

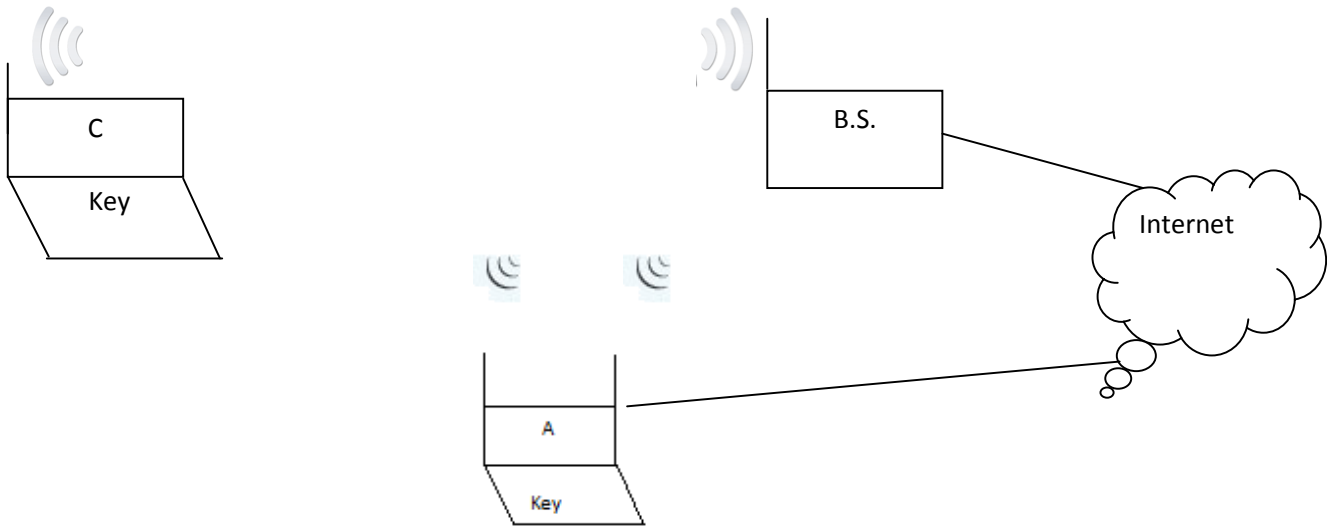
Network Security Notes (September 11 2009)

By Supreet Padhi

WEP (Wired Equivalent Protocol) used in IEEE 802.11a

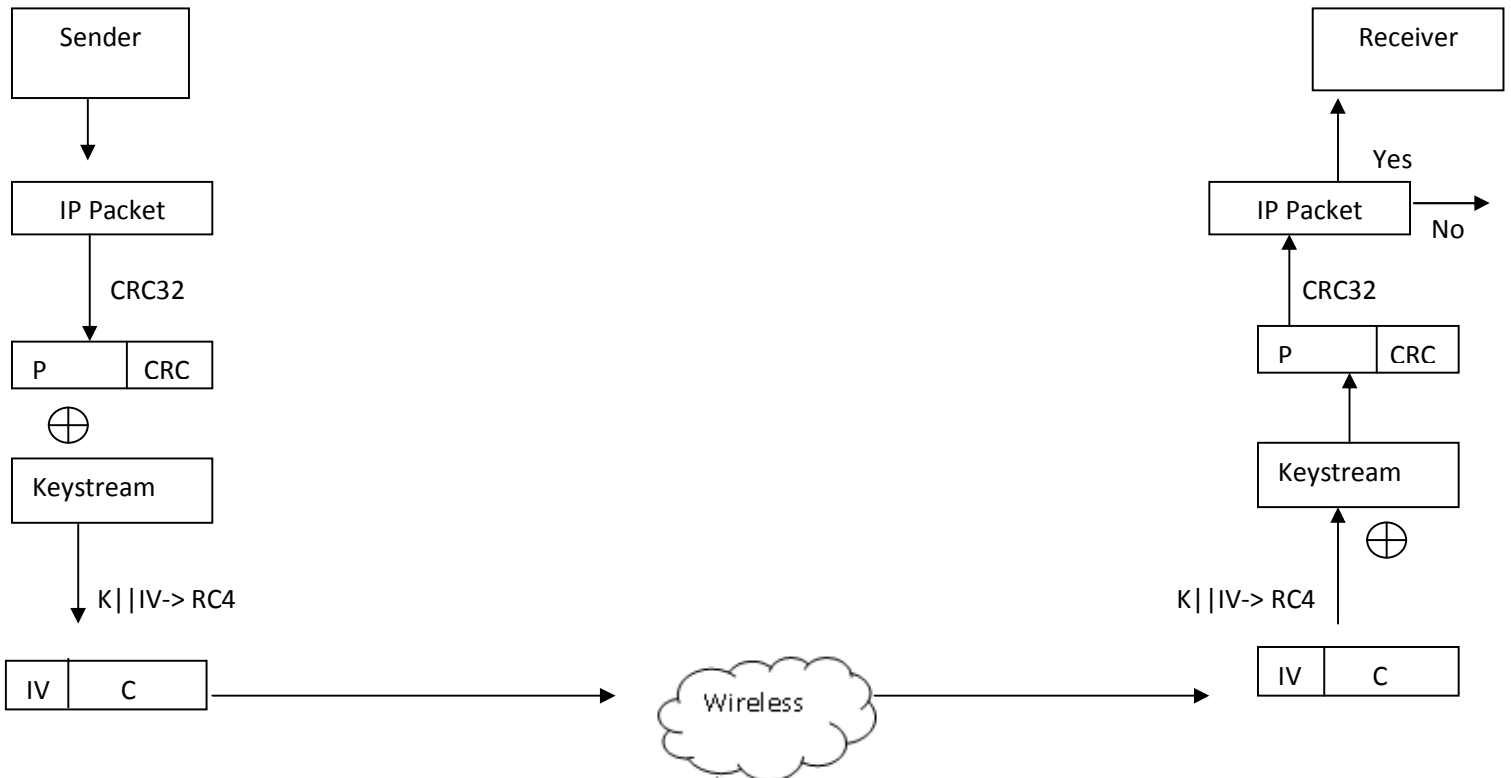
Security Goals

- Secrecy
- Integrity
- Access Control



We have

- K(Key): 104 bits
- IV(Initialization vector):24 bits



Note-RC4 stream ciphers are used widely in WEP,WPA,SSH and SSL etc

IV Choice

1. Pick IV randomly

After l packets,

$$\text{Expected \# of collisions} = \left(\frac{l}{2}\right) 2^{-24} = \frac{l^2}{2^{25}}$$

Considering $l = 2^{20}$

then # of collisions = 2^{15}

2. IV = 0,1,2

Take 2^{24} packets before repetition.

(After system reset IV starts from zero again)

IV Resuse

$$P_1 || CRC_1 \oplus KS$$

$$P_2 || CRC_2 \oplus KS$$

$$\oplus \text{-----}$$

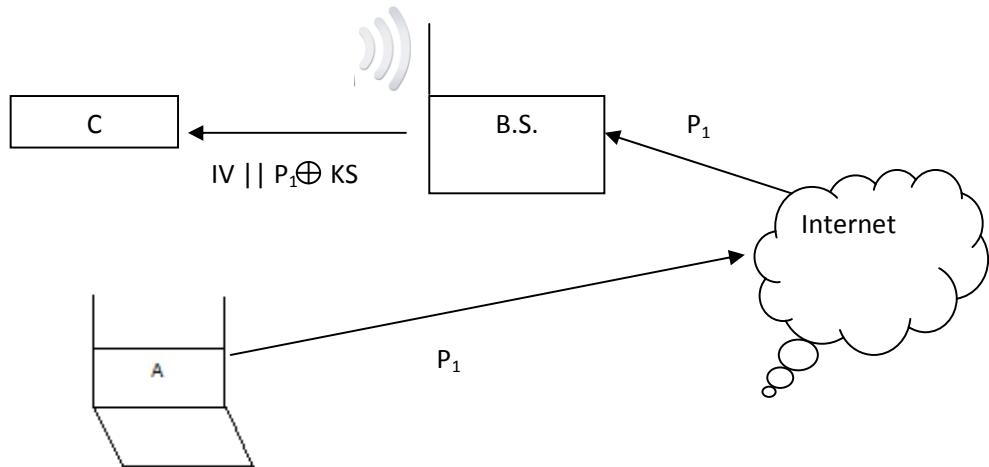
$$P_1 \oplus P_2 || CRC_1 \oplus CRC_2$$

A Table can be maintained in order to check repetitive occurrence of IV again in the ciphertext.

IV	KS
0	KS ₀
1	KS ₁
2	KS ₂

Note- The# of rows in the table would be 2^{24}

1. Chosen Plaintext Attack

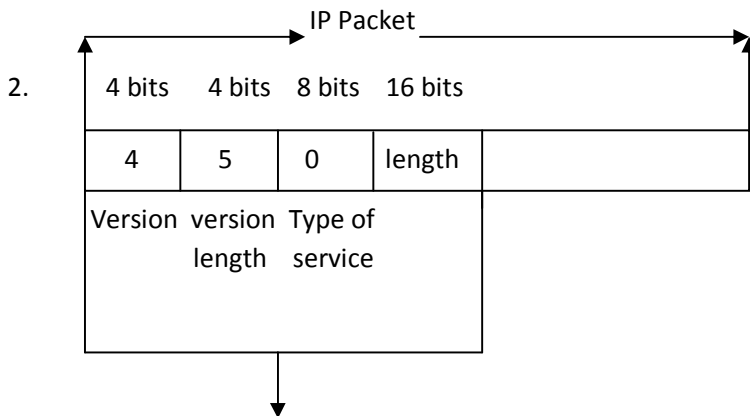


Here the attacker keeps on sending packet P_1 to the Wireless Base station until IV gets repeated in the cipher text to identify the corresponding keystream(KS).

Once the KS is known we can get the plaintext from the ciphertext.

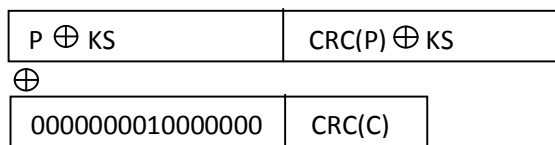
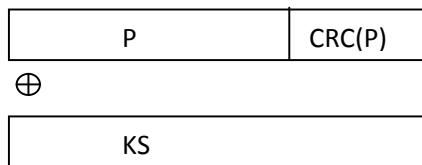
$$C = P_1 \parallel \text{CRC}_1 \oplus \text{KS}$$

$$P_1 \parallel \text{CRC}_1 = C \oplus \text{KS}$$

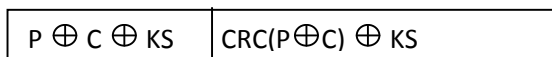
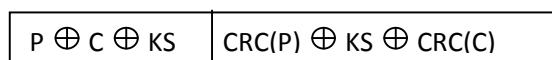


First 4 bytes of the keystream are known

3. $\text{CRC}(X \oplus Y) = \text{CRC}(X) \oplus \text{CRC}(Y)$ -----(A)



----- bits are included in the cipher text



-----use of (A)