

CNT 5412, SPRING 2025

# 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)

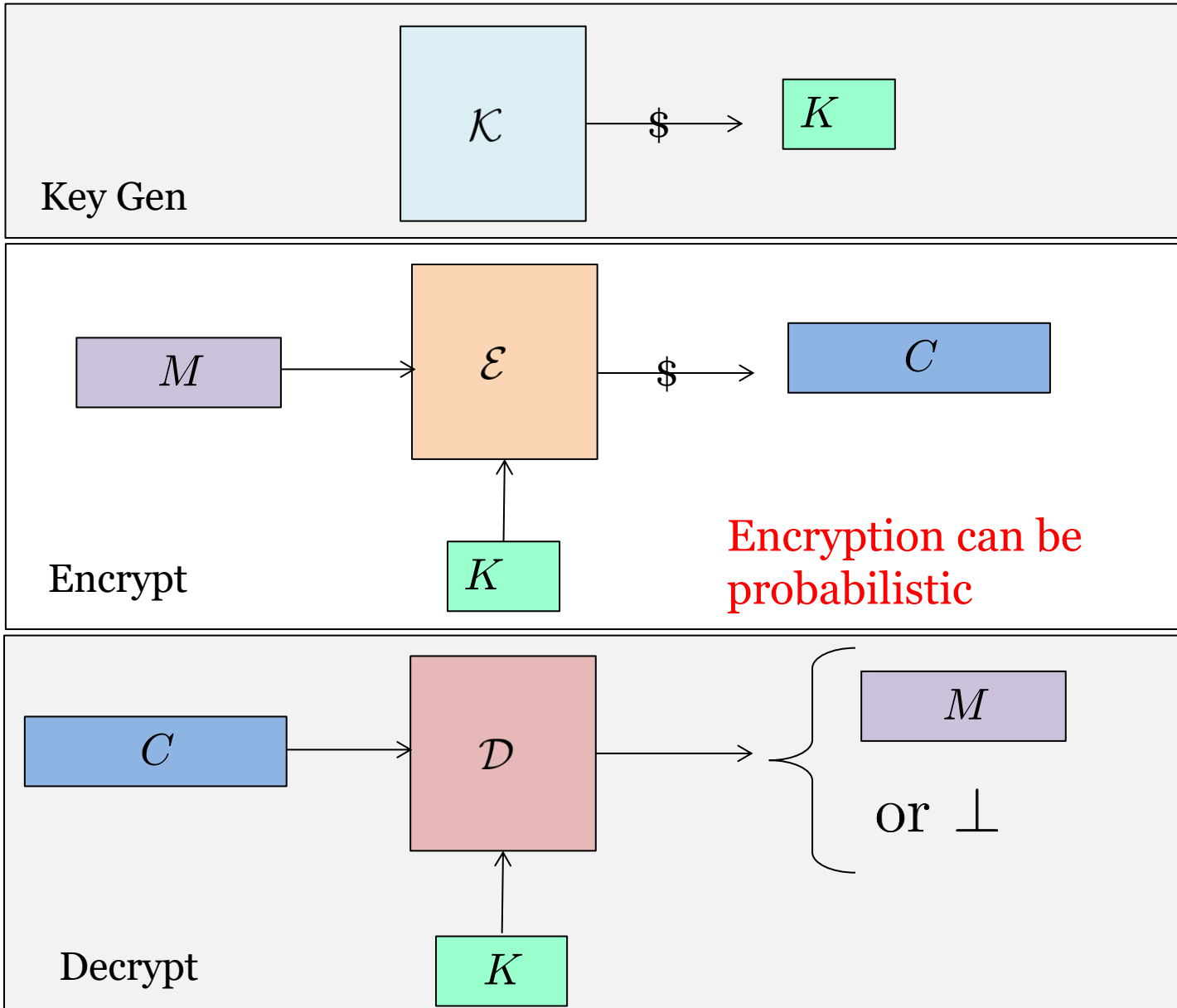
# Agenda

---

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

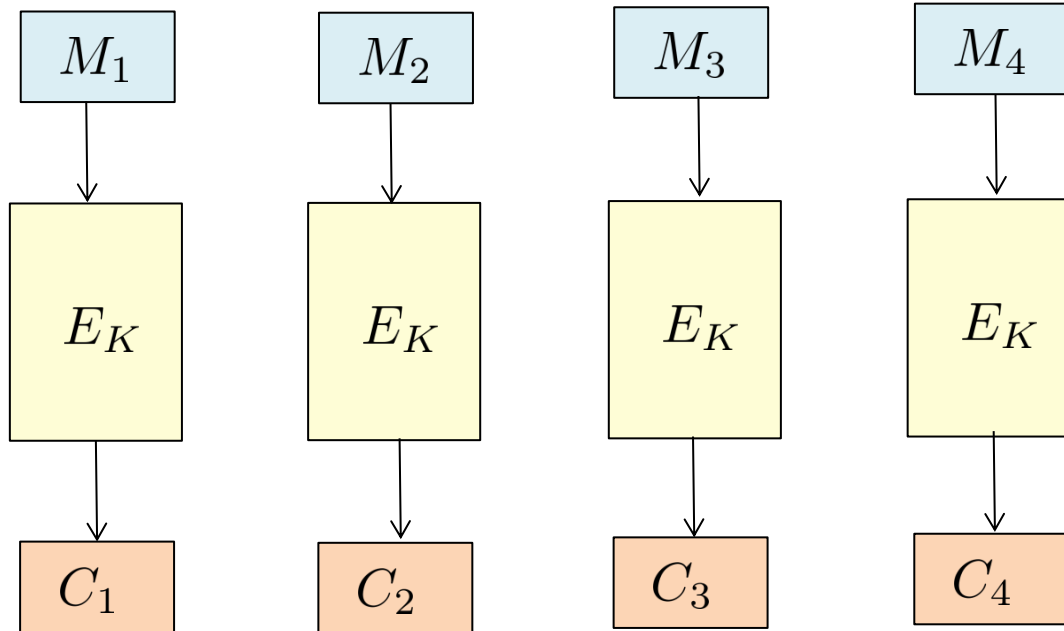
2. Formalizing Security

# Encryption Syntax



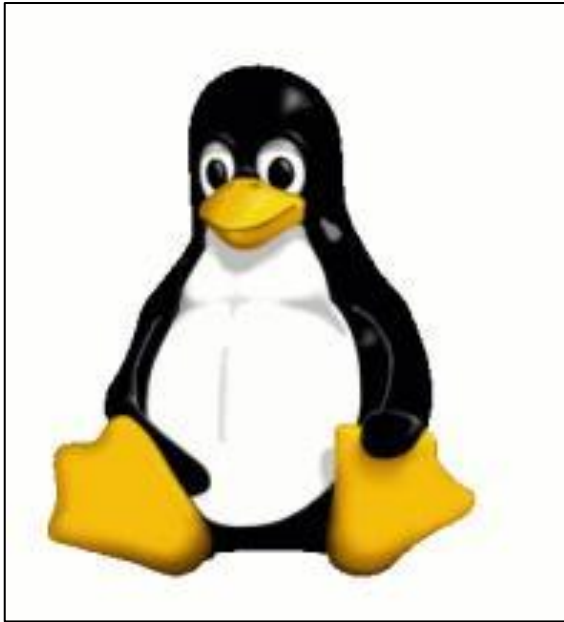
# (Bad) Encryption Using Blockcipher: ECB

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

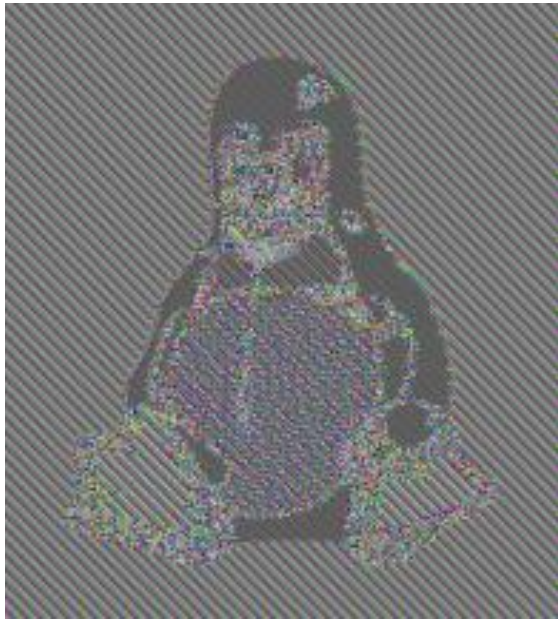


Can encrypt any message whose length is a multiple of  $n$

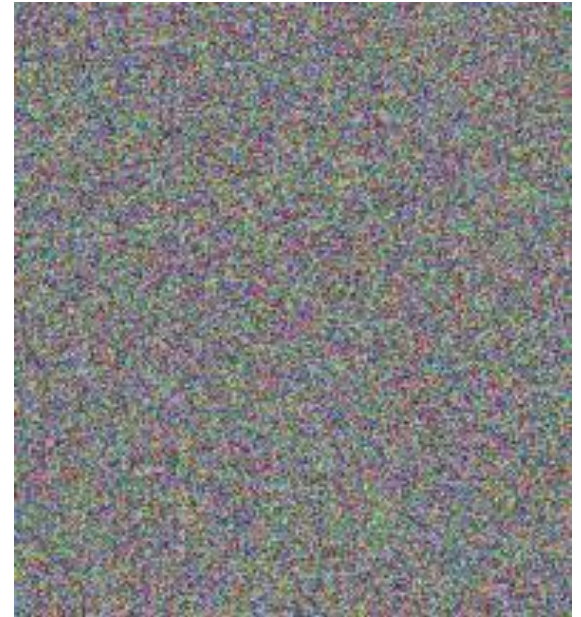
# ECB Is Insecure



Message

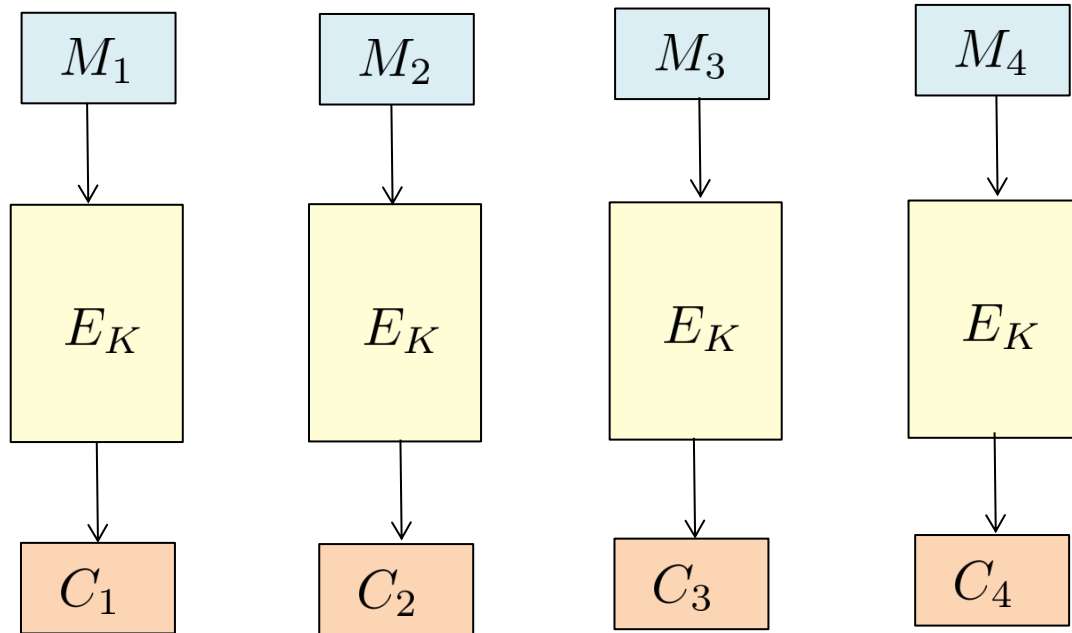


ECB ciphertext



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

 ars TECHNICA

BIZ & IT —

How an epic blunder by Adobe  
could strengthen hand of password  
crackers

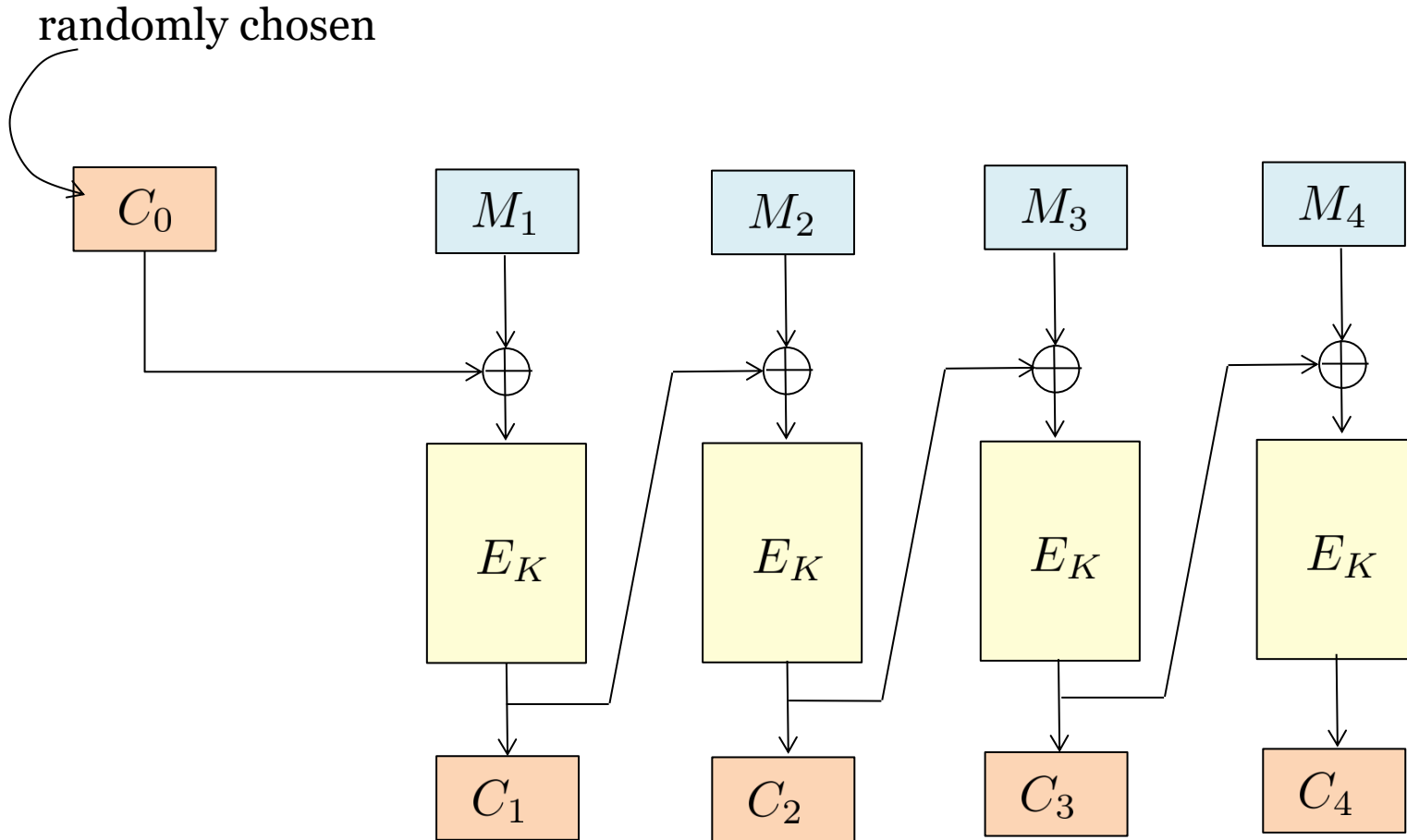
Adobe used ECB to  
encrypt passwords

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

Zoom used ECB to encrypt video conferencing

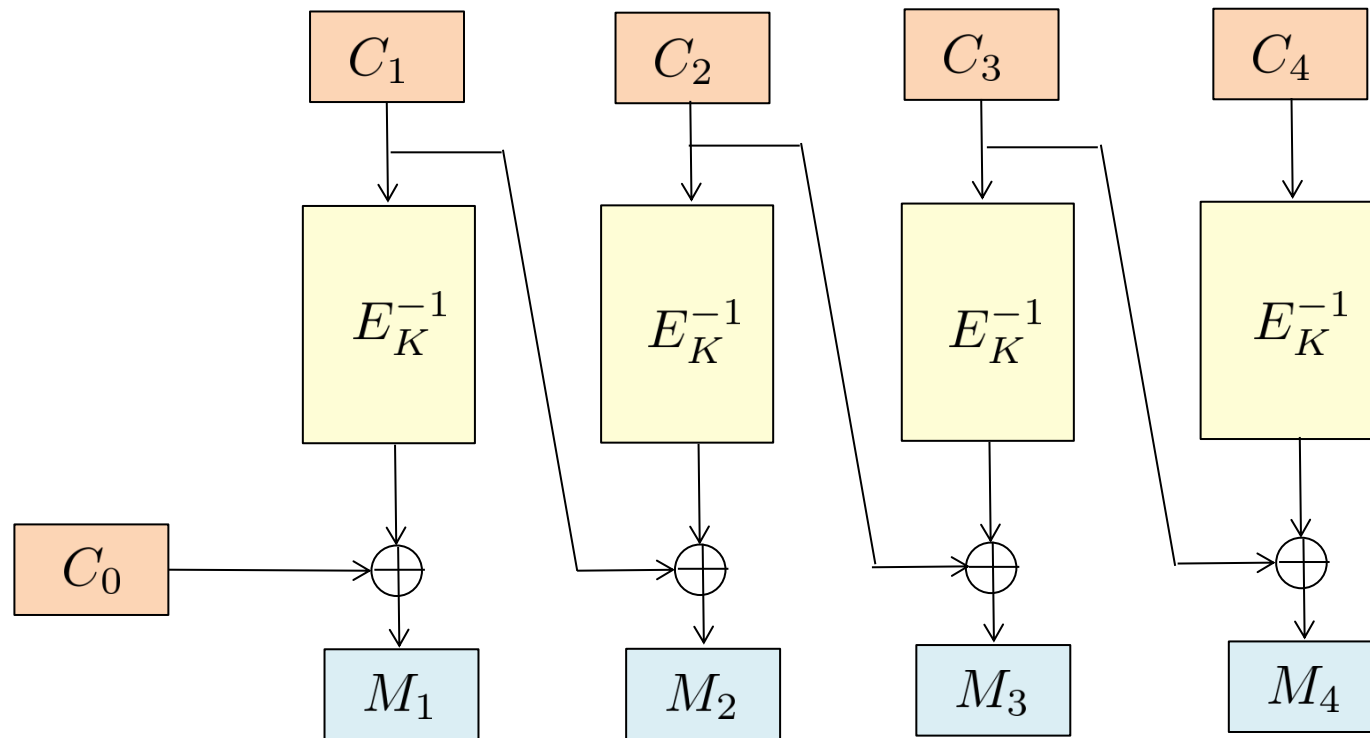
# Randomized Encryption: CBC

sequential





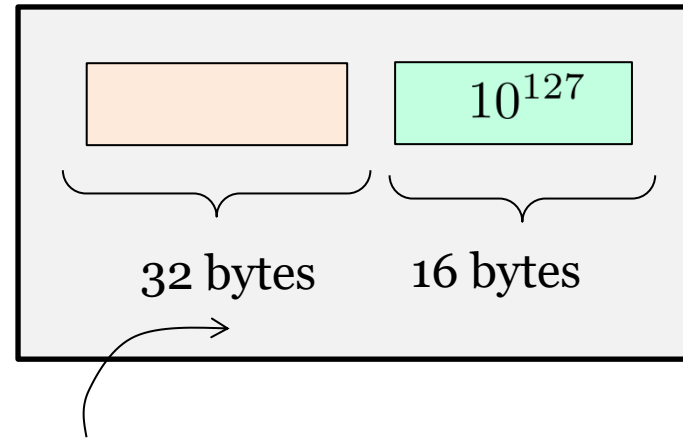
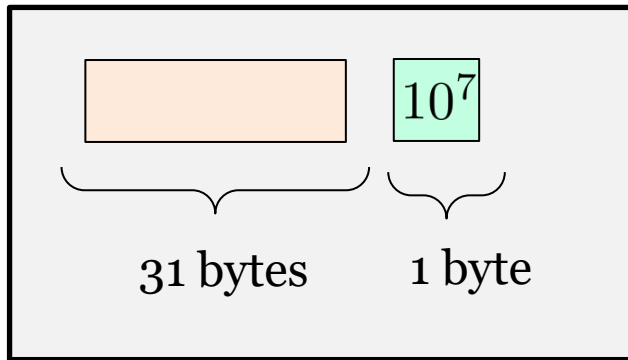
# Decryption of CBC



# Dealing with Fragmentary Data

**Naive solution:** Pad with  $10^*$

**Example:** Suppose that the block length is 16 bytes.

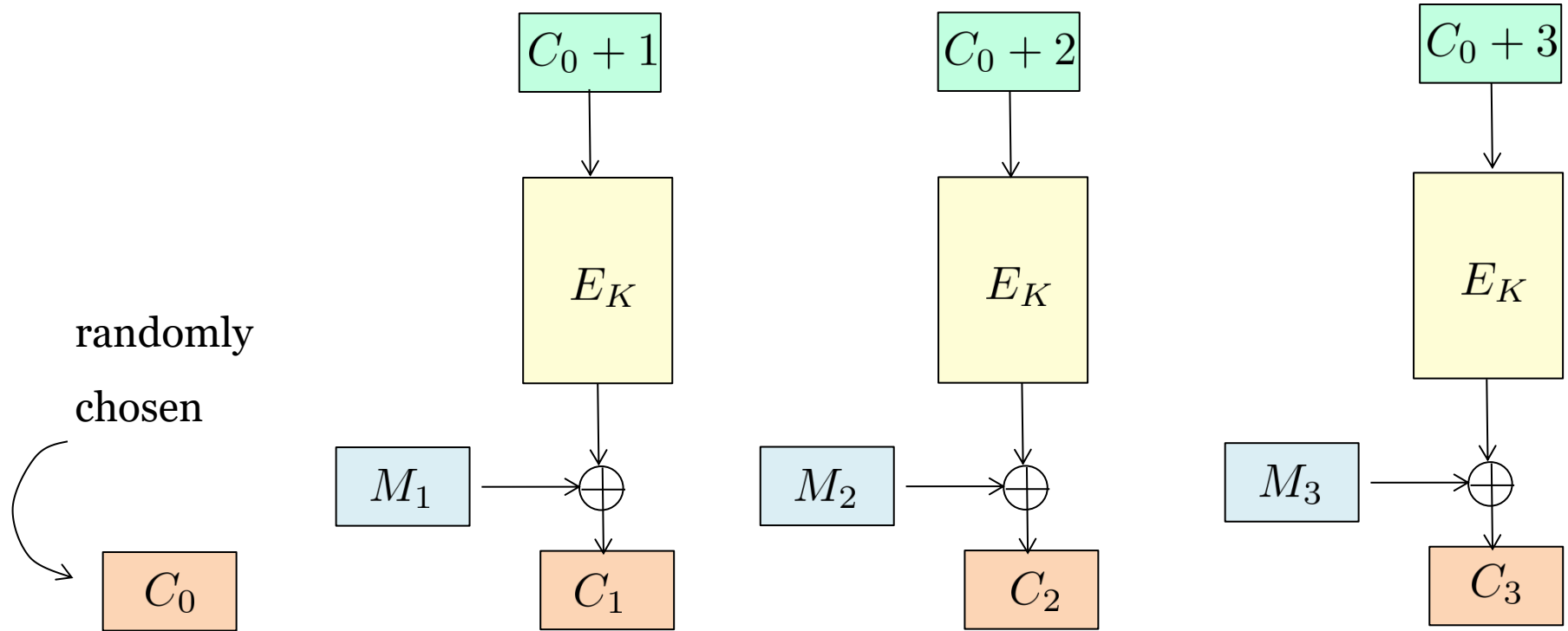


Padding is required, otherwise can't decrypt

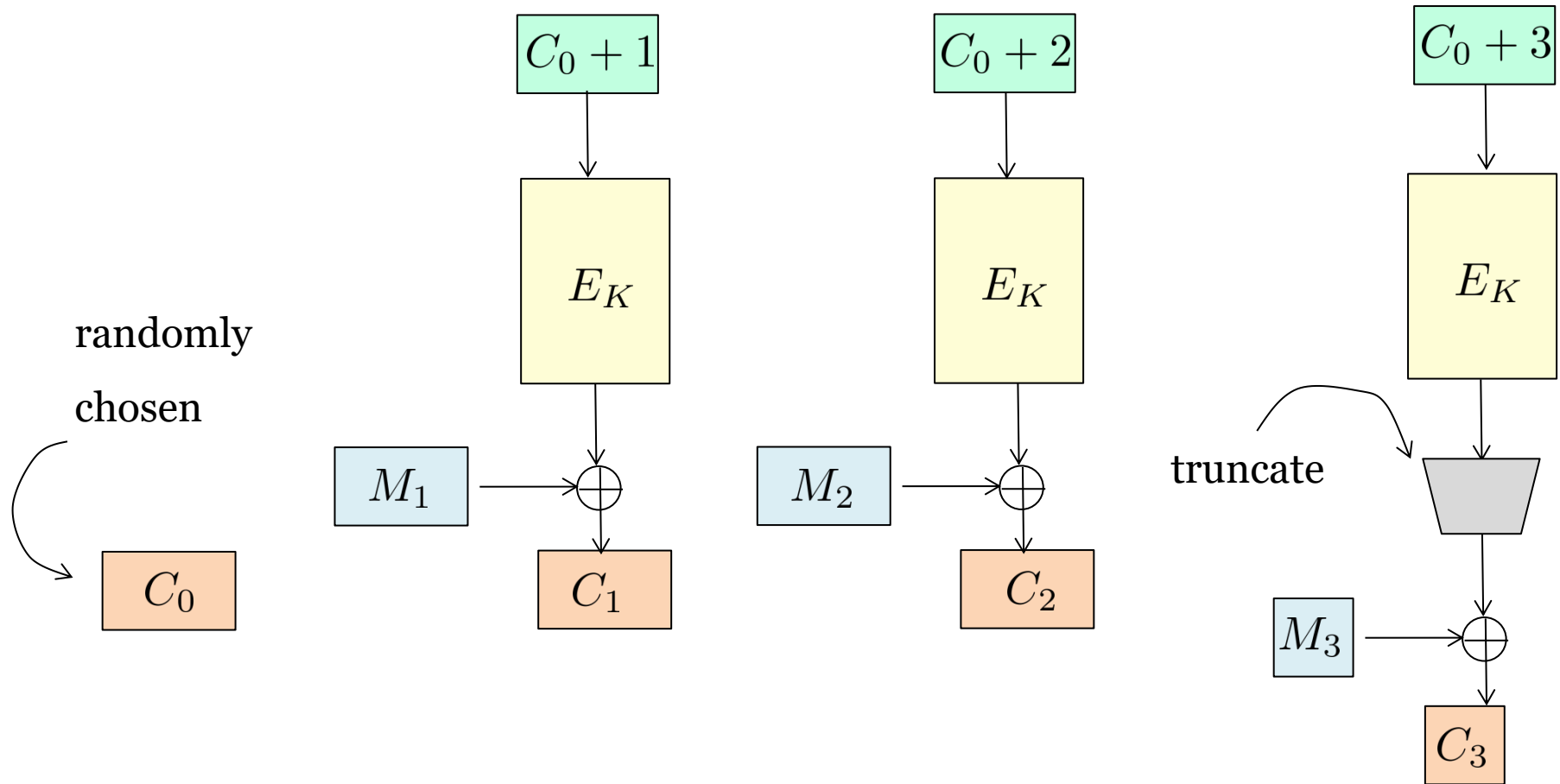
**Problem:** Waste bandwidth, and for full-length msg, waste a blockcipher call

# Randomized Encryption: CTR

fully parallelizable



# Dealing with Fragmentary Data



# Agenda

---

1. Modes of Encryption: ECB, CBC, CTR

**2. Formalizing Security**



1982

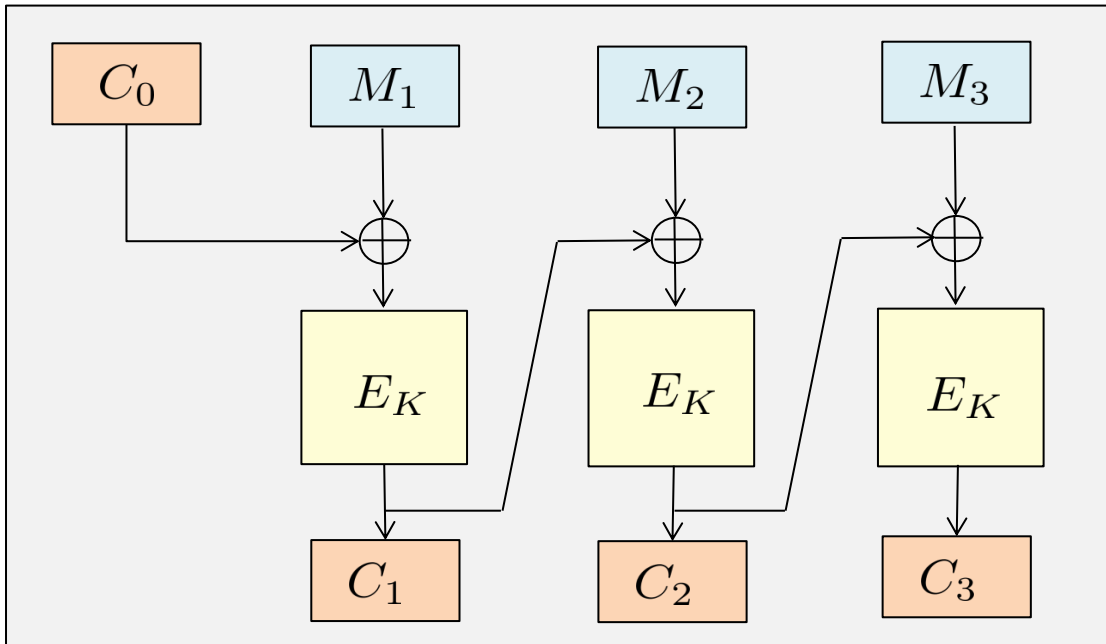
# Formalizing Security: Intuition

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



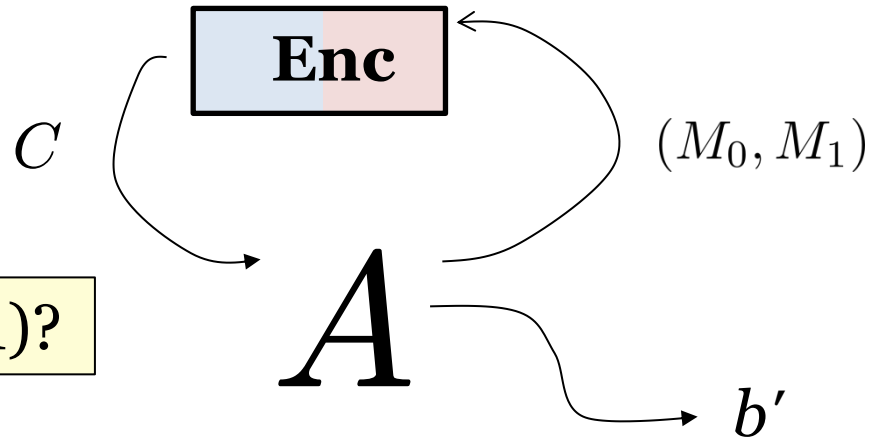
# Formalizing Security: Left-or-Right

**Left** <sub>$\mathcal{E}$</sub>

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

**Right** <sub>$\mathcal{E}$</sub>

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



Left (0) or Right (1)?

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

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

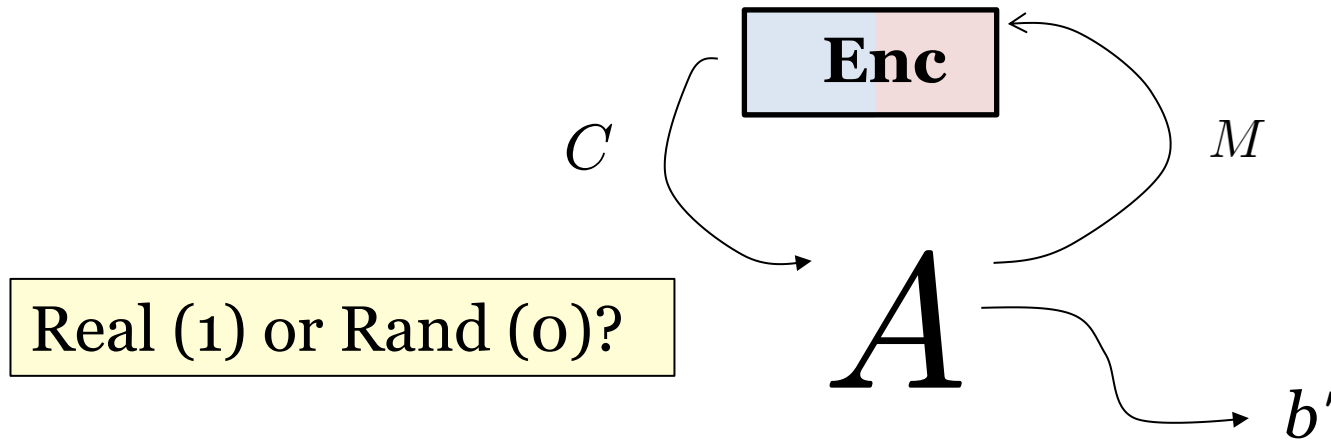
# Formalizing Security: Real-or-Random

**Real** <sub>$\mathcal{E}$</sub>

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

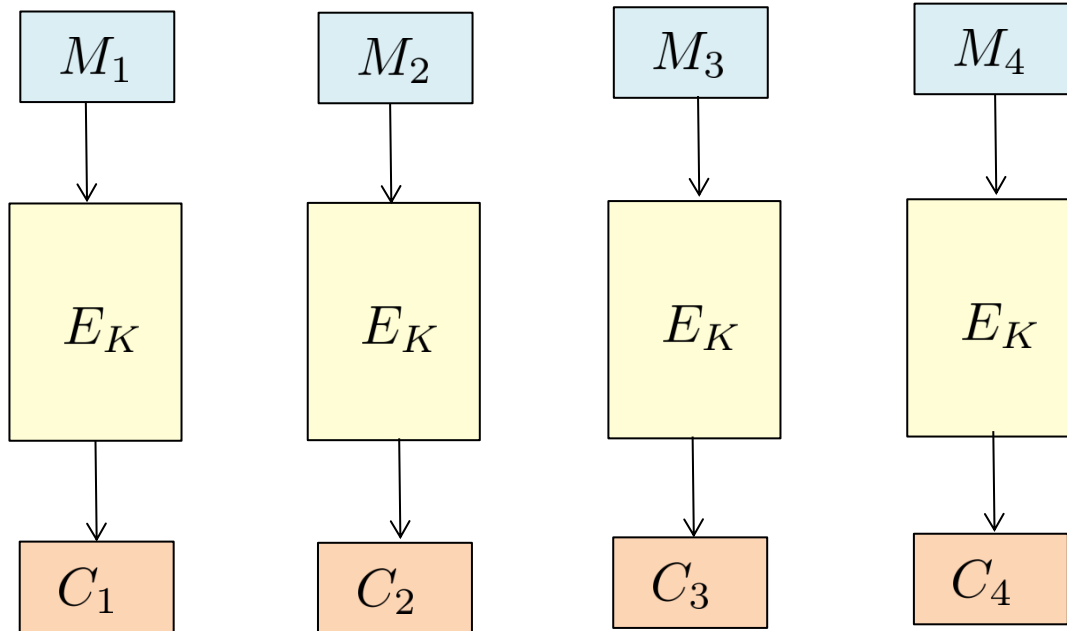
**Rand** <sub>$\mathcal{E}$</sub>

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



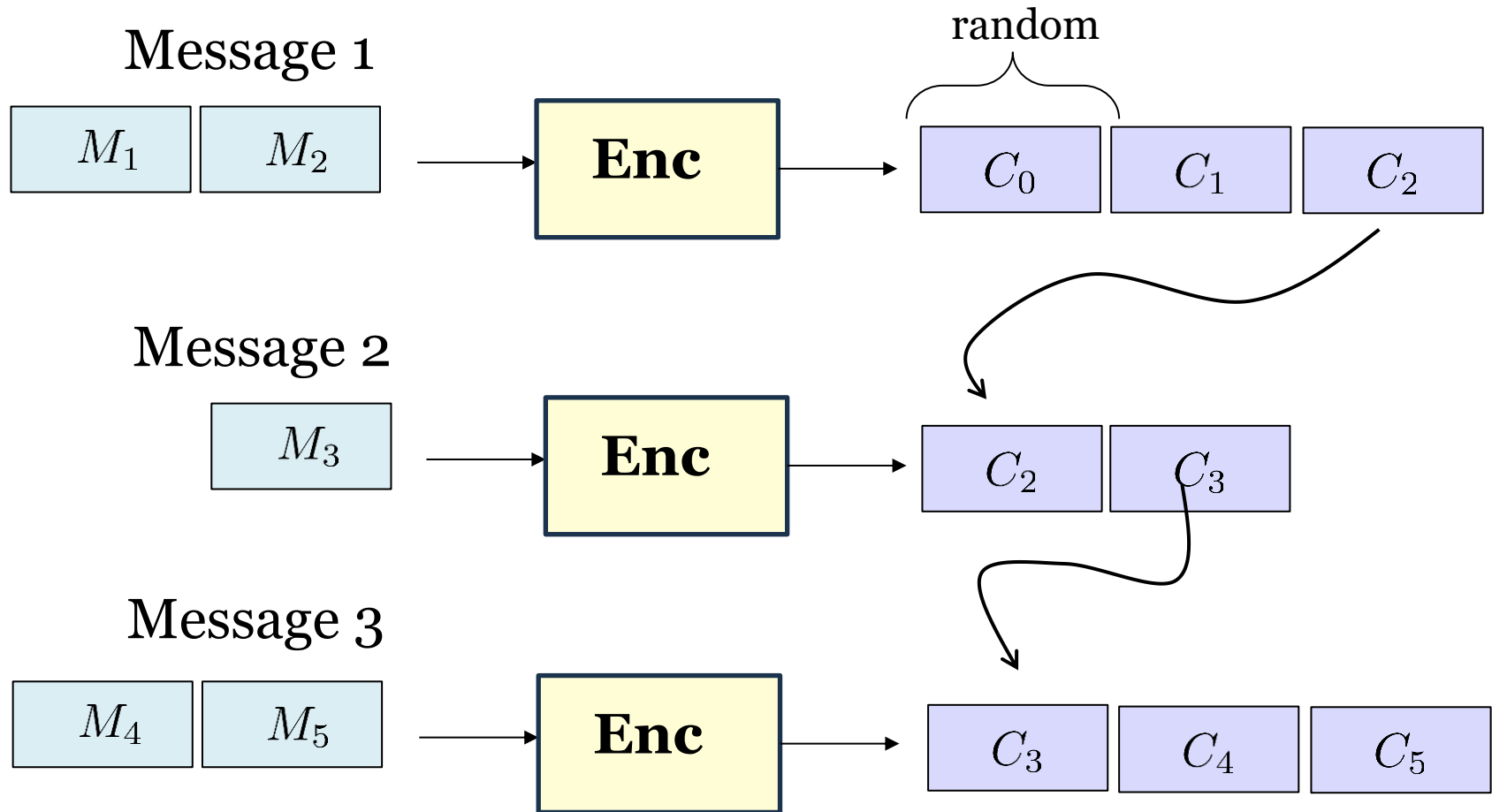
$$\text{Adv}_{\mathcal{E}}^{\text{rr}}(A) = \Pr[\text{Real}_{\mathcal{E}}^A \Rightarrow 1] - \Pr[\text{Rand}_{\mathcal{E}}^A \Rightarrow 1]$$

# 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.