Recap of Lecture 1:

Encryption scheme

- → msg. space $\mathcal{M}$
- → key space $\mathcal{K}$
- → ciphertext space $\mathcal{C}$

$$\mathrm{Enc}(k \in \mathcal{K}, \; m \in \mathcal{M}) \longrightarrow ct \in \mathcal{C}$$

$$\mathrm{Dec}(k \in \mathcal{K}, \; ct \in \mathcal{C}) \longrightarrow m \in \mathcal{M}$$

Security Definition :

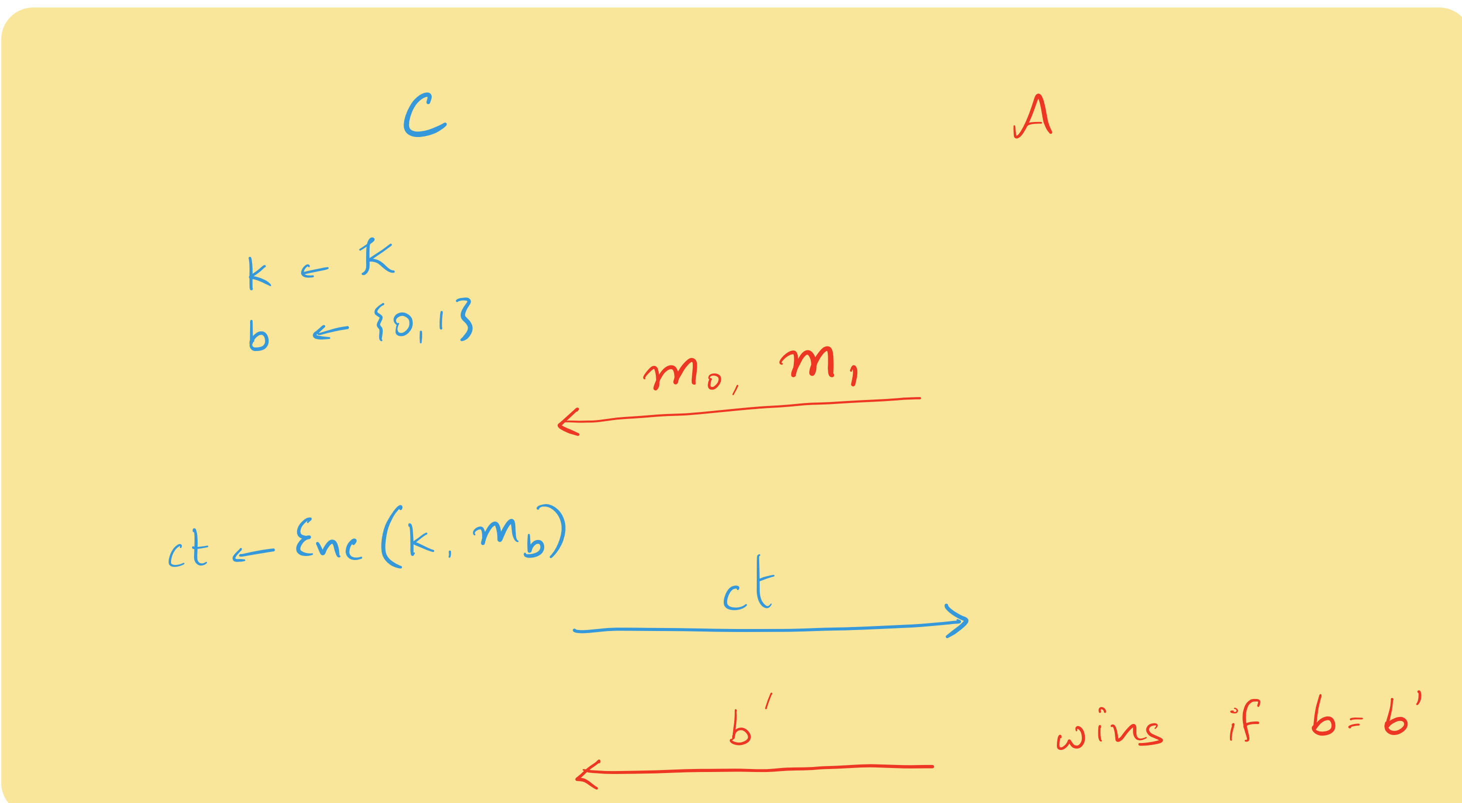
Multiple security def. possible

Lecture 1 : ONE TIME PERFECT SECURITY

Sec Def. 1 (Enc, Dec) satisfies one - time perfect security if

FOR ALL $\mathcal{A}$,

$$\Pr[\mathcal{A} \text{ wins ONE - TIME SEC. GAME}] = 1/2$$



ONE TIME SEC. GAME

Shannon (Thm 1):

$\exists$ one-time perfectly sec. enc. scheme with msg. space and key space $\{0,1\}^n$.

$Enc(k, m) = k \oplus m$ $Dec(k, ct) = k \oplus ct$

Shannon (Thm 2):

$\forall$ one-time perfectly secure enc. scheme, the key space is at least as large as the msg. space.

ONE TIME SECURITY IS IMPRACTICAL

→ key cant be reused. need to store many keys.

→ if it is one-time perfectly secure, then key must be as large as message.

Sec Def. 2 (Enc, Dec) satisfies TWO-time perfect security if

FOR ALL A,

$$\Pr[A \text{ wins TWO-TIME SEC. GAME}] = 1/2$$

C		A
$k \leftarrow \mathcal{K}$ $b \leftarrow \{0,1\}$		
	$\xleftarrow{\quad m_{10},\ m_{11} \quad}$	
$ct_1 \leftarrow Enc(k, m_{1b})$		
	$\xrightarrow{\quad ct_1 \quad}$	
	$\xleftarrow{\quad m_{20},\ m_{21} \quad}$	
$ct_2 \leftarrow Enc(k, m_{2b})$		
	$\xrightarrow{\quad ct_2 \quad}$	
	$\xleftarrow{\quad b' \quad}$	wins if $b = b'$

TWO - TIME SEC. GAME

OBS: (Enc, Dec) with deterministic enc. cannot be two-time perfectly secure.

$$\xleftarrow{\quad m_0,\ m_0 \quad}$$

$$\xrightarrow{\quad ct_1 \quad}$$

$$\xleftarrow{\quad m_0,\ m_1 \quad}$$

$$\xrightarrow{\quad ct_2 \quad}$$

if $ct_1 = ct_2$

guess 0

else guess 1

> Qn: Two-time perfect security with randomized enc.?

$\text{Enc}(\text{key } \underline{k},\ \text{msg } \underline{m}\ ;\ \text{rand. } r) \rightarrow ct$

$\text{Dec}(k,\ ct) \rightarrow m$

Correctness: $\forall k,\ \forall m,\ \Pr_r\left[\text{Dec}(k, \text{Enc}(k, m; r)) = m\right] = 1$

$\mathcal{R} = \{0,1\}^n$, $\mathcal{M} = \{0,1\}^n = \mathcal{K}$

$\mathrm{Rot}_k(m \,\|\, r)$

Attack:

$$\xleftarrow{\quad m_0,\ m_0 \quad}$$

$$\xrightarrow{\quad ct_1 \quad}$$

$$\xleftarrow{\quad m_0,\ m_1 \quad}$$

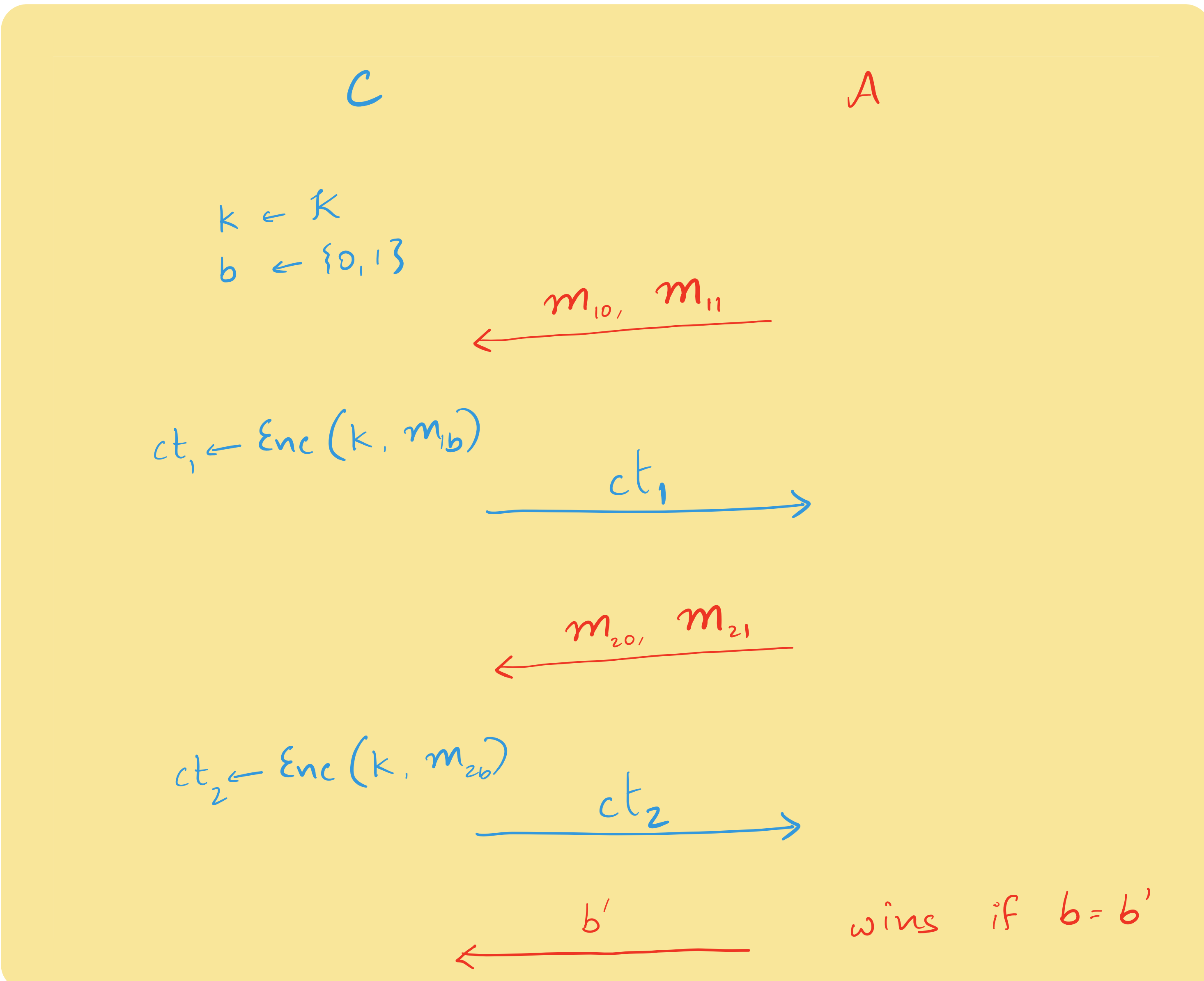
$$\xrightarrow{\quad ct_2 \quad}$$

if $ct_1 = ct_2$
guess '0'
else
pick random b'
send b'

Sec Def. 3 (Enc, Dec) satisfies TWO-time ~~perfect~~ security if

FOR ALL $\mathcal{A}$,

$$\Pr[\mathcal{A} \text{ wins TWO-TIME SEC. GAME}] \ll \frac{1}{2} + \frac{1}{\text{poly}(\text{key size})}$$



TWO-TIME SEC. GAME

Theorem: For any apriori bounded q, $\exists$ (Enc, Dec) that is q-time secure.

- key size grows with q

Sec Def. 3 (Enc, Dec) satisfies MANY-time security if

FOR ALL A,

$$\Pr[A \text{ wins MANY-TIME SEC. GAME}] \approx 1/2$$

$\leq 1/2 + \frac{1}{\text{poly(key size)}}$

$\underline{C}$ $\underline{A}$

$k, \quad b$

$$\xleftarrow{\;m_{i0},\, m_{i1}\;}$$

$ct_i \leftarrow Enc(k, m_{ib})$

$$\xrightarrow{\;ct_i\;}$$

$$\xleftarrow{\;b'\;}$$

wins if $b = b'$

many-time security seems to be the 'right' security notion for encryption

BAD NEWS: MANY TIME SEC. IMPOSSIBLE TO ACHIEVE.

There exist exp. time attacks.

Idea: restrict security def. to allow only poly time adv.

Sec Def. 4 (Enc, Dec) satisfies MANY-time COMPUTATIONAL security if

FOR ALL POLY-TIME A,

$$\Pr[A \text{ wins MANY-TIME SEC. GAME}] \approx 1/2$$

$\leq 1/2 + \frac{1}{\text{poly(key size)}}$

[Goldwasser-Micali 82]: If (Enc, Dec) satisfies Def. 4, then adv. "learns nothing new" from the ciphertexts.

UGLY NEWS : MANY - TIME COMP.
SECURITY SEEMS HARD
TO PROVE.

Proof of many - time comp. sec.

$\Downarrow$

Existence of ONE WAY Functions

$\Downarrow$

$P \neq NP$

Qn: Can we build an enc. scheme and prove it secure assuming $\exists$ one-way functions exist?

$\equiv$

$\exists$ Pseudorandom functions.

OWFs exist if and only if pseudorand. fns. exist. We will build a secure enc. scheme assuming the existence of pseudorandom fns.

Goal: Define pseudorandom functions

Use " " to build secure enc.

PSEUDORANDOM FUNCTION:

key space $\mathcal{K}$.

input space $\mathcal{X}$ $\quad \{0,1\}^n$

output sp. $\mathcal{Y}$

$$F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$$

det. fn.

$F(k, \cdot)$ $\approx$ unif. random fn. from $\mathcal{X}$ to $\mathcal{Y}$

functions that map $\mathcal{X}$ to $\mathcal{Y}$

$$= |\mathcal{Y}|^{|\mathcal{X}|} = 2^{n \cdot 2^n}$$

$\mathcal{C}$ $\qquad\qquad\qquad\qquad$ $\mathcal{A}$

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

if $b=0$,

$\quad k \leftarrow \mathcal{K}$

$\quad f_0 = F(k, \cdot)$

if $b=1$

$\quad f_1 \leftarrow$ unif. rand. fn.

x_i

$f_b(x_i)$

poly

b