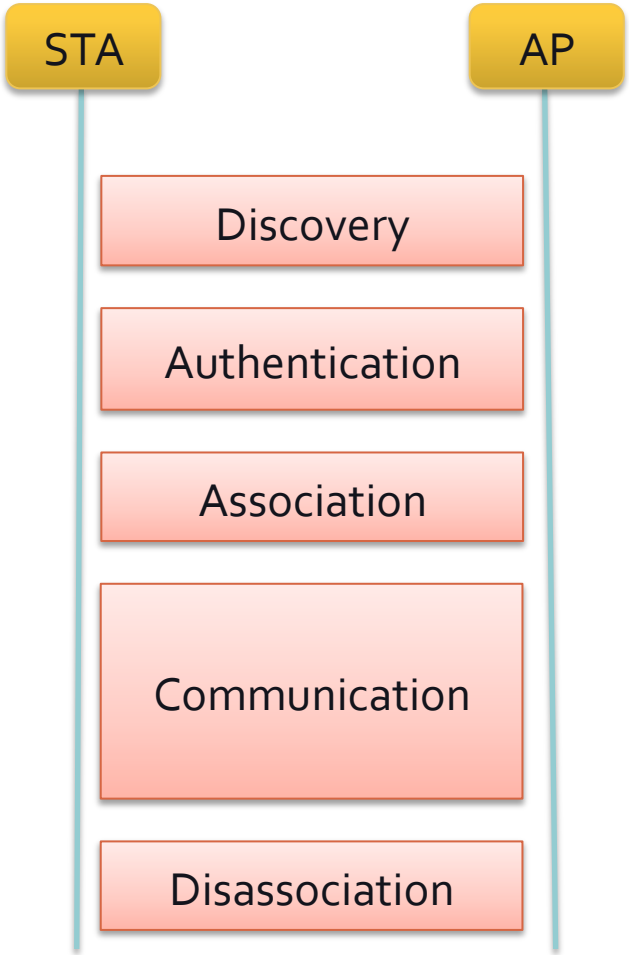
WLAN Security

Joining & Leaving a WLAN

- Discover a WLAN
  - Find an AP with preferred SSID and strong signal
- Authentication
  - Get permission to connect to the WLAN
- Association
  - Join the WLAN
- Disassociation
  - Leave the WLAN



WLAN Discovery (1)

- Beacon
  - Each AP periodically broadcasts a Beacon frame
    - every MIB:aBeaconPeriod
    - on its channel
  - Containing synchronization information
    - AP's clock
    - Parameters for the coordination function
  - IBSS: every STA beacons

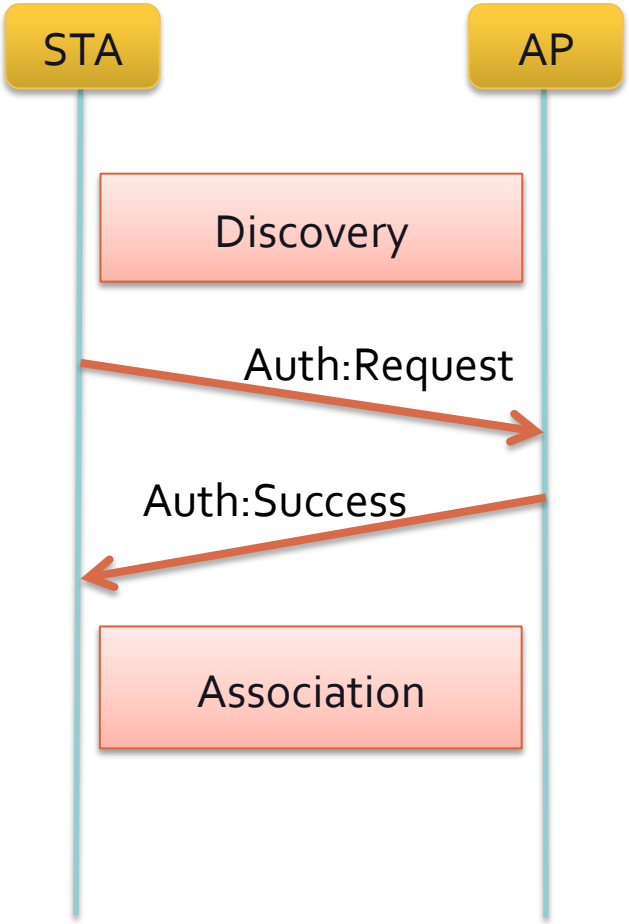
WLAN Discovery (2)

- How an STA finds an AP?
- Passive Scan
  - Collect beacons from all the channels, staying in each channel for MIB:ChannelTime seconds
- Active Scan
  - STA sends a *Probe Request* frame, containing desired SSID
  - AP with the same SSID returns a *Probe Response* frame
  - IBBS: The STA that sent the last Beacon replies
- AP choice
  - STA chooses an AP with the best signal quality

Authentication

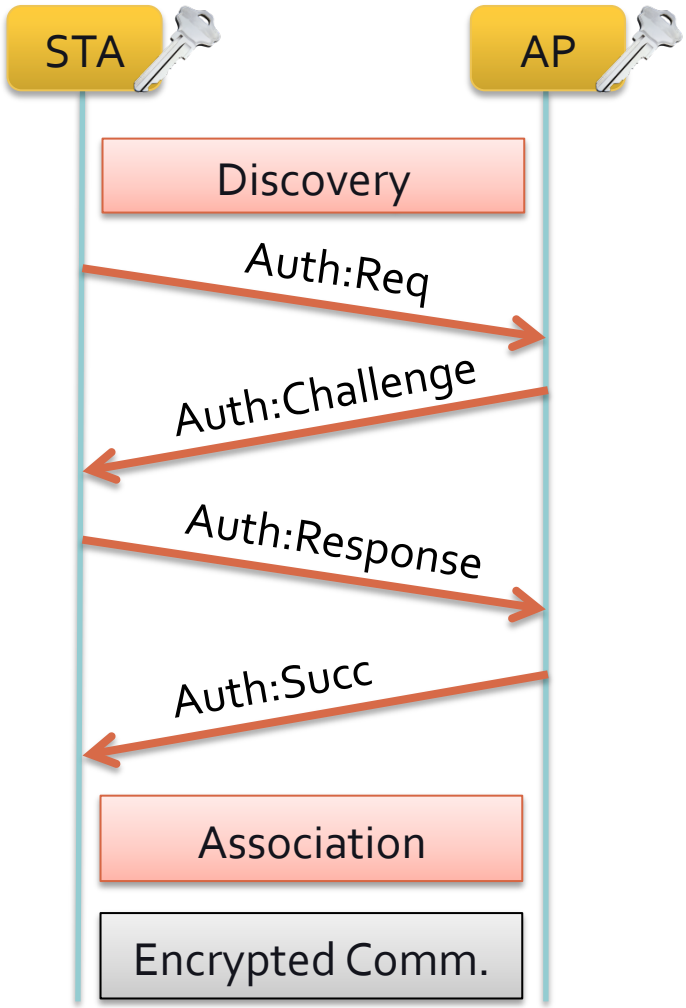
- Open System Authentication
  - Any STA can access the WLAN
- Shared Key Authentication
  - Only STAs that knows the same key with the AP can access the WLAN
  - WEP (Wired Equivalent Privacy)

Open Authentication



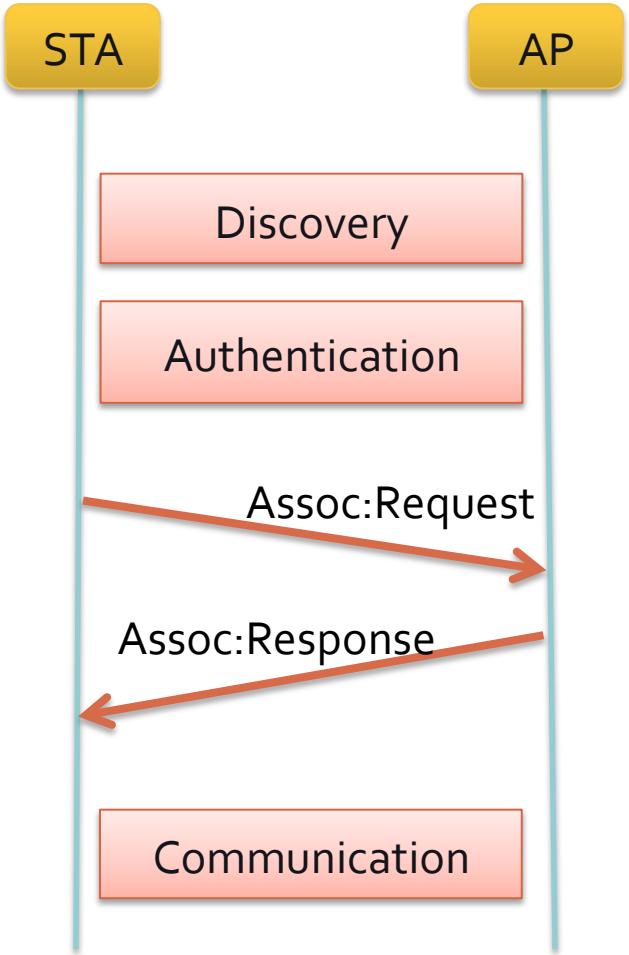
Shared Key Authentication

- WEP
  - STA and AP shares a key
  - STA proves its knowledge by a challenge/ response protocol
  - Auth:Challenge contains a challenge text
  - Auth:Response contains the encryption of the challenge text (128 bits)
  - Authentication is successful if the encryption is correct
  - Subsequent data packets are encrypted



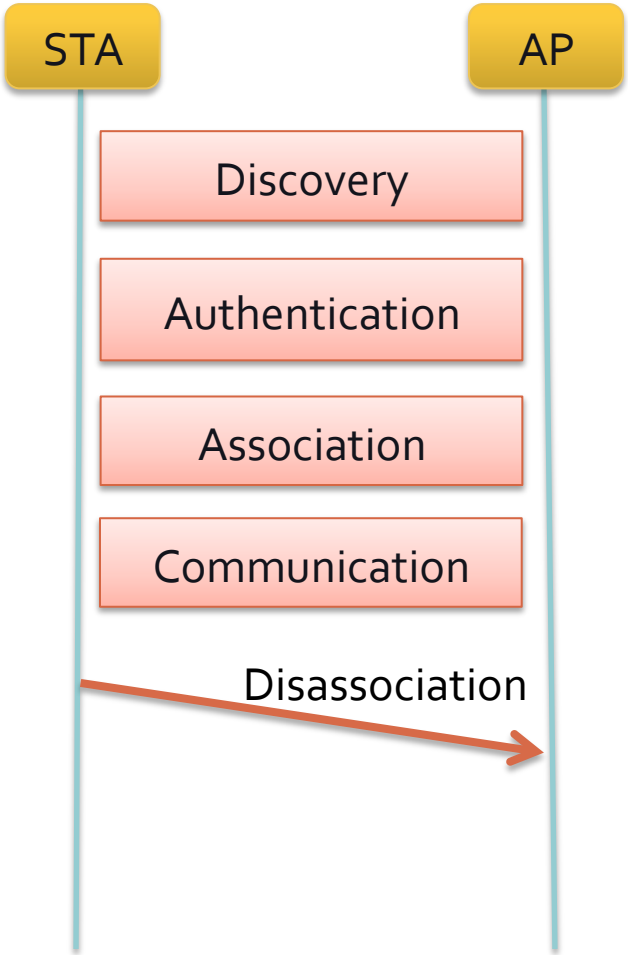
Association

- STA registers itself to the AP so that AP knows the presence of the STA, and handles packets from/to the STA
- Association Request
  - STA's capabilities: supported data rates, WEP support, PHY options, power saving mode
- Association Response
  - Accept/Reject: based on capability, load balancing, security,…
  - Association ID, Supported data rate



Disassociation

- STA notifies the AP of its leaving
- AP notifies the STA of disconnecting
- Reason Code:
  - No reason
  - Authentication invalid
  - Leaving
  - Inactivity
  - Load balancing
  - etc…



WLAN frames

- Frame format
  - http://wifi.cs.st-andrews.ac.uk/animations/wifi%20oframe.swf
- Wireless Sniffing
  - Wireshark

Security of 802.11

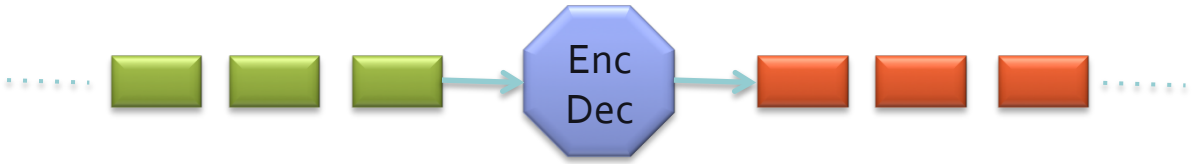
- WEP in 802.11 (1997/1999)
- Weakness of WEP is widely recognized
- WPA by WiFi
- WPA2 by IEEE (802.11i)

WEP (Wired Equivalent Privacy)

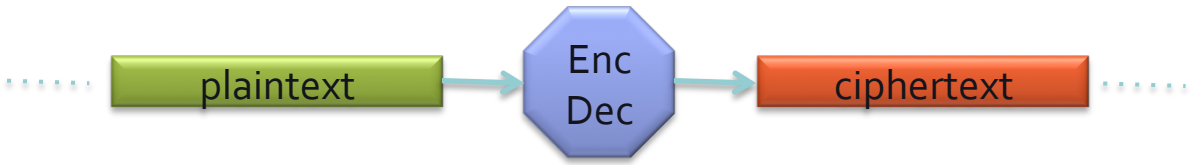
- Goals
  - Authentication: Prove the identity of the user
  - Confidentiality: Nobody can learn the content of packets
  - Integrity: Nobody can modify or forge a packet without detection
  - Efficient
- Building Blocks
  - RC4 / IV
  - Shared Secret Keys
  - Integrity Check Value (ICV)

Types of Ciphers

- Block cipher
  - Encrypt messages by blocks



  - DES, AES, …
- Stream cipher
  - Encrypt messages as a stream



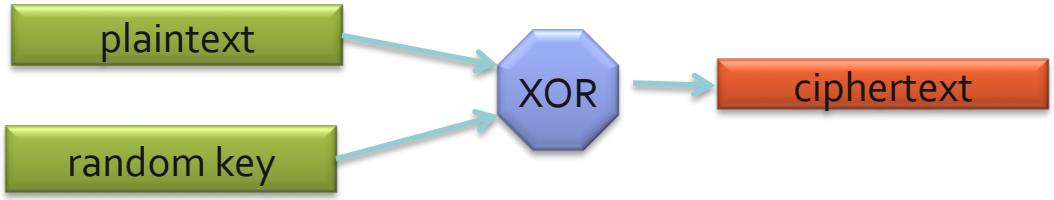
  - RC4

RC4

- Used by WEP
- Developed by Ron Rivest (Rivest Cipher 4)
- Symmetric algorithm
  - Use the same key for both encryption and decryption
- Encryption/Decryption is the same procedure
- Advantages
  - Efficient
  - Easy to implement

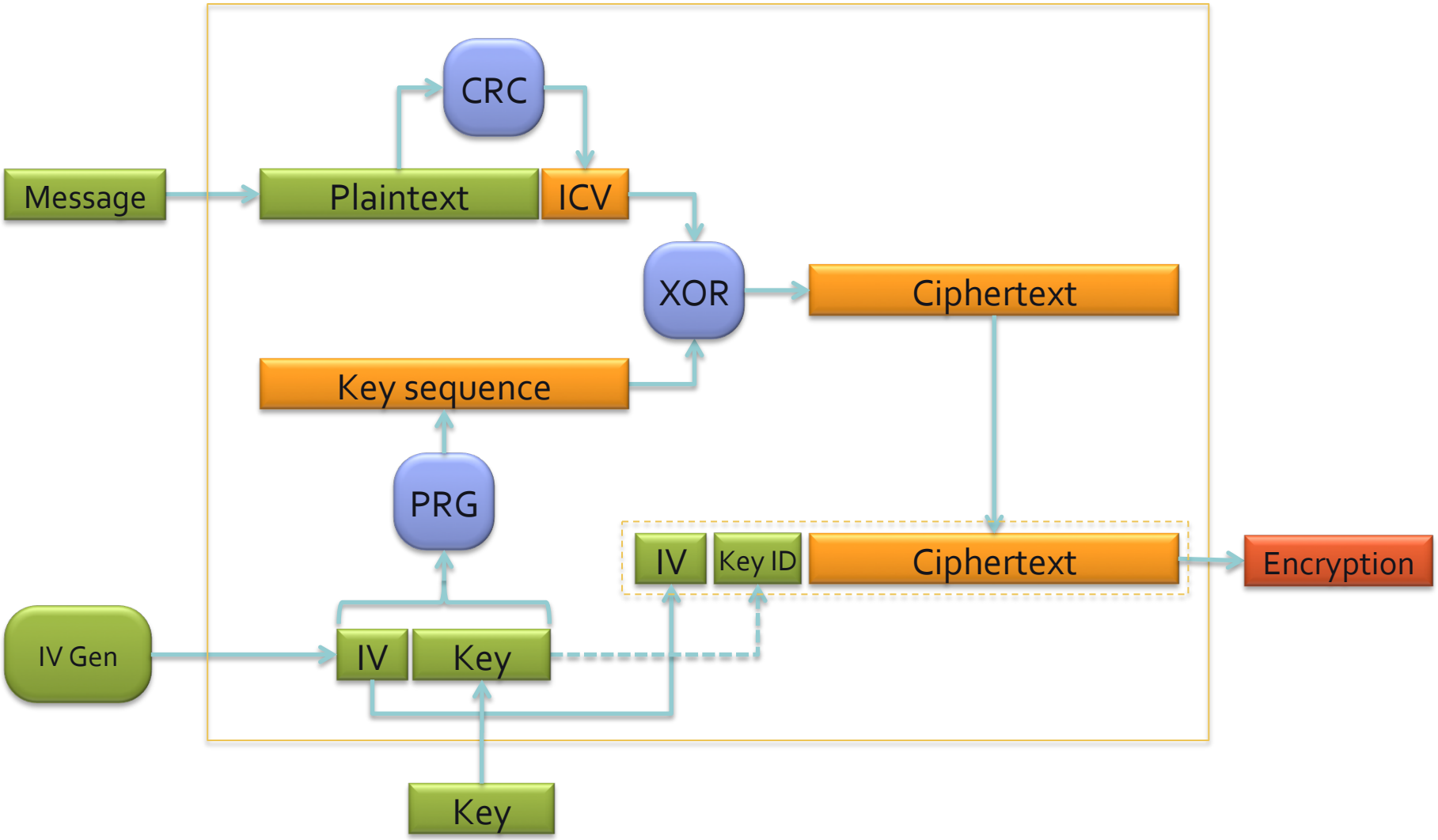
One-time Pad (OTP)

- Encryption algorithm
- Theoretically proven to provide perfect secrecy (Shannon)
  - *As far as the key is truly random and used only once, ever*
- Soviet Union used OTP, but in a wrong way
- RC4 simulates One-time Pad algorithm



Enc/Dec of WEP

Enc/Dec of WEP



WEP: Authentication

- Authentication
  - AP picks a random challenge text: $\boldsymbol{C}$
  - STA encrypts it: $\boldsymbol{R} = Enc(\boldsymbol{C})$
  - AP checks if: $\boldsymbol{C} == Dec(\boldsymbol{R})$
- Only STA that has the right key can encrypt correctly, So authentication works!??

WEP: Integrity

- Integrity
  - Computes CRC of the plaintext: $ICV = CRC(P)$
  - Send $C = Enc(P, ICV)$
  - Receiver Checks if ICV of C equals to $CRC(P)$
- Since P and ICV are encrypted, nobody can change P without breaking P-ICV match!??

WEP: Confidentiality

- Confidentiality
  - Every packet is encrypted using a secret key
    - send *{IV, KeyID, Enc(P, ICV)}*
- IV changes in every packet, so key stream (derived from IV and key, albeit pseudo-random) changes in every packet, so by Shannon, the encryption is perfectly safe!

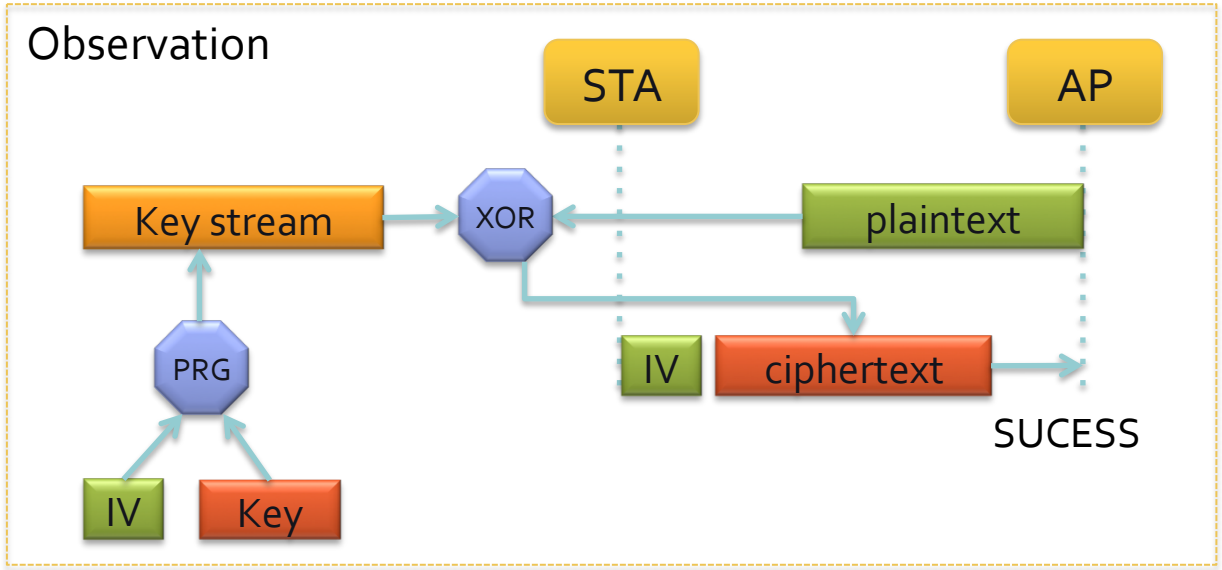
WEP is not secure

- WEP fails to provide
  - Authentication
  - Message Modification Detection
  - Message Privacy
  - Key Protection
- Resolution
  - IEEE working group launched (802.11i)
  - Wi-Fi proposed WPA (TKIP)
  - IEEE proposed WPA2

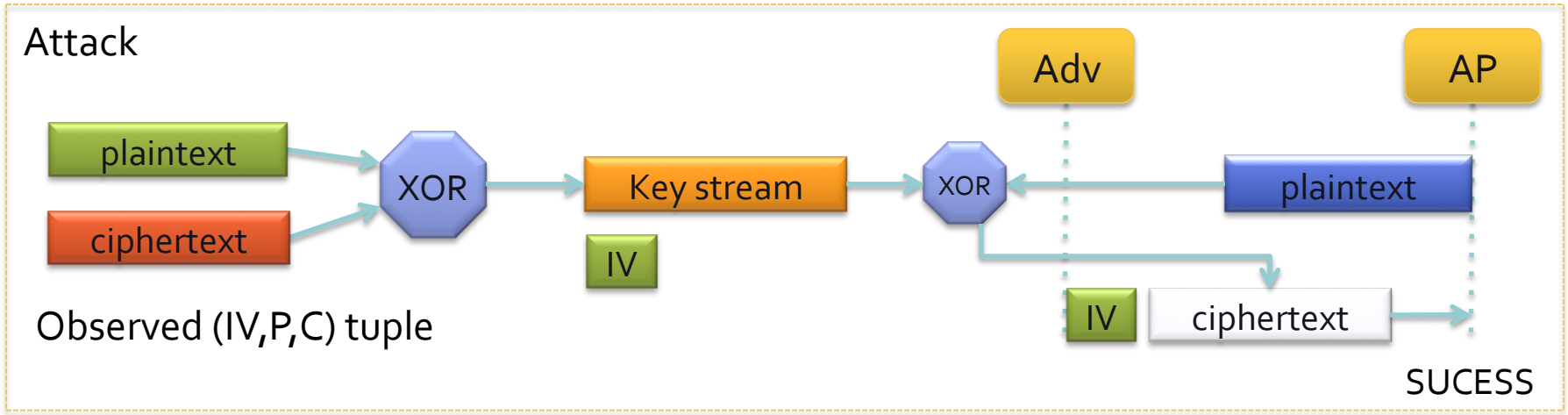
What's wrong: Authentication

- Mutual Authentication: STA does not authenticate AP
- Use the same key for authentication and data encryption?
  - During authentication, we reveal plaintext-ciphertext pairs!

Attack on Authentication



$$\begin{aligned} A \oplus A &= 0 \\ A \oplus 0 &= A \\ A \oplus B \oplus B &= A \end{aligned}$$

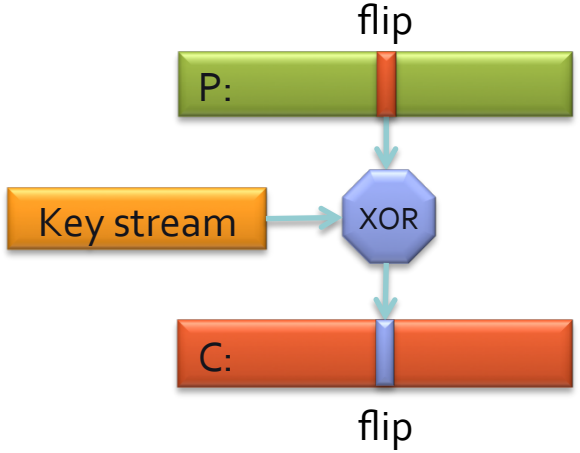


What's wrong: Integrity

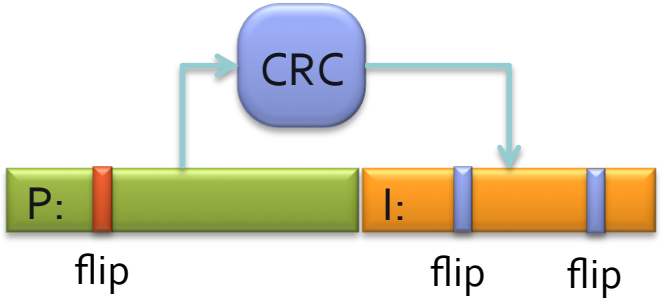
- Attacker shouldn't be able to change a bit in the message without being detected
- But the attacker can flip a bit in the message and fix the ICV (by flipping some bits in it) so that ICV is still correct

Background

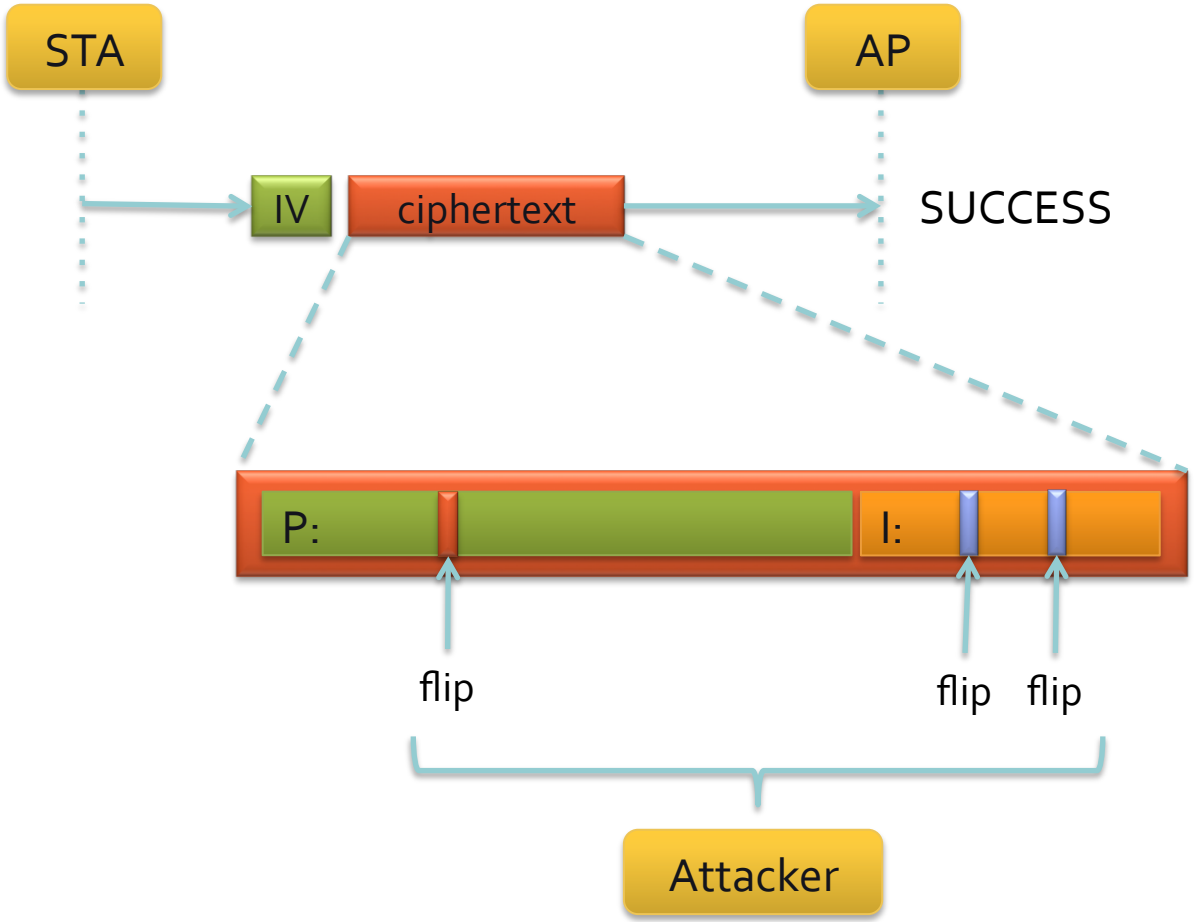
- In RC4, if a bit is flipped in plaintext, the corresponding bit in ciphertext is also flipped, and no other bits are changed



- With CRC, you can compute which bits will be flipped when you flip a bit in the plaintext



Attack on Integrity



What's wrong: Confidentiality

- The attacker can either get the plaintext or get the key
- WEP fails on
  - IV reuse
  - RC_4 weak keys
  - Direct key attack

IV reuse

- IV has 24 bits (=8 million)
  - Random IV: very frequently same IV appears (birthday paradox)
  - Sequential IV:
    - 7 hours to see the same IV for a STA, divided by the number of STAs
    - IV starts with zero after booting??
- Reappearing IV helps the attacker to decrypt the messages if (IV, keystream) is known (see Authentication attack)
- For C1, C2 for the same IV,
  - C1 (+) C2 = P1 (+) K1 (+) P2 (+) K2 = P1 (+) P2
  - This can be used to learn plaintext from known-plaintext

Birthday Paradox

- Prob. of two people having the same B/D
  - 1/365
- Prob of any two people among 3 people having same BD
  - = 1 – Prob of none have same birthday
  - = 1 - (364/365) x (363/365)
- Prob of … among 23 people having same BD
  - > 0.5

RC4's weak keys

- Fluhrer et al. (2001) showed
  - The key-stream generation algorithm is flawed
  - For certain keys, (the beginning of) key-stream is not random
  - So, from the key-stream, the attacker can guess the key

Direct Key Attacks

- Fluhrer et al. (2001) showed
  - By exploiting the weak-key problem, the attacker can learn each byte of the key over time.
  - OOPS!
  - Google "WEP key cracker"

Lessons Learned

- Don’t use WEP
- Don’t use stream cipher as a block cipher
- Security by obscurity doesn’t work

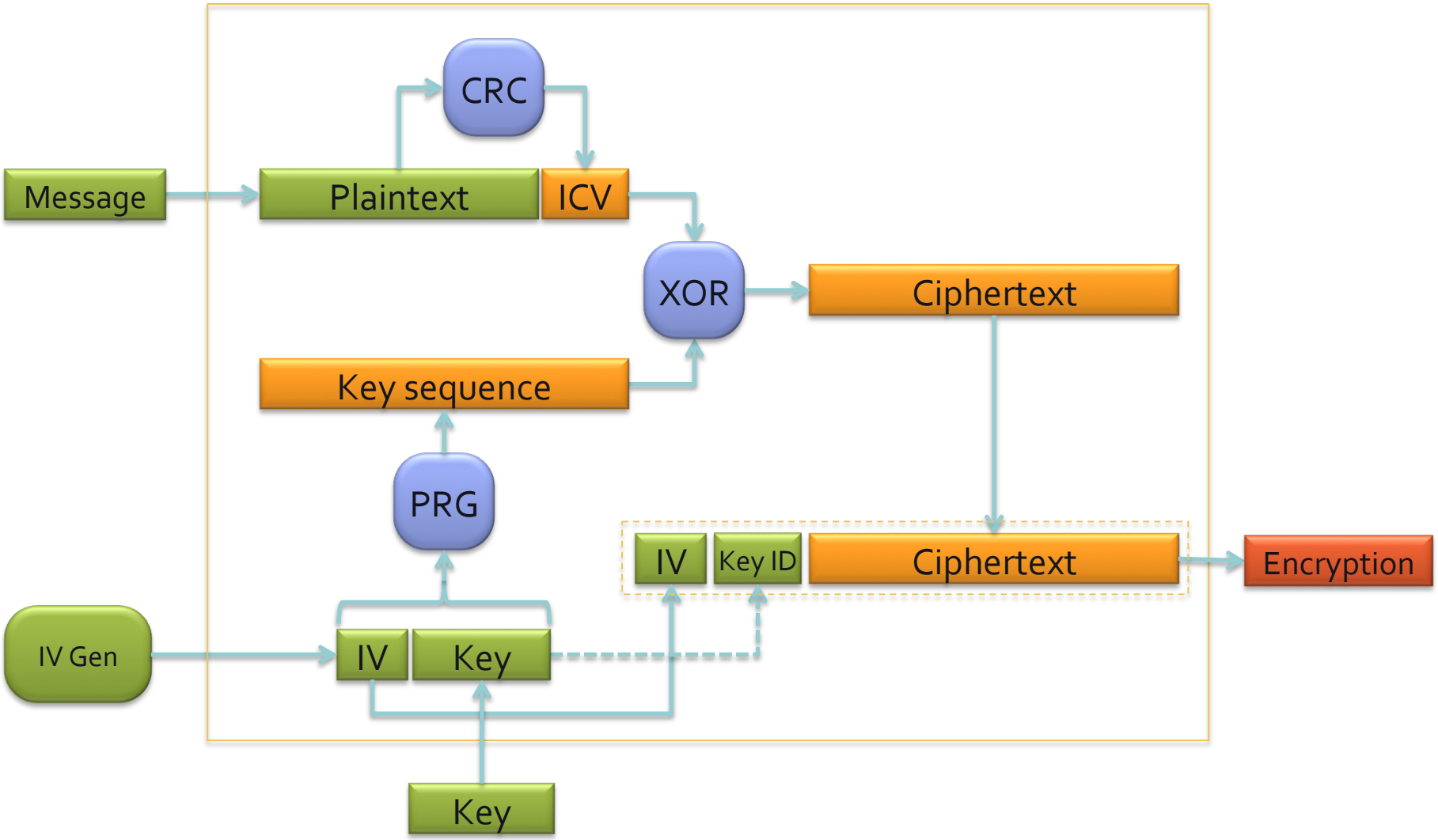
WiFi Protected Access (WPA)

- Need better security than WEP
- 802.11i was not complete
- WiFi alliance defined WPA based on incomplete 802.11i

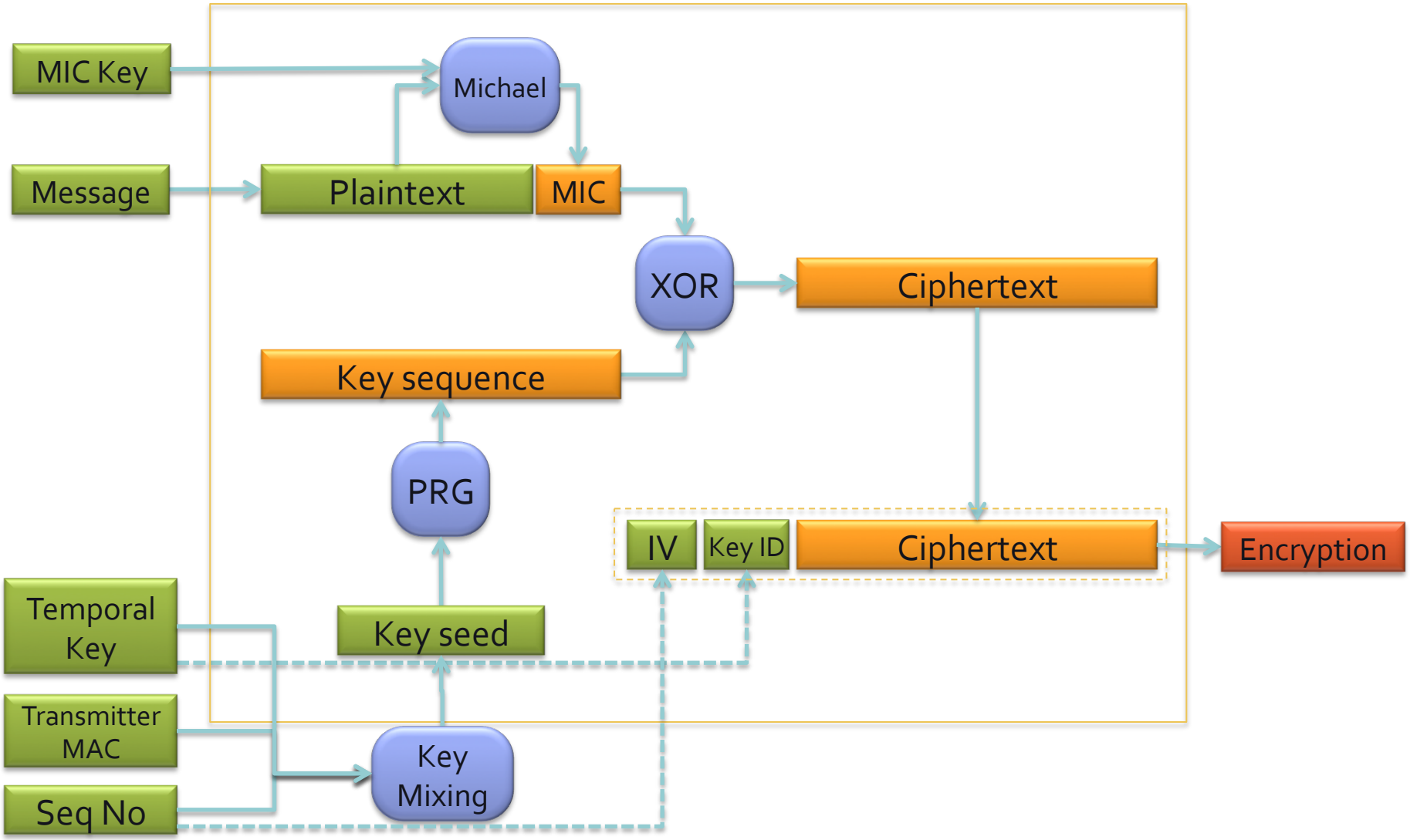
WPA Design

- Overcome WEP
- TKIP (Temporal Key Integrity Protocol)
  - RC_4 with longer IV / Key length
  - Better message integrity
- Authentication
  - WPA enterprise: 802.11x / EAP with RADIUS
  - WPA home: WPA-PSK without RADIUS

Enc/Dec of WEP



Enc/Dec of TKIP



WEP vs. WPA

	WEP	*WPA*
Encryption	Flawed, cracked by scientists and hackers	Fixes all WEP flaws
	40-bit keys	128-bit keys
	Static—same key used by everyone on the network	Dynamic session keys per user, per session, per packet keys
	Manual distribution of keys—hand typed into each device	Automatic distribution of keys
Authentication	Flawed, used WEP key itself for authentication	Strong user authentication, utilizing 802.1x and EAP