Authenticated Encryption

Yan Huang

Credit: Dan Boneh (Stanford, Crypto I)

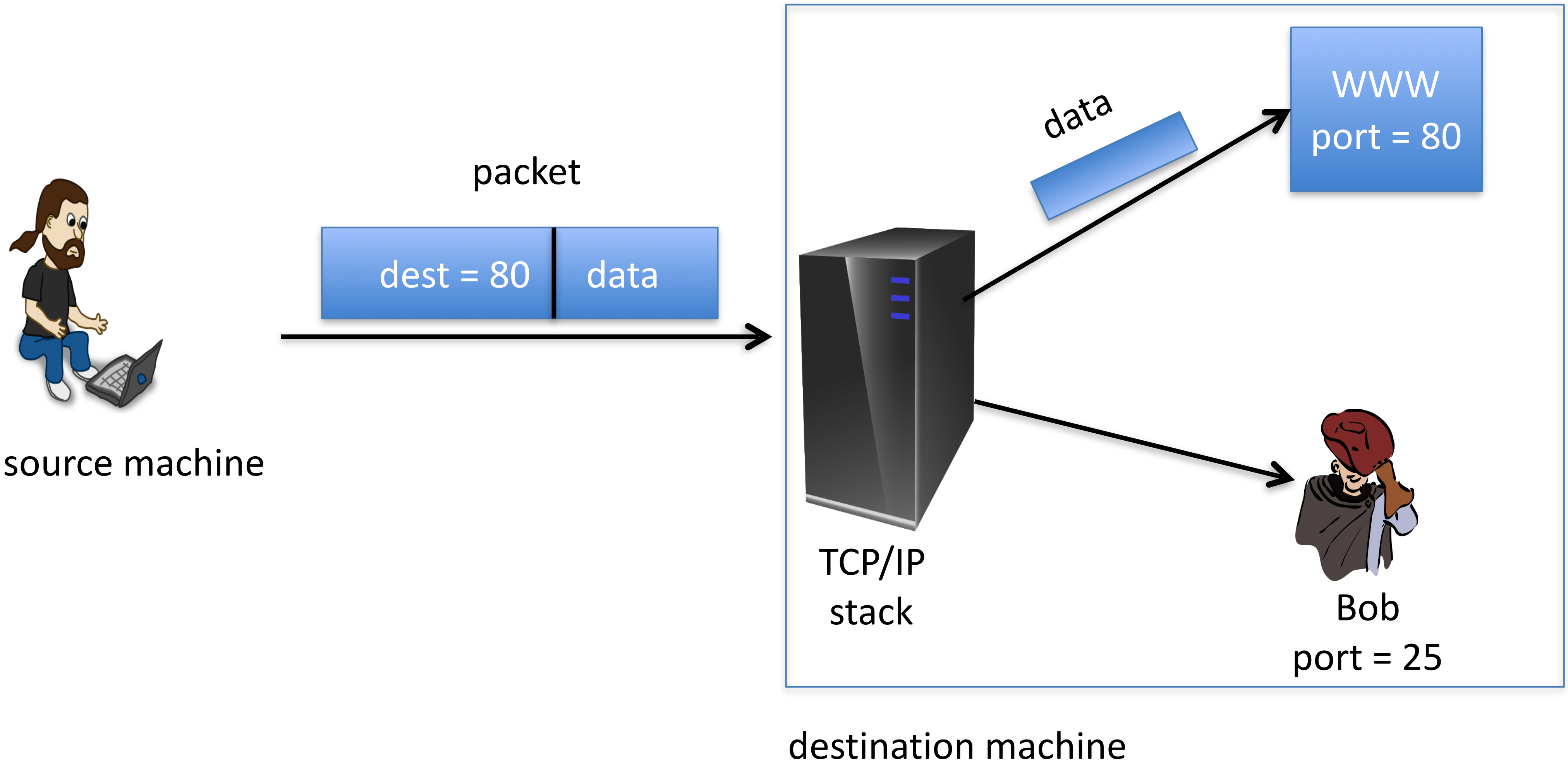
Story So Far …

- **Confidentiality:** Secure Encryption (CPA-secure)
  - Single Block messages
  - Multi-block messages
- **Integrity:** Message Authentication Code
  - Using secure block cipher
  - Using collision-resistant hashing

Can we achieve **Confidentiality** and **Integrity** at the same time?

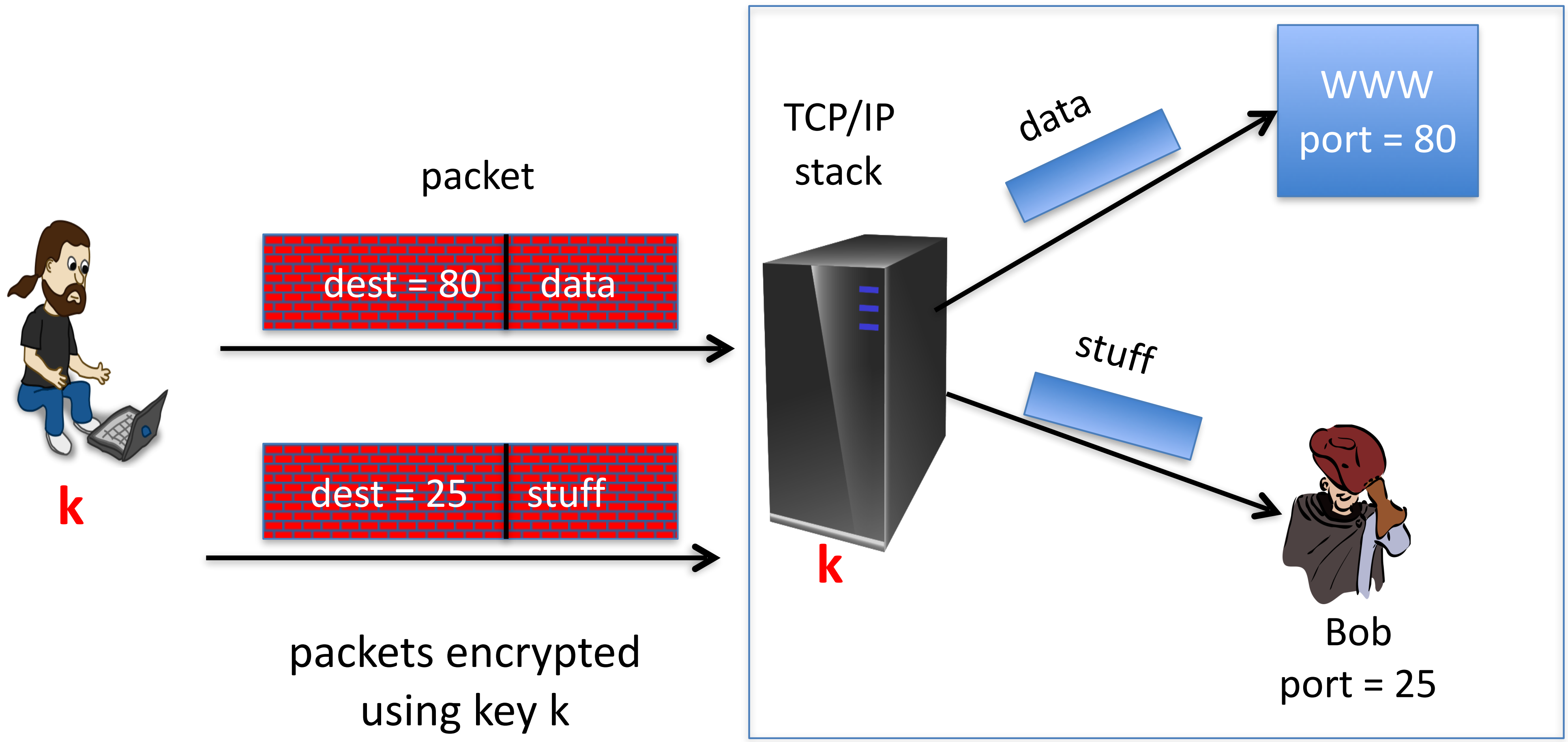
Sample tampering attacks

TCP/IP: (highly abstracted)



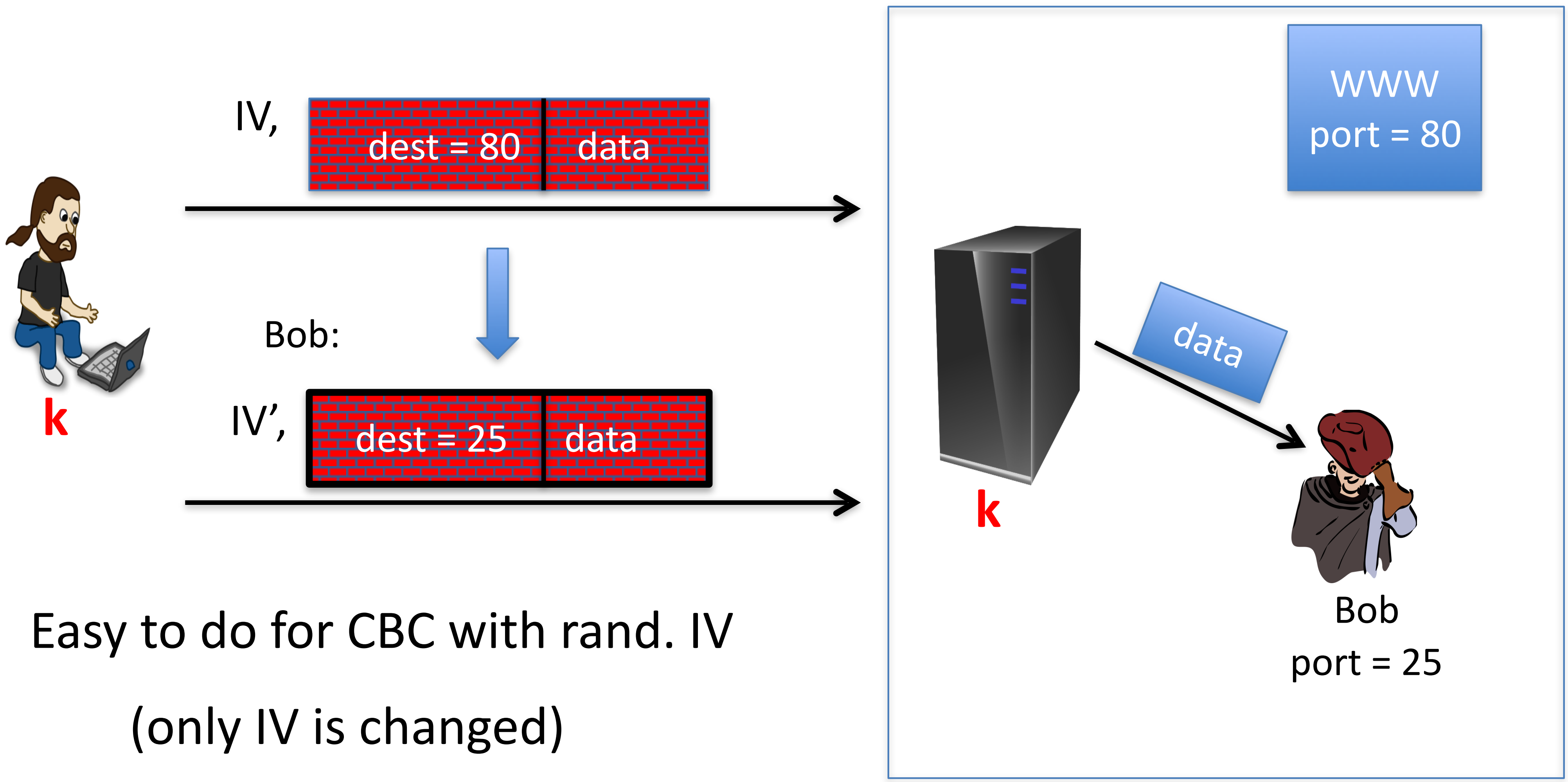
Sample tampering attacks

IPsec: (highly abstracted)



Reading someone else's data

Note: attacker obtains decryption of any ciphertext beginning with "dest=25"



Easy to do for CBC with rand. IV

(only IV is changed)

The lesson

CPA security cannot guarantee secrecy under active attacks.

Only use one of two modes:

- If message needs integrity but no confidentiality:

  use a **MAC**

- If message needs both integrity and confidentiality:

  use **authenticated encryption** modes

The Idea

An **authenticated encryption** system (E,D)

As usual: E: $\mathscr{K} \times \mathscr{M} \longrightarrow \mathscr{C}$

but D: $\mathscr{K} \times \mathscr{C} \longrightarrow \mathscr{M} \cup \{\perp\}$

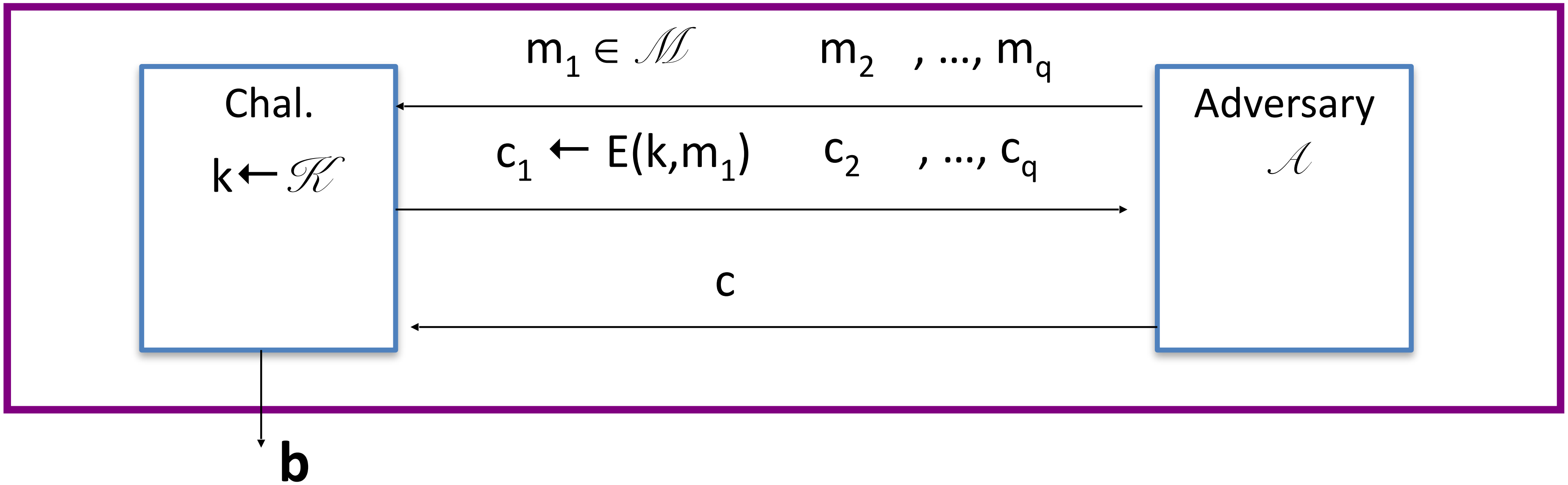
ciphertext is rejected

<u>Security</u>: the system must provide

- semantic security, and
- **ciphertext integrity:**
  attacker cannot create new ciphertexts that decrypt properly

Ciphertext integrity

Let (E,D) be a cipher with message space $\mathcal{M}$.



$$\begin{cases} \mathbf{b}=1 & \text{if } D(k,c) \neq \perp \text{ and } c \notin \{c_1, \ldots, c_q\} \\ \mathbf{b}=0 & \text{otherwise} \end{cases}$$

Def: (E,D) has **ciphertext integrity** if for all "efficient" $\mathcal{A}$:

$\text{Adv}_{\text{CI}}[\mathcal{A}, E]$ = Pr[Chal. outputs 1] is "negligible."

Authenticated Encryption

Def: cipher (E,D) provides **<u>authenticated encryption</u> (AE)** if it is

(1) semantically secure under CPA, and

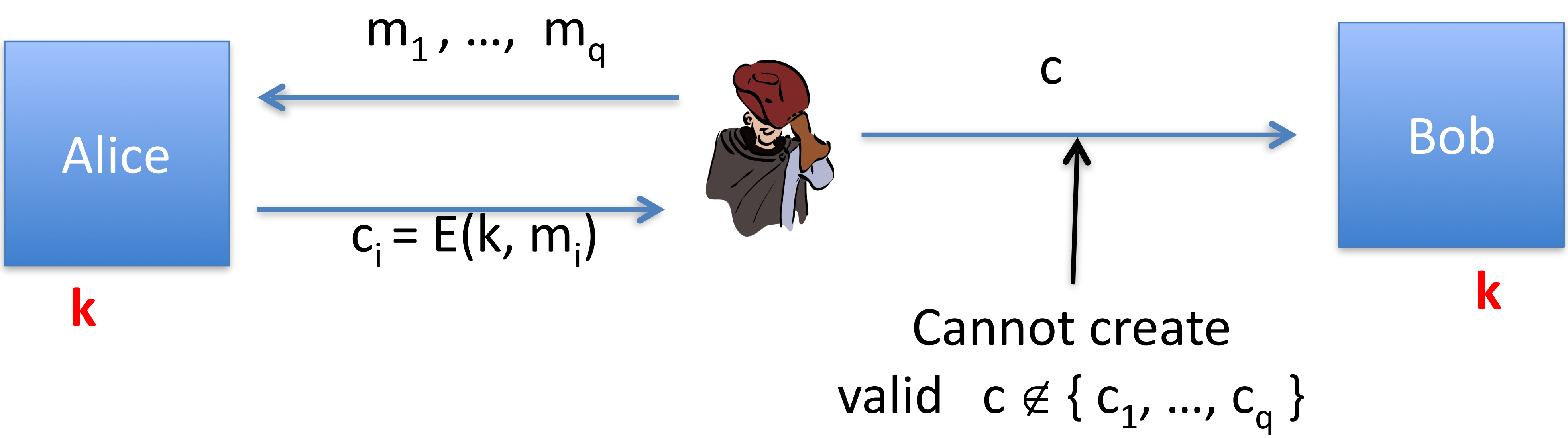
(2) has ciphertext integrity

Bad example: CBC with rand. IV does not provide AE

- $D(k,\cdot)$ never outputs $\perp$, hence adv. easily wins CI game

Implication 1: authenticity

Attacker cannot fool Bob into thinking a message was sent from Alice



$\Rightarrow$ if $D(k,c) \neq \perp$ Bob knows message is from someone who knows k

(but message could be a replay)

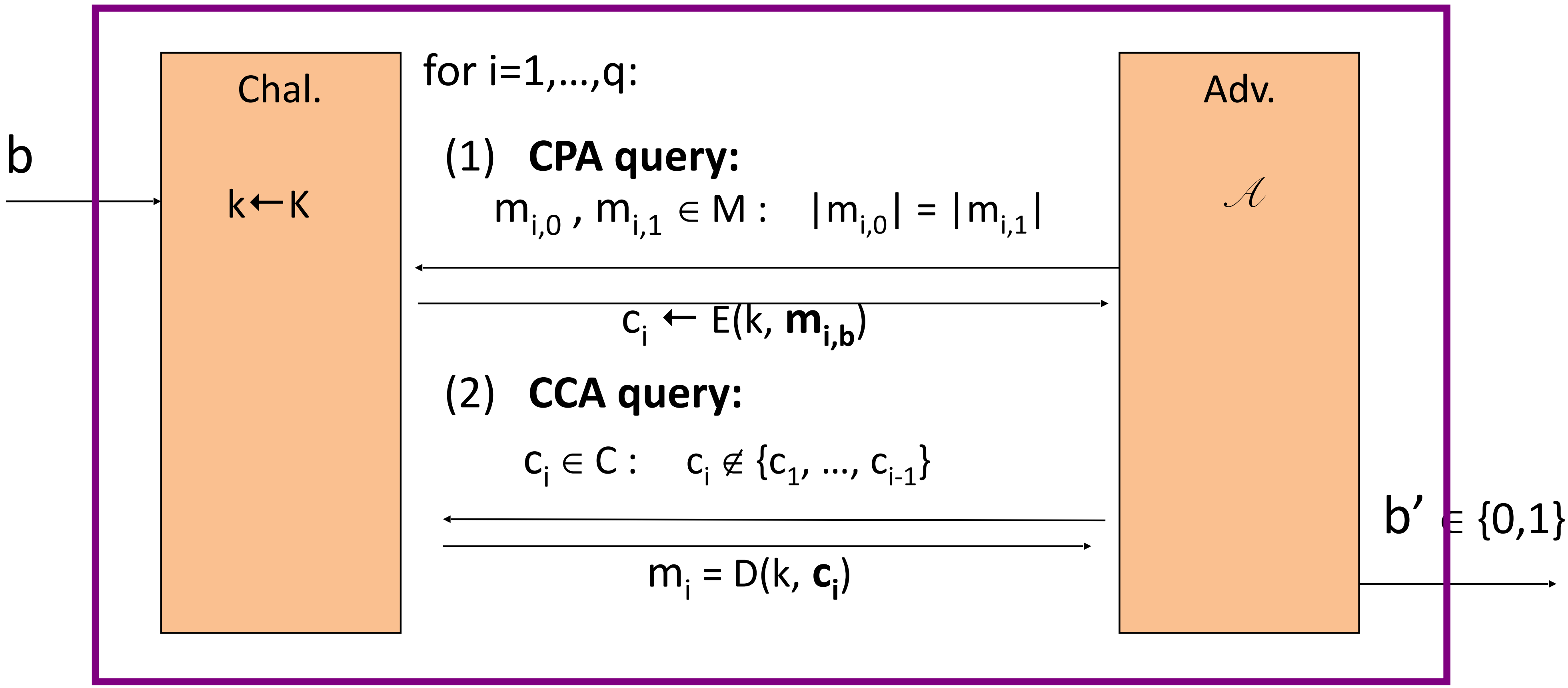
Implication 2

Authenticated Encryption $\Rightarrow$

Security against **Chosen Ciphertext Attacks**

Chosen Ciphertext security -- Definition

For b=0,1 define EXP(b):



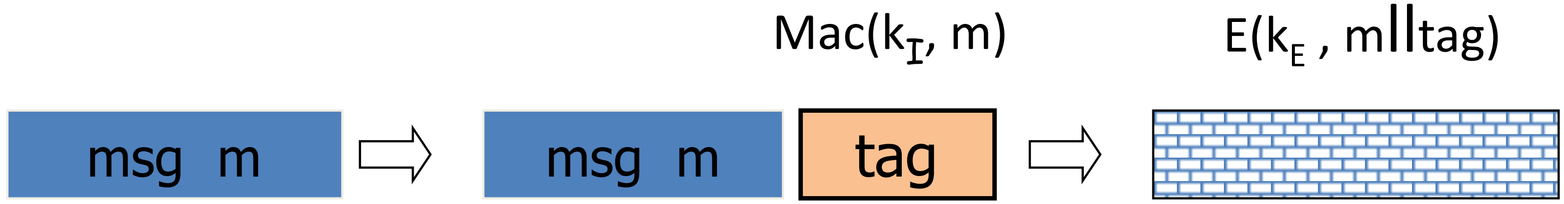
E is CCA secure if for all "efficient" $\mathscr{A}$:

$\mathrm{Adv}_{\mathrm{CCA}}[A,E] = \big|\Pr[\mathrm{EXP}(0)=1] - \Pr[\mathrm{EXP}(1)=1]\big|$ is "negligible."

Combining MAC and Enc (CCA)

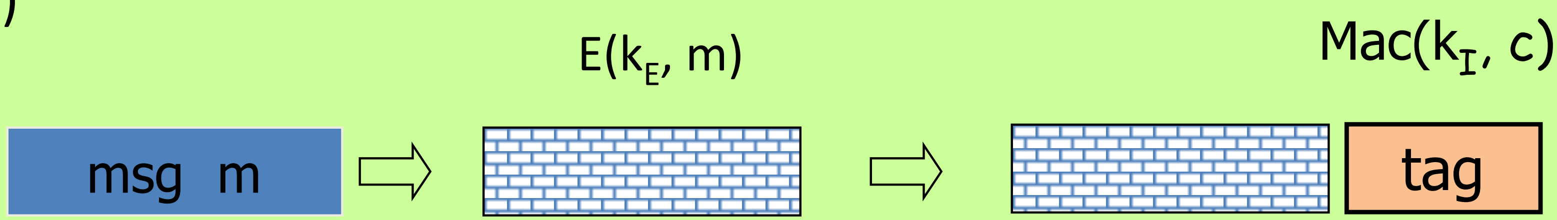
Encryption key k_E. MAC key = k_I

Option 1: (SSL)

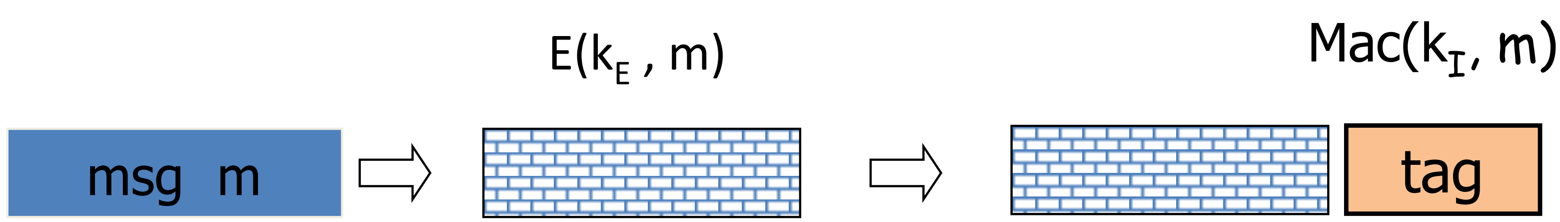


Option 2: (IPsec)

always correct



Option 3: (SSH)



Standards (at a high level)

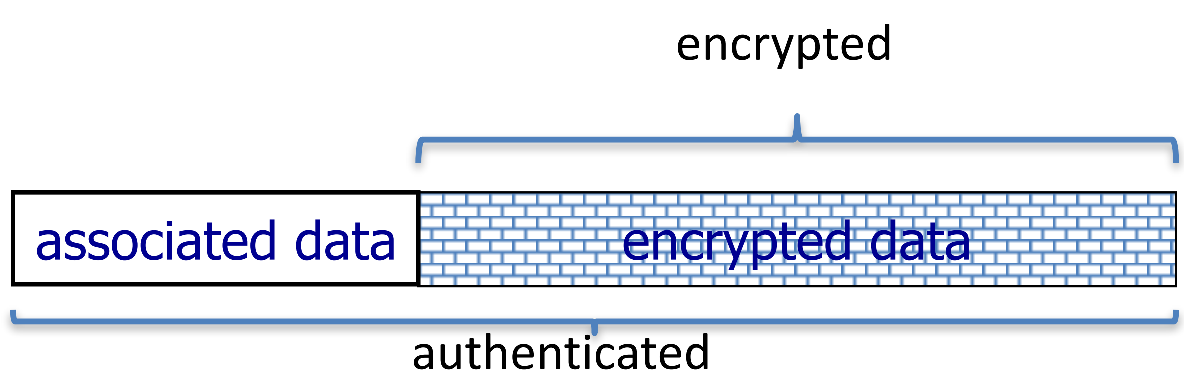
- **GCM**: CTR mode encryption then CW-MAC

  (accelerated via Intel's PCLMULQDQ instruction)

- **CCM**: CBC-MAC then CTR mode encryption
  (802.11i)

- **EAX**: CTR mode encryption then CMAC

All support AEAD: (auth. enc. with associated data). All are nonce-based.



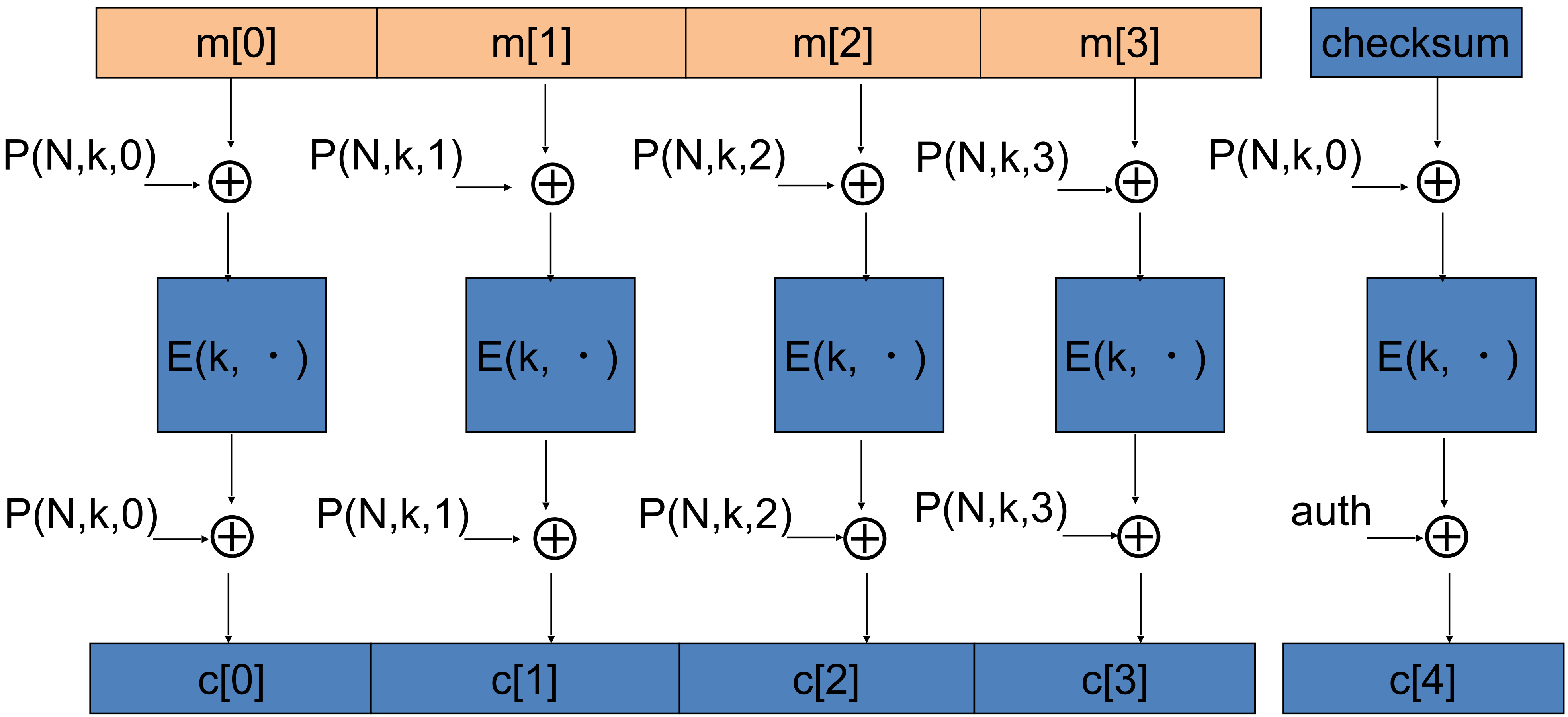
An example API (OpenSSL)

int **AES_GCM_Init**(AES_GCM_CTX *ain,
    unsigned char ***nonce**,   unsigned long noncelen,
    unsigned char ***key**,   unsigned int klen)

int **AES_GCM_EncryptUpdate**(AES_GCM_CTX *a,
    unsigned char ***aad**,   unsigned long aadlen,
    unsigned char ***data**,   unsigned long datalen,
    unsigned char ***out**,   unsigned long *outlen)

OCB: a direct construction from a PRP

More efficient authenticated encryption: one E() op. per block.

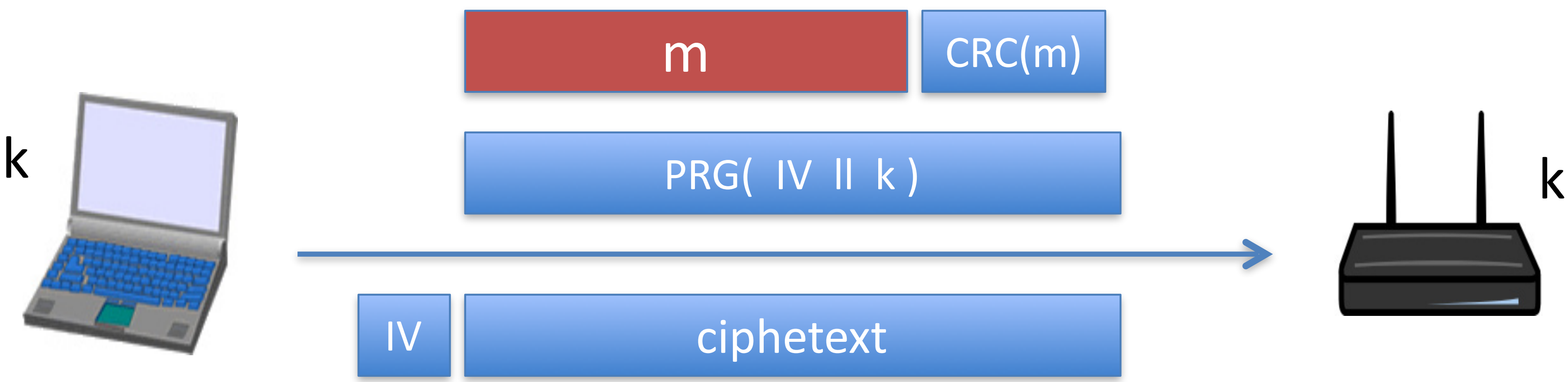


OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption, [RBBK01, CCS]

IETF RFC7253

802.11b WEP: how not to do it

802.11b WEP:



Previously discussed problems:

two time pad and related PRG seeds

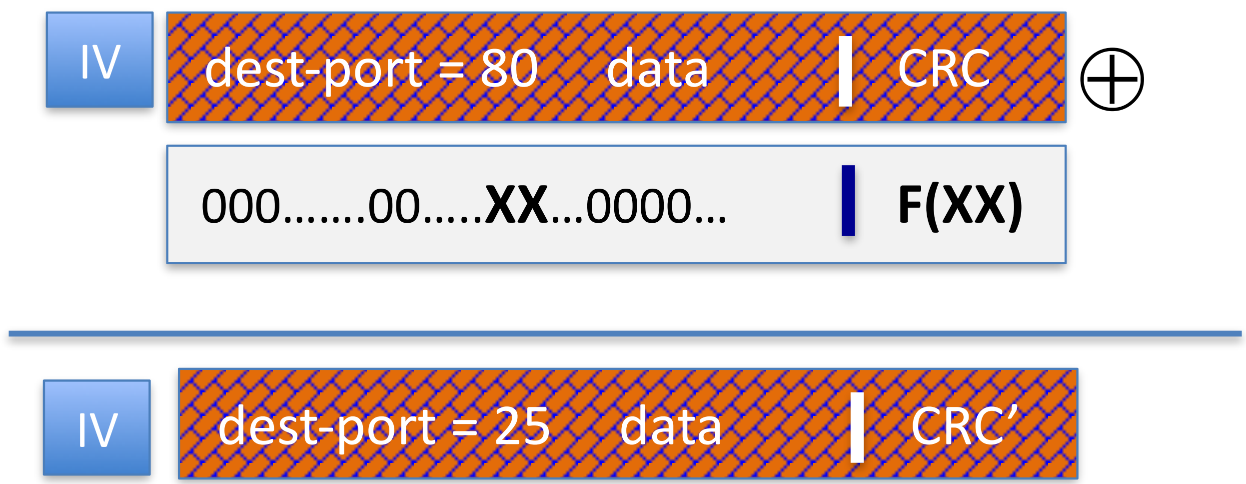
Active attacks

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

WEP ciphertext:

attacker:

XX = $25 \oplus 80$



Upon decryption: CRC is valid, but ciphertext is changed !!