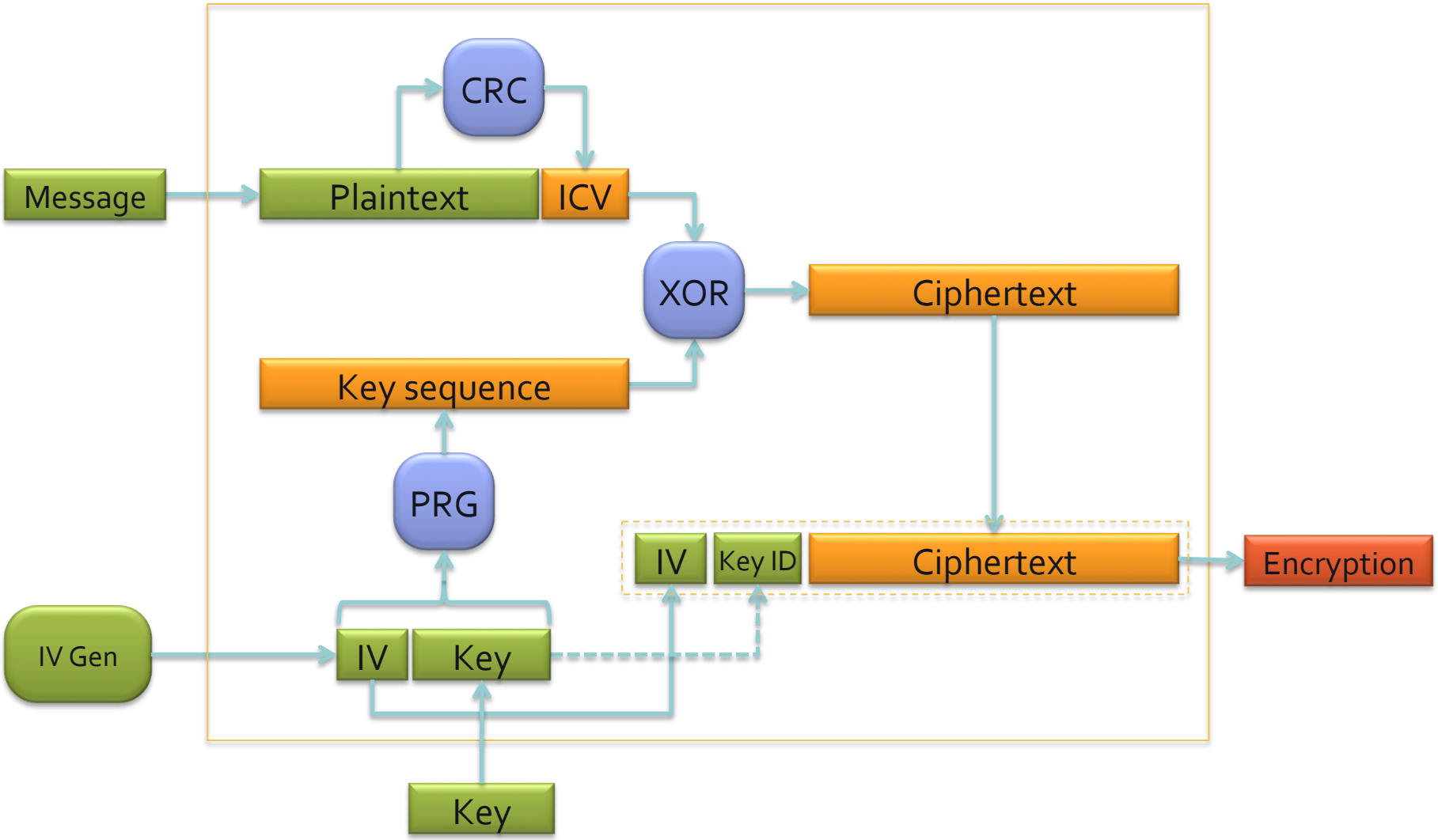
WLAN Attacks

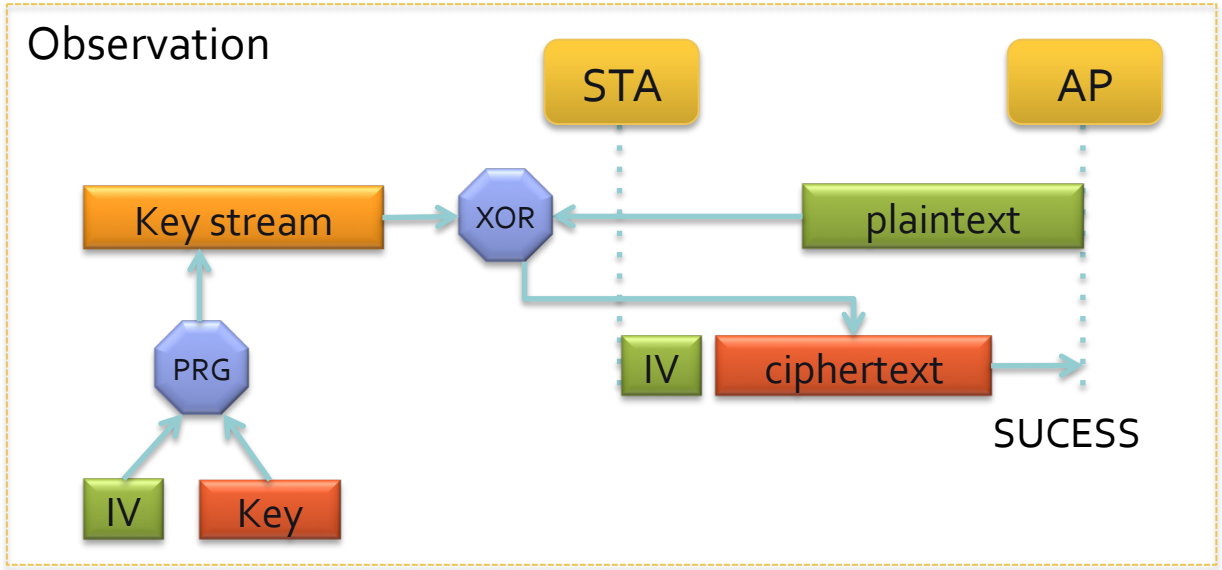
Enc/Dec of WEP



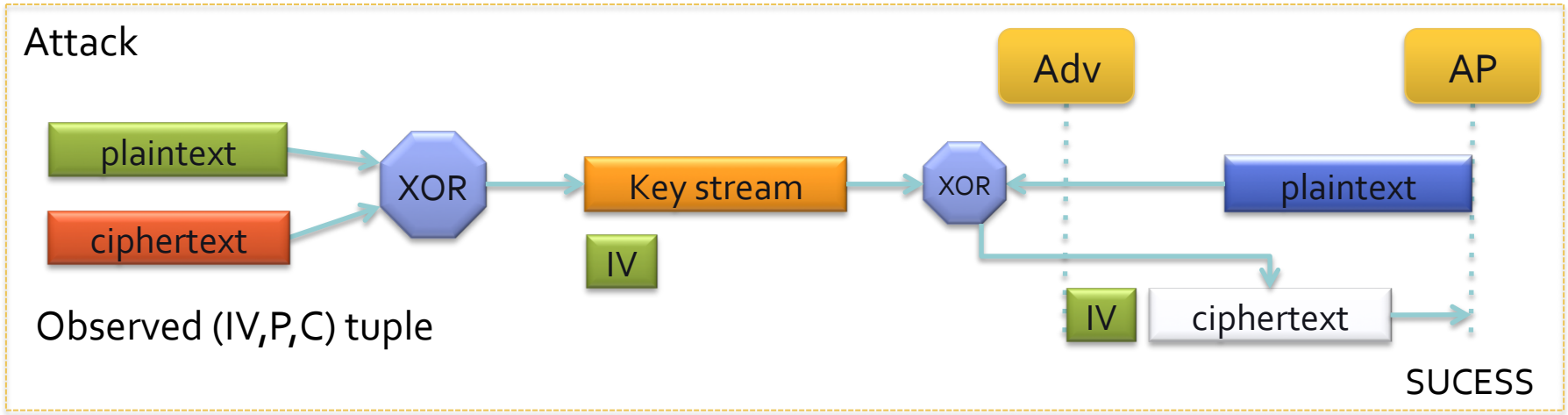
WEP is not secure

- 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

Attack on Authentication



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

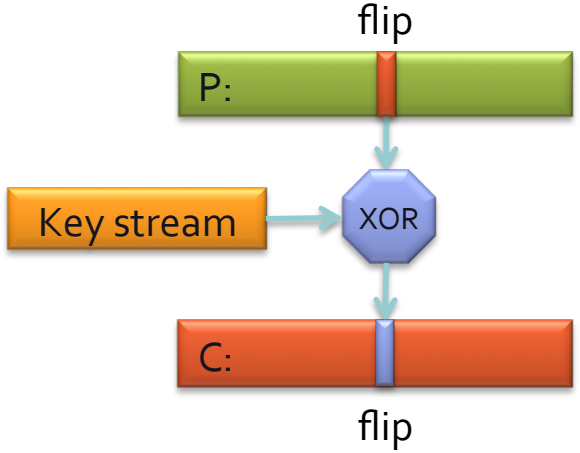


What's wrong: Integrity

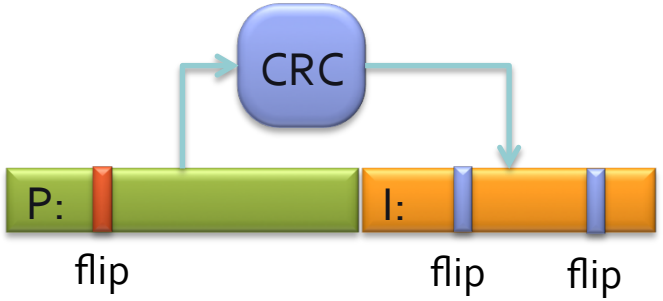
- Attacker shouldn't be able to change a bit in the message without being detected
- But the attacker can flip a bit in the message and fix the ICV (by flipping some bits in it) so that ICV is still correct

Background

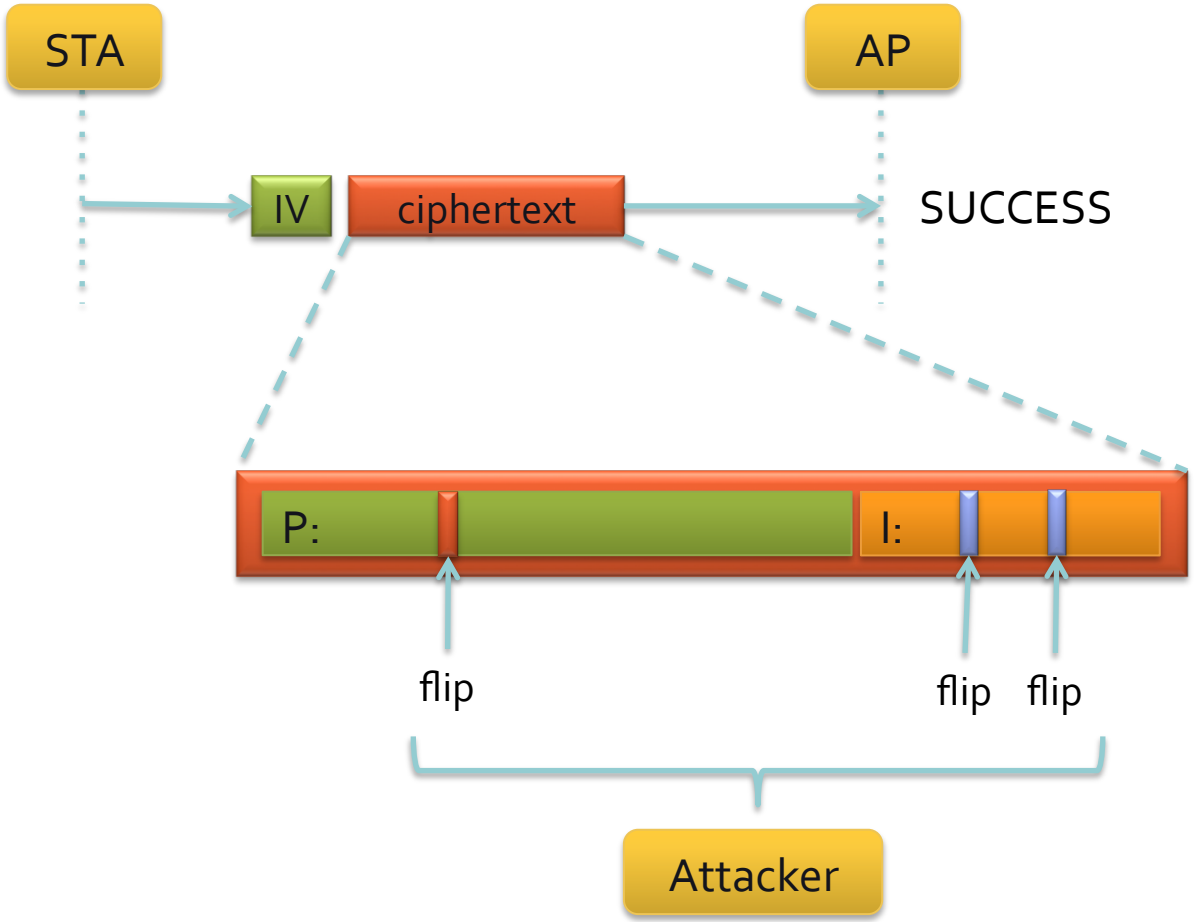
- In RC4, if a bit is flipped in plaintext, the corresponding bit in ciphertext is also flipped, and no other bits are changed



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



Attack on Integrity



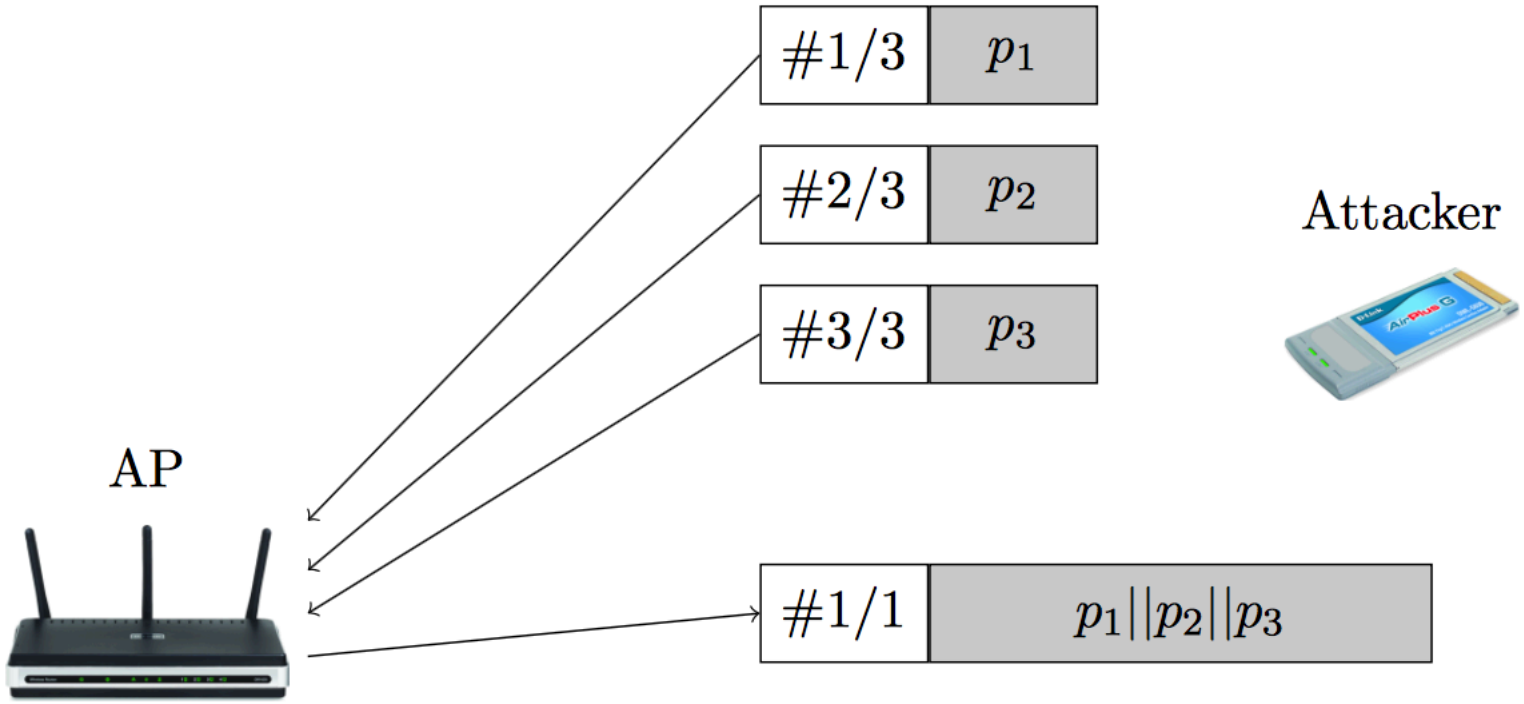
Fragmentation attack

- Attacker can inject a long legitimate message

1. Get a keystream of length m
2. make 16 packets of (m-4) plaintext and 4 CRC, all of which fragmentations of a long message of length (m-4)*16+4

3. observe AP's forward of long packet
4. Get a keystream of length (m-4)*16+4=16m-60
5. Inject a packet of size: plaintext 16m-64, CRC 4

Fragmentation attack



What's wrong: Confidentiality

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

Chopchop attack

1. Chop off the last byte of the message
2. Guess the plaintext byte
3. Compute CRC of the guessed plaintext byte
4. XOR with encrypted CRC to get new CRC
5. Send to AP and see if it accepts
6. If not accept, goto 2

Chopchop attack

Guess	New ICV	Accepted
00	ICV-1	No
01	ICV-2	No
...	...	...
CD	ICV-n	Yes!

Chopchop attack

Guess	New ICV	Accepted
00	ICV-1	No
01	ICV-2	No
...	...	...
FA	ICV-n	Yes!

FA

Chopchop attack

- Can recover the plaintext byte by byte without knowing anything about key nor keystream
- Takes long (128 guesses per byte on average)

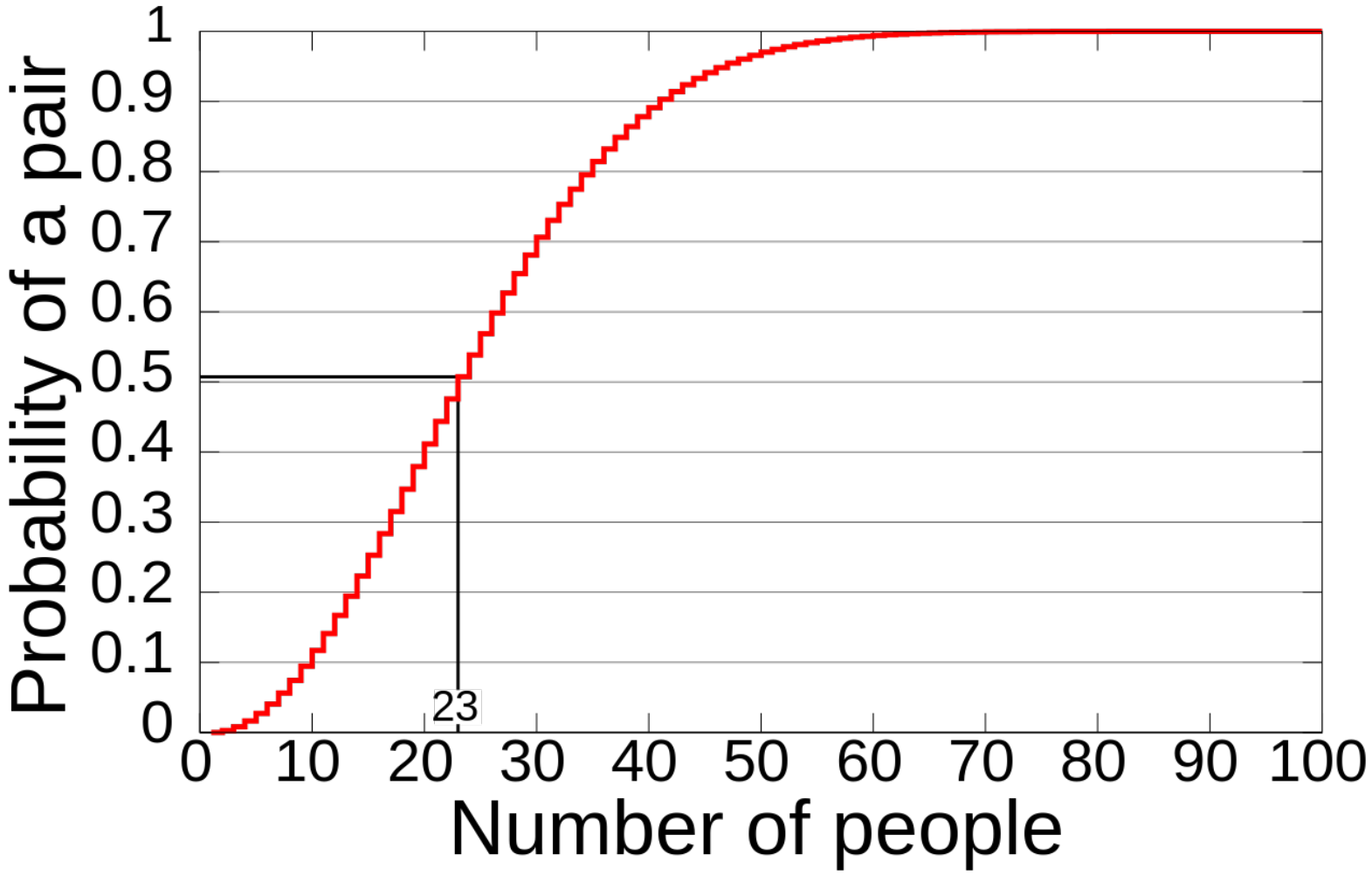
IV reuse

- 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

Birthday Paradox



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

- (FMS attack) 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"

Other Direct Key Attacks

- Korek's key recovery attack (2004)
- Mantin's second round attack (2005)
- PTW attack (2007)

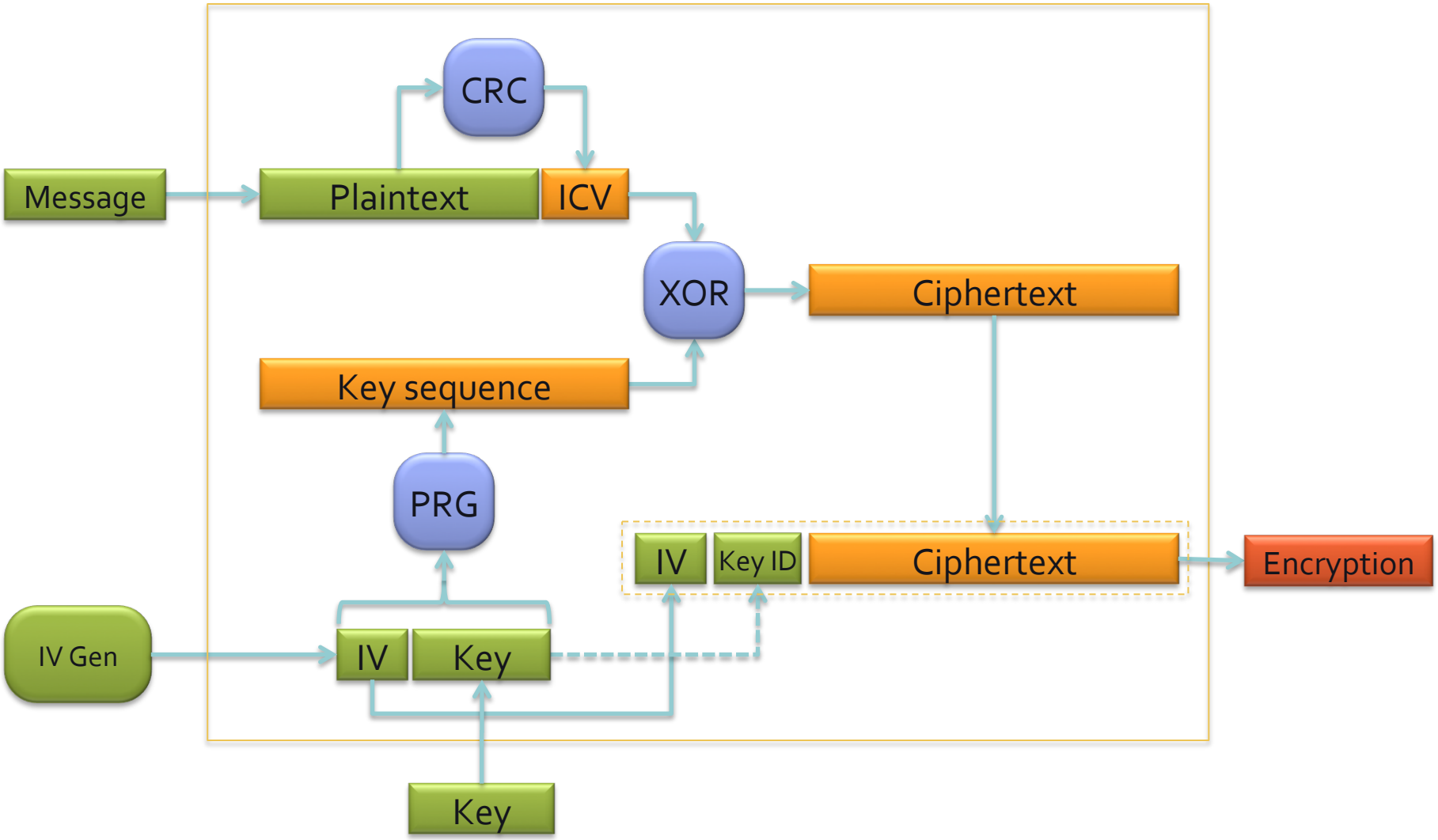
WiFi Protected Access (WPA)

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

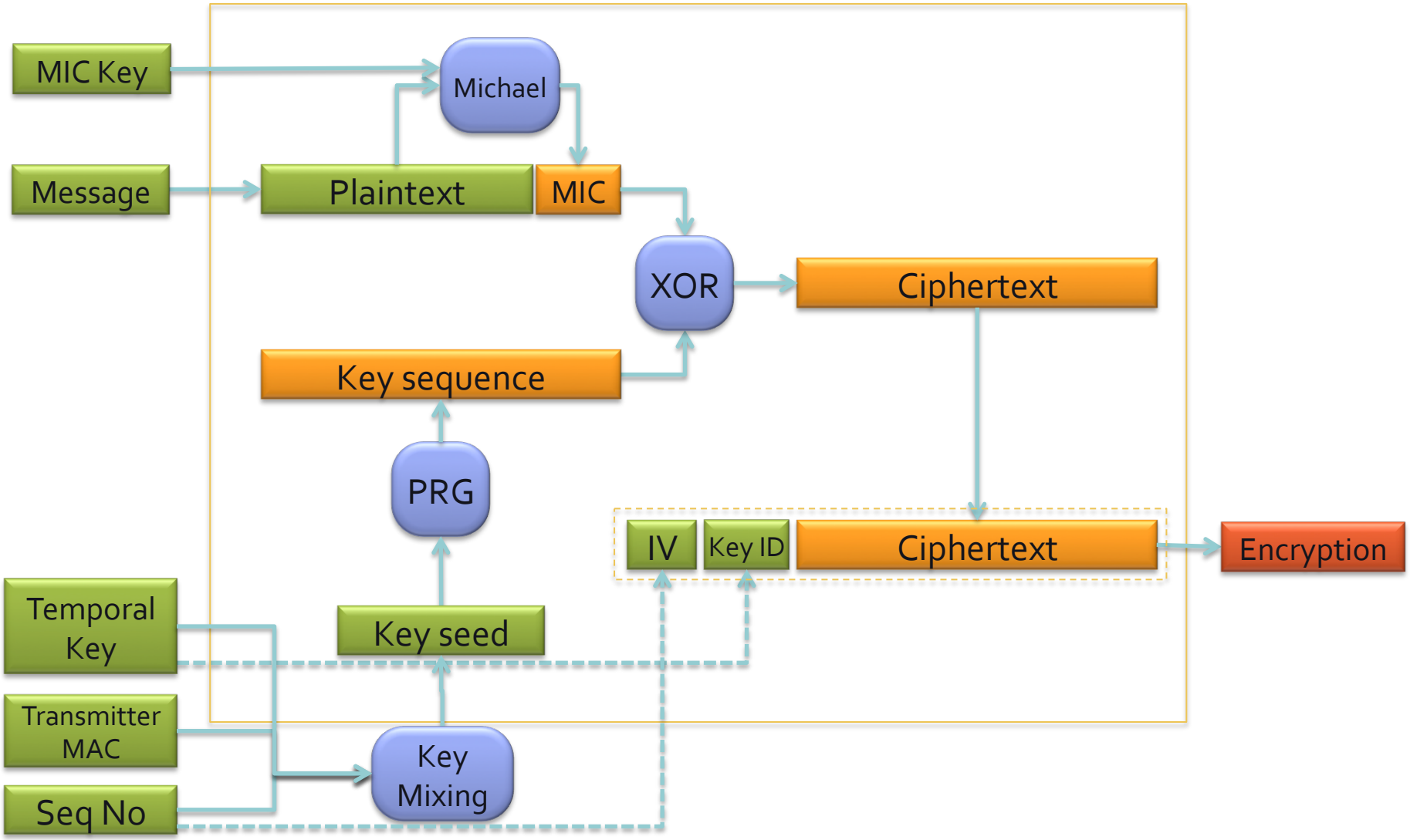
WPA Design

- 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