      - **40-bit keys - small keys**
      - **Based on RC4 algorithm - too simple**
  - **Access Control**
    - » **Shared key authentication - weak**
    - » **+ Encryption - poor**
  - **Data Integrity**
    - » **Integrity checksum computed for all messages – prone to attacks**

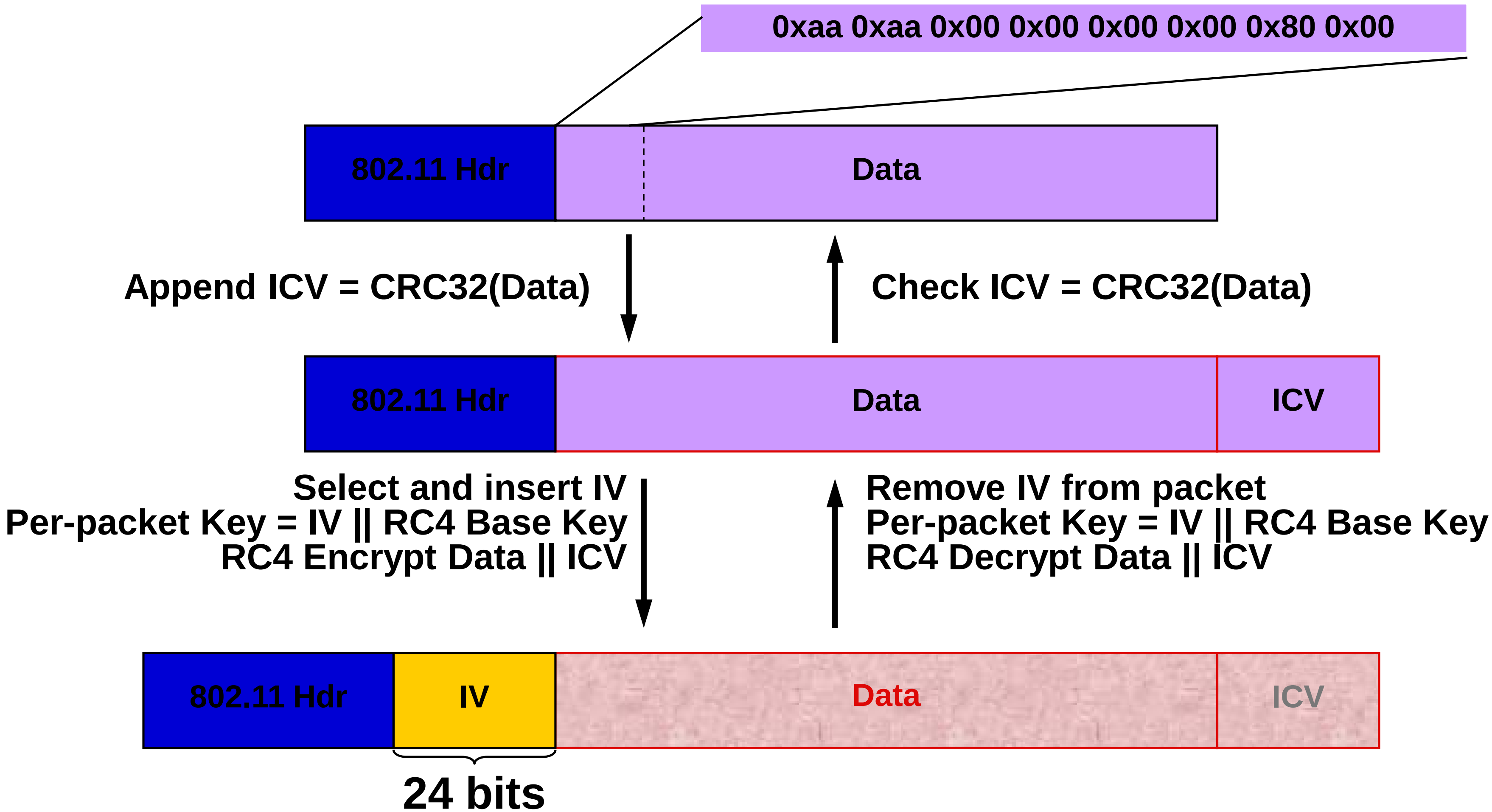
WEP Mechanism





- **WEP Encryption uses RC4 stream cipher**
  - **Each frame can have a new IV, or IV can be reused for a limited time.**
  - **If integrity check fails then frame is ACKed but discarded.**

How does WEP "work"?



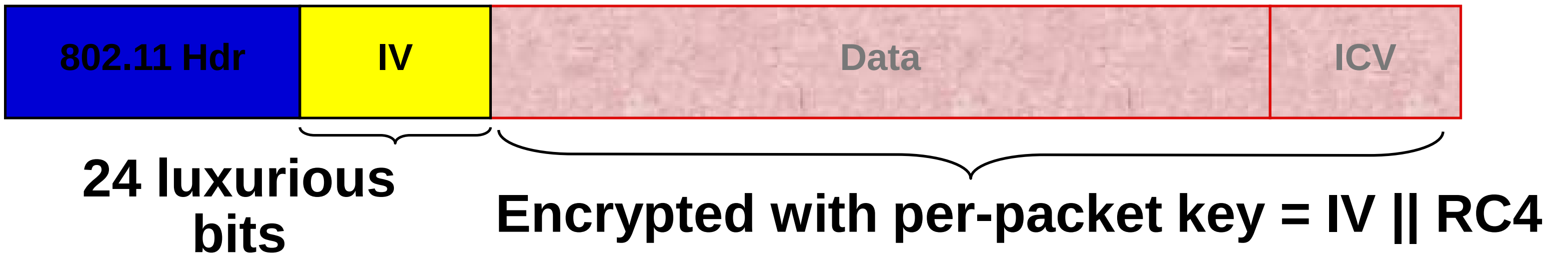
IV: Initial Vector; ICV: Integrity Check Value

WEP Weakness

- **Several major problems in WEP security**
  - **The IV used to produce the RC4 stream is only 24-bit long**
    - » **The short IV field means that the same RC4 stream will be used to encrypt different texts – IV collision**
    - » **Statistical attacks can be used to recover the plaintexts due to IV collision**
  - **The CRC-32 checksum can be easily manipulated to produce a valid integrity check value (ICV) for a false message**

- **Attack types:**
  - **Collision attacks, weak key(key discovery) attacks, replay attacks and forgery attacks.**

Collision attacks

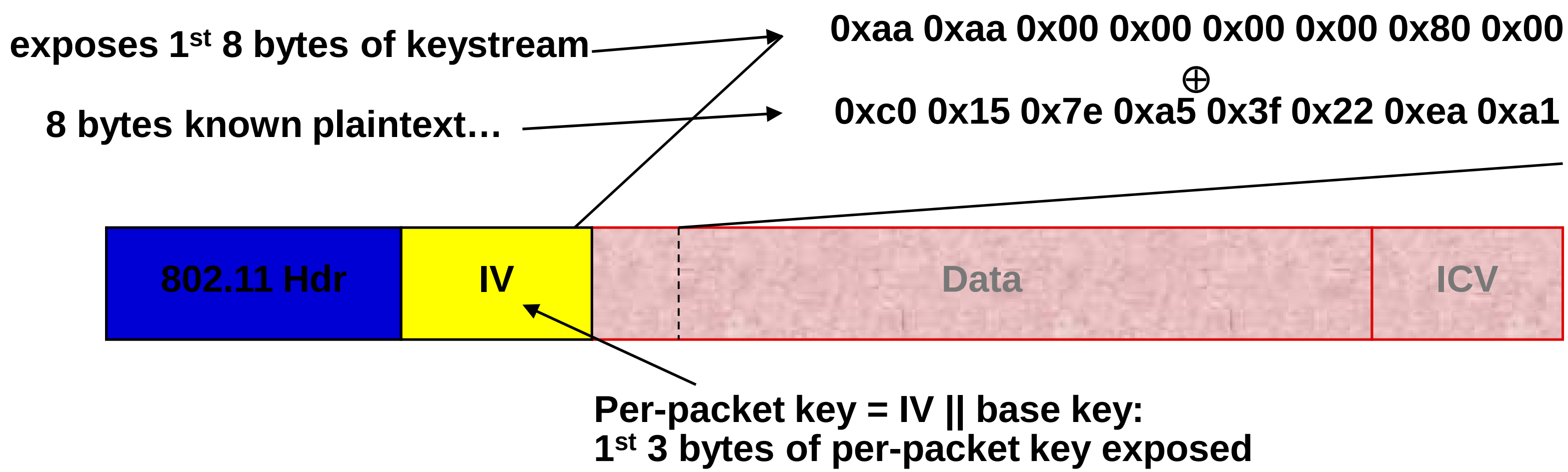


- WEP expands each RC4 key into 2^{24} per-packet keys ⇒ data can be recovered if IV is ever repeated with same key ⇒ RC4 key must be changed at least every 2^{24} packets or data is exposed through IV collisions!

Some implemented IV selection strategies:

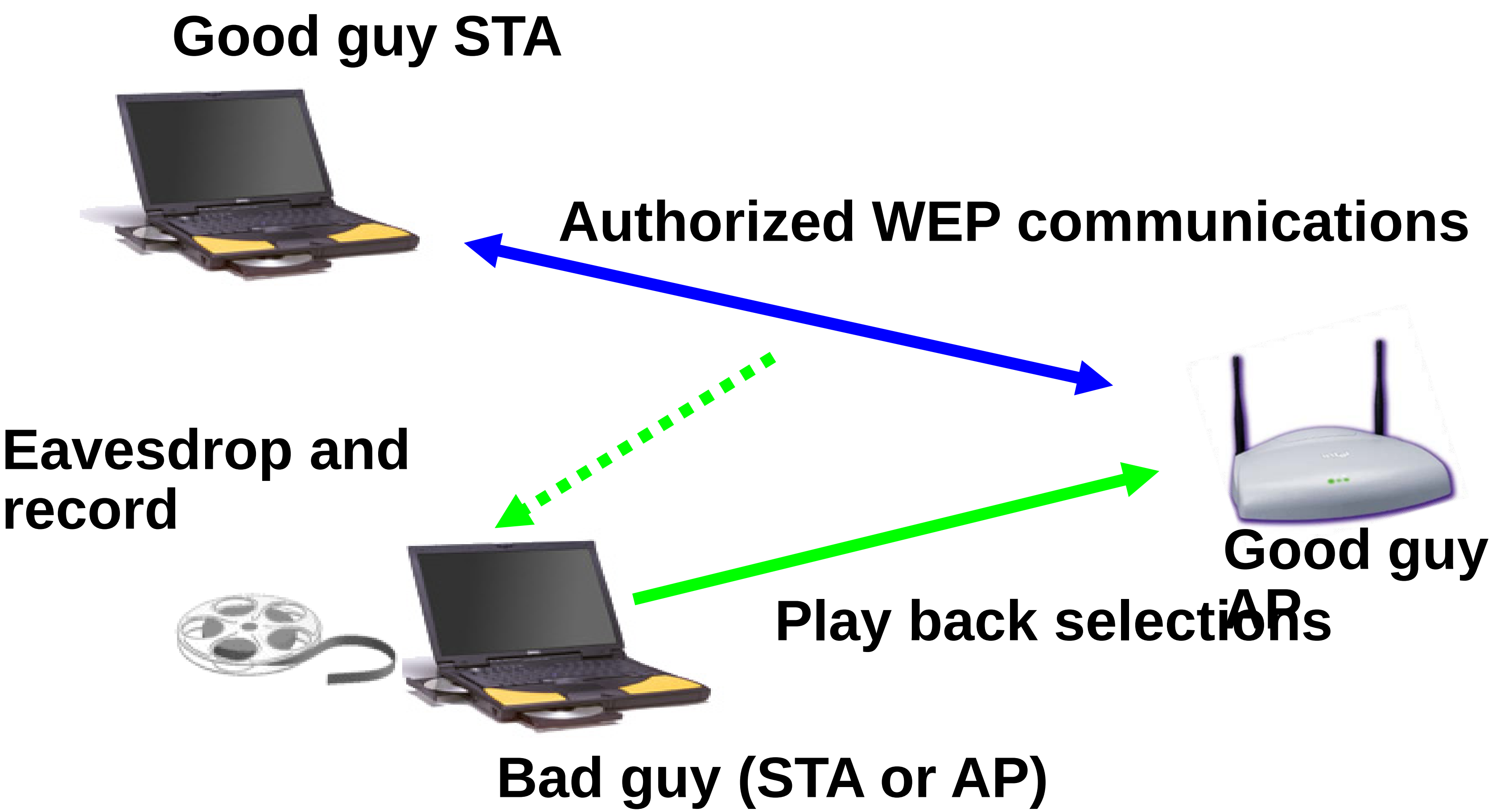
- Random: Collision probability P_n two packets will share same IV after n packets is $P_2 = 1/2^{24}$ for $n = 2$ and $P_n = P_{n-1}+(n-1)(1-P_{n-1})/2^{24}$ for $n > 2$.
  - ❑ 50% chance of a collision exists already after only 4823 packets!!!
- Increment from 0: Collision probability = 100% after *two* devices transmit

Weak key attacks



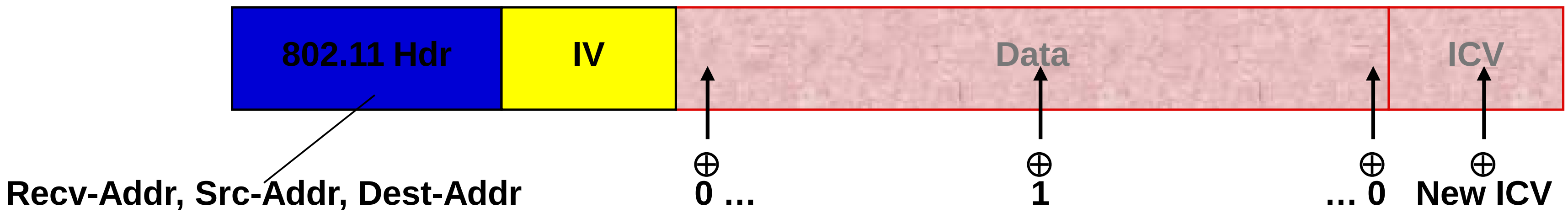
- **Class of RC4 *weak keys* exists where patterns in the 1st 3 bytes of key causes corresponding patterns in 1st few bytes of the generated RC4 key stream.**
- **For each packet, use IV and exposed key stream to identify potential weak keys**
- **Iterate over potential weak keys from a sequence of packets until the RC4 base key is found**

Replay attacks



10

Forgery attacks



- **Sample Attack 1:**
  - ❑ **Recv-Addr, Src-Addr, Dest-Addr are all unprotected**
  - ❑ **On packets from a STA to the AP, corrupt the Dest-Addr**
  - ❑ **The AP will decrypt data and send it to the forged destination**

- **Sample Attack 2:**
  - ❑ **create a blank message with same number of data bytes**
  - ❑ **Flip some bits and compute the ICV**
  - ❑ **XOR resulting bit-flipped message + ICV into captured message**

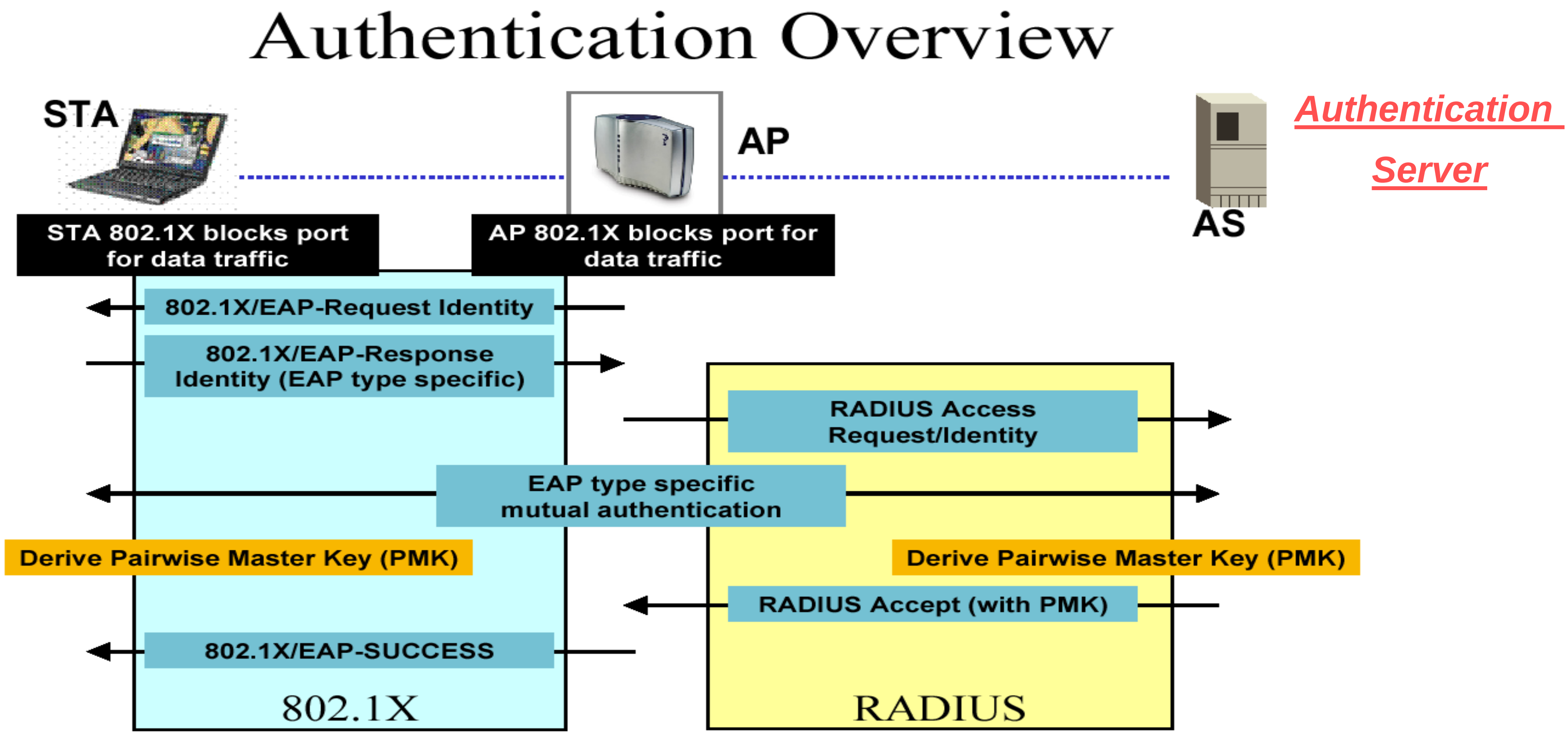
What Can IEEE 802.11i Do?

- Provide security through WEP (wired equivalent privacy)
  - Original Key size was too small (40 bit)
  - Heavy Reuse of keys
  - No Key Management within protocol
  - Not Effective Authentication protocol

- Main areas of improvement in IEEE 802.11i are -
  - Authentication
  - Key management
  - Data transfer

- Implemented in WPA and WPA2 (Wi-Fi Protected Access)

802.11i Authentication -1



802.11i Authentication -2

- **Authentication**
  - **Mutual authentication**
  - **The AS and station derive a Master Key (MK)**
  - **A Pairwise Master Key (PMK) is derived from MK**
  - **The AS distributed PMK to the AP**
  - **In PSK authentication, the authentication phase is skipped**
    - **PMK = PSK**
- **Key management and establishment**
  - **PMK is sent to AP by AS**
  - **Key management is performed between AP and the peer – four-way handshake**
    - **The four-way handshake can also be used for mutual authentication between AP and the peer in PSK mode**
  - **A set of keys are derived from PMK to protect group key exchange and data**
  - **Group key exchange allows AP to distribute group key (for multicast) to the peer**

802.11i Encryption

Summary

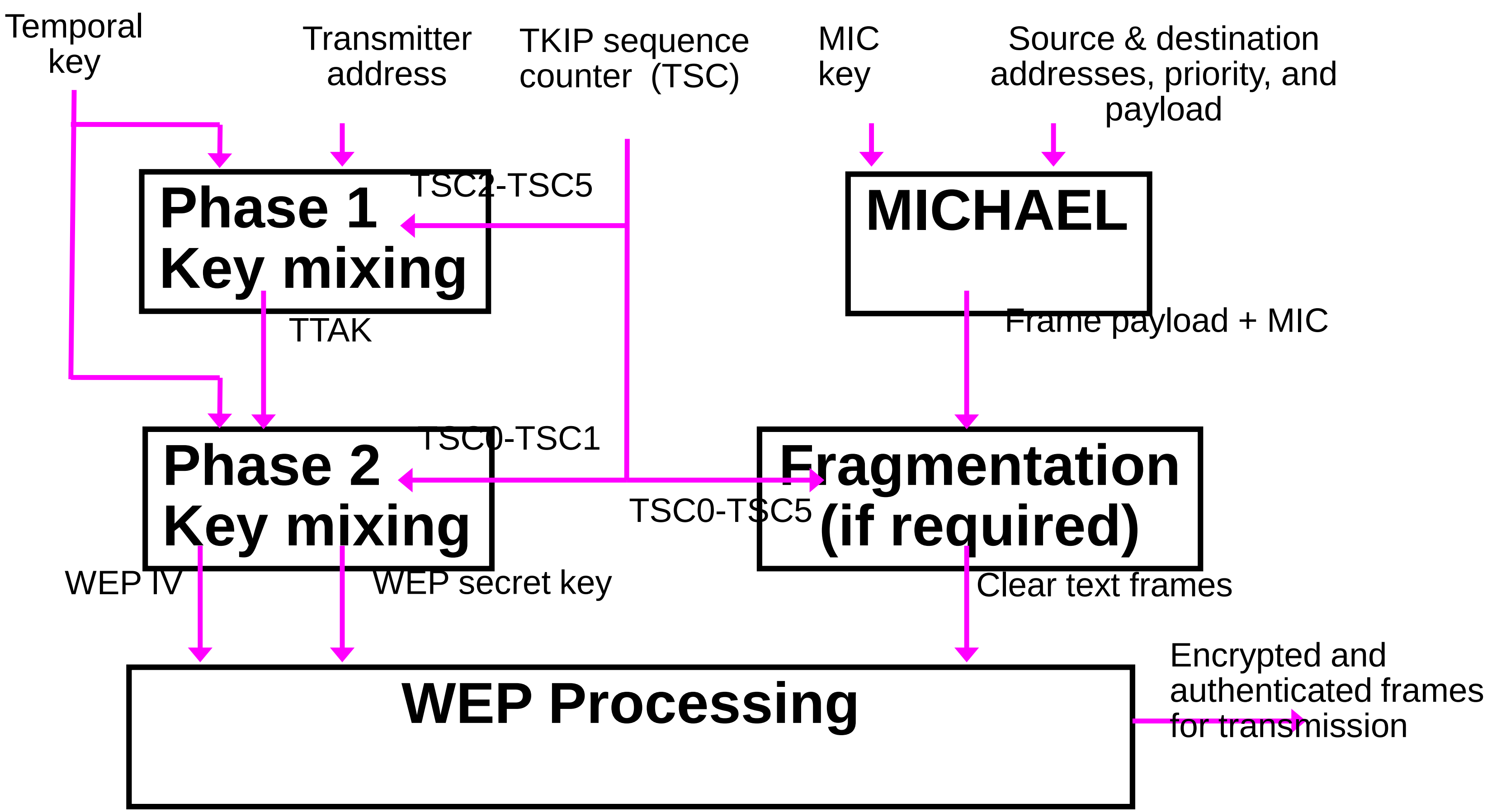
	WEP	TKIP	CCMP
Cipher	RC4	RC4	AES
Key Size	40 or 104 bits	128 bits encryption, 64 bit auth	128 bits
Key Life	24-bit IV, wrap	48-bit IV	48-bit IV
Packet Key	Concat.	Mixing Fnc	Not Needed
Integrity			
Data	CRC-32	Michael	CCM
Header	None	Michael	CCM
Replay	None	Use IV	Use IV
Key Mgmt.	None	EAP-based	EAP-based

Temporal Key Integrity Protocol (TKIP) - 1

- Optional IEEE802.11i protocol for data confidentiality and integrity
  - TKIP is designed explicitly for implementation on WEP legacy hardware
- TKIP three new features:
  - A cryptographic message integrity code (MIC)
  - A new IV sequencing discipline
    - » The transmitter increments the sequence number with each packet it sends
  - A per-packet key mixing function

Temporal Key Integrity Protocol (TKIP) - 2

- **TKIP frame processing**



17

Temporal Key Integrity Protocol (TKIP) - 3

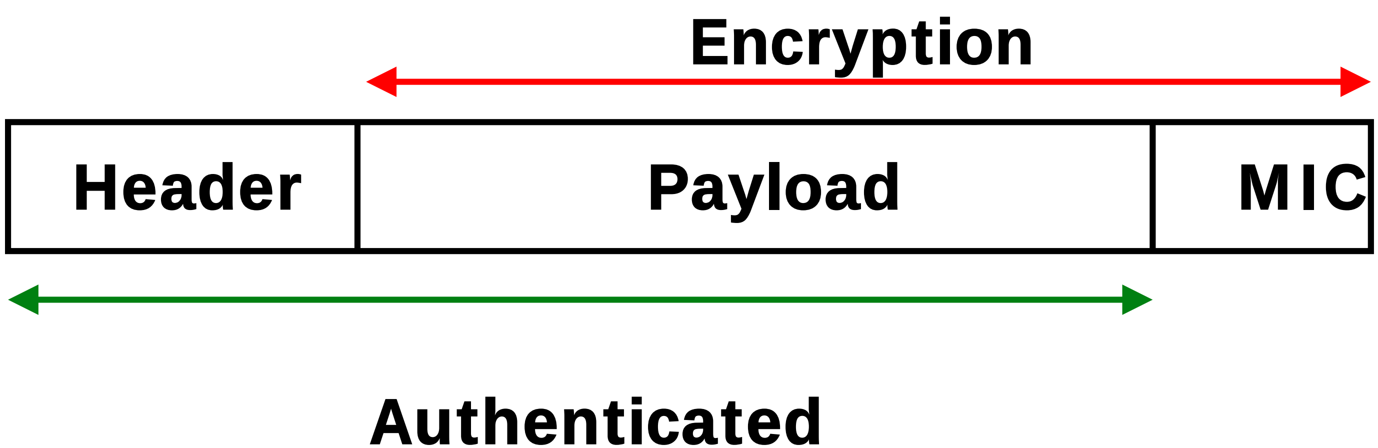
- **Defeating weak key attacks: key mixing**
  - **Transforms a temporal key and packet sequence number into a per packet key and IV**
  - **The key mixing function operates in two phases**
    - » **Phase 1: Different keys used by different links**
      - **Phase 1 needs to be recomputed only once every 2^{16} frames**
    - » **Phase 2: Different WEP key and IV per packet**
  - **Phases 1 and 2 can be pre-computed**

Temporal Key Integrity Protocol (TKIP) - 4

- **Defeating replays: IV sequence enforcement**
  - TKIP uses the IV field as a packet sequence number
  - The transmitter increments the sequence number with each packet it send
  - A packet will be discarded if it arrives out of order
    - » A packet is out-of-order if its IV is the same or smaller than a previous correctly received packet
- **Defeating forgeries: New MIC (Michael)**
  - MIC key is 64-bits
    - » security level of 20 bits

Counter Mode with CBC-MAC (CCMP) - 1

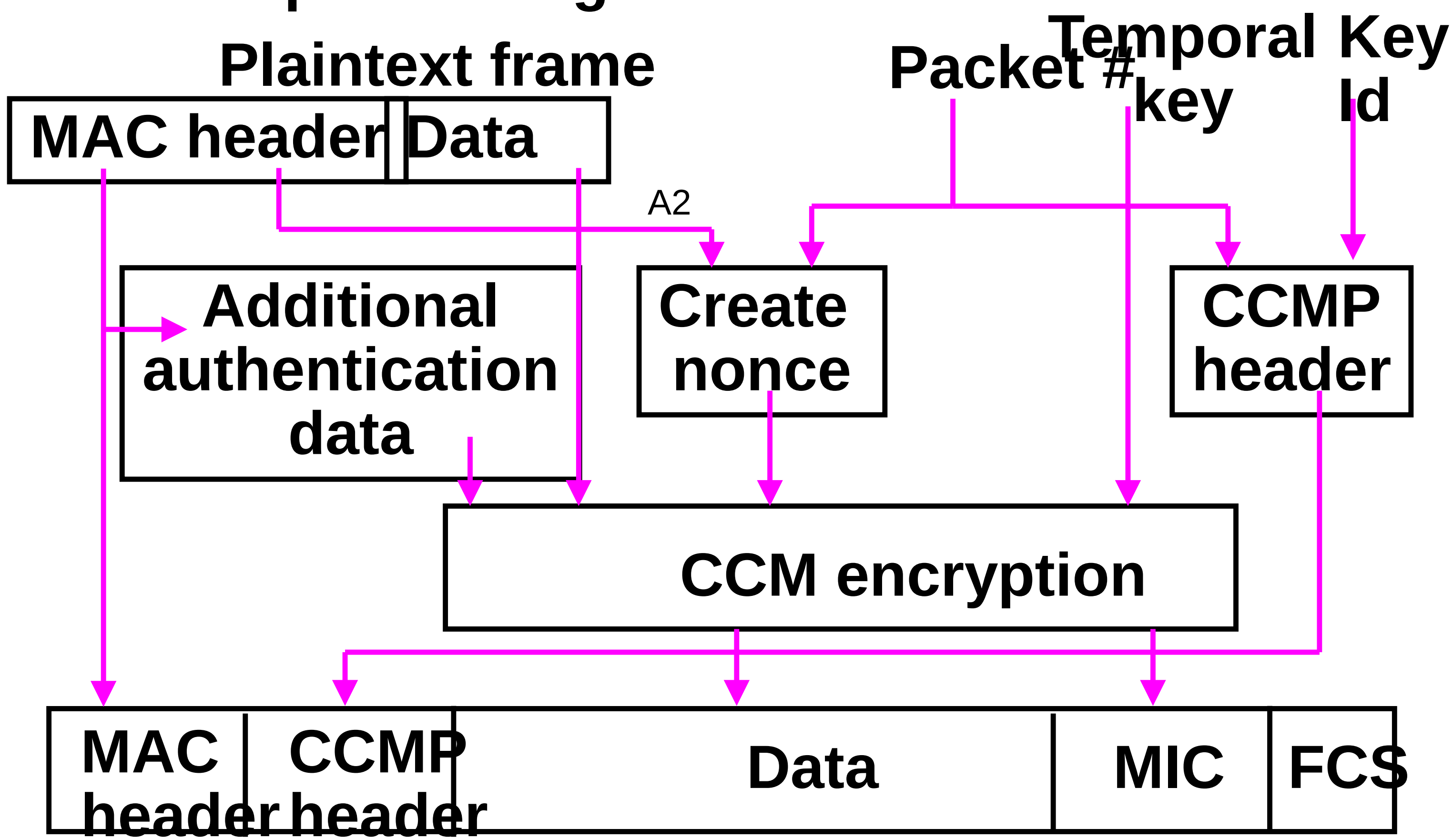
- **Both encryption and MIC use AES**
  - Uses counter Mode (CTR) to encrypt the payload and MIC
  - Uses CBC-MAC to compute a MIC on the plaintext header and the payload
  - Both encryption and authentication use the same key



 CBC-MAC (Cipher Block Chaining Message Authentication Code)

Counter Mode with CBC-MAC (CCMP) - 2

- CCMP data processing



Counter Mode with CBC-MAC (CCMP) - 3

– Each message block has the size of 16 octets

» For CTR encryption, A_i has the following format (i is the value of the counter field):

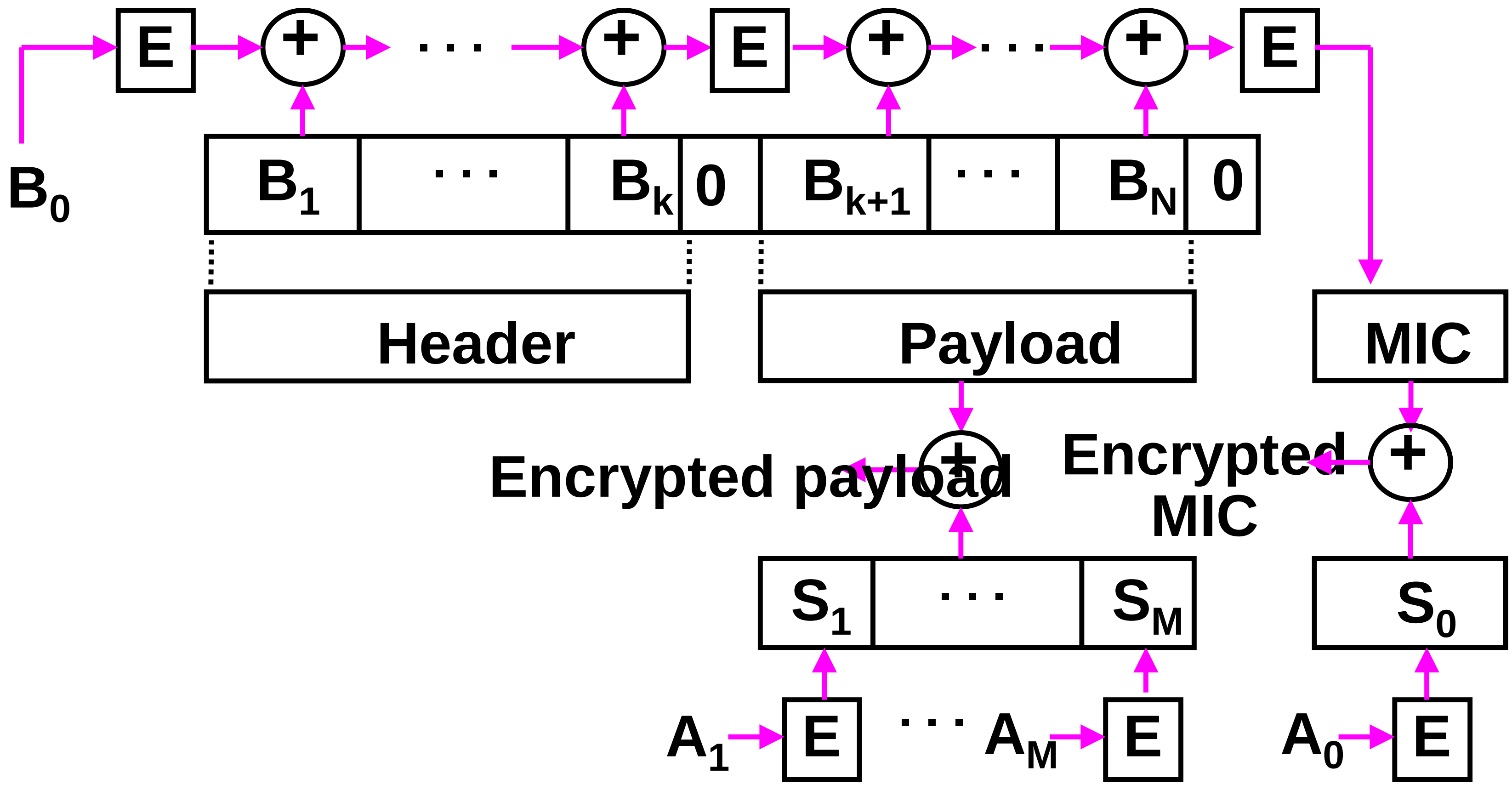
1	13	2
Flags	Nonce	Counter

» For the CBC-MAC authentication, B_0 has the following format (length := size of the payload):

1	13	2
Flags	Nonce	length

Counter Mode with CBC-MAC (CCMP) - 4

- CCM encryption



Whats New in WPA

- **Authentication**
  - Use TKIP (Temporal Key Integrity Protocol), to dynamically change keys
  - Can also be used in a less secure PSK (pre-shared key) mode
- **Encryption**
  - Use RC4 with large key size (128 bit) and IV (48 bit)
  - Defeats the well-known key recovery attacks on WEP
- **Data Integrity**
  - More secure MIC (Message Integrity Code) named "Michael" is used
  - Includes a frame counter, which prevents replay attacks
- **Extra Countermeasures**
  - Special mechanism detects an attempt to break TKIP and temporarily blocks communications with the attacker

Features in WPA2

- Authentication & Integrity
  - Key management and message integrity is handled by a single component built around AES
  - Using a CBC-MAC (Cipher Block Chaining Message Authentication Code)
- Encryption
  - Uses CTR (Counter mode) AES (128 bit)
  - Computationally expensive and adds a significant amount of overhead
- Summary
  - Implements the mandatory elements of 802.11i
  - Use CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) instead of TKIP

802.11i – Potential Weaknesses

- **Hardware requirements**
  - **Hardware upgrade needed for AES support**
    - » **Strength of TKIP and Wrap questionable in the long term**
  - **Authentication server needed for 2-way authentication**
- **Complexity**
  - **The more complex a system is, the more likely it may contain an undetected backdoor. e.g. WPS – turn it off!**
- **Patchwork nature of “fixing” 802.11b**

- **Attacking programms are available on the internet!**

Further Security over WLAN

- **Often you want to connect to a wireless LAN over which you have no control**
- **Options:**
  - **If you can, connect securely (WPA/WAP2, MAC address filtering, etc.)**
  - **If unsecured, connect to your secure systems securely:**
    - » **VPN – Virtual Private Network**
    - » **SSL connections to secure systems**
  - **Be careful not to expose passwords**
  - **Watch for direct attacks on untrusted networks**

Class Quiz

- What are the weak points in convetional WLAN security?
- What is WPA?
- What is WPA2?