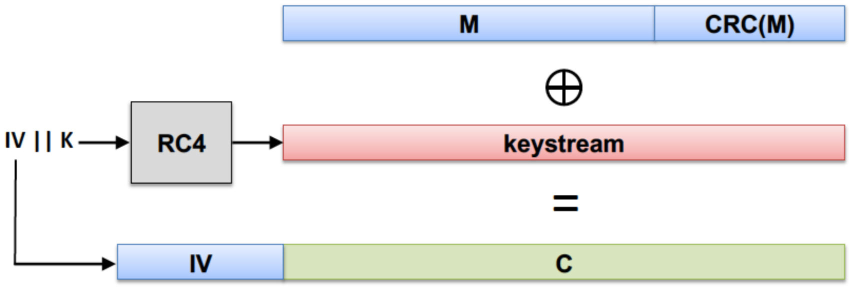
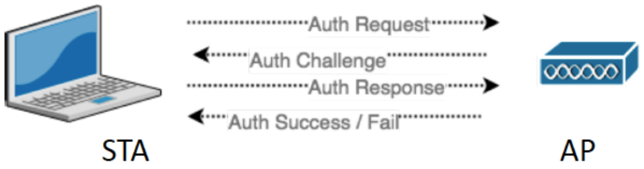
WEP Encryption



- Uses RC4
- IV: 24 bits, K: 104 bits (40 bits)
- IV is used in counter mode (0, 1, 2, …)

IV: Initialization Vector
K: Cryptographic Key
RC4: Rivest Code 4
CRC: Cyclic Redundancy Check

WEP Authentication



- Auth Challenge:
  - AP sends a (random) 128-bit challenge text
- Auth Response:
  - STA encrypts the challenge text with the secret key using WEP and sends the ciphertext to the AP
- Auth Success:
  - AP decrypts and compares the plaintext with the challenge; if it equals the challenge text, authentication succeeds

Question 1: What can a passive adversary find?
Question 2: Is the authentication secure?
Question 3: Is the authentication mutual?
Question 4: What attack does the unilateral authentication facilitates in this case?
Question 5: Suppose there is no CRC. Can the adversary change the bits in the plaintext as he/she wishes (not knowing the initial/changed plaintext, but knowing how he changed the plaintext)?
Question 6: What happens if the IV is the same for a given key K? Does the system remains secure in this situation?
Question 7: How many possible values can IV take?