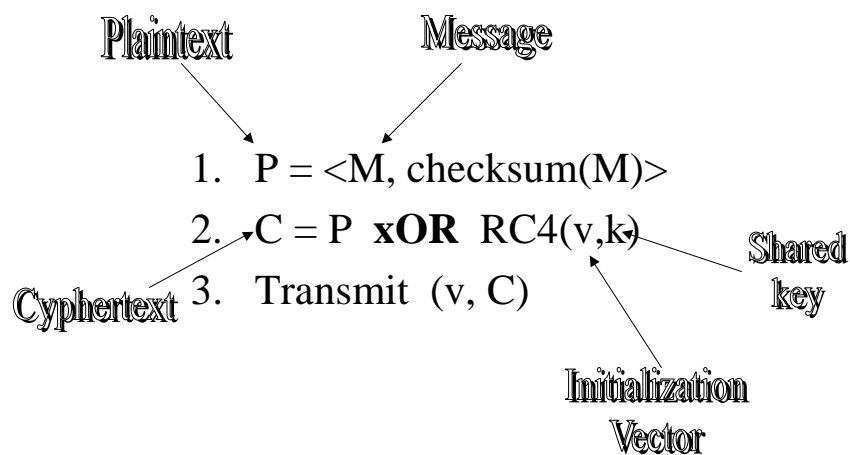


## Security of WEP (Wired Equivalent Privacy)

- The goal of WEP: to provide an equivalent level of privacy as is ordinarily present in an **unsecured** wired LAN by encrypting transmitted data.
- WEP was never intended to be an end-to-end security solution.

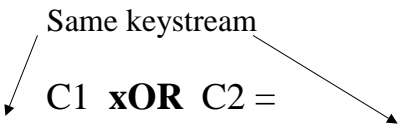
## WEP Protocol Review



## Risks of Keystream Reuse

- Encrypting two messages under the same IV and key (keystream reuse) can reveal information about both messages

Same keystream


$$C1 \text{ XOR } C2 = (P1 \text{ XOR } RC4(IV,k)) \text{ XOR } (P2 \text{ XOR } RC4(IV,k)) = P1 \text{ XOR } P2$$

- If the plaintext for one message is known, it is easy to derive the other message
- Traffic analysis can lead to discovery of plaintext

## Risks of Keystream Reuse (cont)

- To prevent these attacks, WEP uses a per-packet **IV** (initialization vector)
- This still does not prevent Keystream Reuse attacks
  - **k** rarely changes (most networks use 1 key for all hosts), **IV** reuse will occur (only 24 bits), therefore some of the keystreams will be reused (1500 byte packets, 5Mbps, less than 12 hours)
  - Since **IV**'s are public, an attacker can easily detect a reused keystream

## Message Integrity

- WEP uses a integrity checksum field, implemented as a **CRC-32 checksum**, to ensure packets do not get modified in transit
- CRC checksum designed to detect random errors in a message and is NOT resilient against malicious attacks

## Message Integrity (cont)

- Message Modification
  - It is possible to make modifications to the original message **without** fear of detection.

Original Cyphertext:  $C = RC4(v,k) \text{ XOR } \langle M, c(M) \rangle$

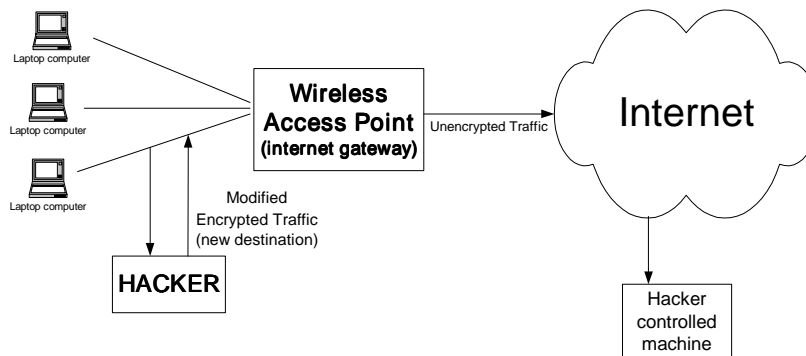
$$\begin{aligned} C' &= C \text{ XOR } \langle \text{delta}, c(\text{delta}) \rangle \\ &= RC4(v,k) \text{ XOR } \langle M, c(M) \rangle \text{ XOR } \langle \text{delta}, c(\text{delta}) \rangle \\ &= RC4(v,k) \text{ XOR } \langle M \text{ XOR } \text{delta}, c(M) \text{ XOR } c(\text{delta}) \rangle \\ &= RC4(v,k) \text{ XOR } \langle M', c(M \text{ XOR } \text{delta}) \rangle \\ &= RC4(v,k) \text{ XOR } \langle M', c(M') \rangle \end{aligned}$$

Note: The WEP checksum is a linear function of the message.  
i.e.,  $c(a \text{ XOR } b) = c(a) \text{ XOR } c(b)$

# Message Decryption

- IP redirection
  - Will work if access point acts as a gateway to the Internet.
  - Attacker can use previously described technique of message modification to change the destination of an encrypted packet to a machine controlled by the attacker.

## Message Decryption (cont)



## Conclusions

- WEP does **not** provide strong link-level security however it may accomplish it's goal
- In order to secure a wireless network, WEP must be supplemented with additional higher level security mechanisms such as access control, authentication, virtual private networks, firewalls...