Modes of operation

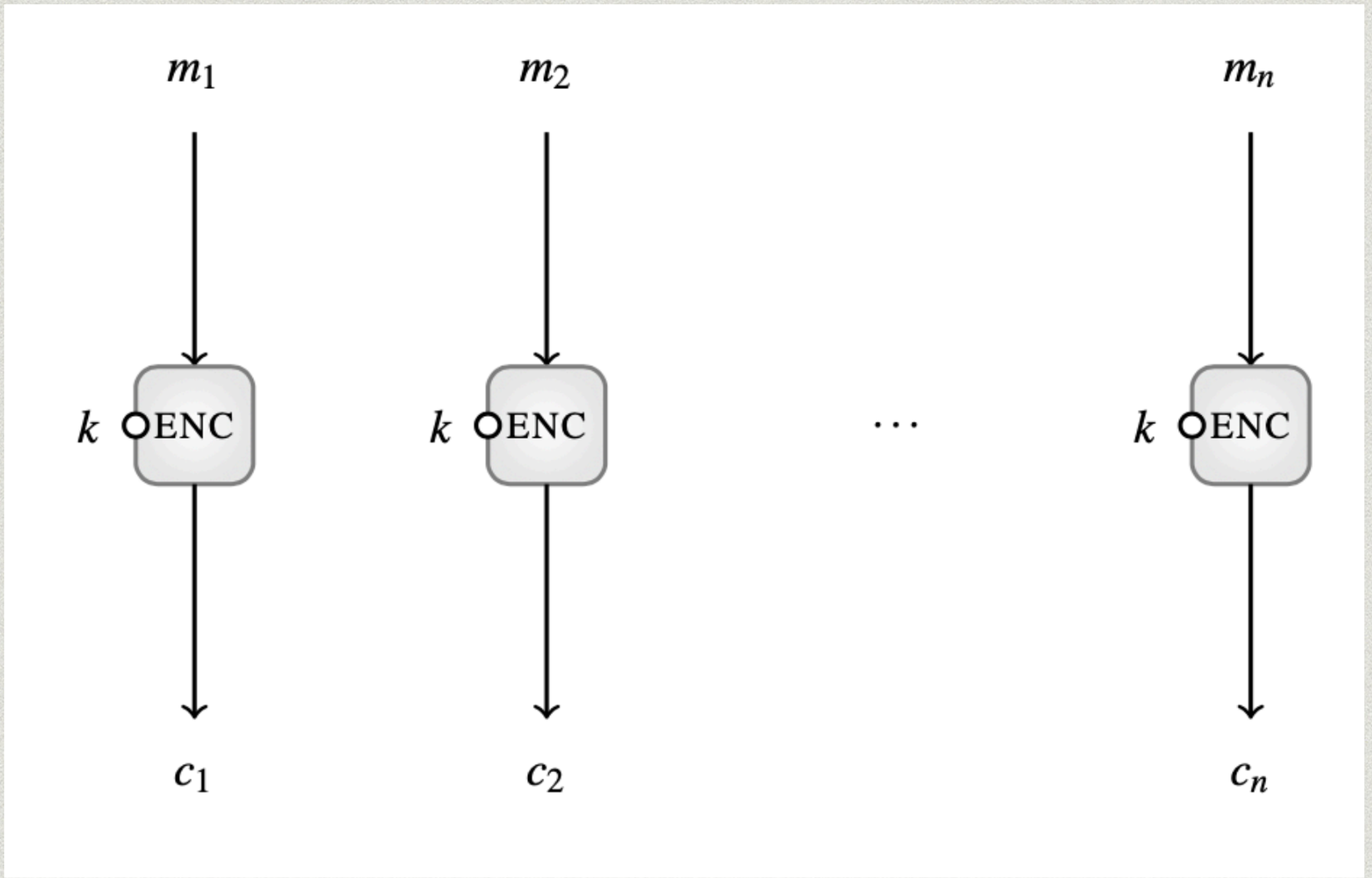
September 29, 2021

What is a mode of operation?

- It is a mechanism that help us to encipher plaintext of any length.
- It adds randomness to the ciphertext.
- It usually is used with a block cipher such as 3DES or AES.

ECB: Electronic Code Book

It is the easiest way to encipher a plaintext of any length.



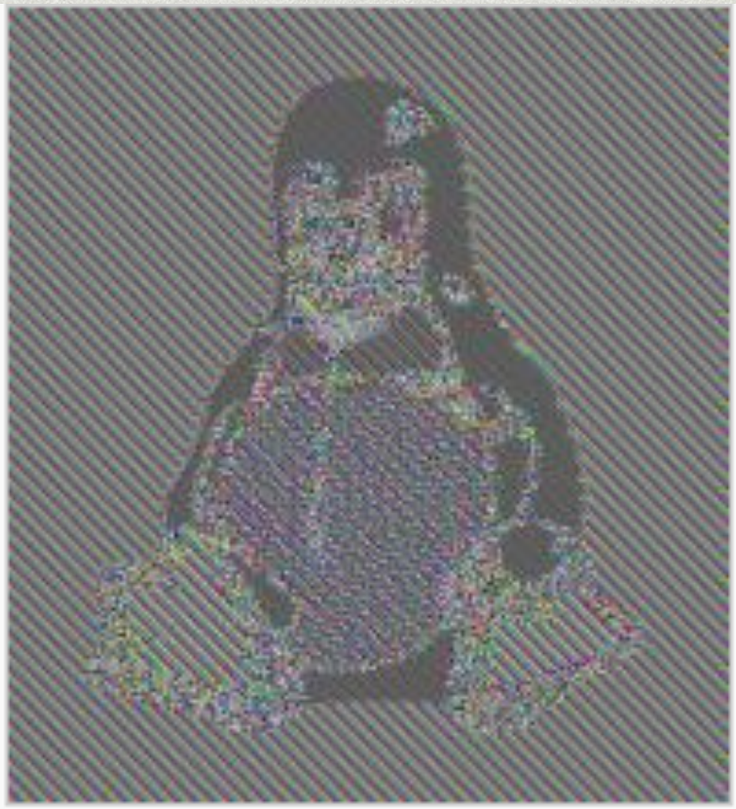
Traditional modes of operation

- ECB: Electronic Code Book
- CBC: Cipher Block Chaining
- CTR: CounTeR mode
- OFB: Output FeeBack mode
- CFB: Cipher FeedBack mode

Unfortunately…

It is not good to use it, because it reveals information about the plaintext

Original image



Encrypted using ECB mode

Modes other than ECB result in pseudo-randomness

Formal definition.

If a block cipher is a function $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$
where $\mathcal{K} = \{0,1\}^k$ and $\mathcal{M} = \mathcal{C} = \{0,1\}^n$

Then a mode operation is a procedure that takes as input:

- A key $K \in \{0,1\}^k$
- A message M of arbitrary length $M \in \{0,1\}^*$
- An initialization vector or *nonce* $IV \in \{0,1\}^v$

The output will be a ciphertext $C \in \{0,1\}^*$

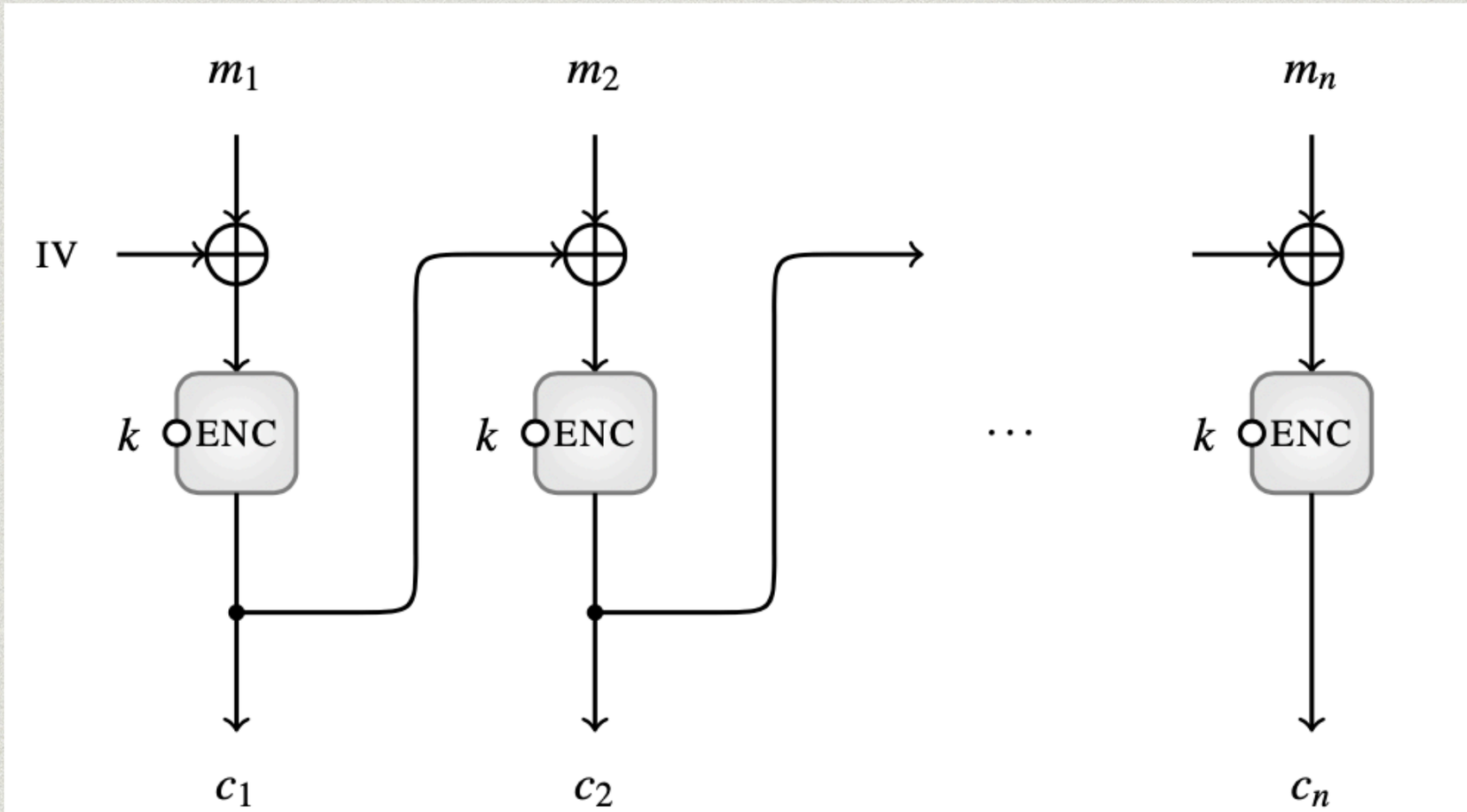
Notation

$$
\begin{aligned}
M = m_1 m_2 \ldots m_n &: \text{plaintext} \\
\oplus &: \text{boolean operation xor} \\
IV &: \text{initialization vector,} \\
\mathrm{ENC} &: \text{any block cipher} \\
k &: \text{secret key} \\
C = c_1 c_2 \ldots c_n &: \text{ciphertext}
\end{aligned}
$$

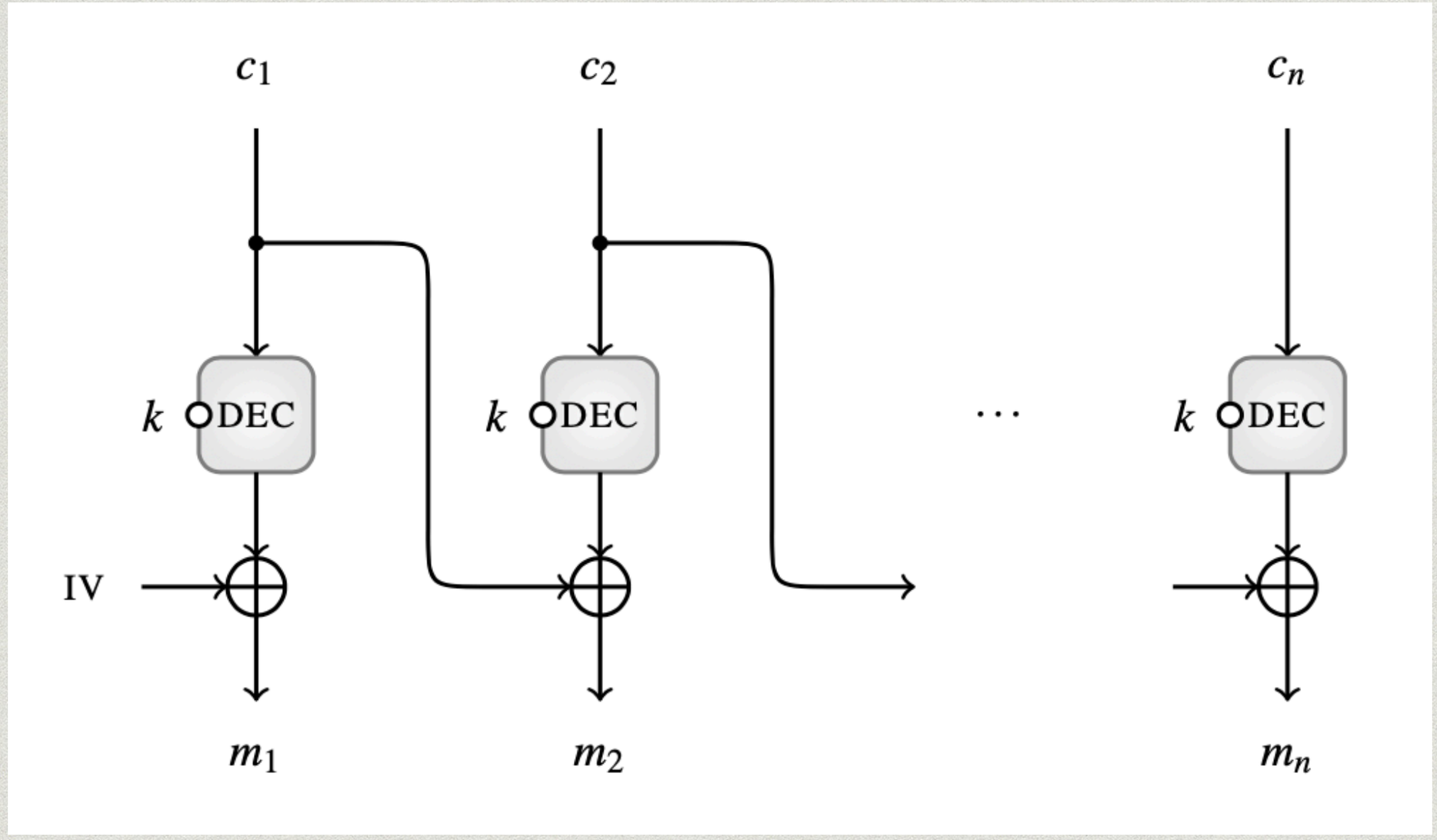
Important note: IV must be **public**, **random** and must be **used only once**

CBC: Cipher Block Chaining

Enciphering:



Deciphering with CBC



What will happen when we decipher if one of the blocks of cipher text is corrupted?

Is it possible or not to decipher the rest of the blocks? Why?

Algorithm for CBC

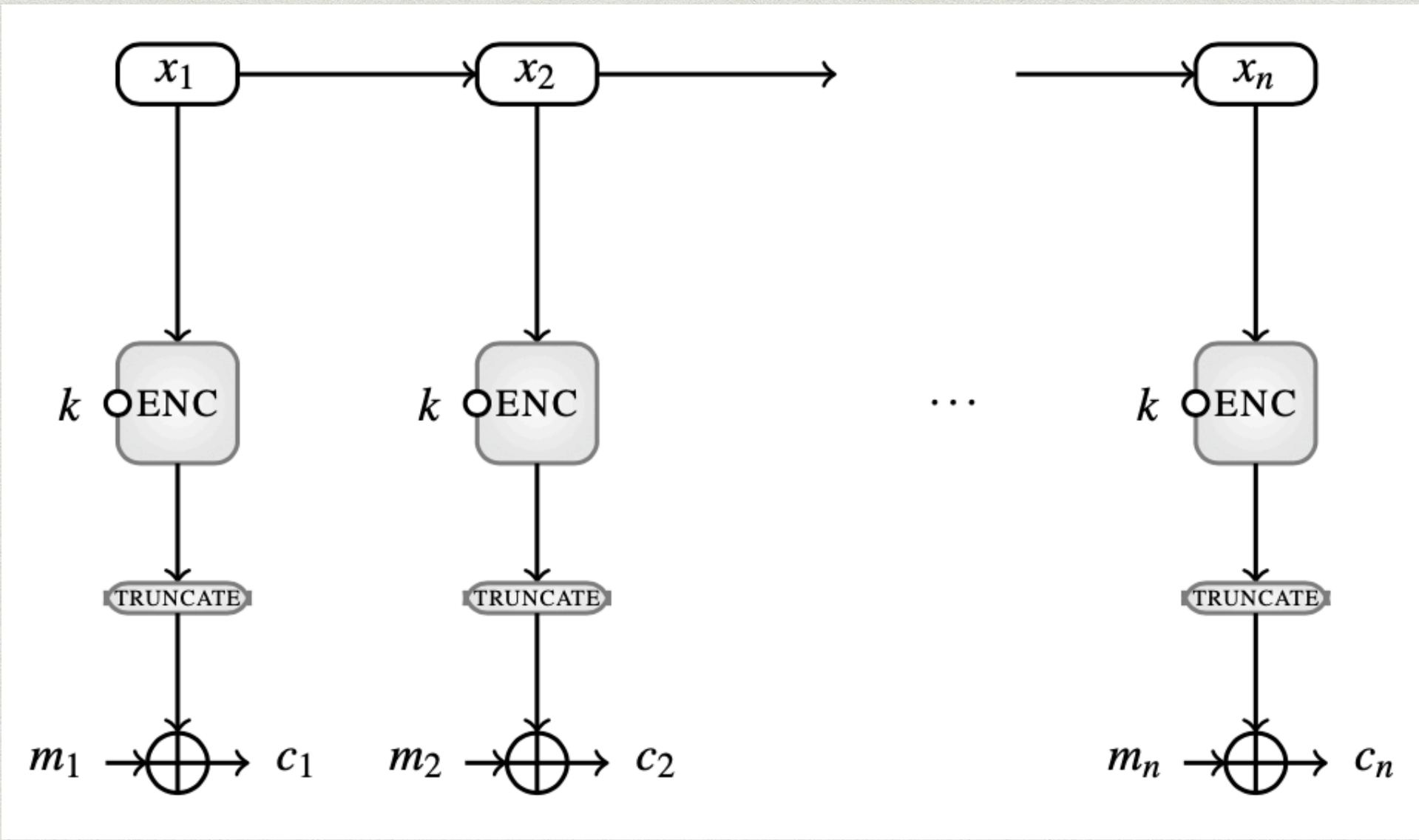
P: plaintext, C: ciphertext, IV: initialization vector

Algorithm $\text{CBC.Encrypt}_K^{\text{IV}}(P)$	**Algorithm** $\text{CBC.Decrypt}_K^{\text{IV}}(C)$
1. Partition P into $P_1, P_2, \ldots, P_m$	1. Partition C into $C_1, C_2, \ldots, C_m$
2. $C_1 \leftarrow E_K(P_1 \oplus \text{IV})$;	2. $P_1 \leftarrow E_K^{-1}(C_1) \oplus \text{IV}$
3. **for** $i \leftarrow 2$ to m	3. **for** $i \leftarrow 2$ to m
4. $\quad C_i \leftarrow E_K(P_i \oplus C_{i-1})$	4. $\quad P_i \leftarrow E_K^{-1}(C_i) \oplus C_{i-1}$
5. **end for**	5. **end for**
6. **return** $C_1, C_2, \ldots, C_m$	6. **return** $P_1, P_2, \ldots, P_m$

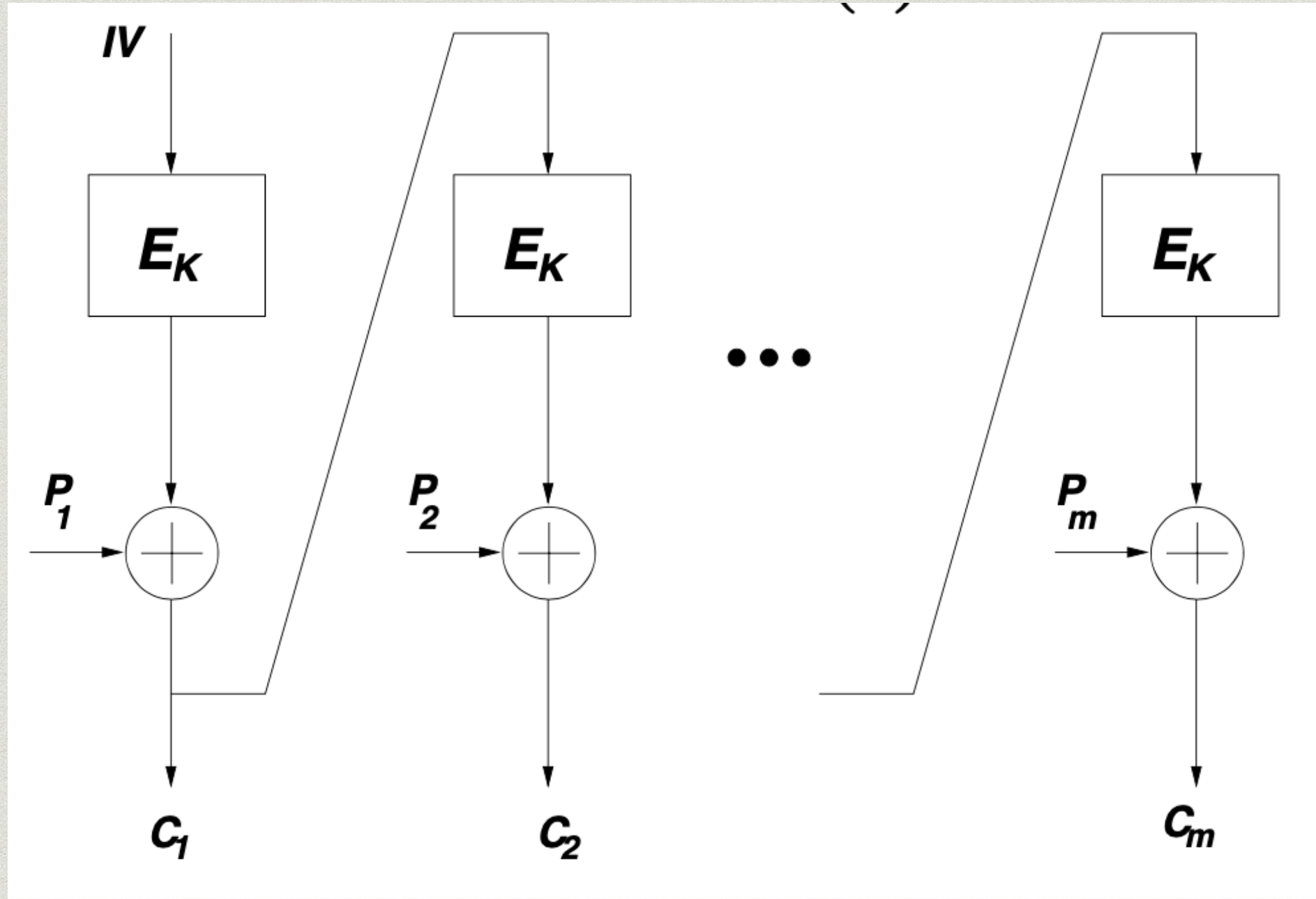
CTR: CounTeR mode

Enciphering.

$x_1, x_2, \ldots, x_n$ are counters



CFB: Cipher FeedBack mode



Pros of CTR

- We can precompute the counters
- We only need to encipher with the block cipher, i.e.we do not need to decipher with the block cipher.
- The block cipher calls can be done in parallel