

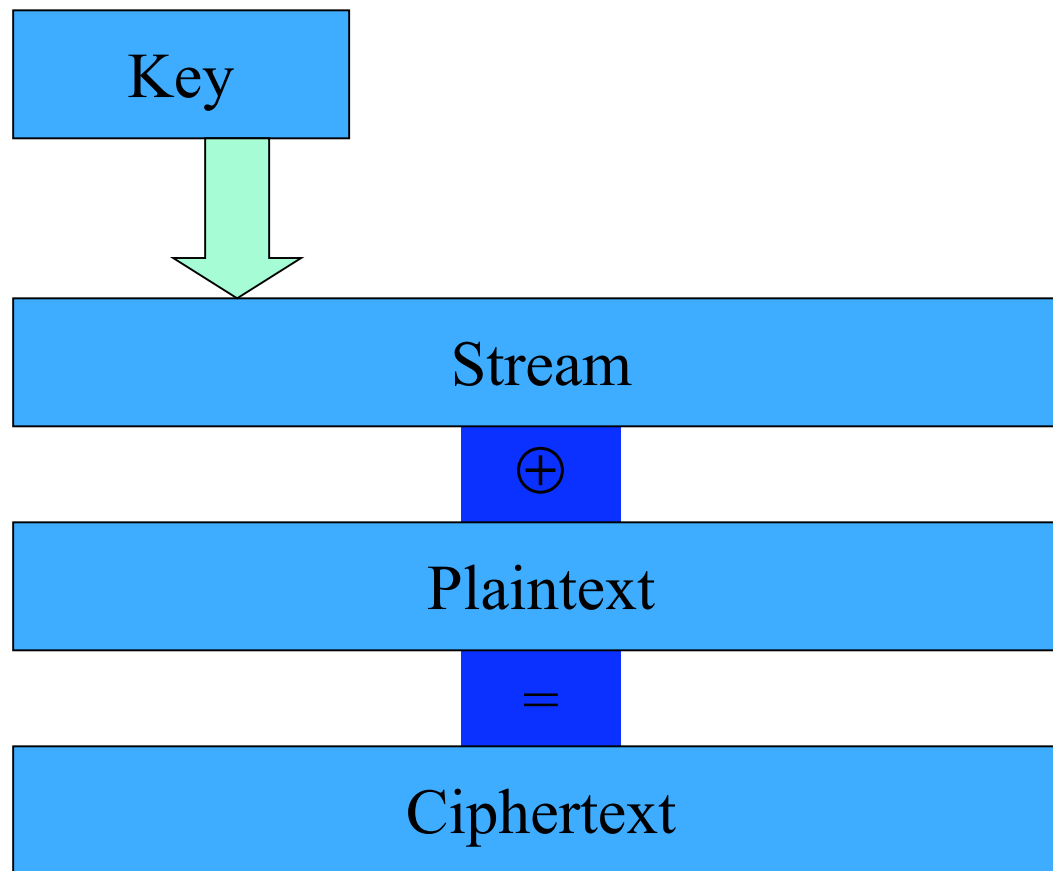
# Crittografia e sicurezza delle reti

WEP: Wired Equivalent Privacy

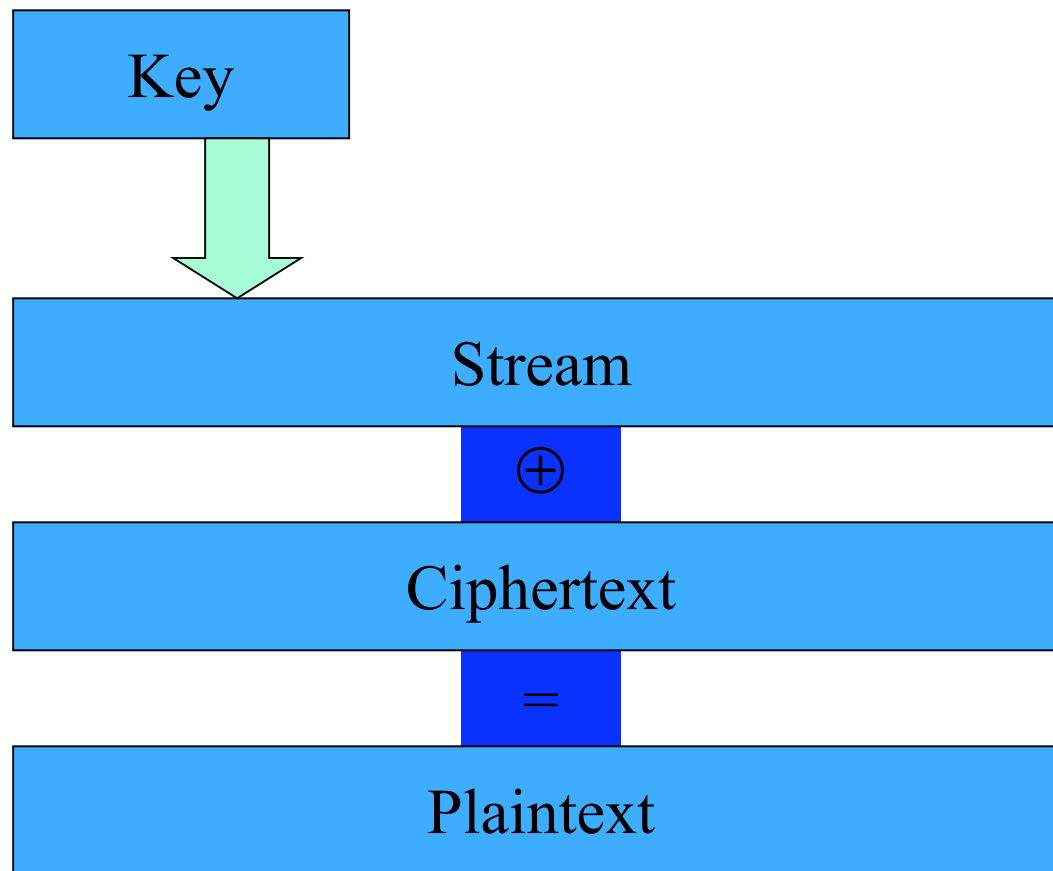
# Stream Ciphers

- Inizia con una chiave segreta ("*seed*")
- Genera uno stream di byte (*Keystream*):
  - byte  $i$  dello stream è funzione della chiave (Stream cypher *sincrono*) oppure
  - della chiave e dei primi  $i-1$  byte del testo crittato (Stream cypher *asincrono*).
- Combina lo stream con il testo in chiaro per ottenere il testo crittato (tipicamente con *XOR*)

# Stream Cipher Binari e additivi



# Decodifica



# RC4: proprietà

- Dimensione chiave variabile (orientata ai byte)
- Sincrono
- Genera una permutazione che appare casuale; la permutazione è ciclica con un periodo molto lungo (più di  $10^{100}$  )
- Efficiente: 8-16 operazioni per byte in output

# RC-4 Creazione Key-stream

Dopo aver generato permutazione casuale  $S_i$  ( $S_i$  in 0-255)

Genera un output byte  $B$  del Key-stream:

1.  $i = (i+1) \bmod 256$
2.  $j = (j + S_i) \bmod 256$
3. Scambia  $S_i$  e  $S_j$
4.  $t = (S_i + S_j) \bmod 256$
5.  $B = S_t$

Codifica di un byte del messaggio:  $B$  è in XOR con il prossimo byte del testo in chiaro

# Proprietà Stream Cipher

Se  $C1 = M1 \text{ xor } RC4(IV,K)$

e  $C2 = M2 \text{ xor } RC4(IV,K)$

allora

$C1 \text{ xor } C2 =$

$(M1 \text{ xor } RC4(IV,K)) \text{ xor } (M2 \text{ xor } RC4(IV,K))$

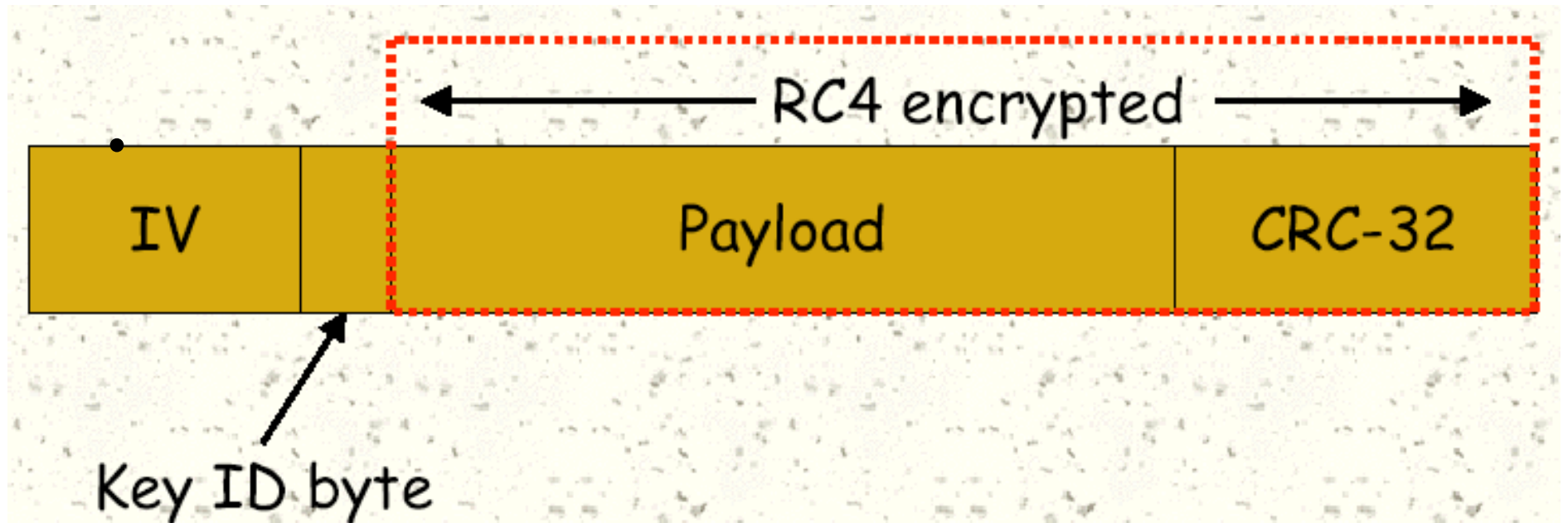
$= M1 \text{ xor } M2$

# WEP

## Standard proposto per sicurezza in 802.11

- Stazioni Mobili condividono chiave con Access point
- Ogni pacchetto è codificato con RC4 usando chiave condivisa e initialization vector (IV)
- Ogni pacchetto include un Check di integrità (CRC)
- Check integ. fallisce => si rifiuta il pacchetto
- Opzion. rifiuta tutti i pacchetti non crittati
- Autentica: challenge con nonce di 128 byte

# WEP - codifica



- IV è di soli 24 bit!
- La chiave (40-104 bit) è selezionata in un insieme ridotto di possibili chiavi (4)!!
- In alcuni casi Syst. Manager usa la stessa chiave per tutti gli utenti !!! (Anche se non nota pone problemi di attacchi dall'interno)

# WEP - Attacchi

- Chiavi di diversa lunghezza (40-104)
- L'attacco si basa su proprietà "exor" di RC4 (e di tutti gli stream cipher):
  - sufficiente codificare due pacchetti con stessa chiave e IV
  - per questo WEP propone di cambiare IV per ogni pacchetto (ad es. da 0 si incrementa di 1 per ogni pacchetto)
  - alcune schede rinizializzano IV a zero ogni volta che sono inserite nel laptop
  - quindi valori bassi di IV sono più probabili

# WEP - Attacchi

IV è solo 24 bit e l'insieme delle chiavi è ridotto. Quindi

- con la stessa chiave ci sono circa 4 milioni di IV
- se si inviano pacchetti da 1500 byte a 5Mbps (max 11 Mbps) basta mezza giornata per esaurire lo spazio possibile
- con IV casuale ogni volta bastano 5000 pacchetti per trovare una collisione (perchè 5000?)

Inoltre la chiave utente non viene cambiata spesso (richiede configurazione scheda)

# WEP - Attacchi

Da  $M1 \oplus M2$  non è difficile risalire a  $M1, M2$ .  
Ancora più facile se lo stesso vale per più pacchetti

- protocolli implicano regolarità messaggi
- attaccante attivo
- in alcune implementazioni si inviano messaggi crittati e non crittati allo stesso tempo (es. pacchetti controllo, o utenti che richiedono codifica e altri no)

Conclusioni: Con codici stream cipher si deve garantire che la chiave usata su pacchetti diversi sia SEMPRE diversa.

# WEP - Autentica messaggi

WEP usa CRC-32 per verificare integrità messaggio.

- $MAC(M) = CRC(M)$  (ultimi 32 bit messaggio crittato)
- $P = (M, CRC(M))$
- $C(P) = RC4(IV, K) \text{ xor } (M, CRC(M))$
- CRC è lineare:  $CRC(P1 \text{ xor } P2) = CRC(P1) \text{ xor } CRC(P2)$

# WEP - Modifica messaggi

Dato  $C(P) = RC4(IV, K) \text{ exor } (M, CRC(M))$  si ottiene MAC di  $M' = M \text{ exor } D$ , con  $D$  arbitrario!

Sia  $P' = (M', CRC(M'))$

$$\begin{aligned} C(P') &= RC4(IV, K) \text{ exor } (M', CRC(M')) \\ &= RC4(IV, K) \text{ exor } (M \text{ exor } D, CRC(M \text{ exor } D)) \\ &= RC4(IV, K) \text{ exor } (M, CRC(M)) \text{ exor } \\ &\quad (D, CRC(D)) \\ &= C(P) \text{ exor } (D, CRC(D)) \end{aligned}$$

# WEP - Invio messaggi falsi

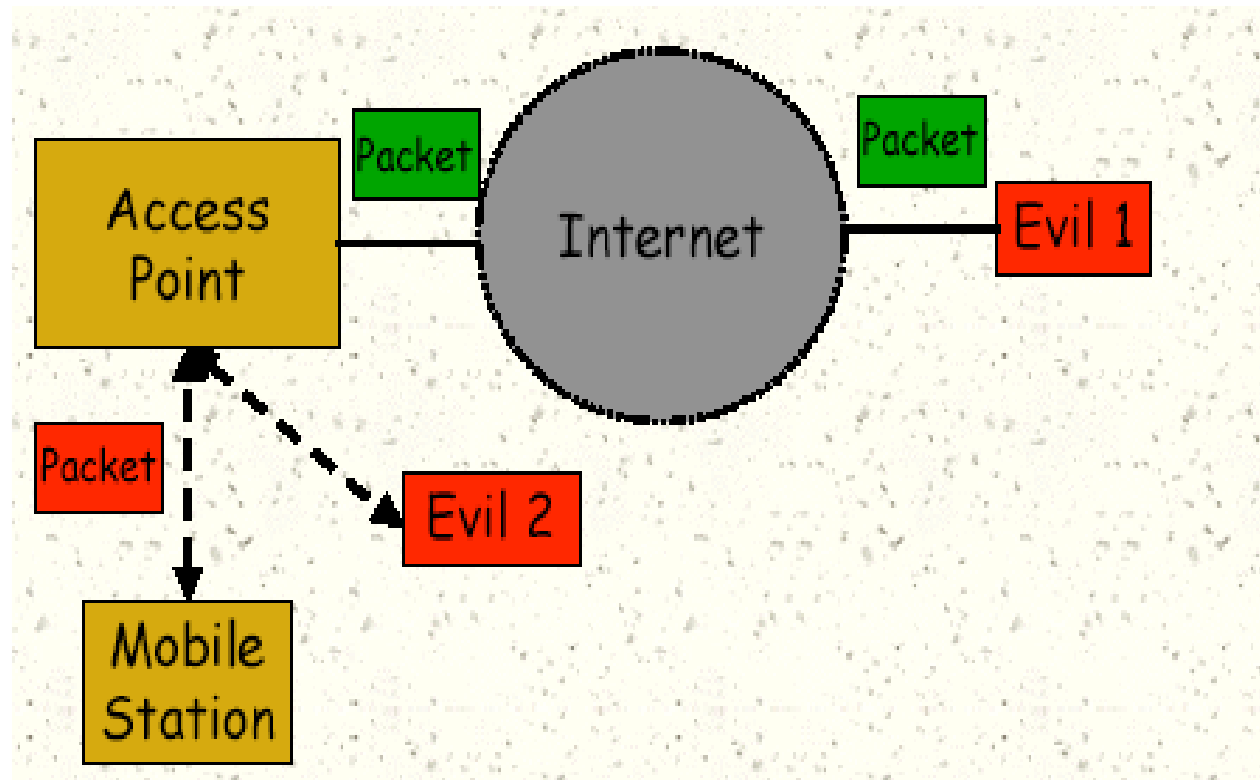
Se avversario conosce  $C(M)$  per qualche messaggio  $M$  è in grado di spedire un qualunque pacchetto considerato "autentico"

Dati  $M, C(M)$  si ha  $RC4(IV, k) = M \text{ exor } C(M)$

Si utilizza la proprietà di WEP di accettare messaggi con lo stesso IV usato più volte per codificare un altro messaggio!

Inoltre Autentica utenti diventa automatica!!

# Scenario di attacco



# Scenario di attacco - codifica

Trudy vuole conoscere codifica di un messaggio

1. Trudy invia messaggio a attaccato da Internet
2. AP codifica e invia a destinatario
3. Trudy sniffa messaggio crittato!

# Scenario di attacco - decodifica

Trudy vuole conoscere decodifica di un messaggio crittato

- T può modificare messaggio
- Supponi indovina indir. IP pacchetto
- Cambia indir. IP - host controllato da Trudy (ci sono trucchi per fare questo)
- AP invia pacchetto crittato a host di T
- Poni porta 80 per bypassare firewall
- Errore in TCP checksum non verificato fino a destinazione





# Rimedi

- WEP2: aumentare IV valore iniziale; richiedere codifica a 128 bit: non rimedia riesce solo ad aumentare il lavoro dell'attaccante
- WEP +: proprietario; non permette IV deboli; non è effettivo ad attacchi di replay
- WPA e WPA2: scelta consigliata

# WPA: Wi-Fi Protected Access

Proposto da WI-FI alliance:

- usa RC4, chiave 128 bit e 48 bit di valore iniziale
- il valore iniziale è cambiato dinamicamente (protocollo TKIP)

1 e 2 sconfiggono attacco che recupera chiavi

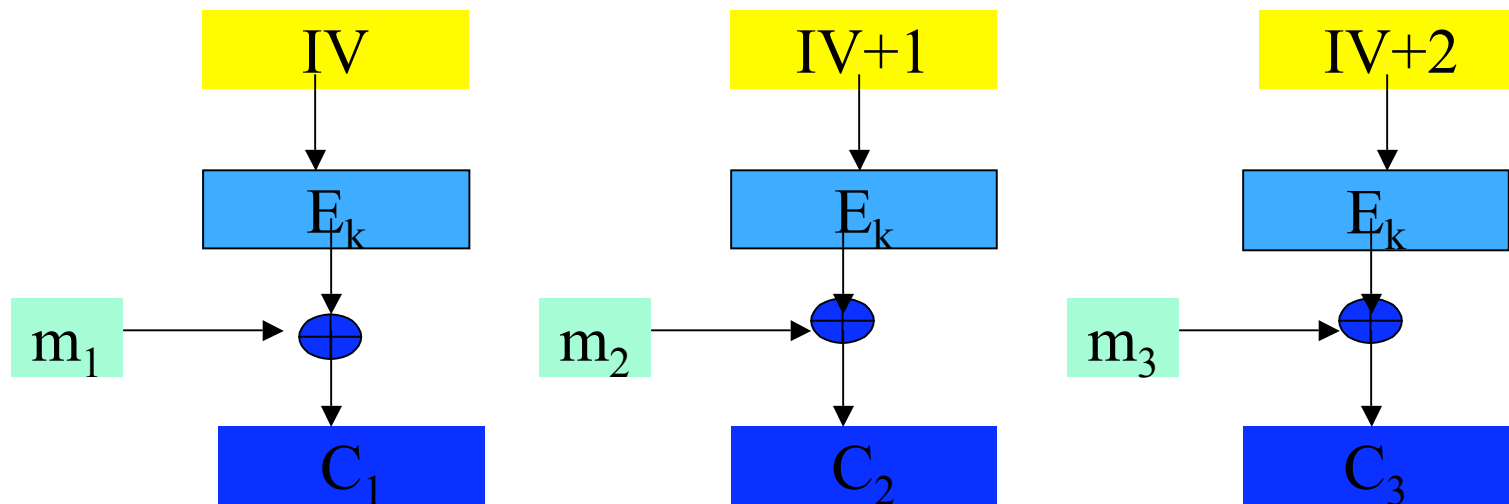
3. non usa CRC ma utilizza un metodo per la verifica di integrità dei messaggi (MIC); attaccabile ma compatibile con le schede di rete vecchie
4. per evitare attacchi di replay il MIC utilizza un contatore di pacchetti (aggiornato automaticamente)

# WPA2

Sviluppo successivo (obbligatorio da 2006 per certificazione WI-FI)

1. oltre a TKIP e MIC introduce un sistema crittografico CCMP basato su AES
2. CCMP (Cipher Block Chaining Mess. Authent. Code)
  - codifica usa CTR con AES
  - autentica dati con CBC
3. Come in WPA l'integrità comunicazione è basata su MIC (per evitare attacchi di replay)

# CTR (Counter Mode)



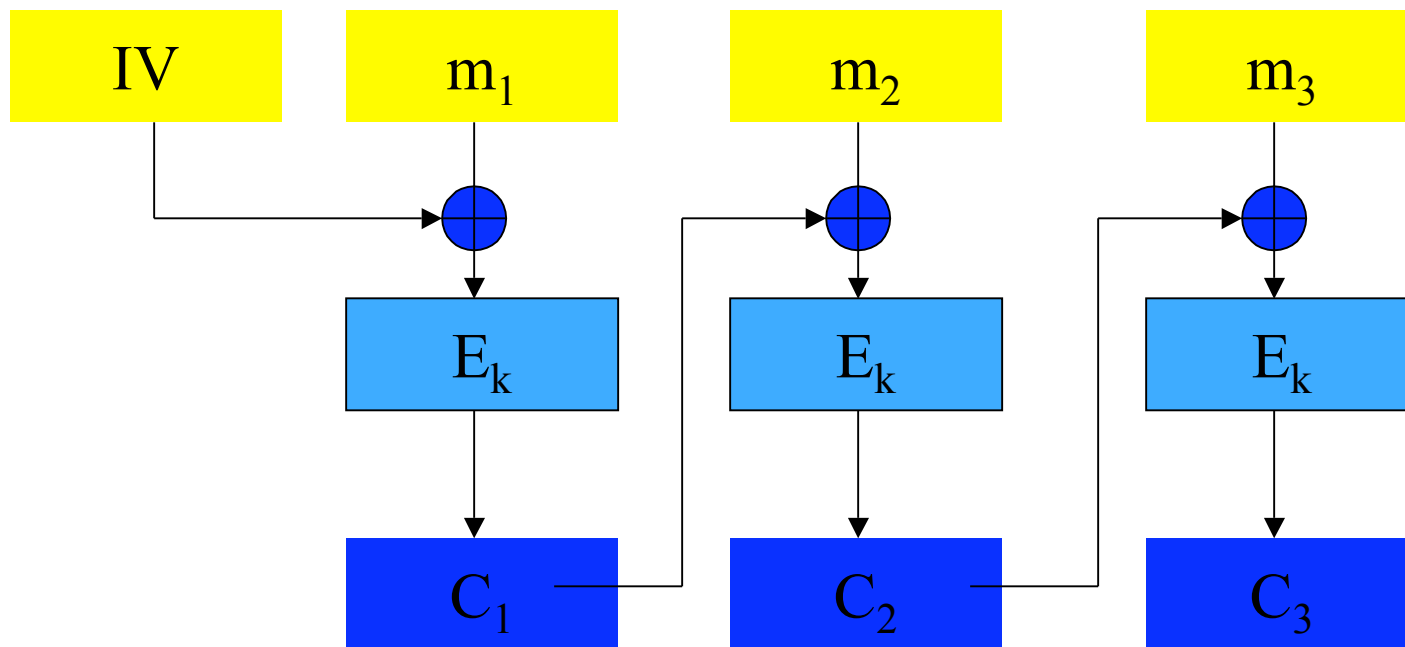
simile a OFB calcolato prima

come OFB ha problemi nell'uso ripetuto di IV

vantaggio

puoi calcolare il messaggio ad ogni punto e non dall'inizio

# Codifica CBC (Cipher Block Chaining)



Si la codifica dell'ultimo blocco rappresenta il MAC del messaggio

# WEP - Conclusioni

- Tipi di attacco in genere noti PRIMA del rilascio del protocollo
- Lista possibili attacchi a WEP non è finita
- Versioni iniziali di IPSEC avevano problemi simili
- Problemi di checksum (SSH usa CRC)
- Microsoft PPTP si basava su RC4

# WEP - Conclusioni 2

- Il Progetto di un protocollo crittografico è meno banale di quello che sembra ...
- Uso di revisione pubblica aumenta i tempi ma dà maggiori garanzie
- Analizzare bene errori precedenti
- In Wireless LAN usa VPN e poni firewall oltre la rete wireless oppure usa end-to-end crittografia