CNT 4406, Spring 2024

Symmetric Encryption

Viet Tung Hoang

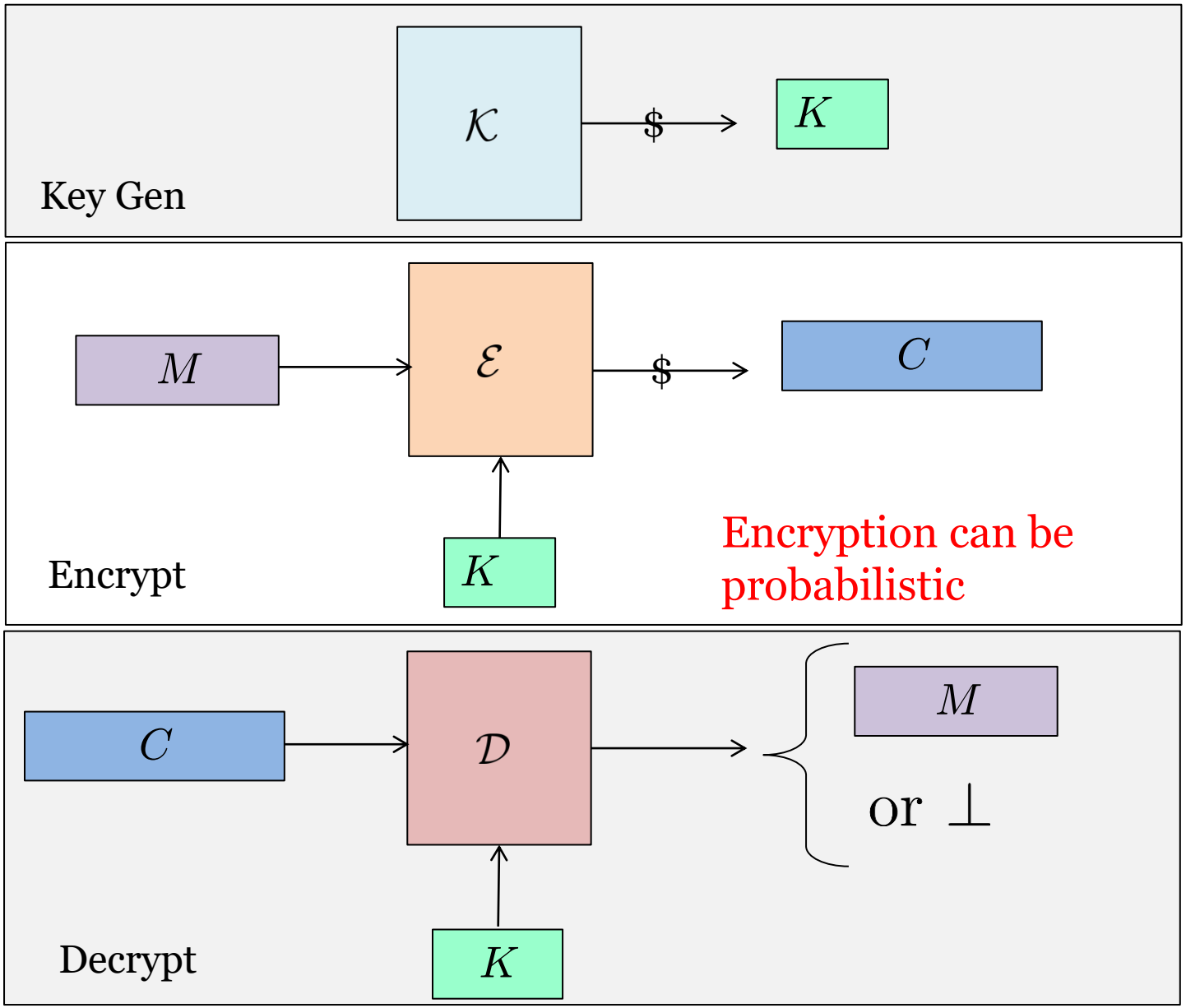
The slides are loosely based on those of Prof. Mihir Bellare (UCSD), Prof. Dan Boneh (Stanford), and Prof. Stefano Tessaro (UW)

Agenda

1. **Modes of Encryption: ECB, CBC, CTR**

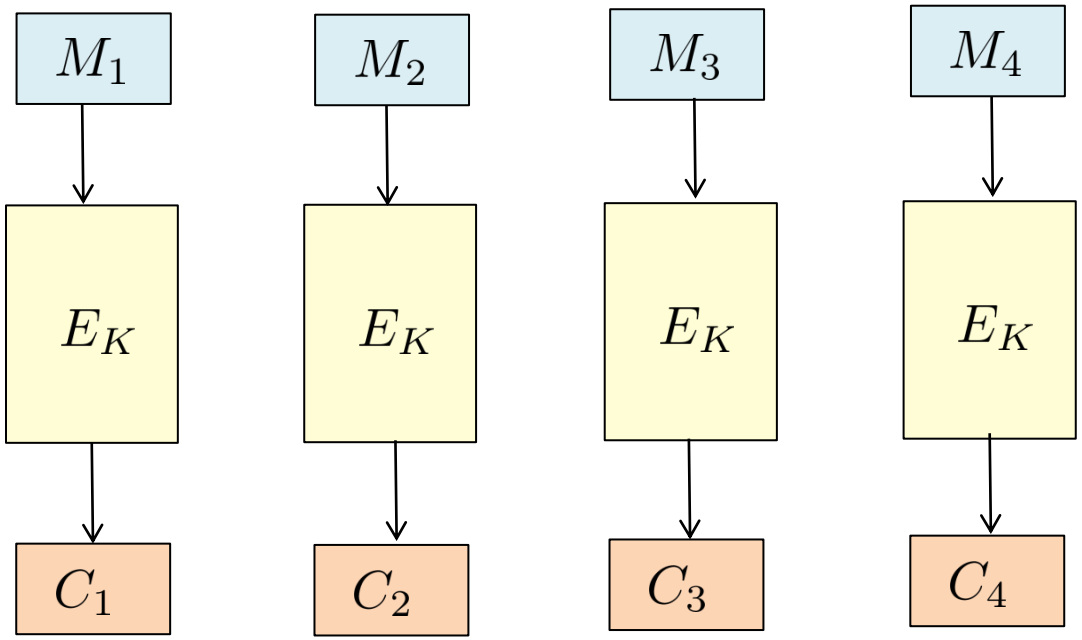
2. Formalizing Security

Encryption Syntax



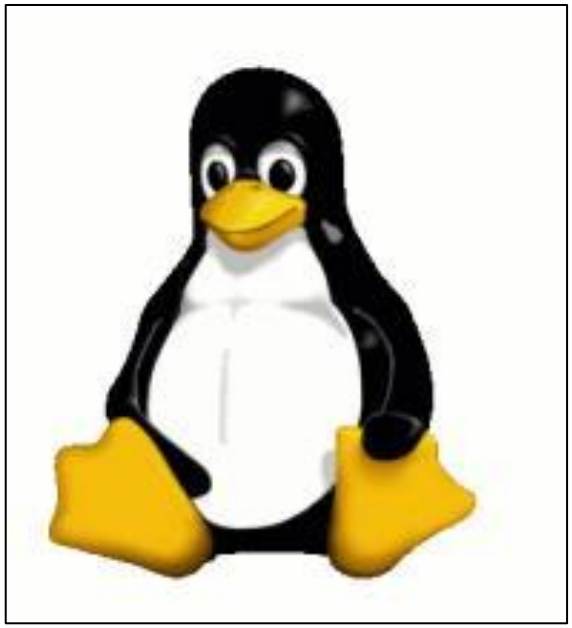
(Bad) Encryption Using Blockcipher: ECB

$$E : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$$

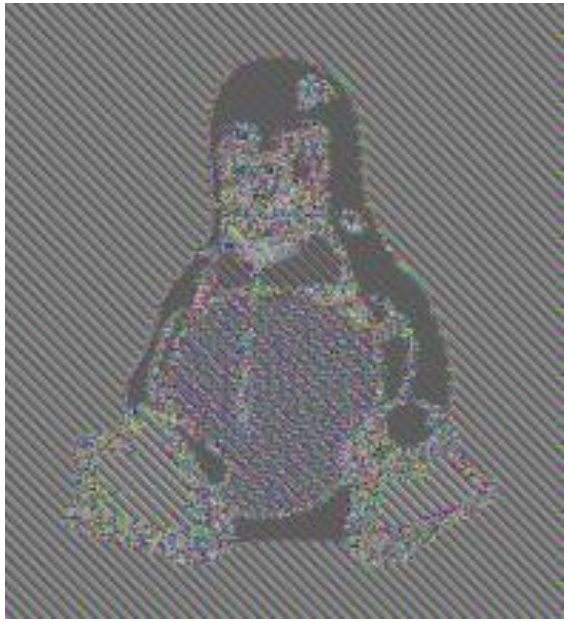


Can encrypt any message whose length is a multiple of n

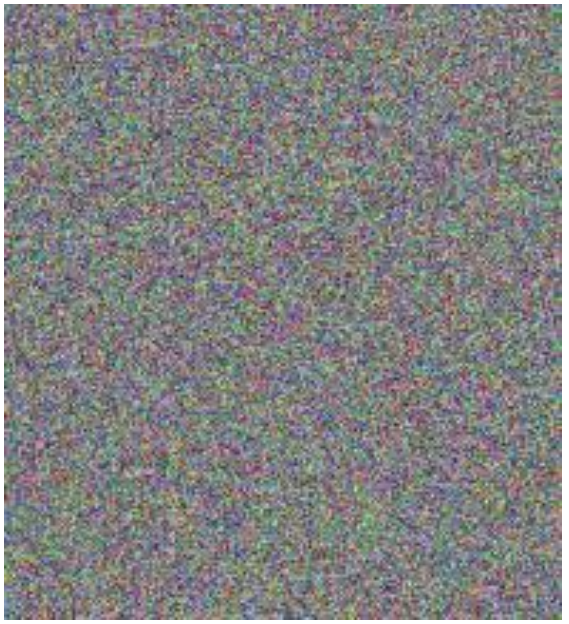
ECB Is Insecure



Message

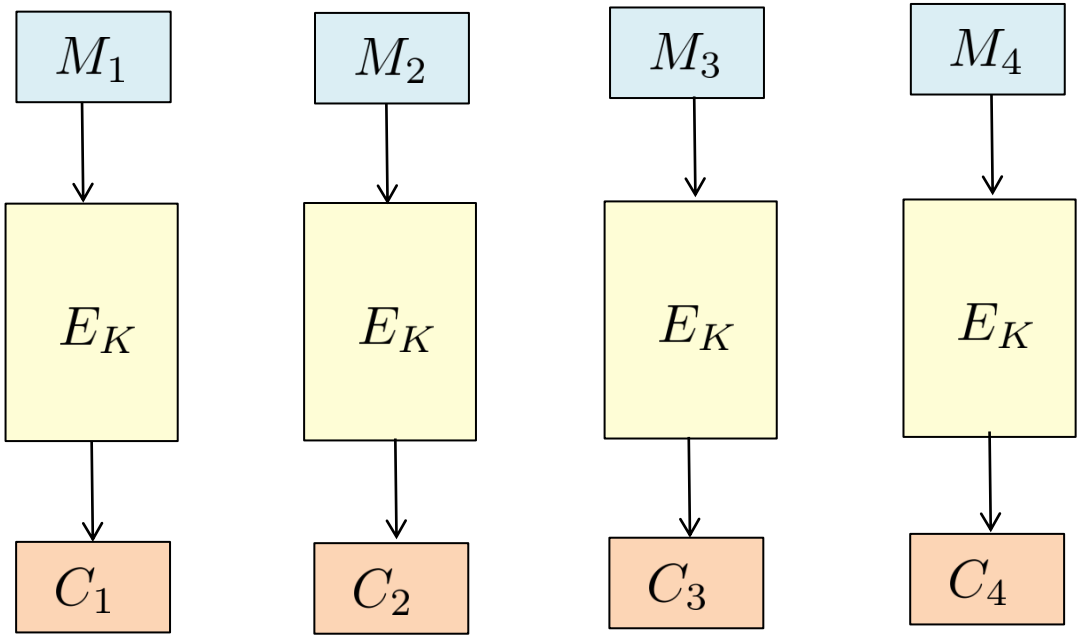


ECB ciphertext



Properly encrypted ciphertext

Why Is ECB So Bad?

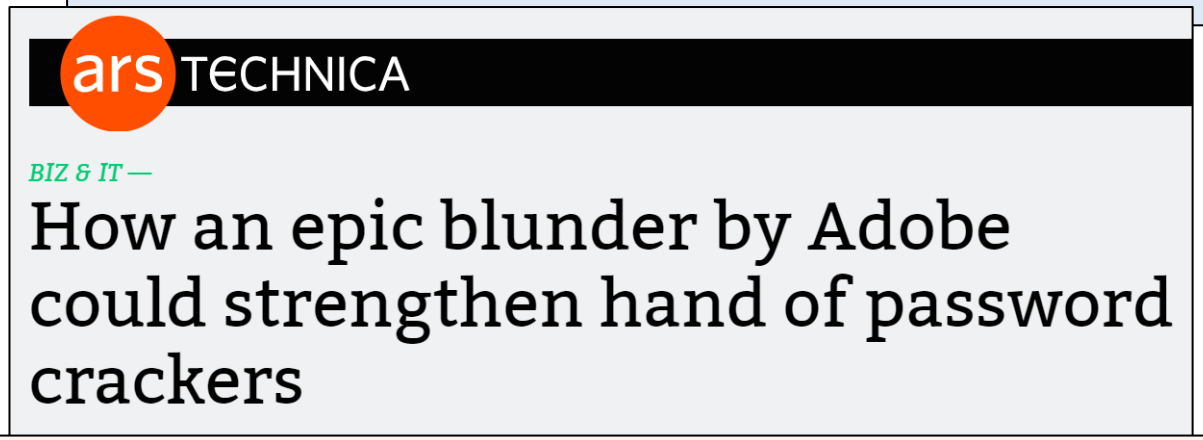


If $M_i = M_j$ then $C_i = C_j$

ECB Horror Stories

Half the apps in Android used ECB to encrypt data

An Empirical Study of Cryptographic Misuse in Android Applications



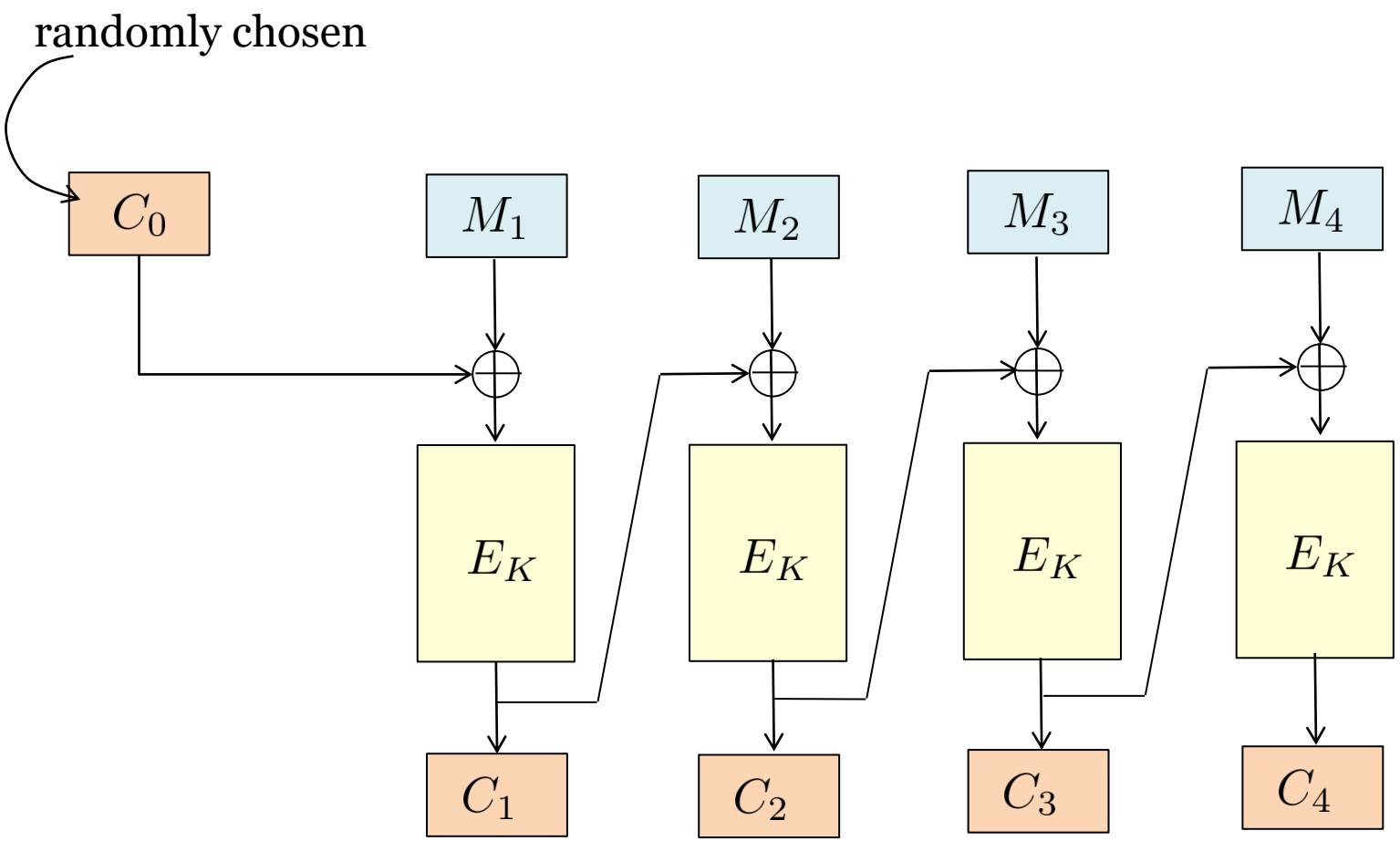
Adobe used ECB to encrypt passwords

Zoom concedes custom encryption is substandard as Citizen Lab pokes holes in it

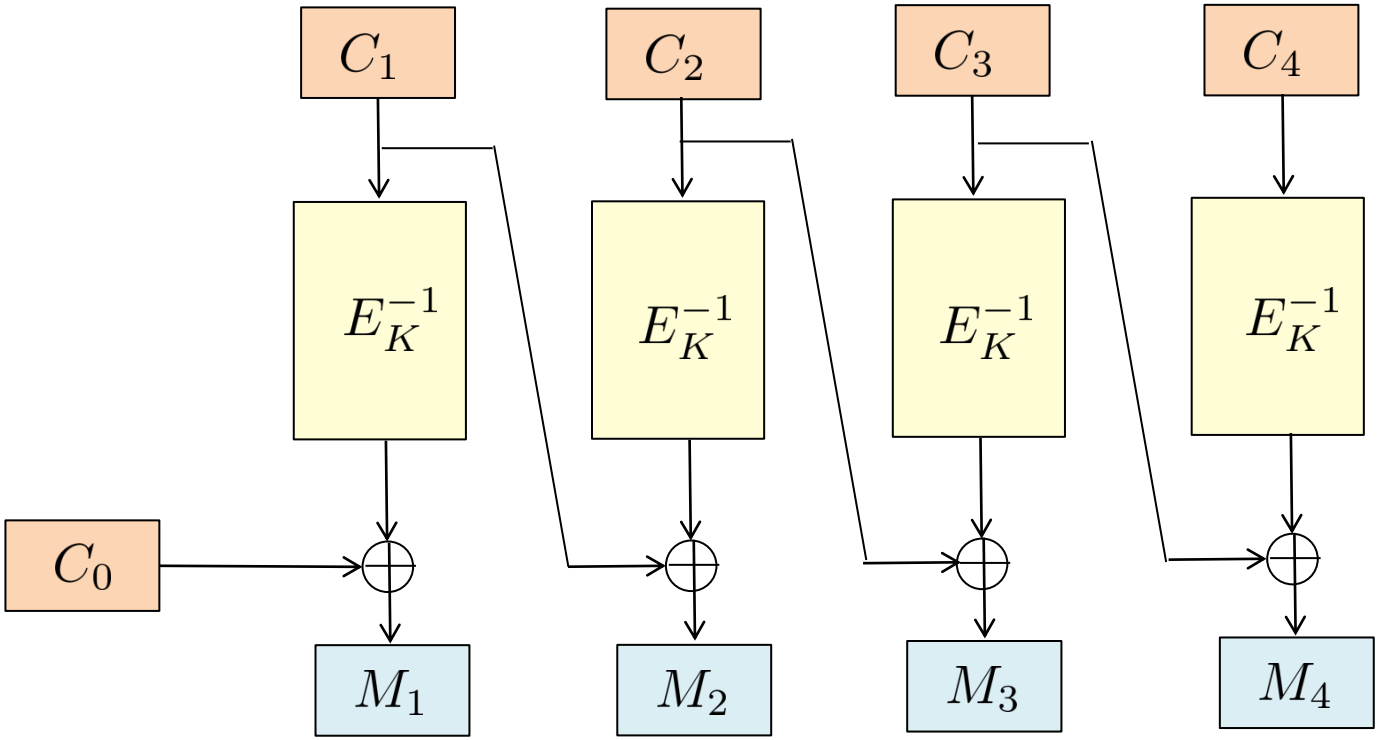
Zoom used ECB to encrypt video conferencing

Randomized Encryption: CBC

sequential



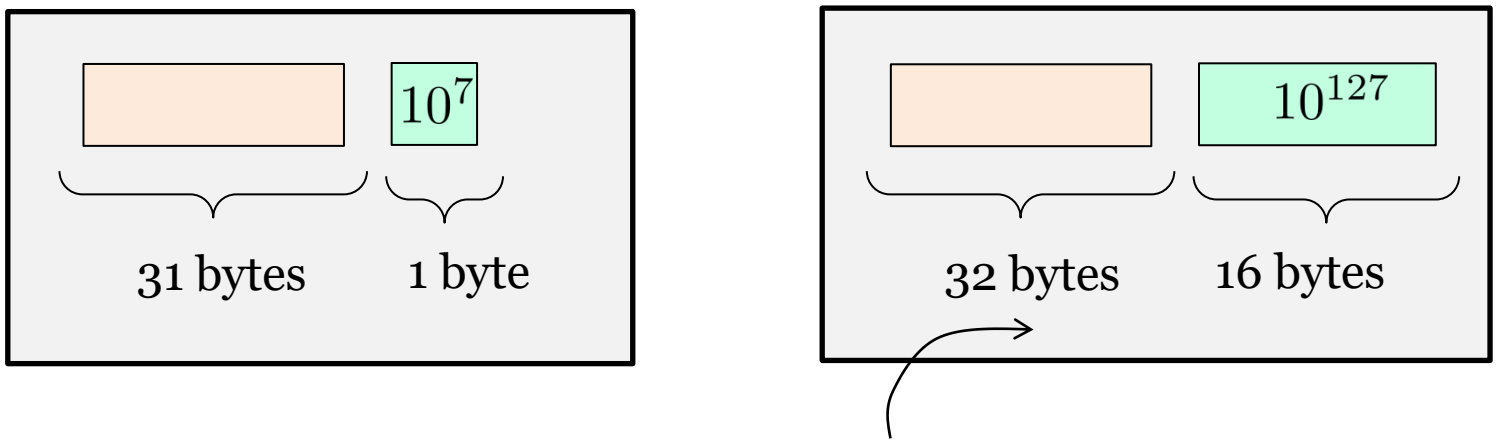
Decryption of CBC



Dealing with Fragmentary Data

Naive solution: Pad with 10^*

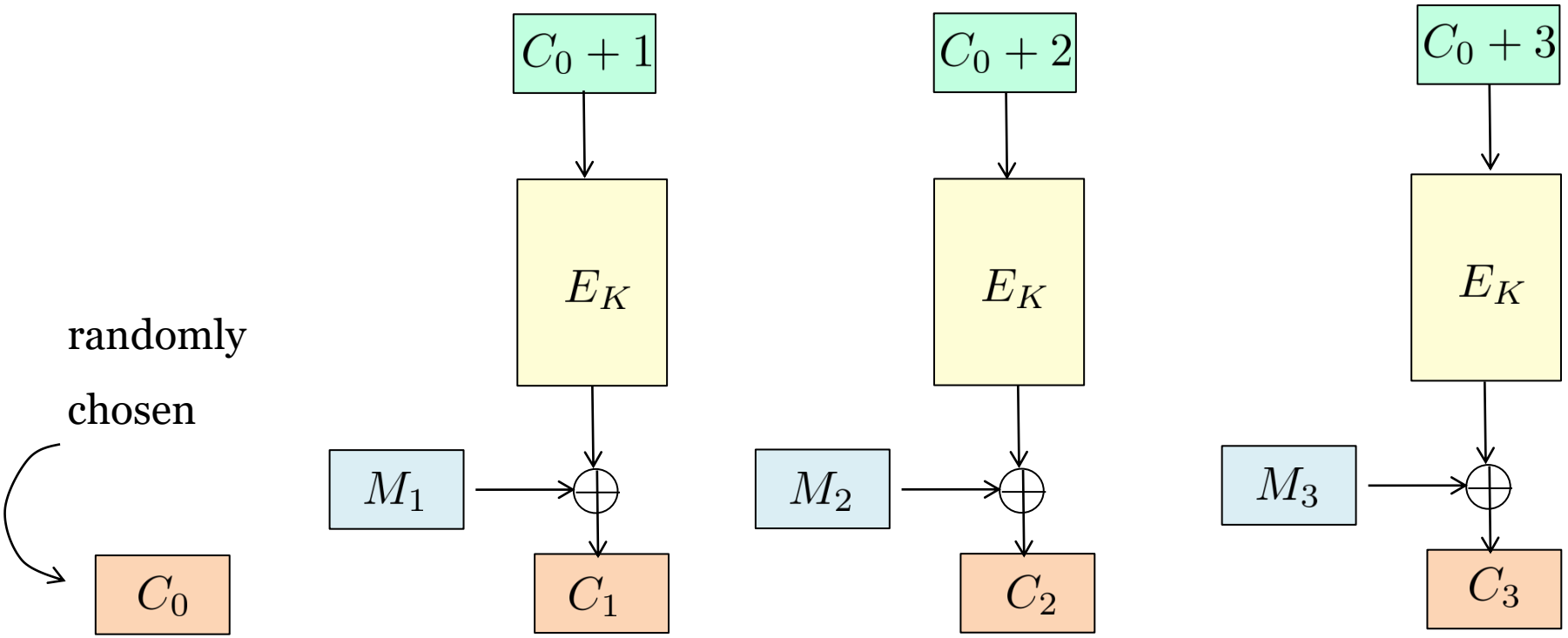
Example: Suppose that the block length is 16 bytes.



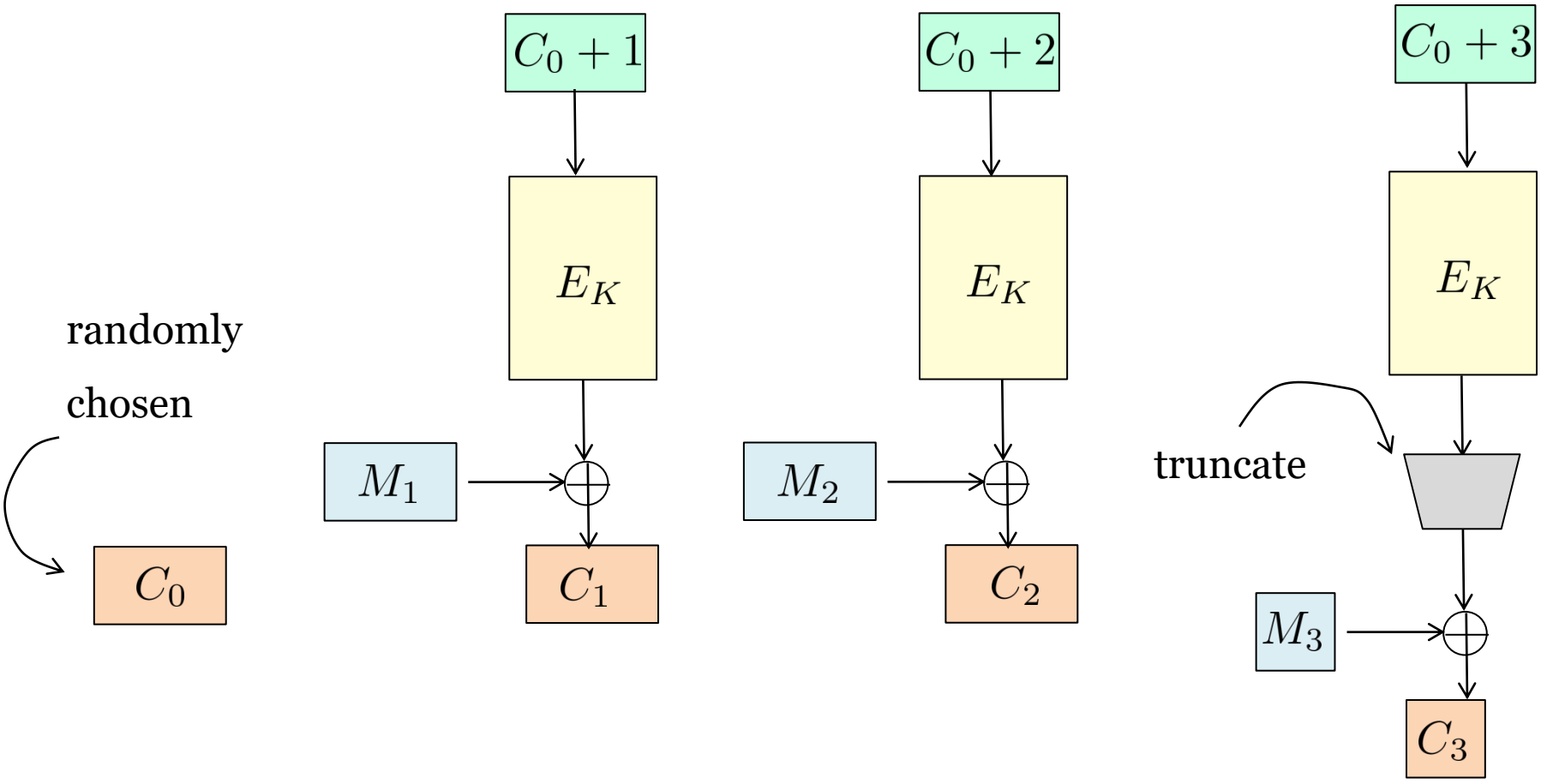
Problem: Waste bandwidth, and for full-length msg, waste a blockcipher call

Randomized Encryption: CTR

fully parallelizable



Dealing with Fragmentary Data



Agenda

1. Modes of Encryption: ECB, CBC, CTR

2. Formalizing Security


1982

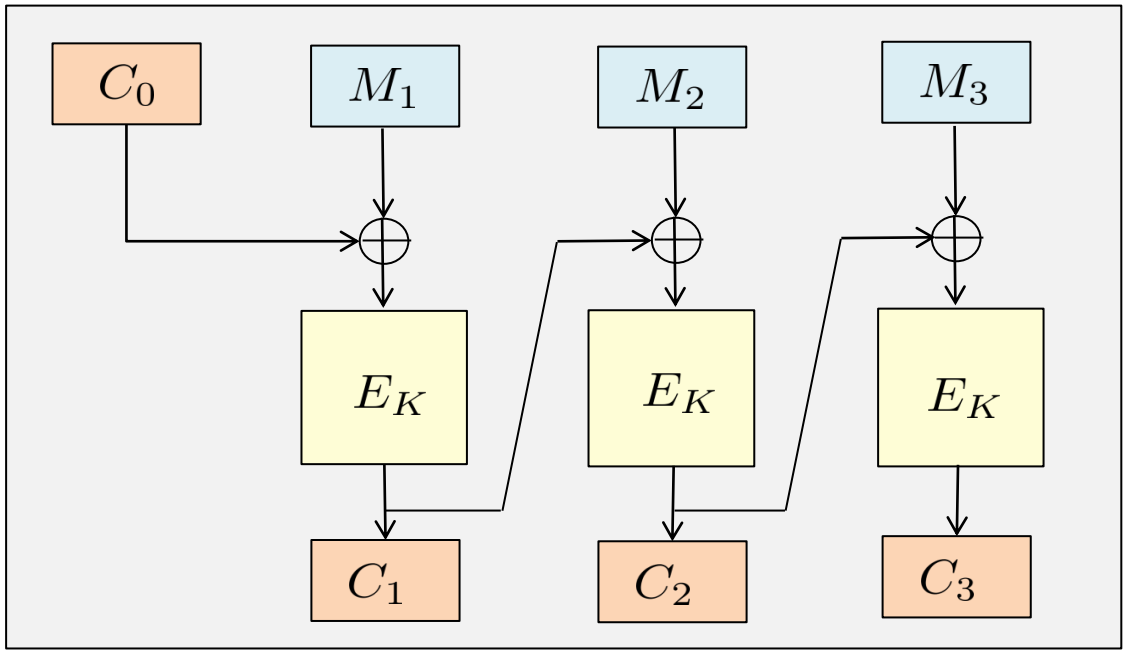
Formalizing Security: Intuition

Should hide

all partial information

about the plaintexts

Except message length



CBC trivially leaks message length

Formalizing Security: Informal Definition

Adversary can't even distinguish the encryption of its **own chosen messages**

"A good disguise should not allow a mother to distinguish her own children"

Goldwasser and Micali

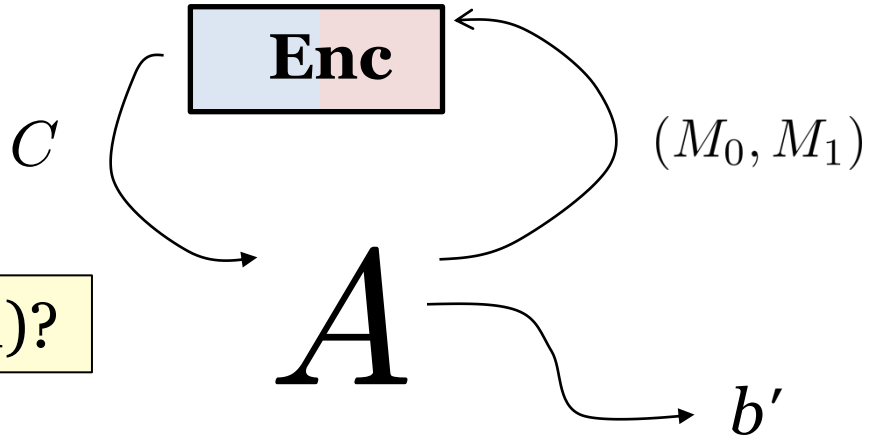
Formalizing Security: Left-or-Right

$\mathbf{Left}_{\mathcal{E}}$

procedure Enc(M_0, M_1)
Return $\mathcal{E}_K(M_0)$

$\mathbf{Right}_{\mathcal{E}}$

procedure Enc(M_0, M_1)
Return $\mathcal{E}_K(M_1)$



Left (0) or Right (1)?

$$\mathbf{Adv}^{\mathrm{lr}}_{\mathcal{E}}(A) = \Pr[\mathrm{Right}^{A}_{\mathcal{E}} \Rightarrow 1] - \Pr[\mathrm{Left}^{A}_{\mathcal{E}} \Rightarrow 1]$$

In each query, the two messages must have the same length

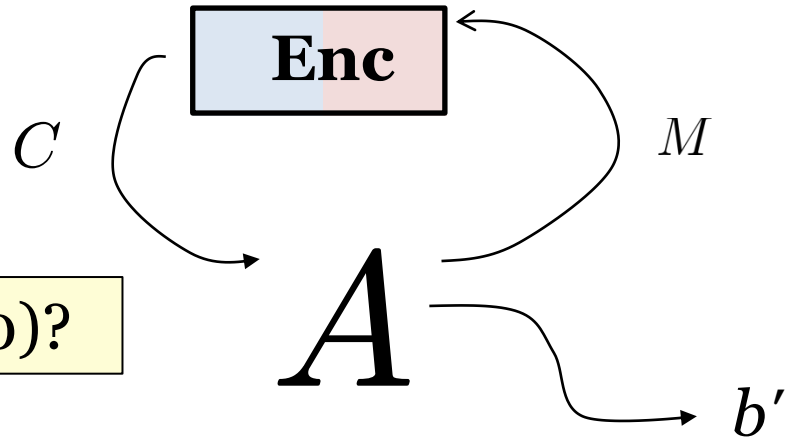
Formalizing Security: Real-or-Random

$\mathbf{Real}_{\mathcal{E}}$

procedure Enc(M)
Return $\mathcal{E}_K(M)$

$\mathbf{Rand}_{\mathcal{E}}$

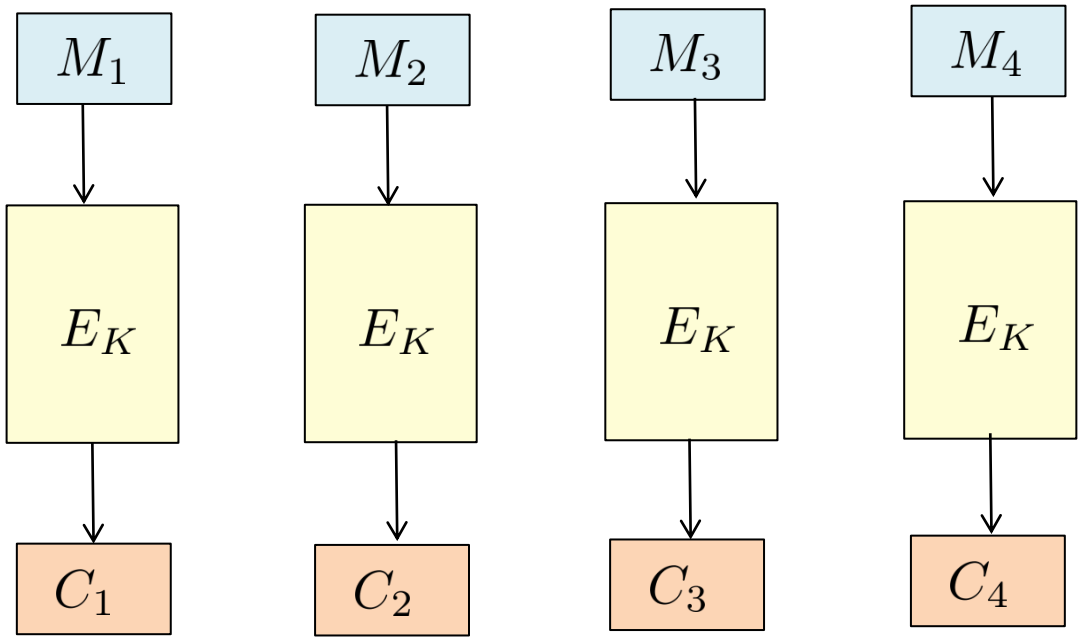
procedure Enc(M)
$C \xleftarrow{\$} \mathcal{E}_K(M')$; $C' \xleftarrow{\$} \{0,1\}^{|C|}$; Return C'



Real (1) or Rand (0)?

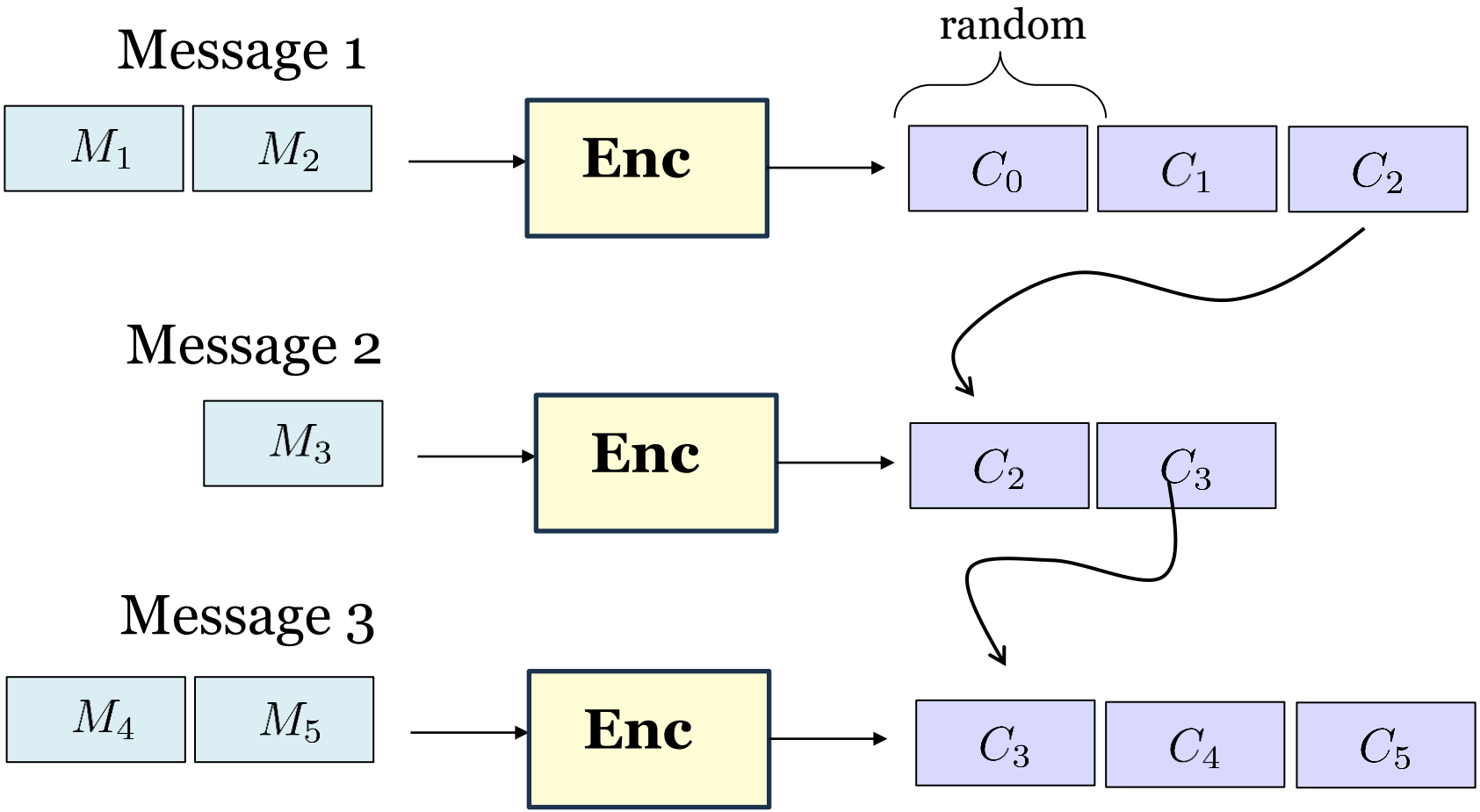
$$\mathbf{Adv}^{\mathrm{rr}}_{\mathcal{E}}(A) = \Pr[\mathrm{Real}^{A}_{\mathcal{E}} \Rightarrow 1] - \Pr[\mathrm{Rand}^{A}_{\mathcal{E}} \Rightarrow 1]$$

Exercise: Break LR Security of ECB



Case Study: SSH Encryption

CBC with IV Chaining



Design rationale: save bandwidth and avoid the cost of generating randomness

Question: Break the real-or-random security of CBC Chaining using two queries.