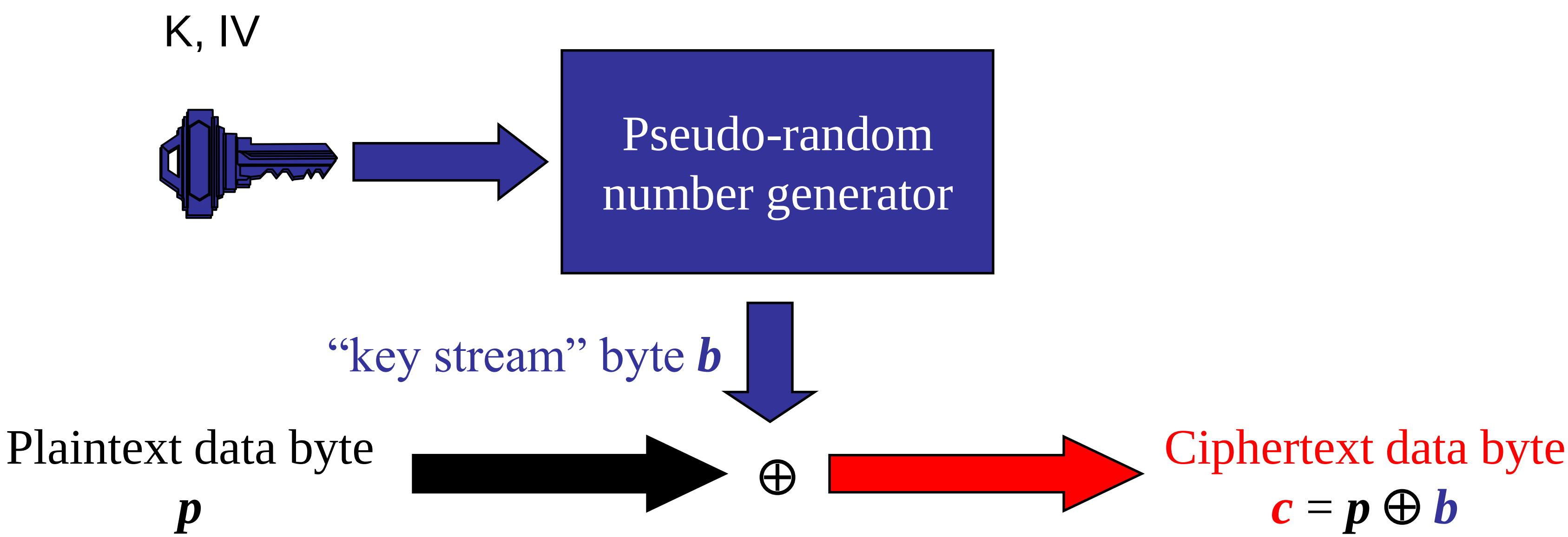
Tutorial 7

Review of the cipher RC4



Decryption works the same way: $p = c \oplus b$

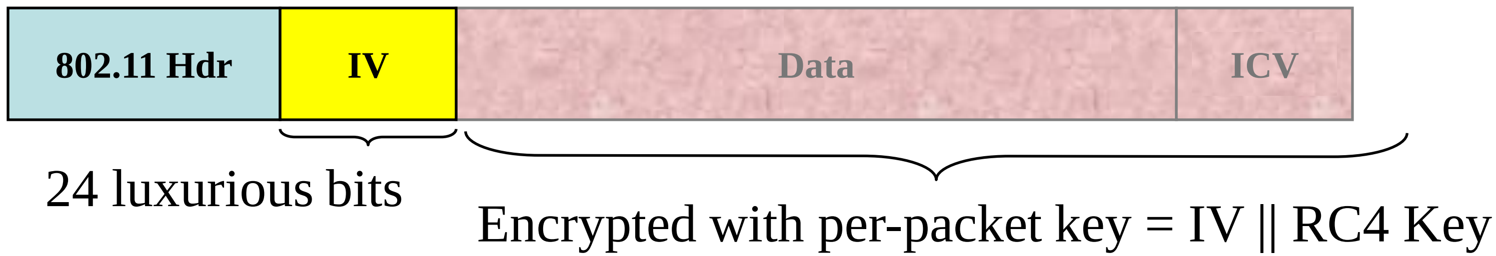
WEP IV Reuse

- Same shared key used in both directions
- Some implementations reset IV to 0 when initialized
  - Low IV values get reused at the beginning of every session
- IV reuse exposes the system to keystream reuse attacks.

WEP IV Reuse

- How about using random IVs?
- IV space – 2^{24} possibilities
- Collision after 5000 packets
  - Birthday Paradox!
- Rough estimate: a busy AP sends 1000 packets/sec
- Collision every 5 sec

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!

A Property of RC4

- Keystream leaks, under known-plaintext attack
  - Suppose we intercept a ciphertext C, and suppose we can guess the corresponding plaintext P
  - Let Z = RC4(K, IV) be the RC4 keystream
  - Since $C = P \oplus Z$, we can derive the RC4 keystream Z by $P \oplus C = P \oplus (P \oplus Z) = Z$
- This is not a problem ... unless keystream is reused!

A Risk of Keystream Reuse

IV, P ⊕ RC4(K, IV)

IV, P’ ⊕ RC4(K, IV)

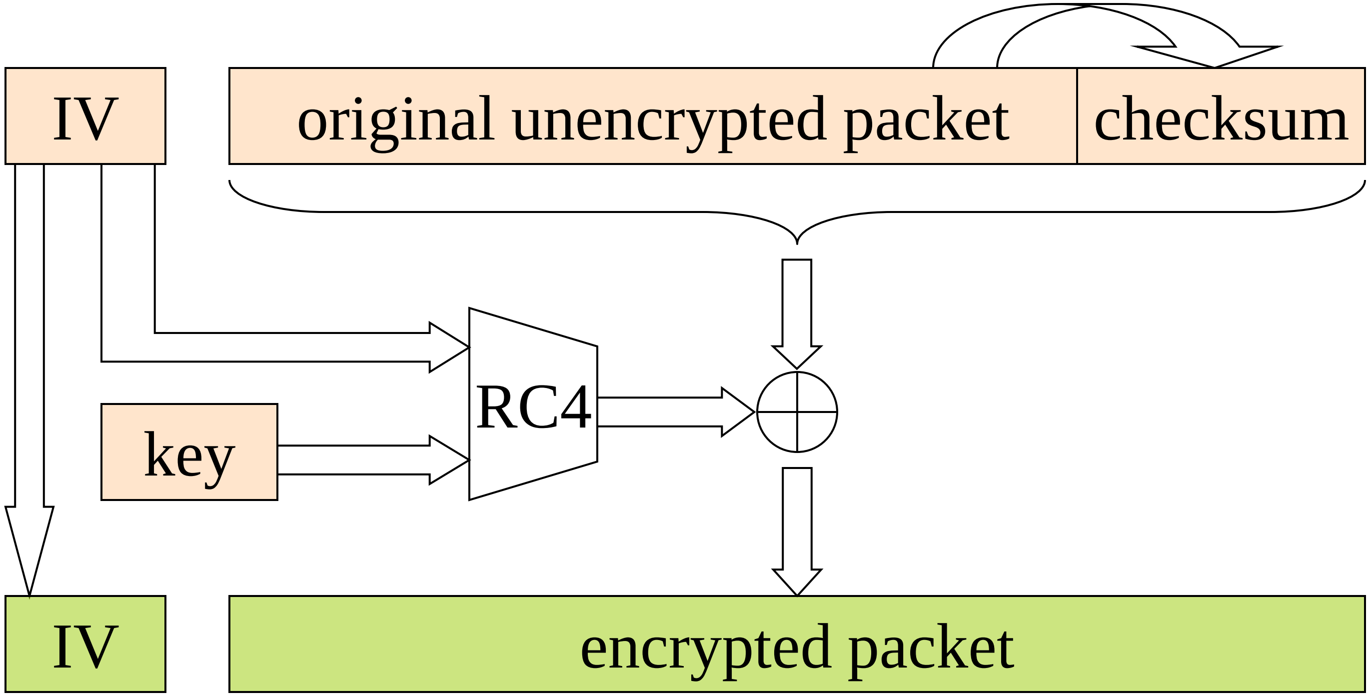
- If IV’s repeat, confidentiality is at risk
  - If we send two ciphertexts (C, C’) using the same IV, then the xor of plaintexts leaks (P ⊕ P’ = C ⊕ C’), which might reveal both plaintexts

➤ Lesson: If RC4 isn’t used carefully, it becomes insecure

Attack #1: Keystream Reuse

- WEP didn't use RC4 carefully
- The problem: IV's frequently repeat
  - The IV is often a counter that starts at zero
  - Hence, rebooting causes IV reuse
  - Also, there are only 16 million possible IV's, so after intercepting enough packets, there are sure to be repeats
- ➤ Attackers can eavesdrop on 802.11 traffic
  - An eavesdropper may decrypt intercepted ciphertexts even without knowing the key

WEP -- More Detail

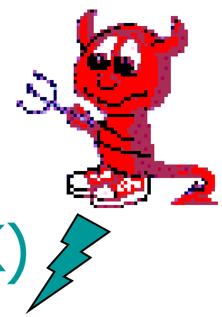


Attack #2: Spoofed Packets

- Attackers can inject forged 802.11 traffic
  - Learn RC4(K, IV) using previous attack
  - Since the checksum is unkeyed, you can then create valid ciphertexts that will be accepted by the receiver

➤ Lesson: checksum must be keyed, preferably using an authentication key different from the encryption key

Attack #3: Reaction Attacks



$(P||crc(P)) \oplus RC4(K)$

$(P||crc(P)) \oplus RC4(K) \oplus (P'||crc(P'))$

- CRC-32 is linear crc(P XOR P’) = crc(P) XOR crc(P’)

  $(P||crc(P)) \oplus RC4(K) \oplus (P'||crc(P'))$
  $= (P \oplus P')||((crc(P) \oplus crc(P')) \oplus RC4(K)$
  $= (P \oplus P')||(crc(P \oplus P') \oplus RC4(K)$

- The checksum on received packet is valid, but the message has been modified.

1. Why is WPA more secure than WEP?

2. Does EAP or EAPOL define a fixed authentication scheme?

3. How are WPA and 802.11i related?

4. Does 802.11 require the mobile IP technology?

5. How are Mobile IP and wireless systems related? Can a connection be wireless and mobile?

- Wireless are kind of short range mobile, they need to have some sort of authorisation to connect locally. Mobile IP relates to establishing a global identity, whether the connection itself is wired or wireless,
- A connection can certainly be wireless and mobile. The wireless relates to not having wires, while the mobile relates to allowing mobility, i.e. not having a fixed entry point.