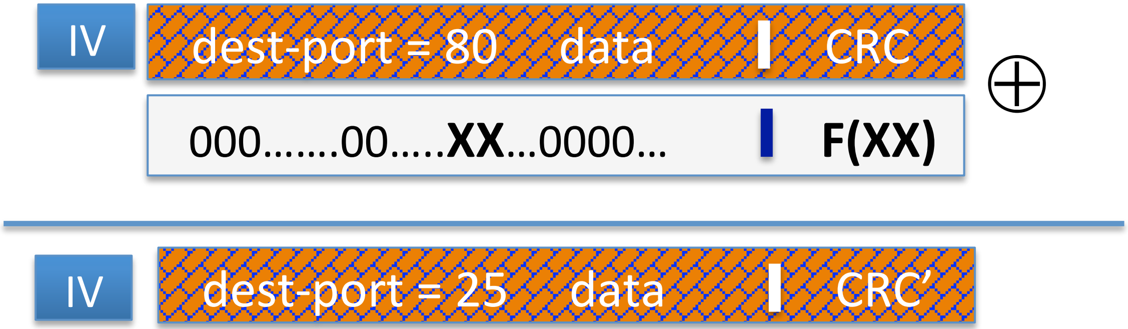
Fact: CRC is linear, i.e. $\forall m,p$: $\mathbf{CRC(m \oplus p) = CRC(m) \oplus F(p)}$

WEP ciphertext:

attacker:

XX = 25⊕80



IV | dest-port = 80 data | CRC

000…….00…..**XX**…0000… | **F(XX)**

⊕

IV | dest-port = 25 data | CRC’