Symmetric Encryption: CPA, Padding Oracle Attacks, and CCA

Yan Huang

Credits: Vitaly Shmatikov (Cornell Tech)

Quiz: Write down the Shanon's definition of perfect security.

Shannon's perfect secrecy

Let (E, D) be a cipher over $(\mathscr{K}, \mathscr{M}, \mathscr{C})$

(E,D) has perfect secrecy if $\forall\ m_0, m_1 \in \mathscr{M}$, $|m_0| = |m_1|$

$$\{ E(k,m_0) \} \quad = \quad \{ E(k,m_1) \} \qquad \text{where} \quad k \leftarrow \mathscr{K}.$$

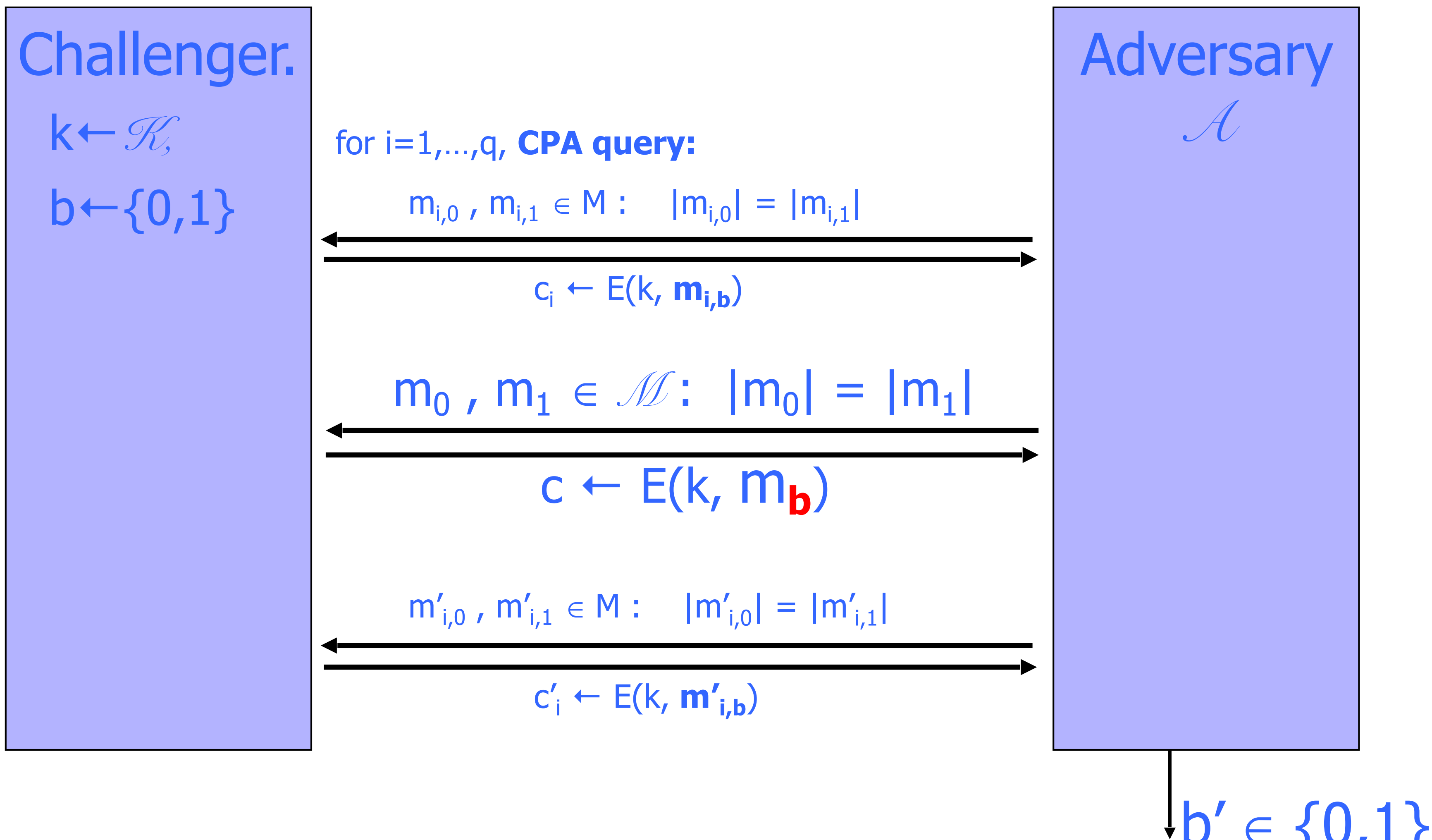
Does this help to define CPA-Security?

The Chosen-Plaintext Game

1. k←KeyGen(1^n). b←{0,1}. Give Enc(k, ·) to $\mathscr{A}$.
2. $\mathscr{A}$ chooses as many plaintexts as he wants, and receives the corresponding ciphertexts via Enc(k, ·).
3. $\mathscr{A}$ picks two plaintexts M_0 and M_1. (Picking plaintexts for which A previously learned ciphertexts is allowed!)
4. $\mathscr{A}$ receives the ciphertext of M_b, and continues to have accesses to Enc(k, ·).
5. $\mathscr{A}$ outputs b'.

$\mathscr{A}$ wins if b'=b.

CPA Secure (one-time key)

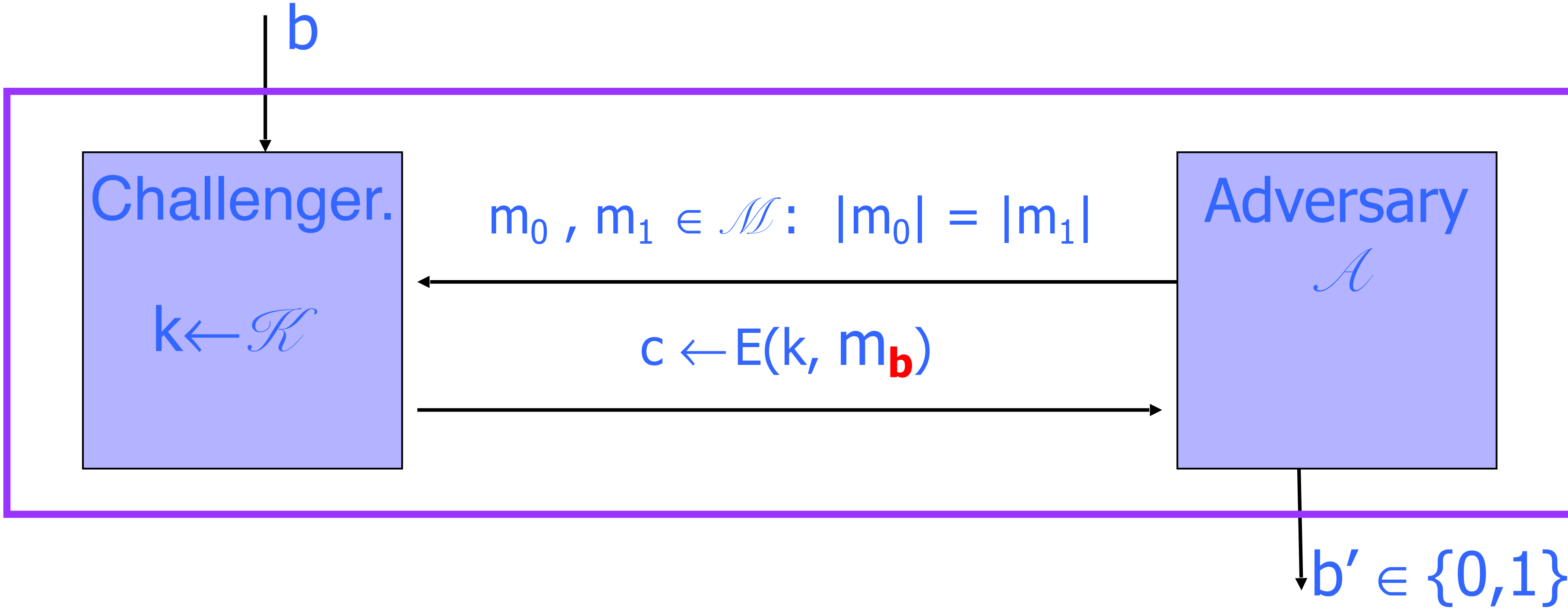


For all efficient adversary $\mathcal{A}$,

| Pr[b=b'] - 1/2 | is "negligible".

Alternative Definition of CPA-Security (one-time key)

For $b \leftarrow \{0,1\}$, define experiment EXP(b) as:



Define W_b := [event that EXP(b)=1].

$$\mathrm{Adv}(\mathcal{A}, \mathbf{E}) := \left| \Pr[W_0] - \Pr[W_1] \right| \in [0,1]$$

Alternative Definition of CPA-Security (one-time key)

E is **computational secure** if for all efficient adversary $\mathscr{A}$

Adv ($\mathscr{A}$, E) is "negligible".

Negligible

- Concrete sense:
  e.g., $< 2^{-40}$
- Asymptotic sense:
  negl(n) < any inverse polynomial of n, as long as n is sufficiently large.

Defining Perfect Security (one-time key)

E is **perfectly secure** if for all adversary $\mathscr{A}$

$$\text{Adv}(\mathscr{A}, \text{E}) \text{ is } 0.$$

$\Leftrightarrow$ For all explicit m_0, $m_1 \in M$:

$$\{\, E(k,m_0) \,\} \;=\; \{\, E(k,m_1) \,\}, \text{ where } \; k \leftarrow \mathscr{K}.$$

A Simple Example

- Any deterministic, stateless symmetric encryption scheme is insecure
  - Attacker can easily distinguish encryptions of different plaintexts from encryptions of identical plaintexts
  - This includes ECB mode of common block ciphers!

Attacker A interacts with Enc(-)

query Enc(0)

Let x=0, y=1 be any two different plaintexts

Send x, y to the challenger

If C_1=Enc(0) then b=0 else b=1

- The advantage of this attacker A is 1

Message Padding

- What if the original message can't be divided into a whole-number of blocks?
  - Block size: *L* bytes
  - Append *b* bytes to the message to make whole blocks.

Message Padding

- What if the original message is already exactly an whole-number of blocks?
  - Block size: *L* bytes
  - Still append *L* bytes to the message

How to Un-pad?

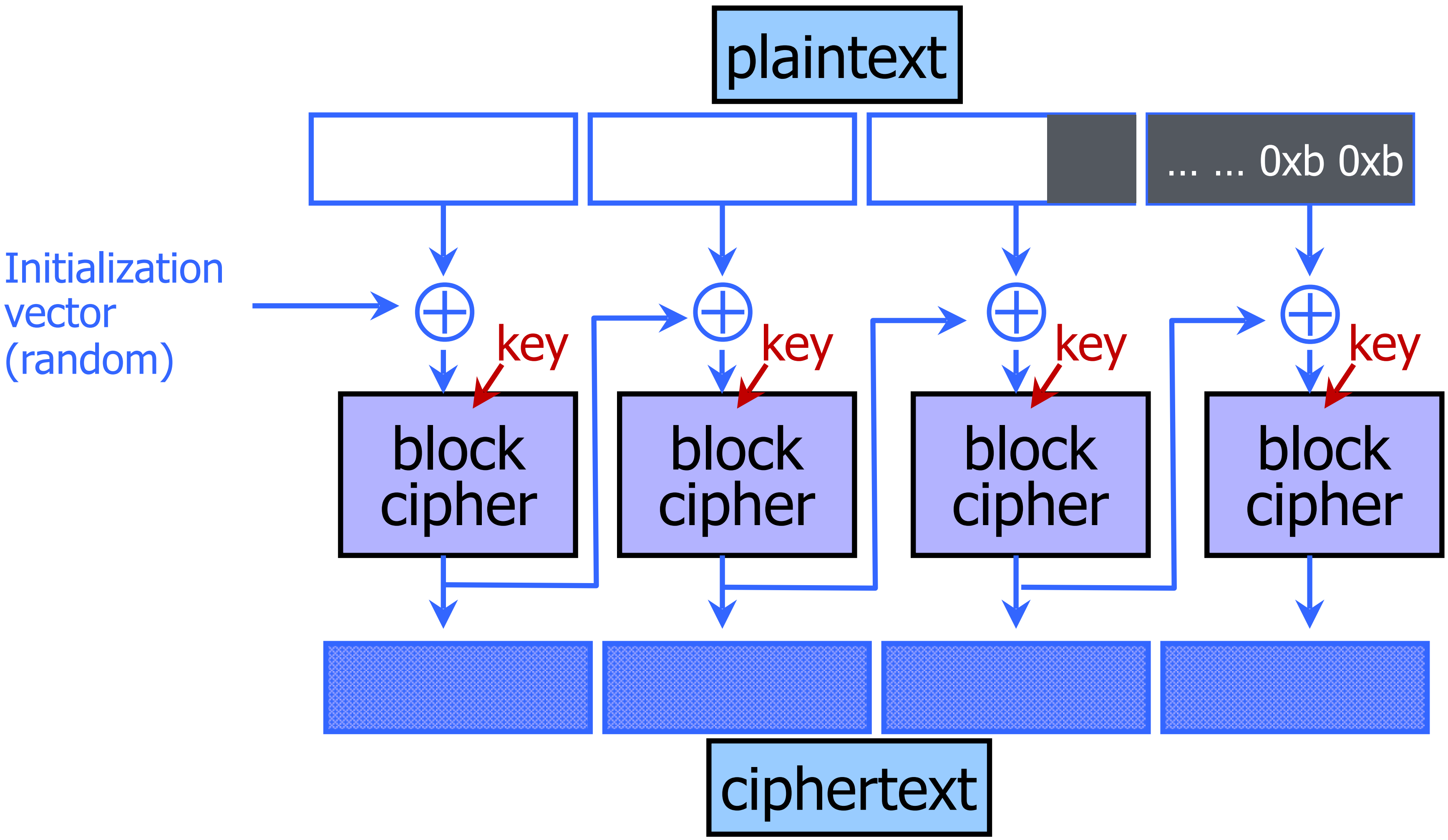
1. Read the last byte of the padded message to learn *b*

2. Verify that 0x*b* repeats b times in the last block

What if this check fails?

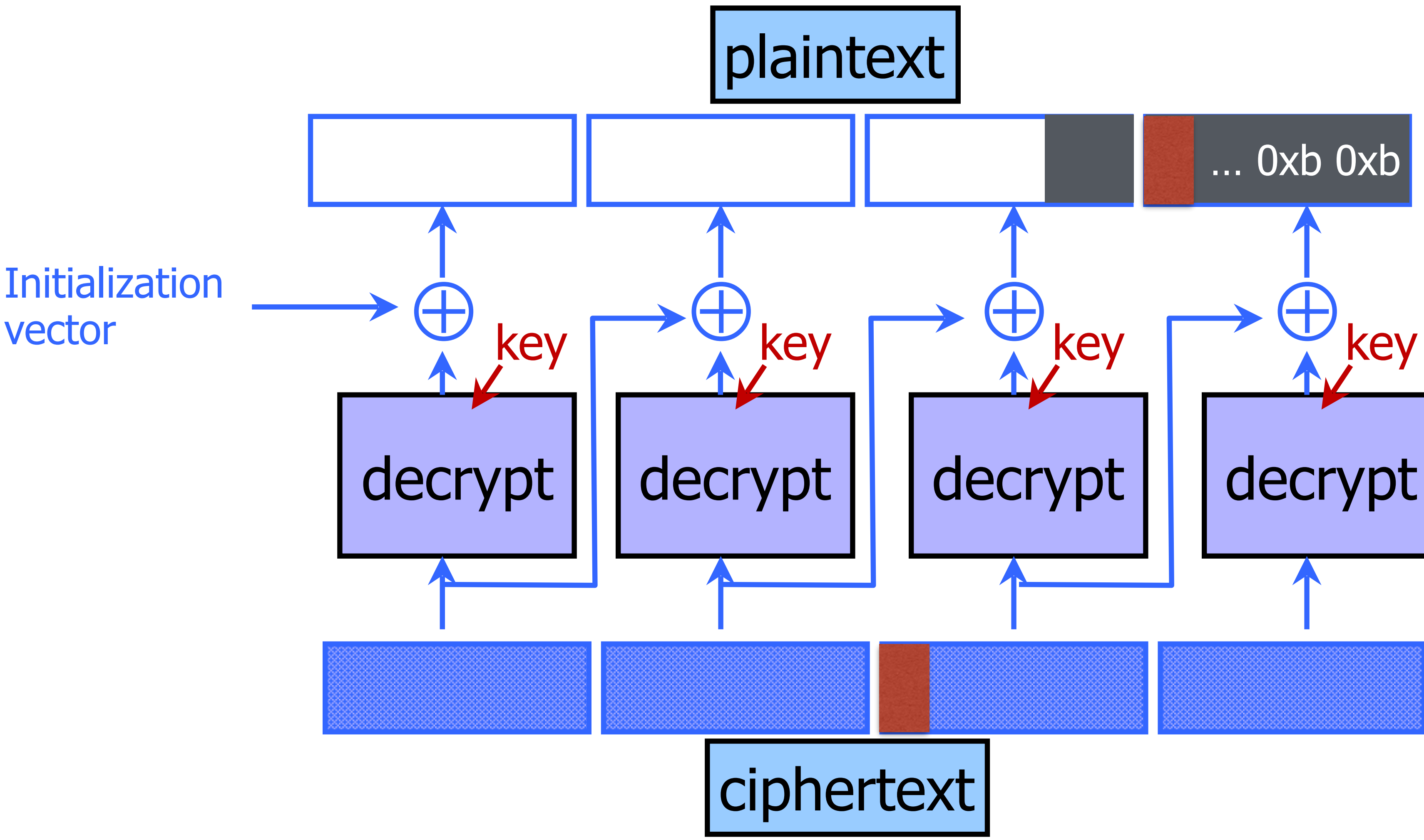
3. Remove the last block plus *b* types in the second to the last block

Padding Oracle Attacks to CBC Encryptions



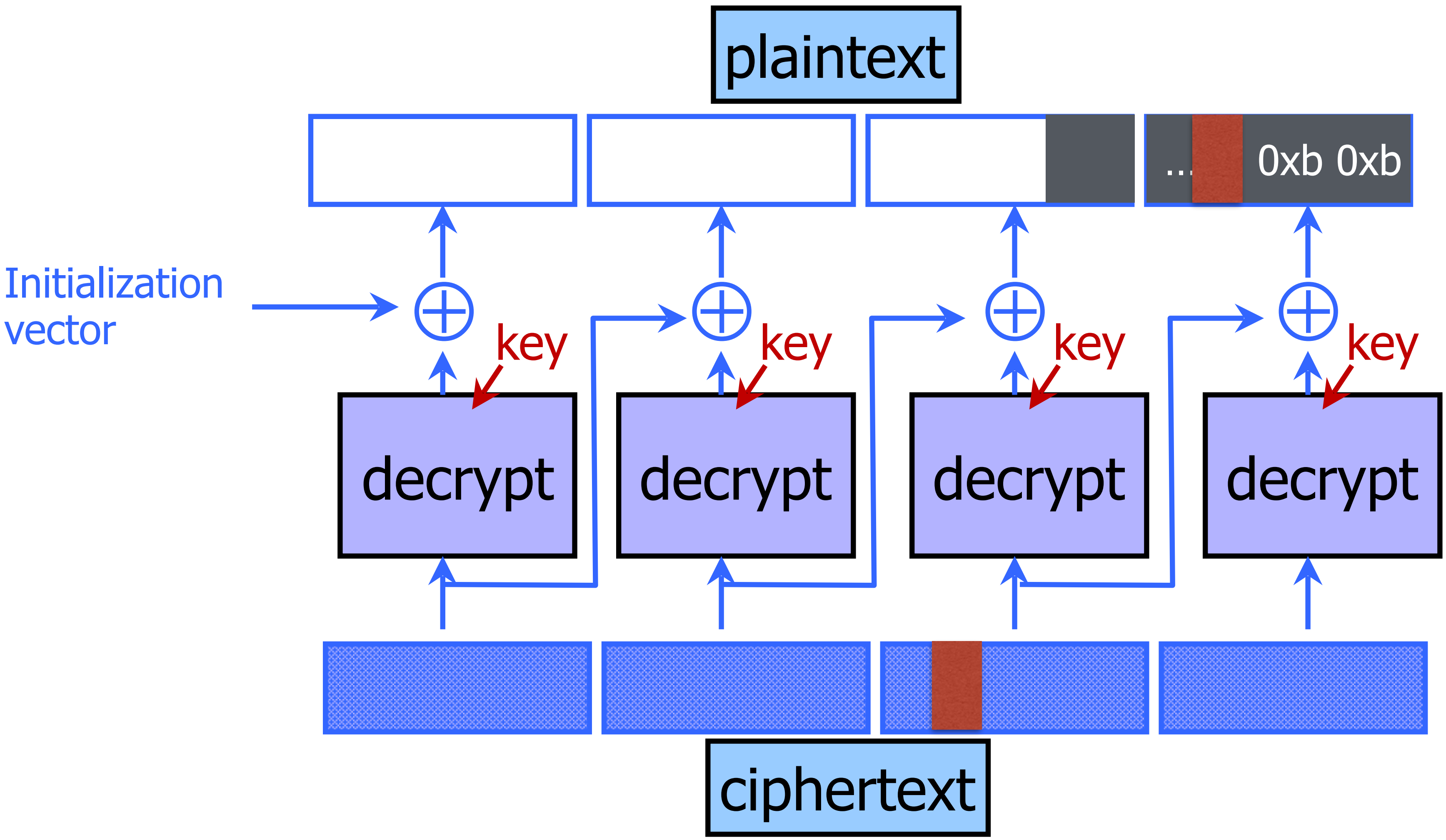
- Can the attacker learn the length of the padding?

Padding Oracle Attacks to CBC Encryptions



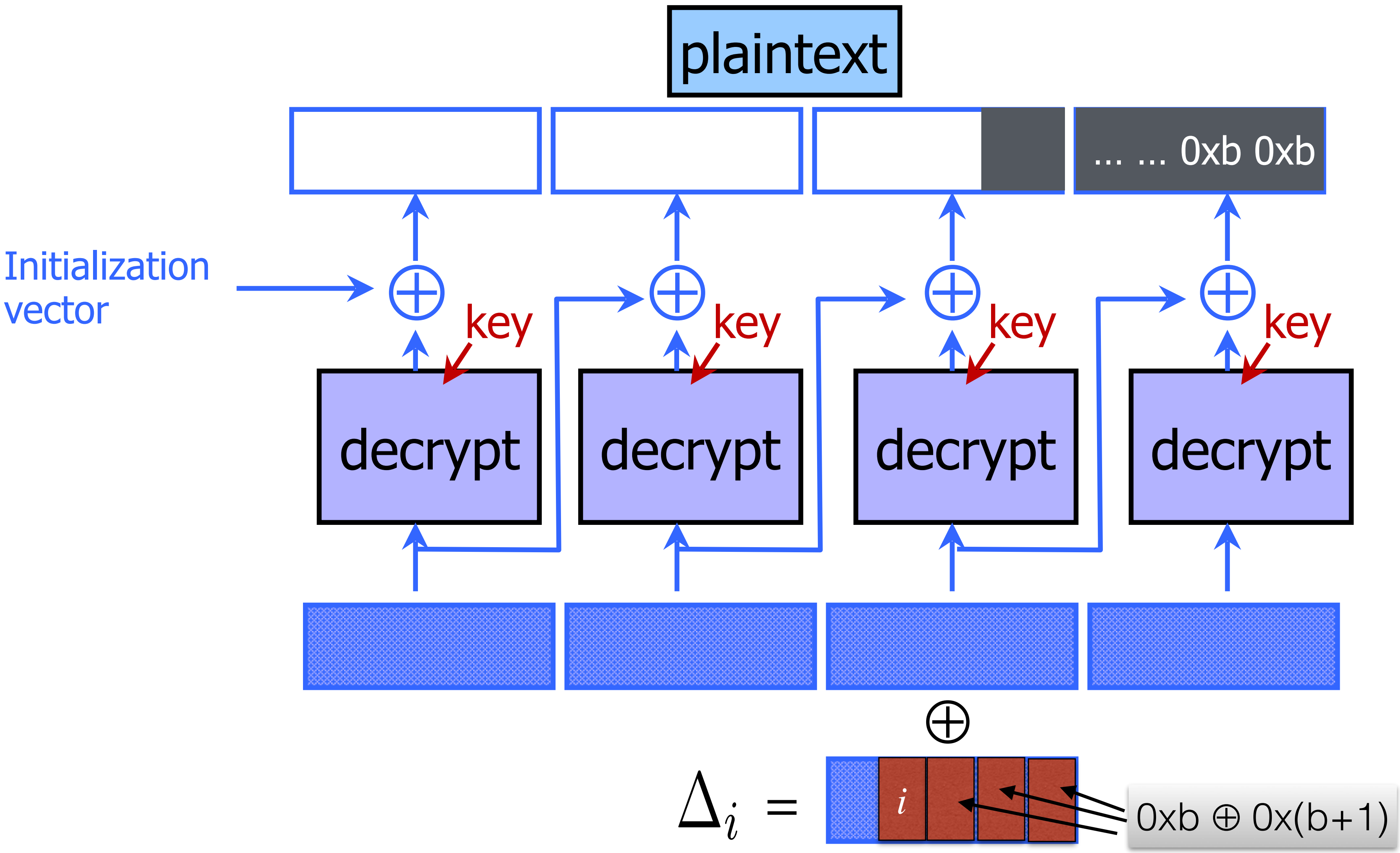
What happens if flip a bit in the left-most byte of the second to the last ciphertext block?

Padding Oracle Attacks to CBC Encryptions



Shift left the tampered byte until you find *b*

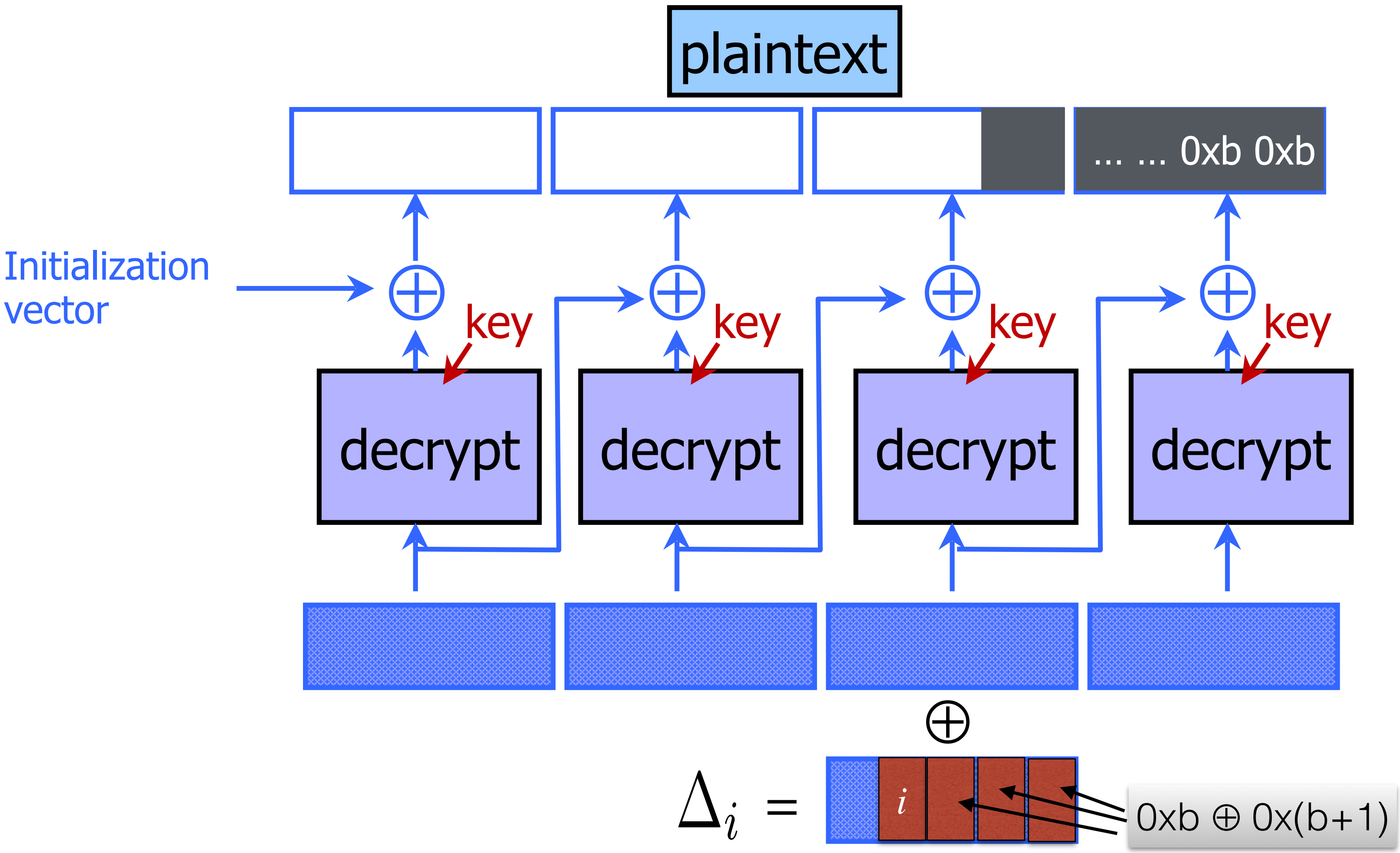
Padding Oracle Attacks to CBC Encryptions



$\Delta_i =$

Assume the attack knows *b*, can he manipulate the ciphertext to set the padding bytes to “0x(b+1) 0x(b+1) … 0x(b+1)”?

Padding Oracle Attacks to CBC Encryptions



Every byte can be learn by trying out i=0,1,2,...,127.

The Lesson

Innocent looking user-friendly feedback messages could be exploited and extremely insecure!

We need some notion of security stronger than CPA.

CCA Security (one-time key)

Challenger.

$k \leftarrow \mathcal{K}$

$b \leftarrow \{0,1\}$

Adversary $\mathcal{A}$

for i=1,…,q, **CCA query:**

$m_{i,0}\ ,\ m_{i,1} \in M :\quad |m_{i,0}| = |m_{i,1}|$

$c_{i,0}\ ,\ c_{i,1} \in C$

$c'_i \leftarrow E(k, \mathbf{m_{i,b}})\qquad m'_i \leftarrow Dec(k, \mathbf{c_{i,b}})$

$m_0\ ,\ m_1 \in \mathcal{M} :\quad |m_0| = |m_1|$

$c \leftarrow E(k, m_{\mathbf{b}})$

$m'_{i,0}\ ,\ m'_{i,1} \in M :\quad |m'_{i,0}| = |m'_{i,1}|$

$c_{i,0}\ ,\ c_{i,1} \in C$

$c'_i \leftarrow E(k, \mathbf{m'_{i,b}})\qquad m'_i \leftarrow Dec(k, \mathbf{c_{i,b}})$

$b' \in \{0,1\}$

For all efficient adversary $\mathcal{A}$,

| Pr[b=b'] - 1/2 | is "negligible".

The Chosen-Ciphertext Game

1. k←KeyGen(1^n). b←{0,1}. Give Enc(k, ·) to $\mathscr{A}$.
2. $\mathscr{A}$ is given oracle access to Enc(k, ·) and Dec(k, ·).
3. $\mathscr{A}$ picks two plaintexts M_0 and M_1. (Picking plaintexts for which A previously learned ciphertexts is allowed!)
4. $\mathscr{A}$ receives the ciphertext of M_b, and continues to have accesses to Enc(k, ·) and Dec(k, ·).
5. $\mathscr{A}$ outputs b'.

$\mathscr{A}$ wins if b'=b.