CIS 4360: Computer Security Fundamentals

Symmetric Encryption

Viet Tung Hoang

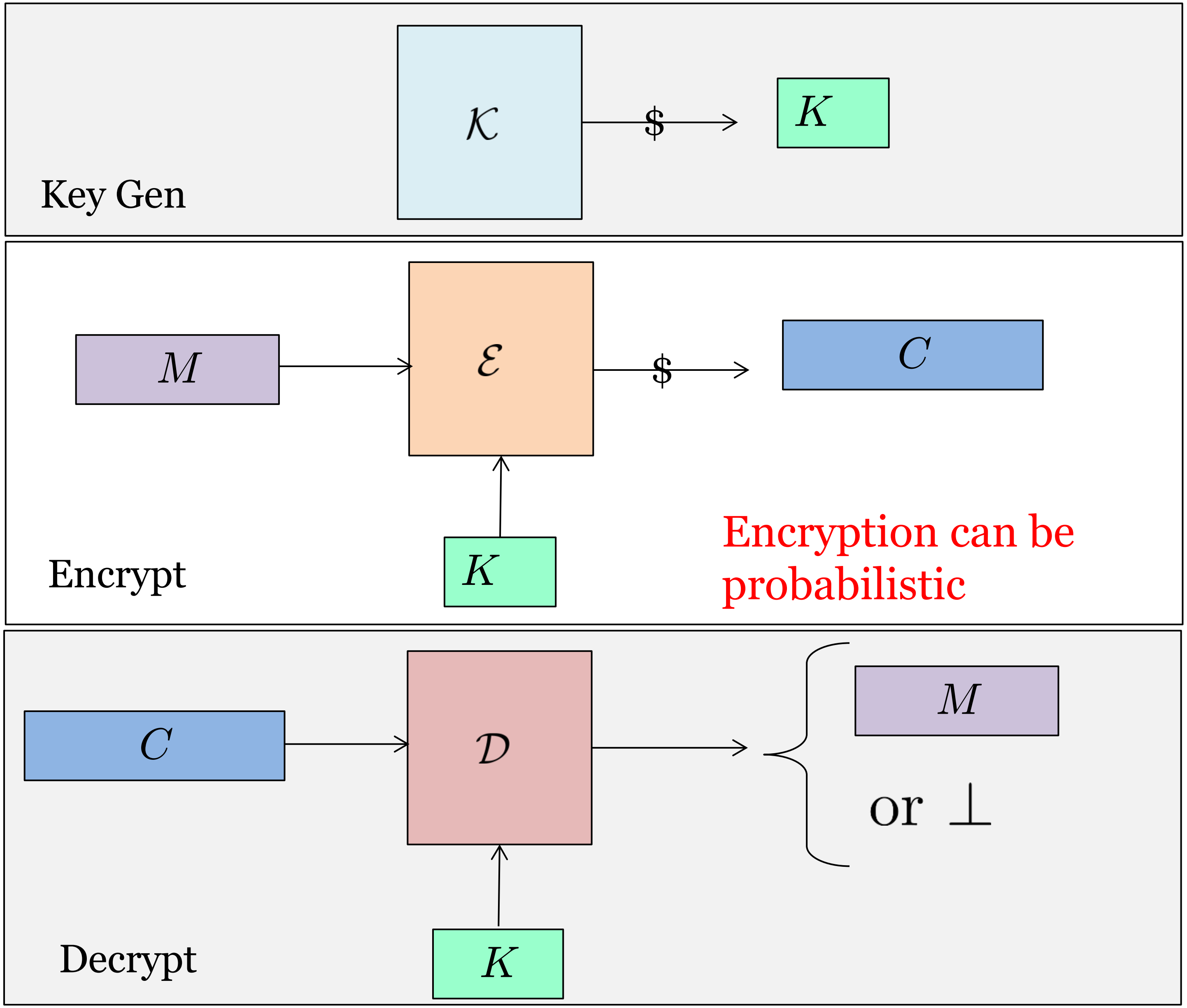
The slides are loosely based on those of Prof. Mihir Bellare (UCSD), Prof. Dan Boneh (Stanford), and Prof. Stefano Tessaro (UW)

Agenda

1. Modes of Encryption: ECB, CBC, CTR

2. Formalizing Security

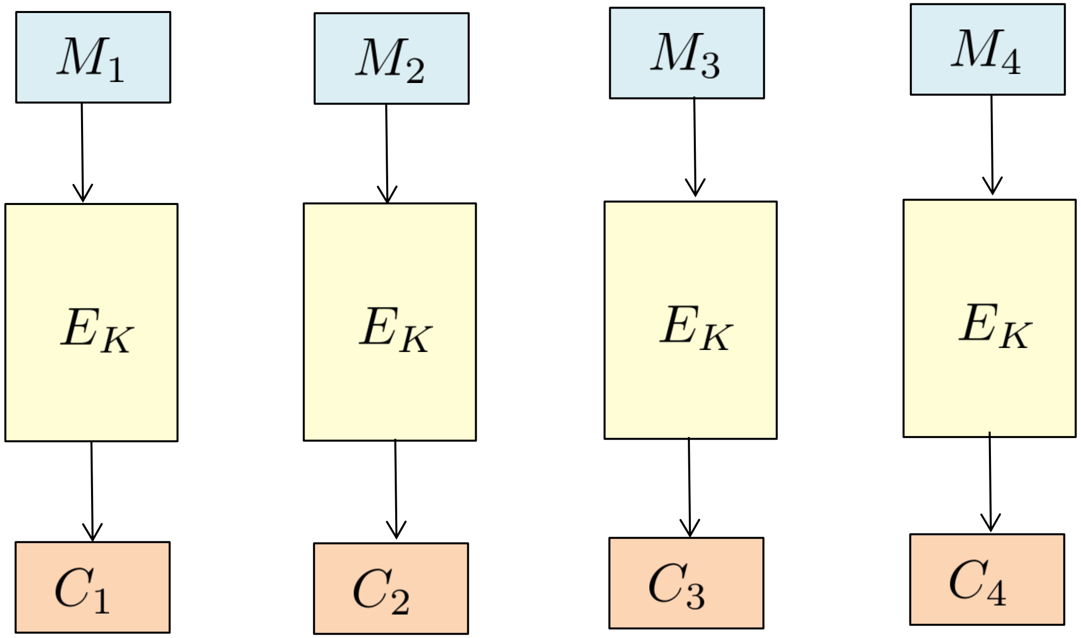
Encryption Syntax



Encryption can be probabilistic

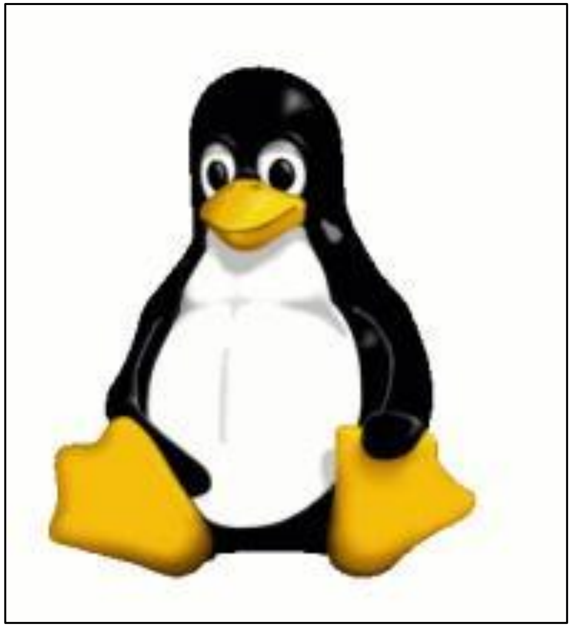
(Bad) Encryption Using Blockcipher: ECB

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

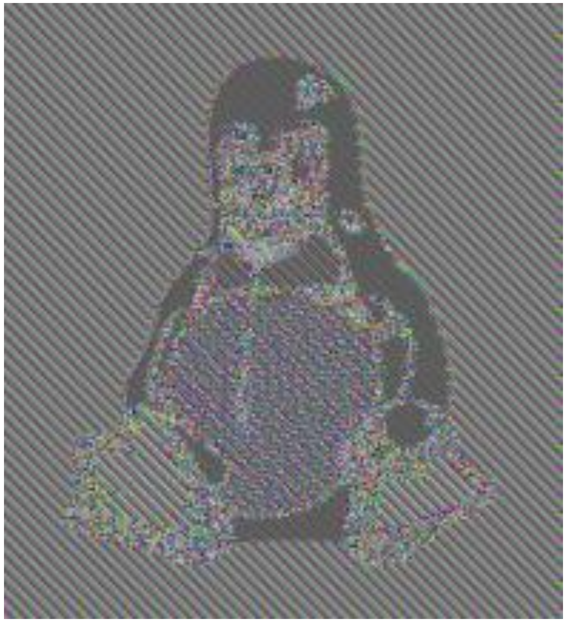


Can encrypt any message whose length is a multiple of n

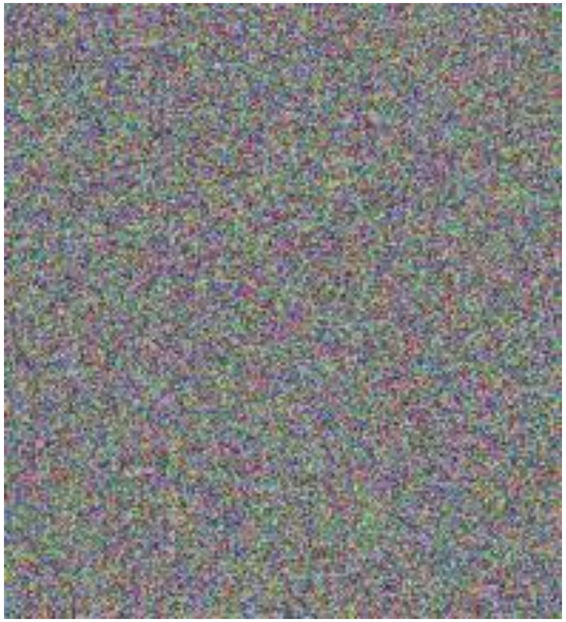
ECB Is Insecure



Message

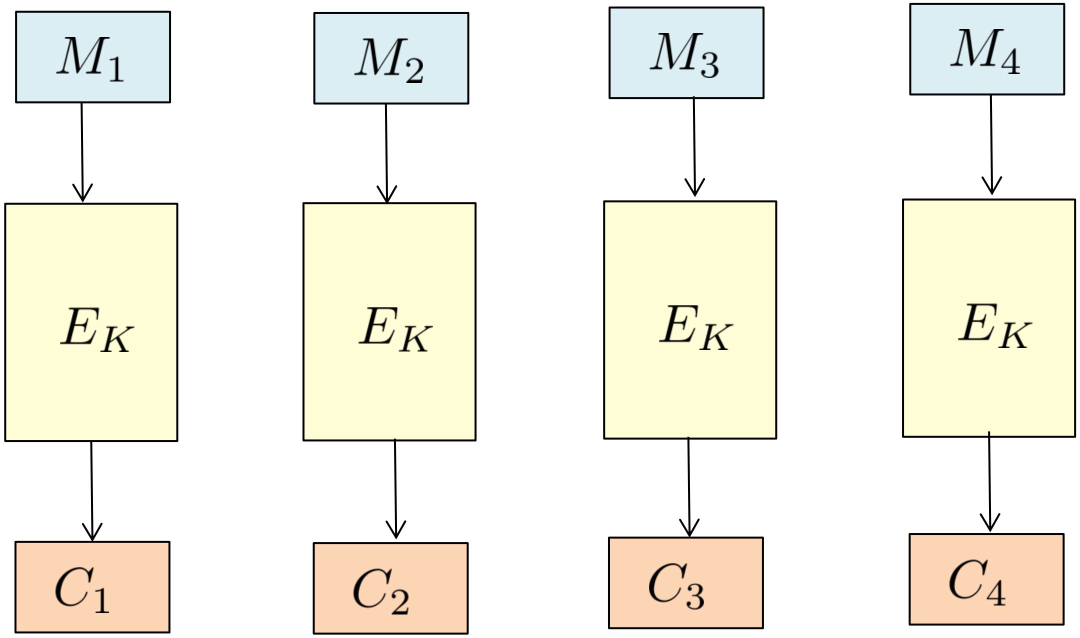


ECB ciphertext



Properly encrypted ciphertext

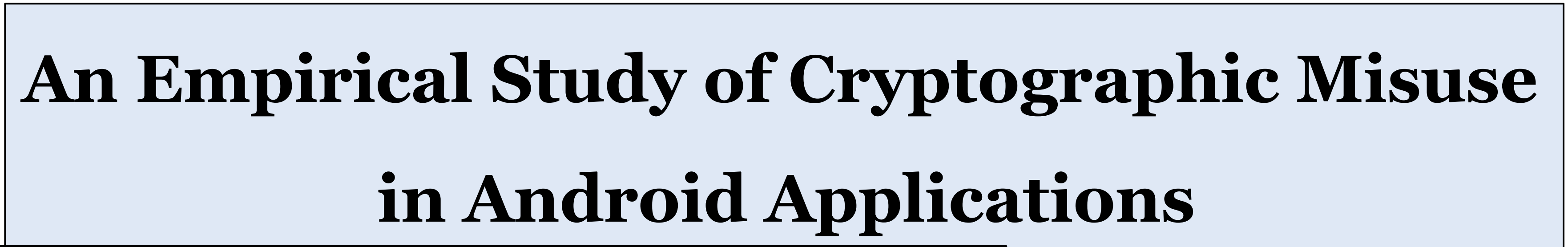
Why Is ECB So Bad?



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

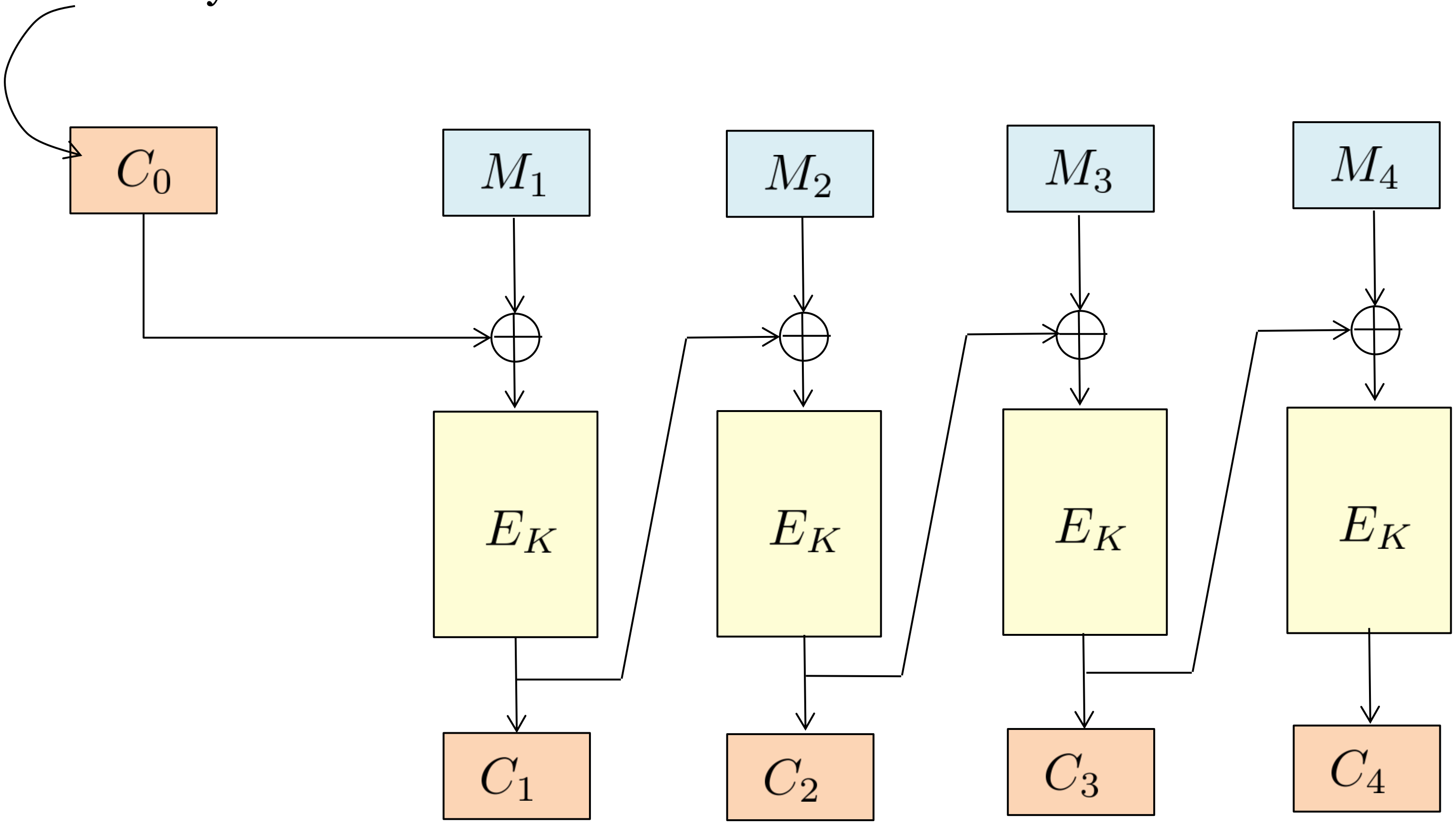
Zoom concedes custom encryption is substandard as Citizen Lab pokes holes in it

Zoom used ECB to encrypt video conferencing

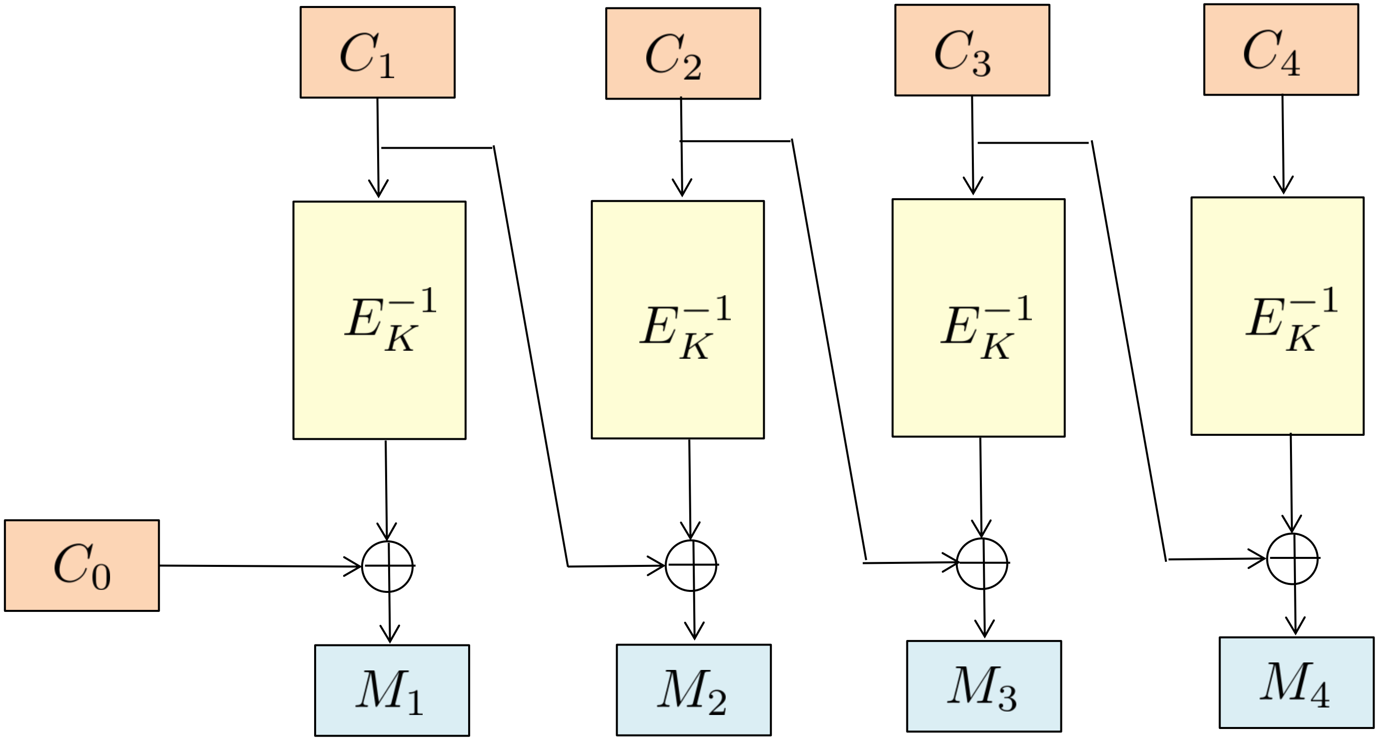
Randomized Encryption: CBC

sequential

randomly chosen



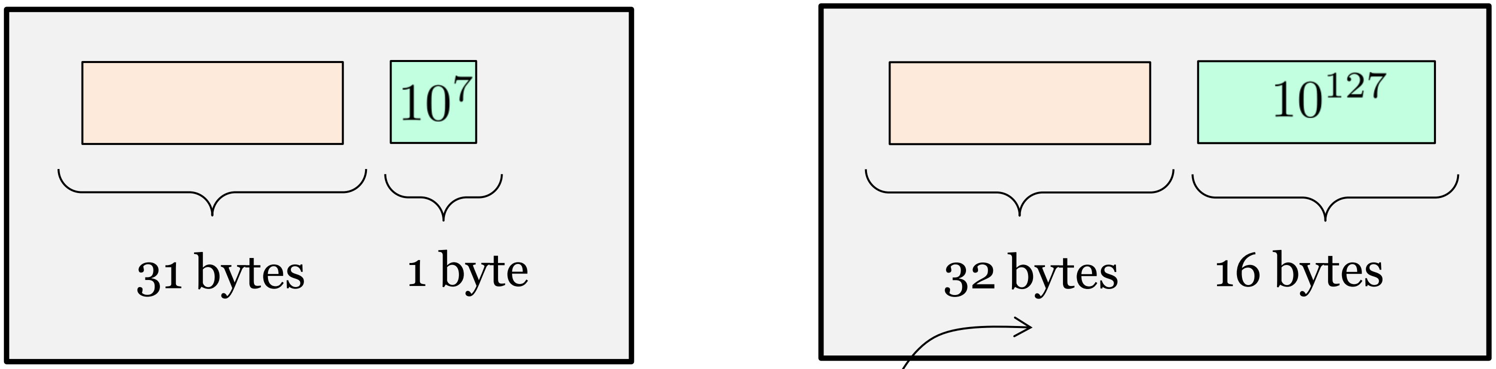
Decryption of CBC



Dealing with Fragmentary Data

Naive solution: Pad with 10^*

Example: Suppose that the block length is 16 bytes.

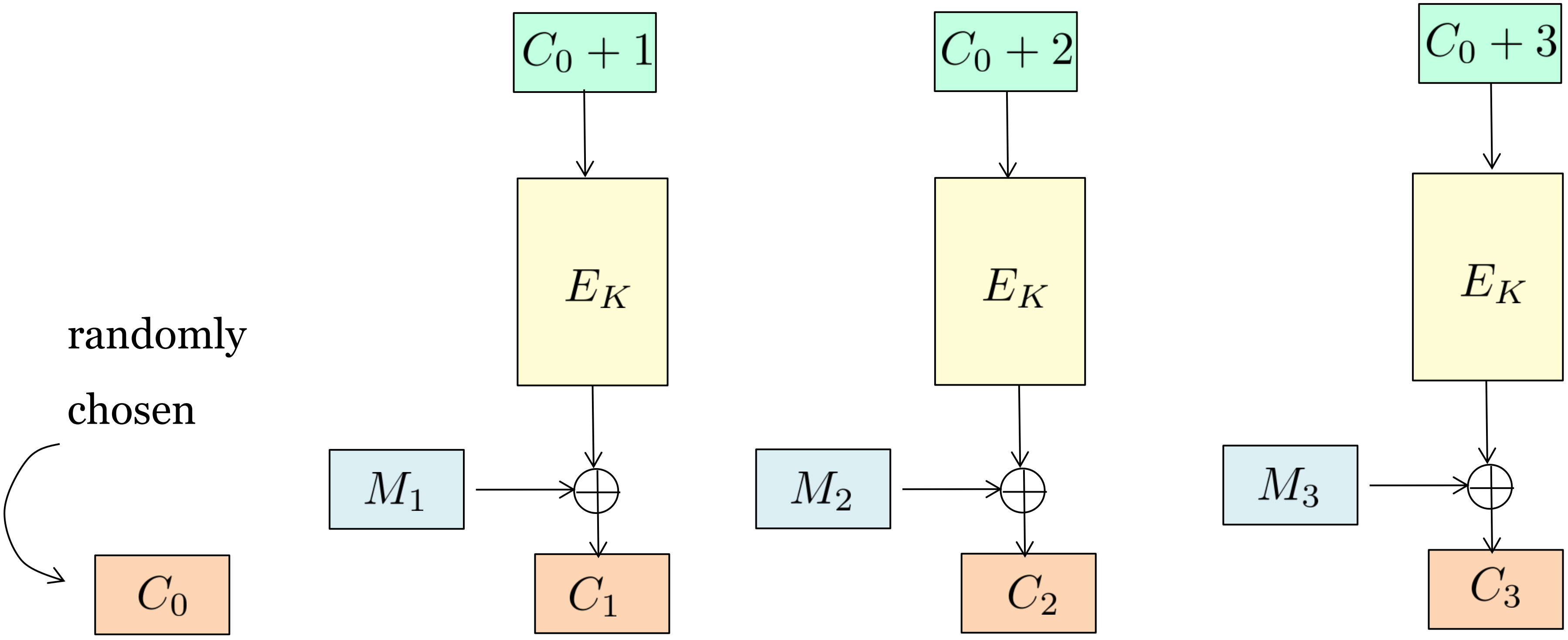


Padding is required, otherwise can't decrypt

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

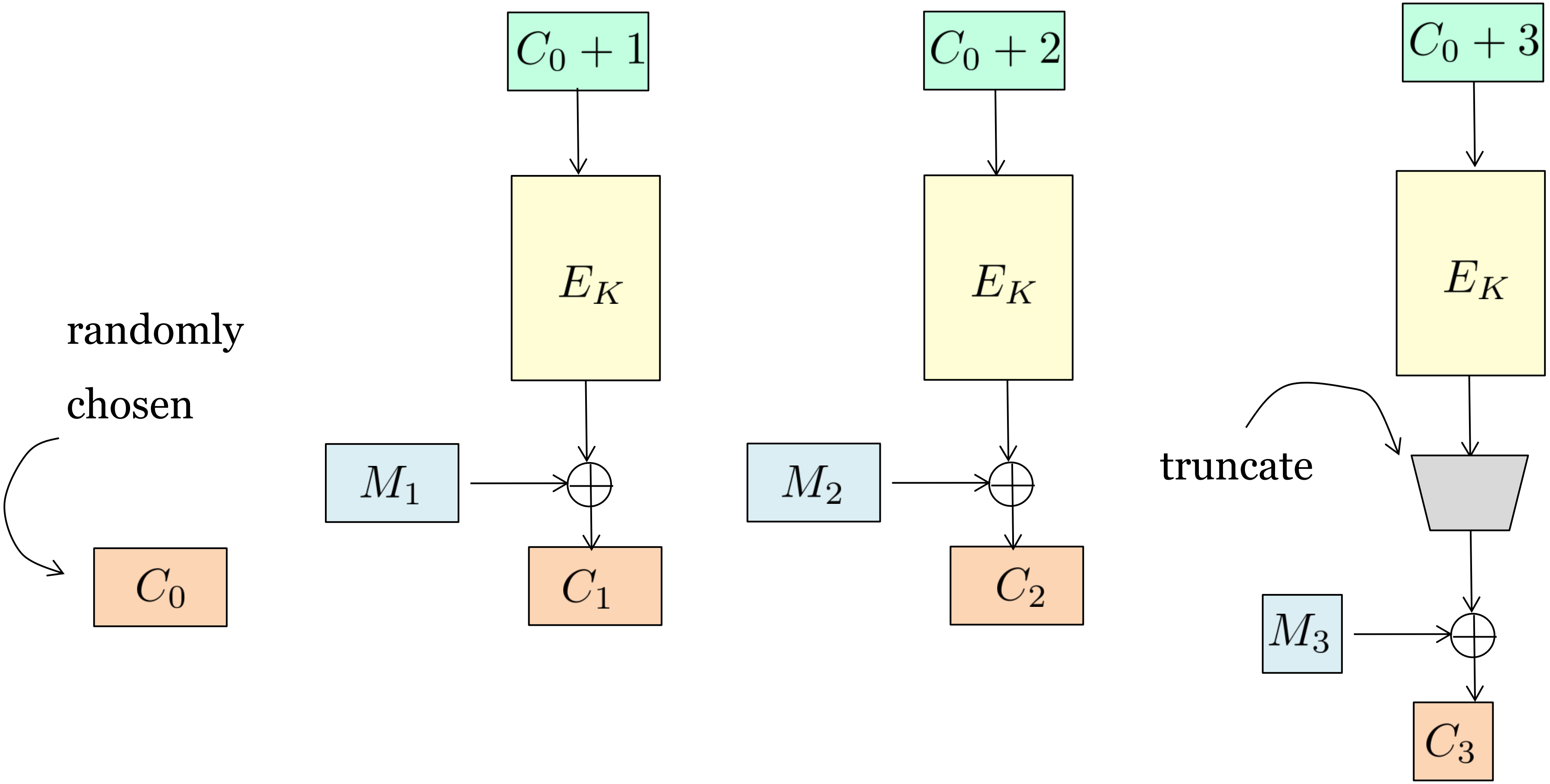
Randomized Encryption: CTR

fully parallelizable



randomly chosen

Dealing with Fragmentary Data



Agenda

1. Modes of Encryption: ECB, CBC, CTR

2. **Formalizing Security**

1982

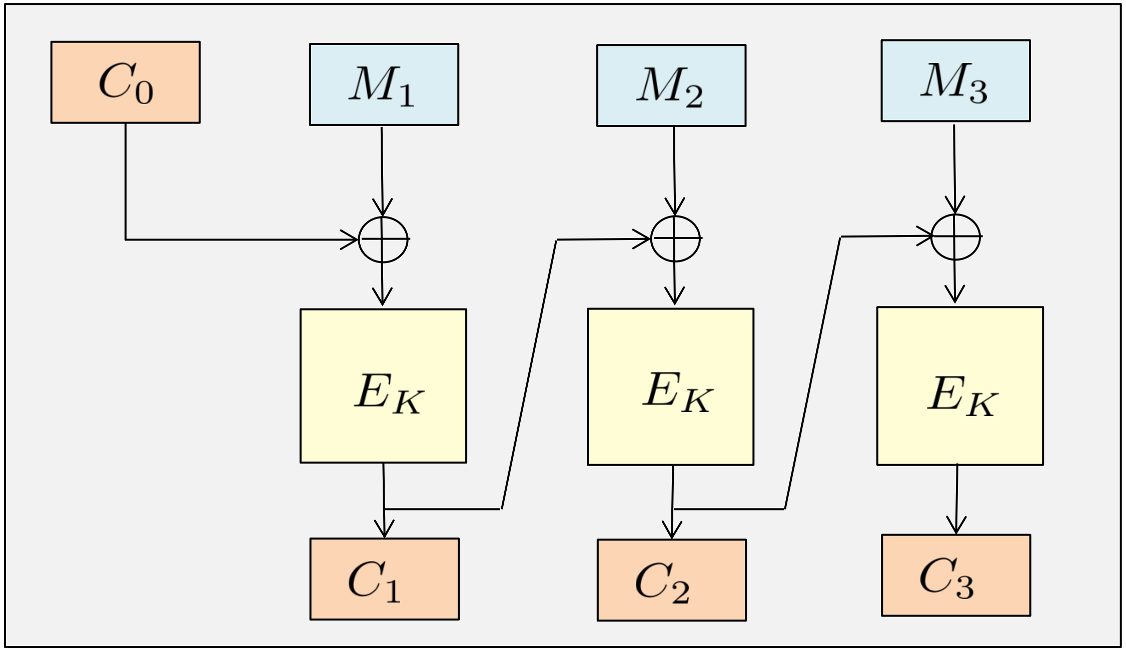
Formalizing Security: Intuition

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

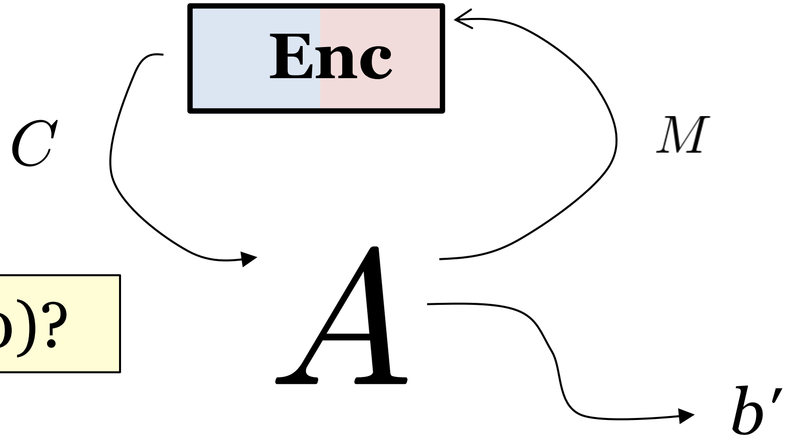
Formalizing Security: Real-or-Random

Real$_{\mathcal{E}}$

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

Rand$_{\mathcal{E}}$

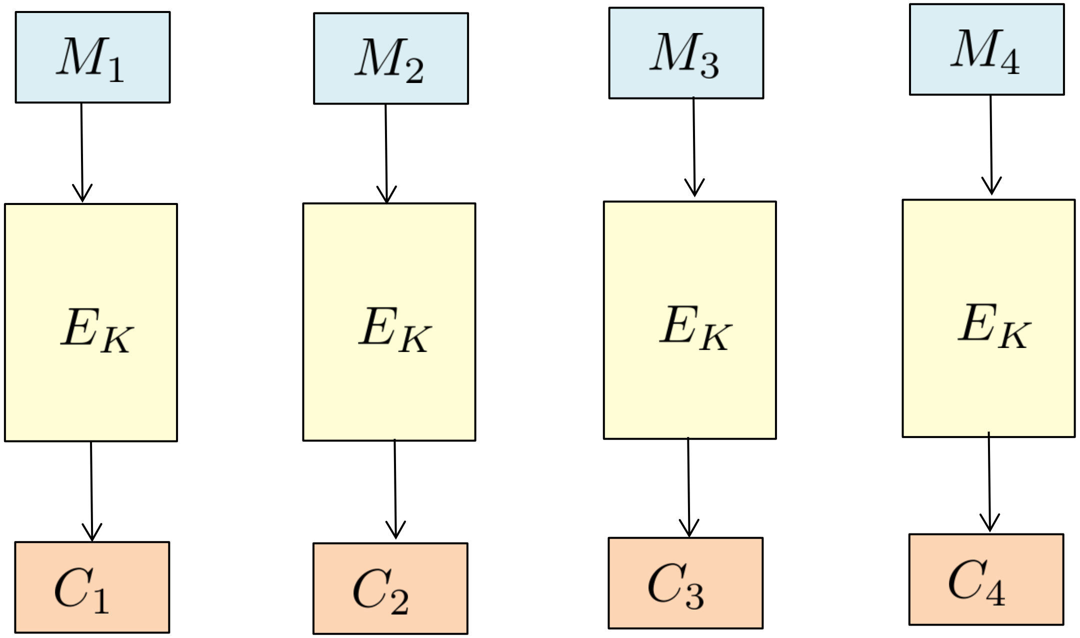
procedure Enc(M)
$C \stackrel{\$}{\leftarrow} \mathcal{E}_K(M')$; $C' \stackrel{\$}{\leftarrow} \{0,1\}^{|C|}$; Return C'



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


M_1
M_2
M_3
M_4
E_K
E_K
E_K
E_K
C_1
C_2
C_3
C_4