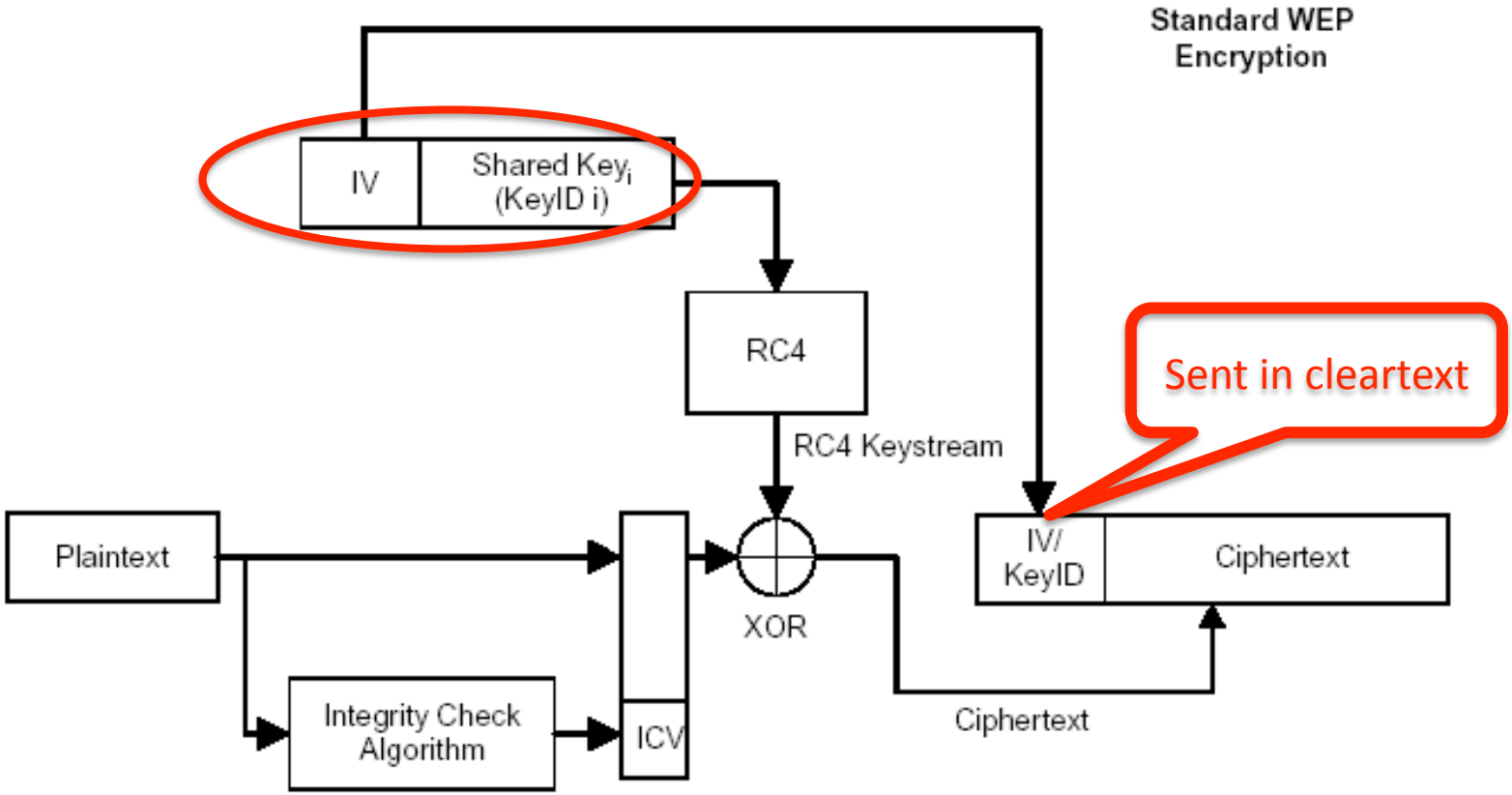
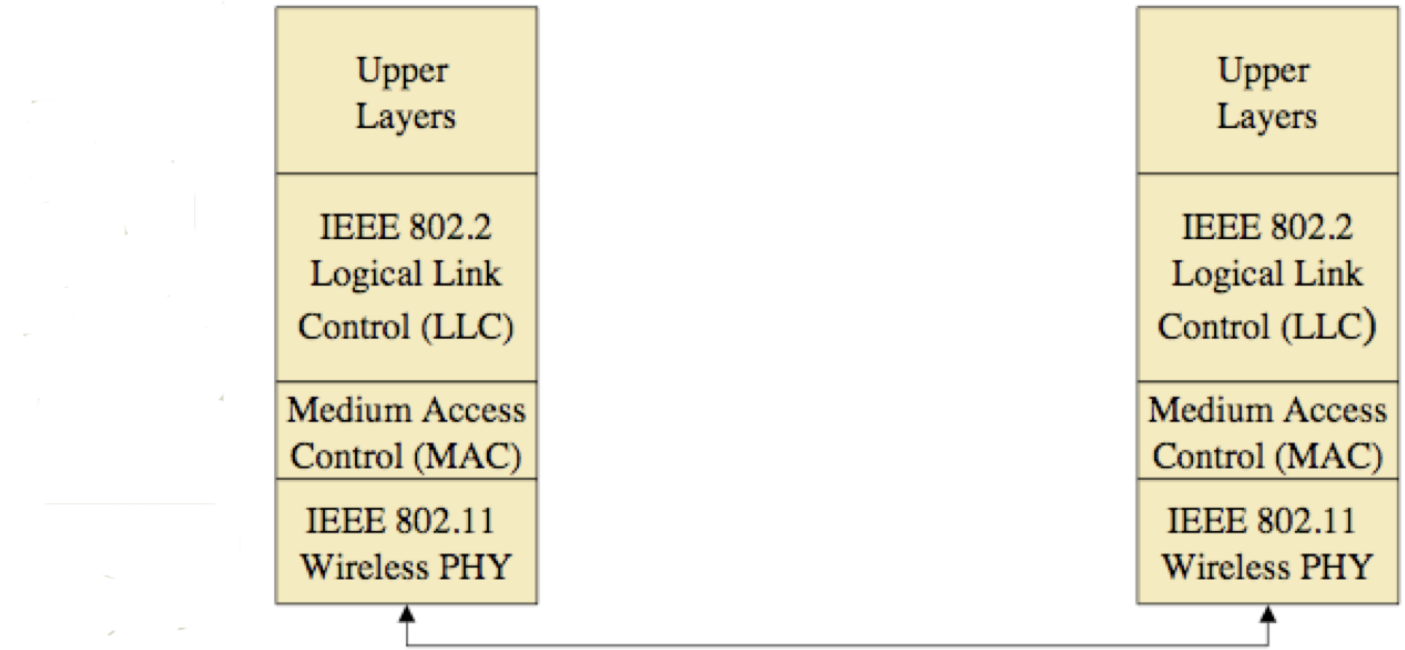
WEP

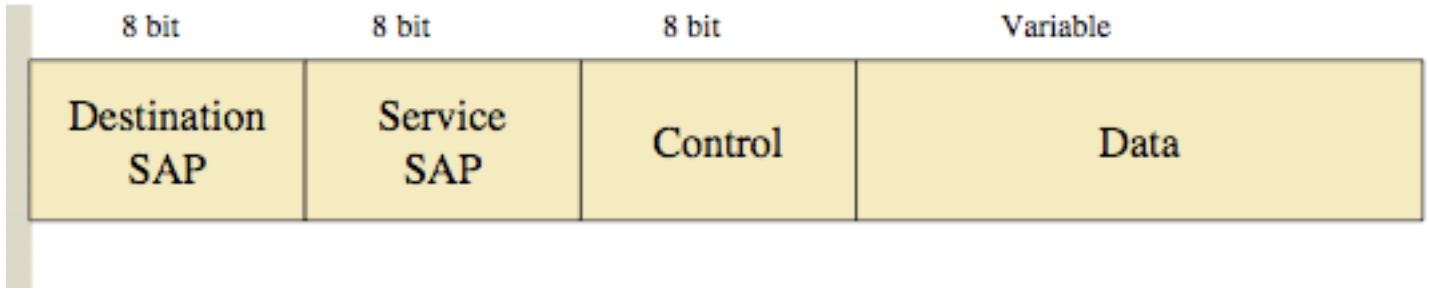
- Goals
  - Authentication
    - A pre-shared key K, shared among all APs and STAs members of the WLAN
    - Same key used for authentication and confidentiality
  - Confidentiality
    - RC4
  - Integrity Protection
    - CRC-32 (non-crypto primitive)

RC4

Figure 1. Standard WEP Encryption Process




Upper Layers
IEEE 802.2 Logical Link Control (LLC)
Medium Access Control (MAC)
IEEE 802.11 Wireless PHY
Upper Layers
IEEE 802.2 Logical Link Control (LLC)
Medium Access Control (MAC)
IEEE 802.11 Wireless PHY


8 bit
8 bit
8 bit
Variable
Destination SAP
Service SAP
Control
Data

- RC4 uses the key and the IV to initialize a state machine via ksa()
- RC4 modifies the state and generates a new byte of the keystream from the new state using prga();
- first byte of the plaintext comes from the WEP SNAP header,
  - the first byte of the keystream can be obtained from

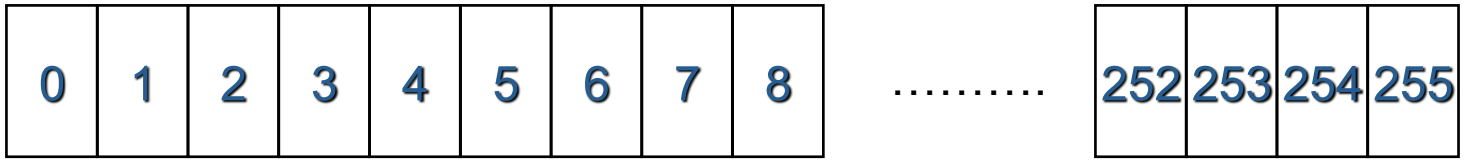
$$B \oplus 0xAA$$

- We can simulate the start of KSA because IV is sent in cleartext and K = IV|K
- Attacker knowing a byte of the keystream can derive a byte of the key (weakness in PRNG)
- Weak IV: (A+3, n-1, X)
  - Initialization vector that with 5% of probability allow to recover a byte of the key
  - The byte of keystream is linked to the value of the key

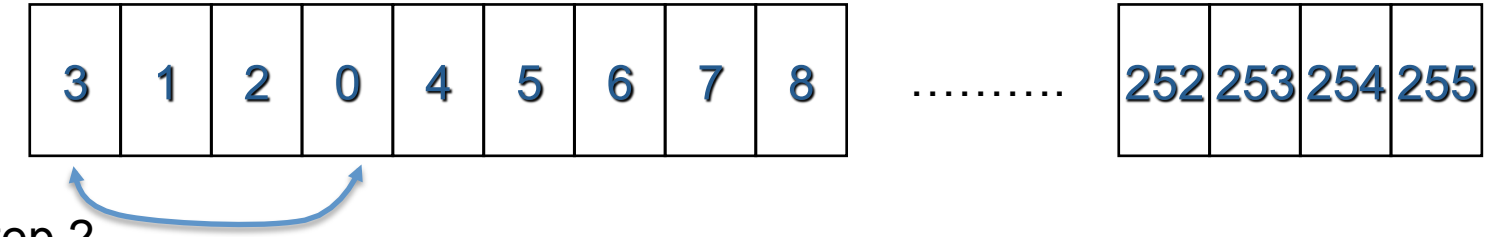
KSA

- key scheduling algorithm (KSA).
  - begin ksa(with int keylength, with byte key[keylength])
    - for i from 0 to 255
      - S[i] := i
    - Endfor
    - j := 0
    - for i from 0 to 255
      - j := (j + S[i] + key[i mod keylength]) mod 256
      - swap(S[i],S[j])
    - Endfor
    - end

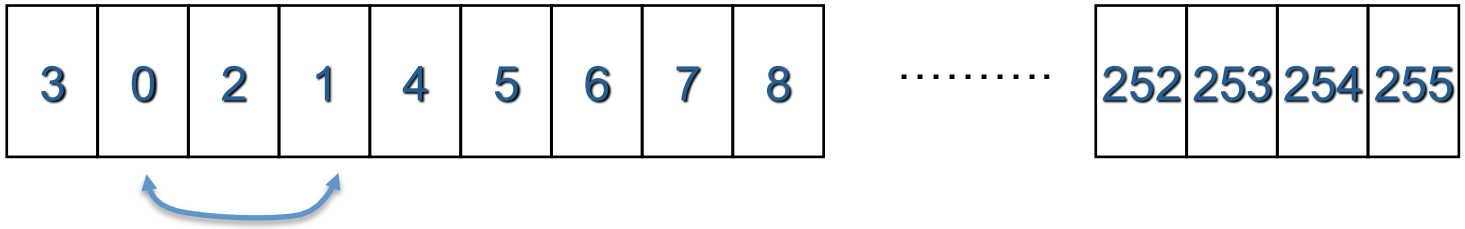
KSA: scrambling the byte array



Step 1



Step 2



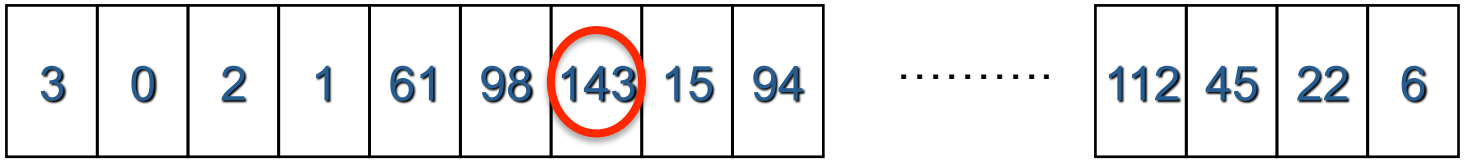
Step 3

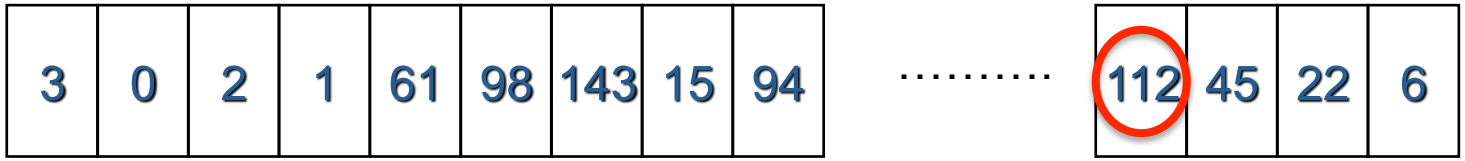
IV = 3,255,X

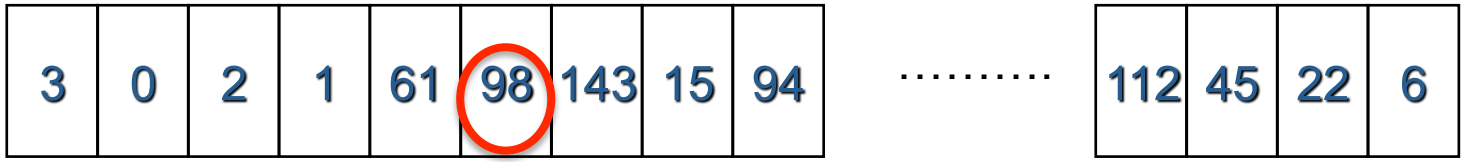
PRGA

- pseudo-random generation algorithm (PRGA)
  - begin prga(with byte S[256])
    - i := 0
    - j := 0
    - while GeneratingOutput:
      - i := (i + 1) mod 256
      - j := (j + S[i]) mod 256
      - swap(S[i],S[j])
      - output S[(S[i] + S[j]) mod 256]
    - Endwhile
  - end

PRGA: extract a byte of keystream







- If S is a permutation, S^{-1} is the inverse permutation
- If an attacker knows the first *l* bytes of an RC4 key used to generate a keystream X ().
  - He can simulate the first *l* steps of the RC4-KSA (S_l and j_l known)
  - $S_l[1] < l$
  - $S_l[1] + S_l[S_l[1]] = l$
  - $S^{-1}{}_l[X[0]] \neq 1$
  - $S^{-1}{}_l[X[0]] \neq S_l[1]$
- The function F() will take the value of K[*l*] with a probability of about 5%
  - $F(K[0], \ldots, K[l-1], X[0]) = S^{-1}[X[0]] - j - S[l]$

WPA-PSK

[Message 1: A → S]

AA, ANonce, sn, msg1

[Message 2: S → A]

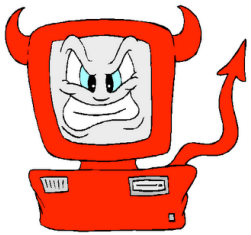
SPA, SNonce, sn, msg2, MIC_{PTK}{SNonce, sn, msg2}

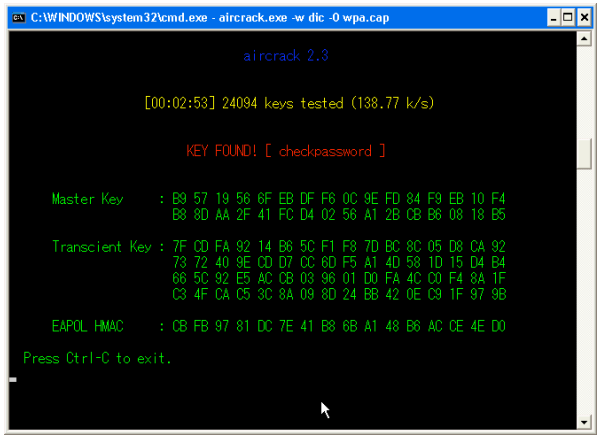
[Message 3: A → S]

AA, ANonce, sn+1, msg3, MIC_{PTK}{ANonce, sn+1, msg3}

[Message 4: S → A]

SPA, sn+1, msg4, MIC_{PTK}{sn+1, msg4}




C:\WINDOWS\system32\cmd.exe - aircrack.exe -w dic -0 wpa.cap
aircrack 2.3
[00:02:53] 24094 keys tested (138.77 k/s)
KEY FOUND! [checkpassword]
Master Key : B9 57 19 56 6F EB DF F6 0C 9E FD 84 F9 EB 10 F4
B8 8D AA 2F 41 FC D4 02 56 A1 2B CB B6 08 18 B5
Transcient Key : 7F CD FA 92 14 B6 5C F1 F8 7D BC 8C 05 D8 CA 92
73 72 40 9E CD D7 CC 6D F5 A1 4D 58 1D 15 D4 B4
66 5C 92 E5 AC CB 03 96 01 D0 FA 4C C0 F4 8A 1F
C3 4F CA C5 3C 8A 09 8D 24 BB 42 0E C9 1F 97 9B
EAPOL HMAC : CB FB 97 81 DC 7E 41 B8 6B A1 48 B6 AC CE 4E D0
Press Ctrl-C to exit.

- **Password cracker (GPLv2 Licence)**
  - http://www.openwall.com/john/
  - Support for DES, MD5, Blowfish and others
- **Single Crack Mode**
  - Uses correlation with “username field”
- **Wordlist mode**
  - Dictionary password attack
    - Dictionaries at ftp://ftp.ox.ac.uk/pub/wordlists
- **Incremental Mode**
  - it can try all character combinations as passwords
- **External Mode**
  - heavily programmable

- **Syntax based on Crack 5.0a**
  - **ftp://ftp.cert.dfn.de/pub/tools/password/Crack/**
- **Examples:**
  - **-c[rules]:ignore this rule if password are not case sensitive**
  - **> 3: do no process di word of smaller than 3 characters**
  - **/: convert alla characters to lowecase**