

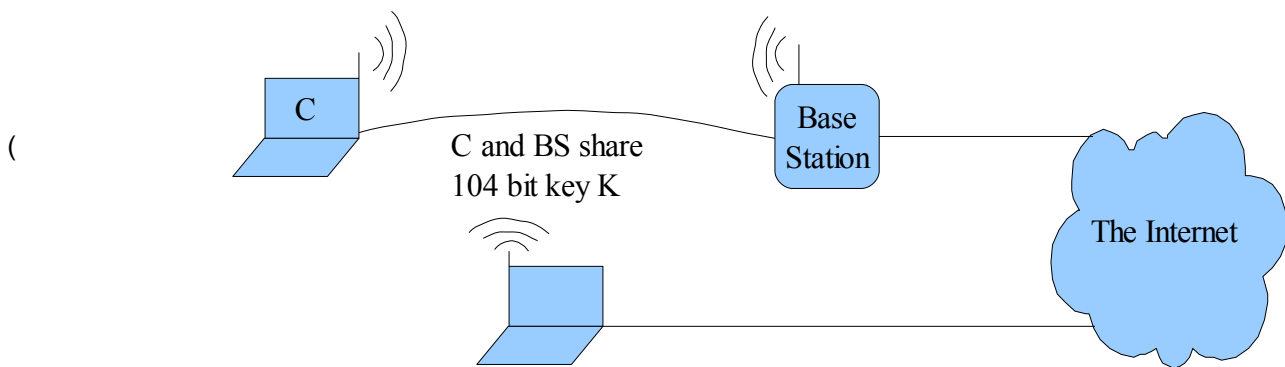
**Wired Equivalent Privacy (WEP):**

- is a protocol for encrypting wirelessly transmitted packets on IEEE 802.11 networks.
- uses the stream cipher RC4 for encryption
- key is shared by all radio stations
- For each packet, a 24-bit initialization vector (IV) IV is chosen. The IV concatenated with the root key yields the per packet key
- ,An Integrity Check Value (ICV) is calculated as a CRC32 checksum over the data to be encrypted. The key K is then used to encrypt the data followed by the ICV using the RC4 stream cipher.
- The IV is transmitted in the header of the packet.

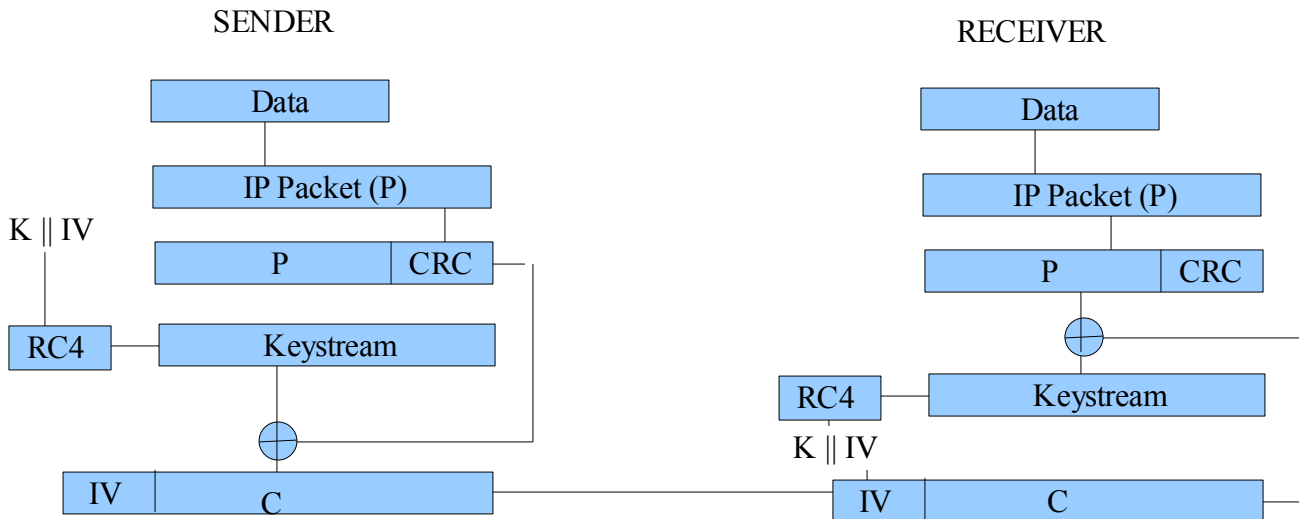
**Security Goals:**

- Secrecy
- Integrity
- Access Control

WEP can be attacked by both, attacking RC4 and attacking WEP implementation itself.



Sender and Receiver stacks for WEP. Both share the 104 bit secret key K. The IV for each packet is prepended to the packet itself. RC4 is reset for each packet with the concatenation of K and new IV as the seed.



**Remark:** XOR is a cheap, invertible, and fully parallelizable operation. Because of these desirable properties, it is used for many cryptographic operations.

There are two strategies to pick the IV for the next packet:

1. **Randomly:** The IV is chosen randomly for each packet.

For each packet pair, the probability of collision is  $2^{-24}$

For  $l$  packets the probability of collision is  $l^2 / 2^{25}$

Expect a collision after 6000 packets

2. **As a Counter:** The IV is chosen as a counter and the IV repeats after the full range ( $2^{24}$  packets).

**What happens if there is a collision in IV values:**

For the same values of key (K) and IV, RC4 generates the same key-stream. This property can be used for a variety of attacks on the system.

1. For the minimum, the attacker can recover the XOR of the two messages encrypted with the same key-stream.
2. Attacker can do frequency analysis on the XOR of the two messages and can recover information about the messages.
3. If one of these two messages is known to the attacker or he can guess it, he can find out the other one. He can even glean useful information about the messages if he only knows part of messages e.g. if he knows the message structure, he can know if the two messages were sent to the same recipient.
4. Attacker can insert a message into the network multiple times and exhaust the IV range. Now he has the pair of all the IVs and corresponding key-streams, which he can save. Later if the key is not changed, he can just pick the message from the network and decrypt it. For a 24bit IV, there will be  $2^{24}$  values to be saved and  $2^{24}$  messages to be sent, which is not computationally hard to do.

Key Recovery Attacks on WEP, use the first 4 bytes of the packet to exploit some inefficiencies in RC4. For any transmission protocol, the initial few bytes generally contain the meta-data about the packet and are easy to know.

**Attack on WEP due to inefficiency of CRC:**

CRC has the following property:

$$\text{CRC}(x \text{ XOR } y) = \text{CRC}(x) \text{ XOR } \text{CRC}(y)$$

Due to this property, it is possible to invert arbitrary bits in the message ciphertext and make corresponding changes to the CRC so that the message will still be accepted as authentic.

If the attacker knows the structure of the message, or if he has some idea about the location of important information in the message, he can flip a few bits to change the message without being detected.