

10/19/26

COMP 435:

Computer Security Concepts



Lecture 23: Block Ciphers



The University
of North Carolina
at Chapel Hill

<https://tinyurl.com/comp435-fa26>

Logistics Update



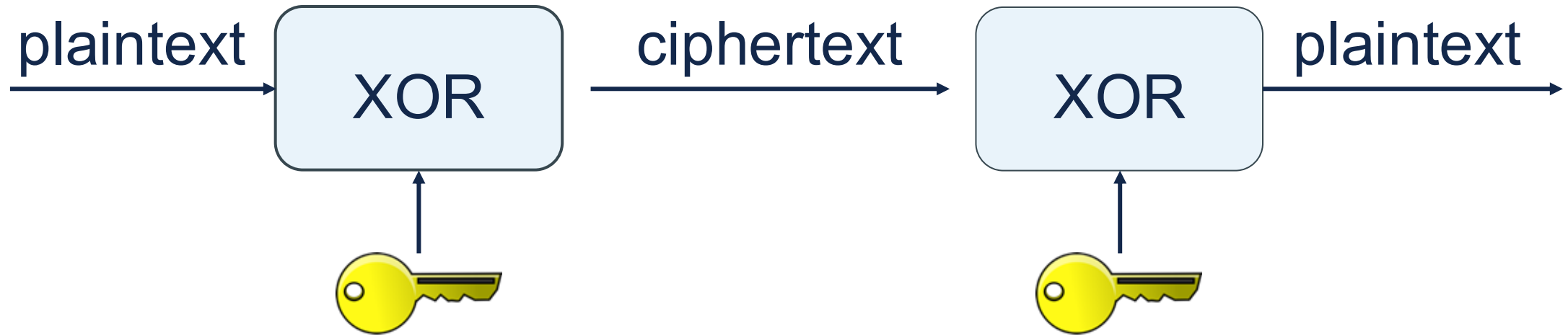
- Details about final project posted
 - First milestone due 10/21
- WA4 Next Friday. Crypto in Practice. I will post Monday!
 - Part 1 due 10/22
 - Part 2 in-class



X perfect Security

One Time Pad

One Time Pad (Vernam Cipher)



$$c_i = p_i \oplus k_i$$

$$p_i = c_i \oplus k_i$$

One Time Pad (Vernam Cipher)



- Symmetric encryption algorithm
- ***Stream cipher***
- Substitution cipher



each unit of the
plaintext is
encrypted
individually using
the corresponding
unit of the key



One Time Pad

- Key material is as long as message
- Key material is never reused
- Key material is kept secret
- Key material is chosen uniformly at random

OTP offers ***information-theoretical security***

A hand-drawn, dark brown wavy line that starts with a small peak, dips into a valley, and then rises back to a level slightly higher than the start.



Information-Theoretical Security

Def'n: Security derives from information theory

OTP is information-theoretically secure:

- Attacker cannot recover plaintext without the key
- Not susceptible to cryptanalysis
- Not susceptible to exhaustive search

Lec22 Worksheet 😊 -- The Front

OTP



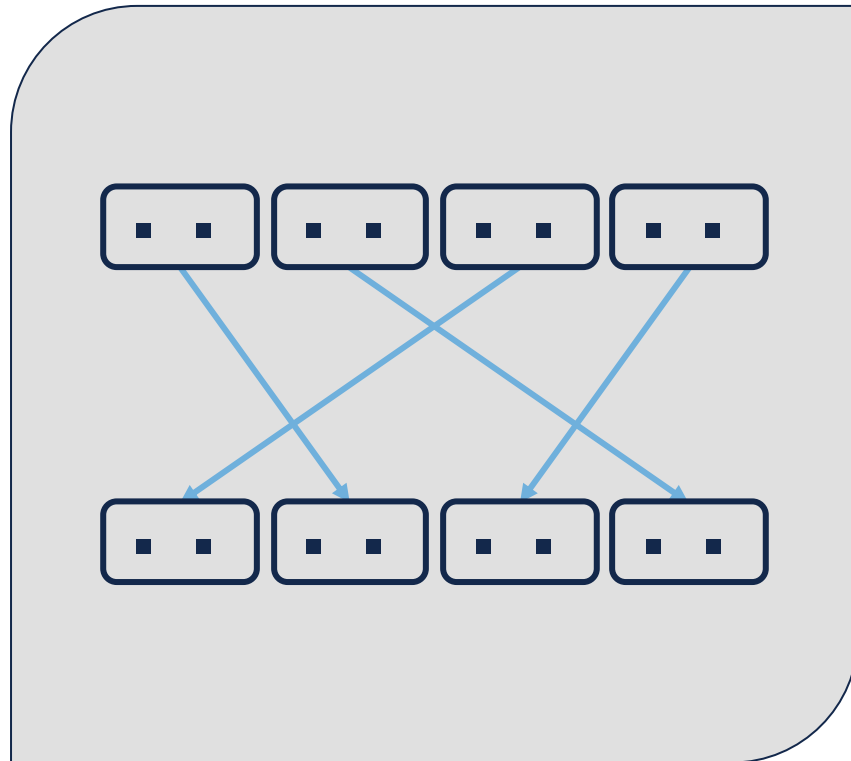
~~X~~ Confidential

- Provides **perfect secrecy**
- Does not provide integrity
 - Even though attacker can't read msg, attacker can modify it in a predictable way
- Difficult to use in practice
 - Managing key distribution & key storage is hard!

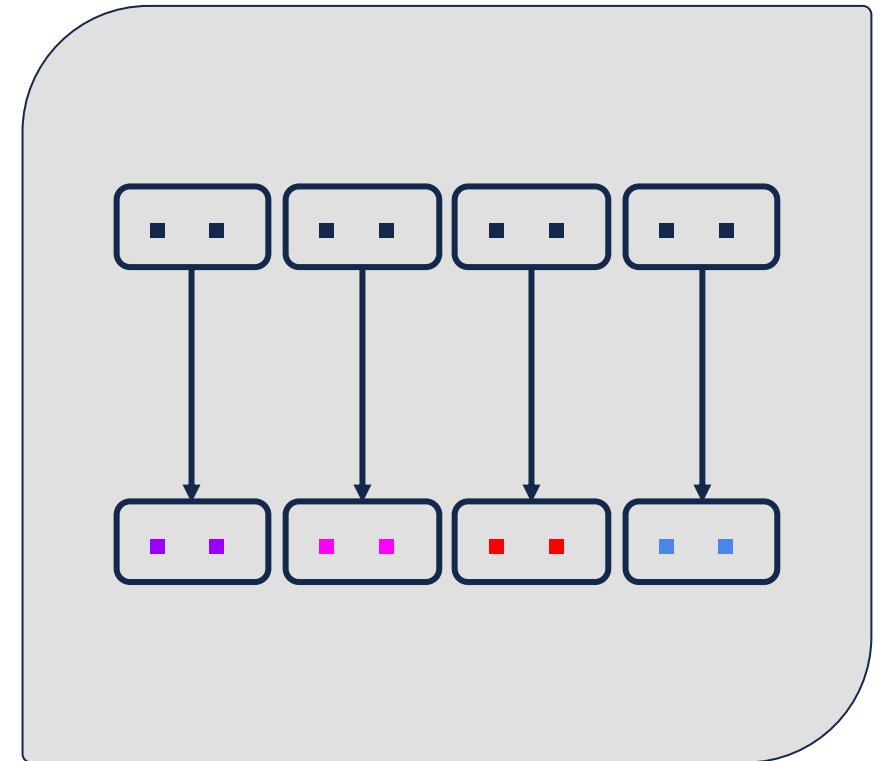


Symmetric Encryption

Building Blocks of Symmetric Encryption Ciphers



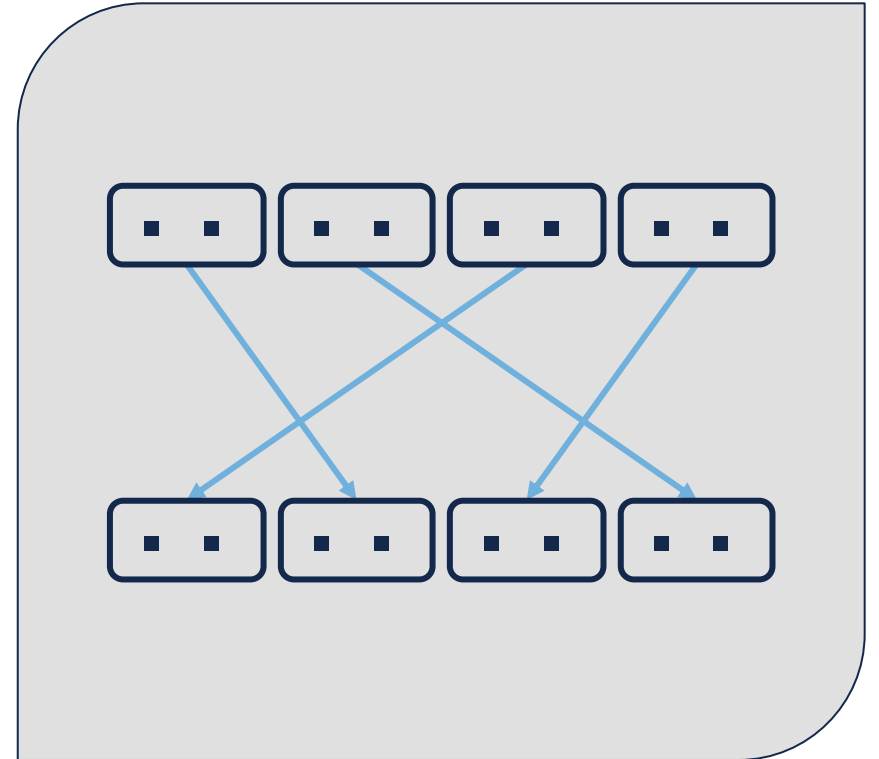
Transposition



Substitution



Transposition



Transposition



Def'n: symbols of plaintext are rearranged and reordered in the ciphertext

E.g., security $\rightarrow$ cresiytu

Without Transposition



This is a slide. In this presentation there are many slides. If you go through all the slides, you will see the complete presentation.

Bpqa qa i atqlm. Qv bpqa xzmamvbibqvv bpmzm izm uivg atqlma.
Qn gwc ow bpzwcop itt bpm atqlma, gwc eqtt amm bpm kwuxtmbm
xzmamvbibqvv.

Without Transposition



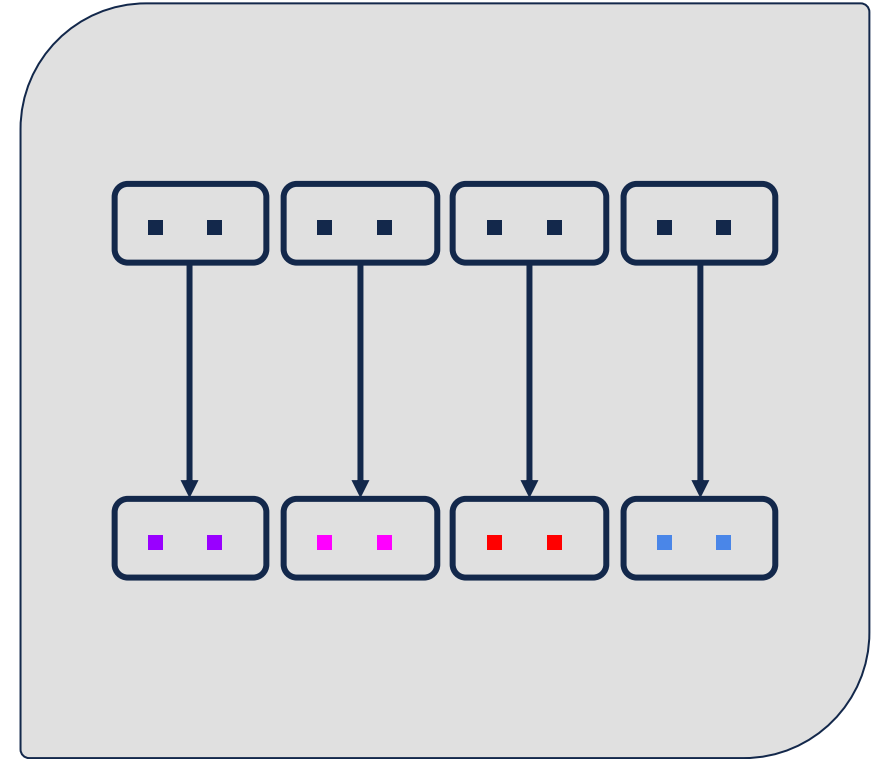
This is a slide. In this presentation there are many slides. If you go through all the slides, you will see the complete presentation.

Bpqa qa i atqlm. Qv bpqa xzmamvbibqwv bpmzm izm uivg atqlma.
Qn gwc ow bpzwcop itt bpm atqlma, gwc eqtt amm bpm kwuxtmbm
xzmamvbibqwv.

Transposition breaks up patterns



Substitution



Substitution



Def'n: each symbol of plaintext is replaced with a new symbol

E.g, Caesar cipher, shift cipher, mono-alphabetic substitution, poly-alphabetic shift, one time pad



Without Substitution

(1) This is a slide about substitution. I hope it is useful to you.

(2) htsi si a ldies tbauo tttssuuiionb. I poeh ti si suelfu ot ouy.

Substitution obscures original symbols

Fixed Substitution Scheme



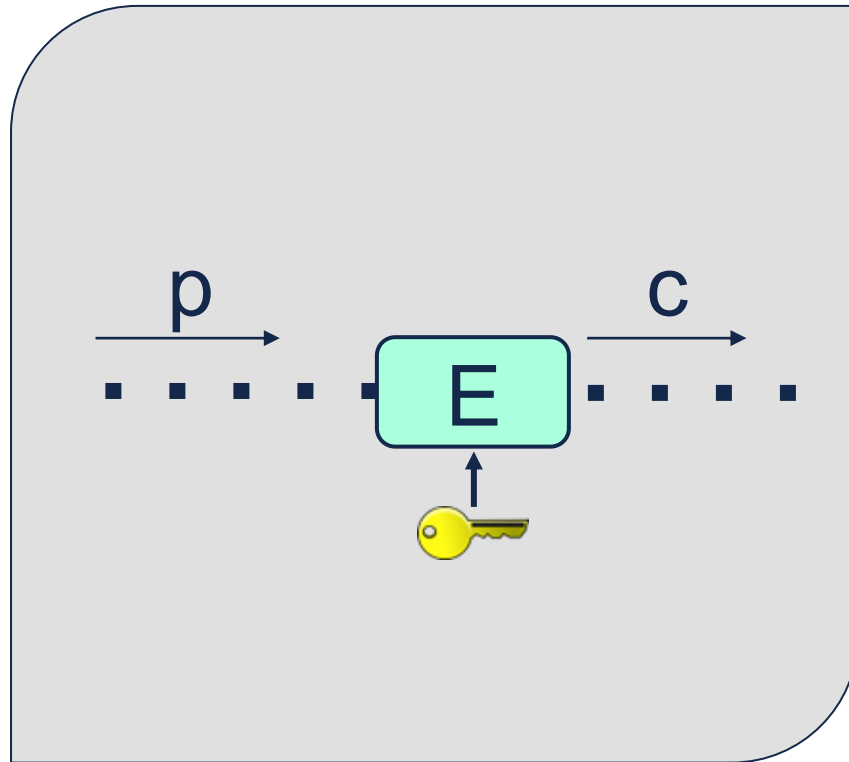
Yvd, yvd, yvd fvby ivha,

Nluasf kvdu aol zaylht.

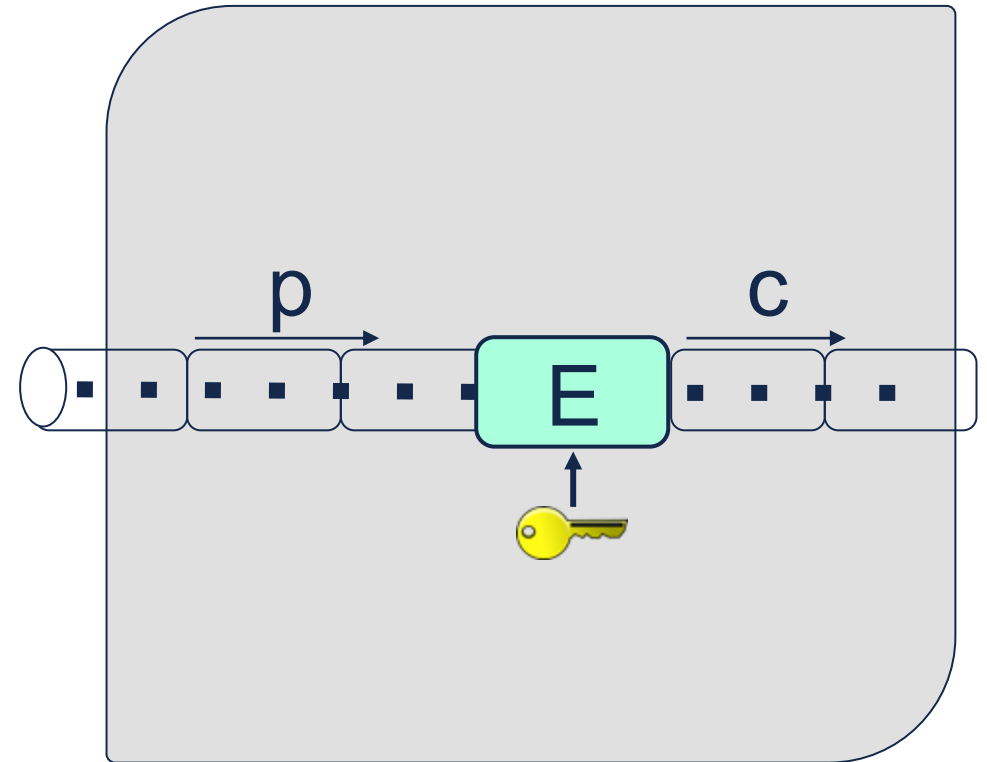
Tlyypsf, tlyypsf, tlyypsf, tlyypsf,

Spml pz iba h kylht.

Symmetric Encryption Algorithms



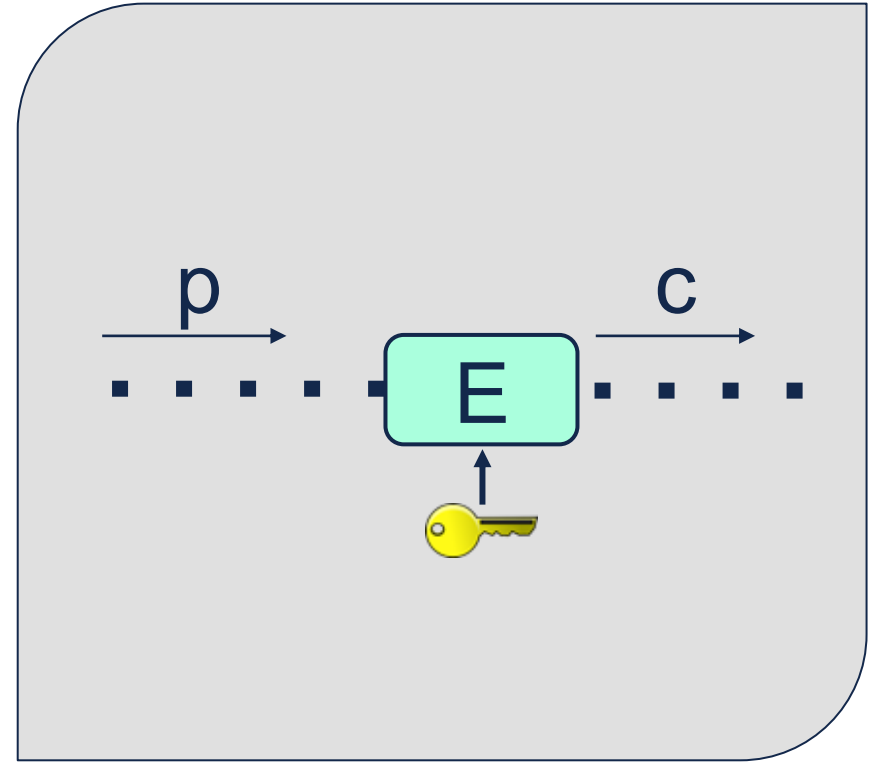
Stream Ciphers



Block Ciphers



Stream Ciphers



Stream Cipher

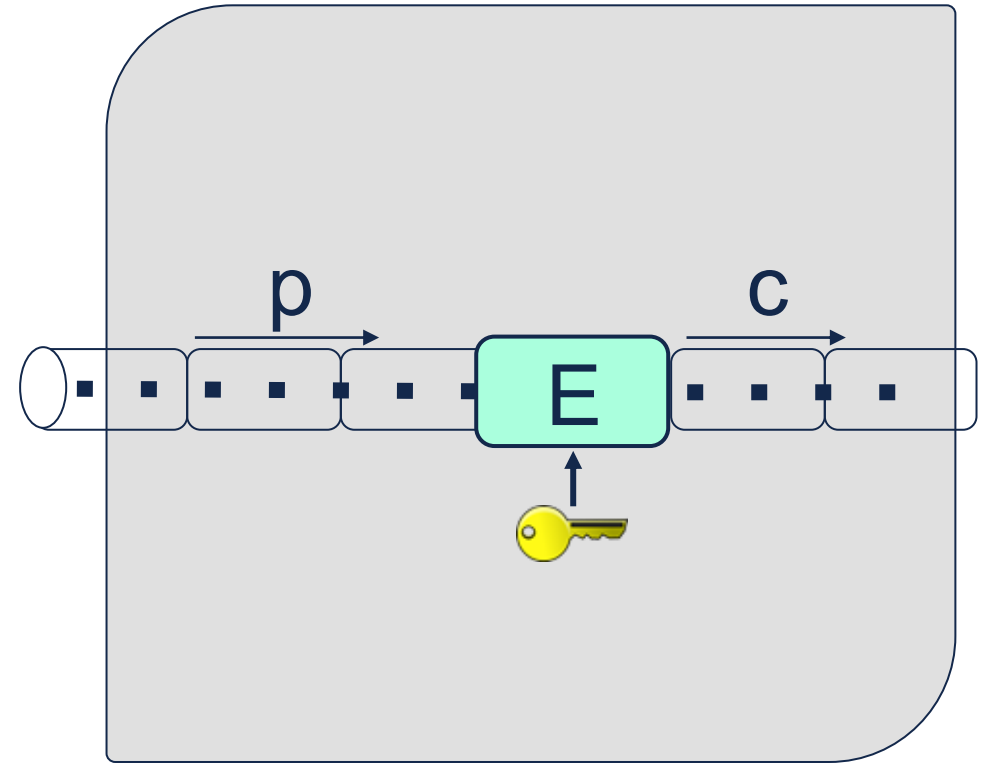


Def'n: each symbol of plaintext (e.g., bit, byte, char, digit) is encrypted separately

E.g., Caesar cipher, poly-alphabetic shift, OTP, RC4



Block Ciphers



Block Cipher



Def'n: groups of symbols are encrypted together as a single block

E.g., AES, DES, 3DES

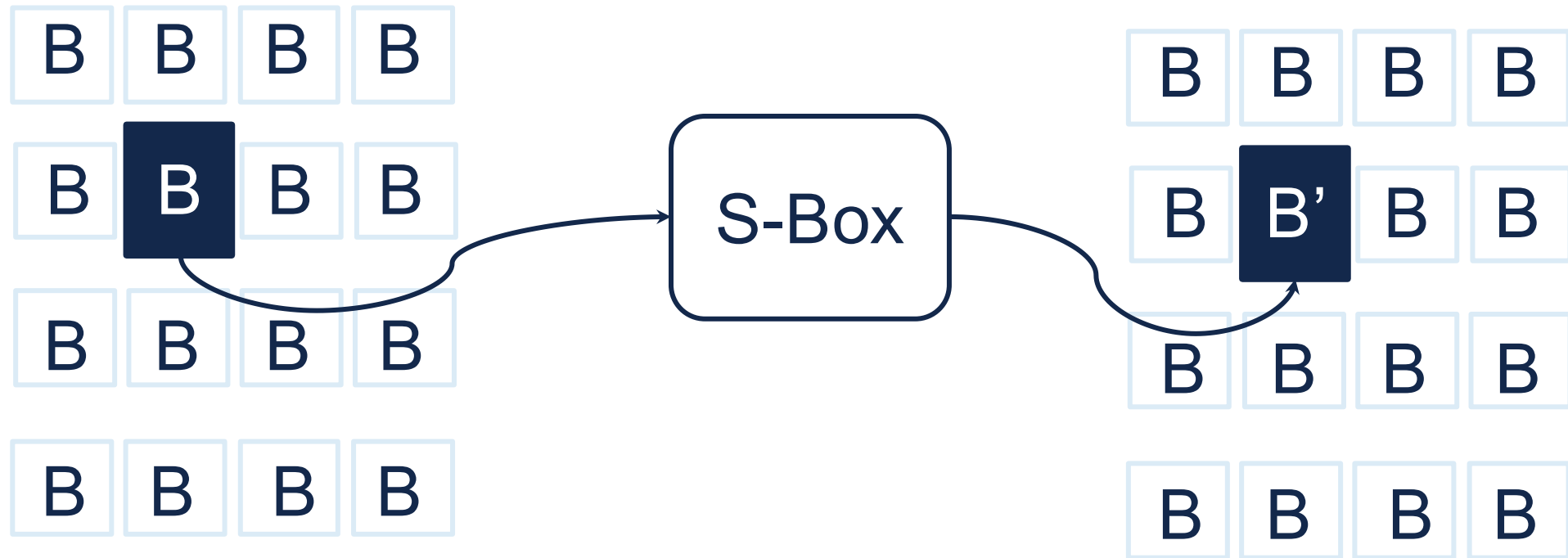
AES



- 1.SubBytes
- 2.ShiftRows
- 3.MixColumns
- 4.AddRoundKey



SubBytes



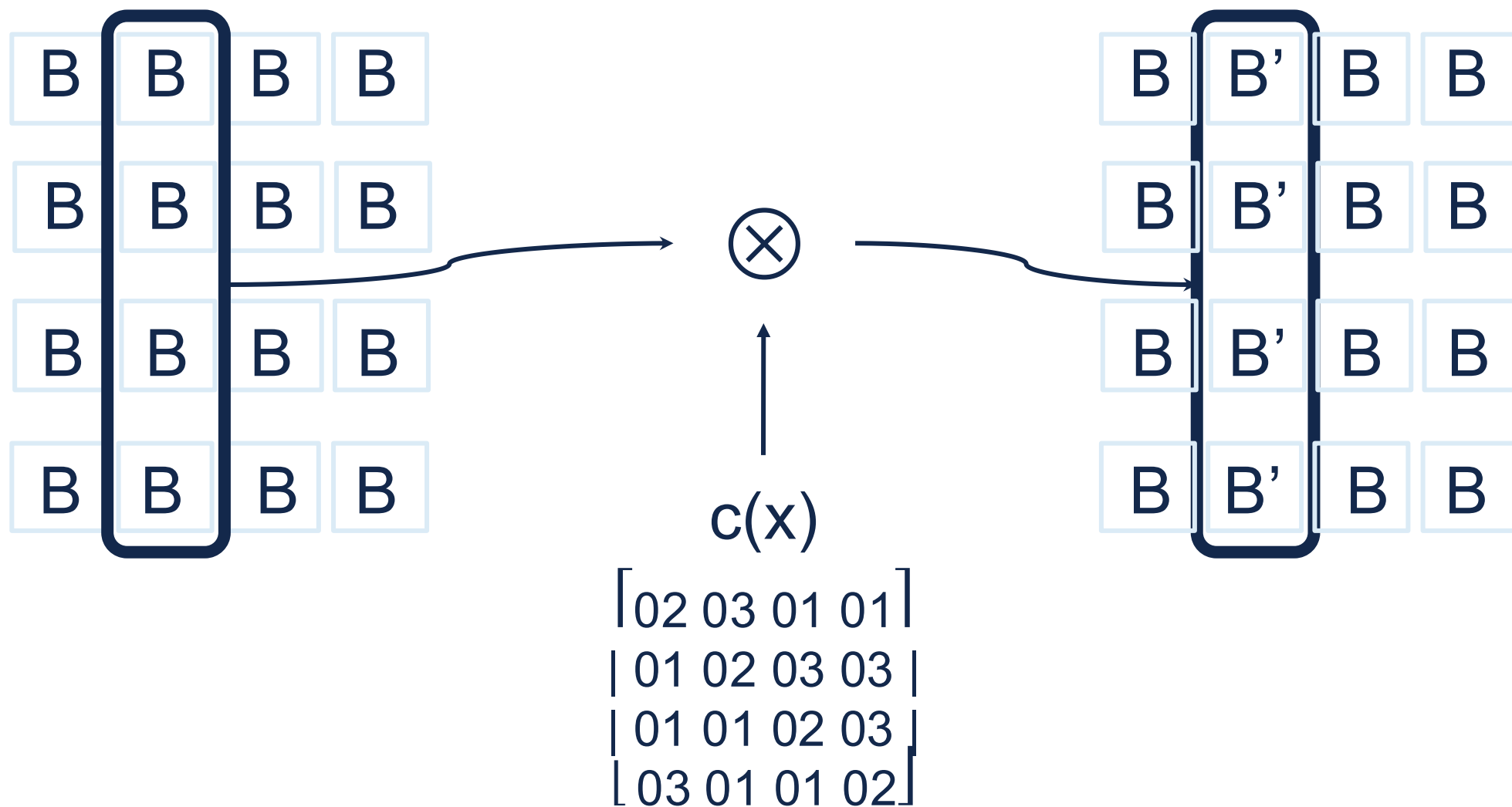
ShiftRows

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

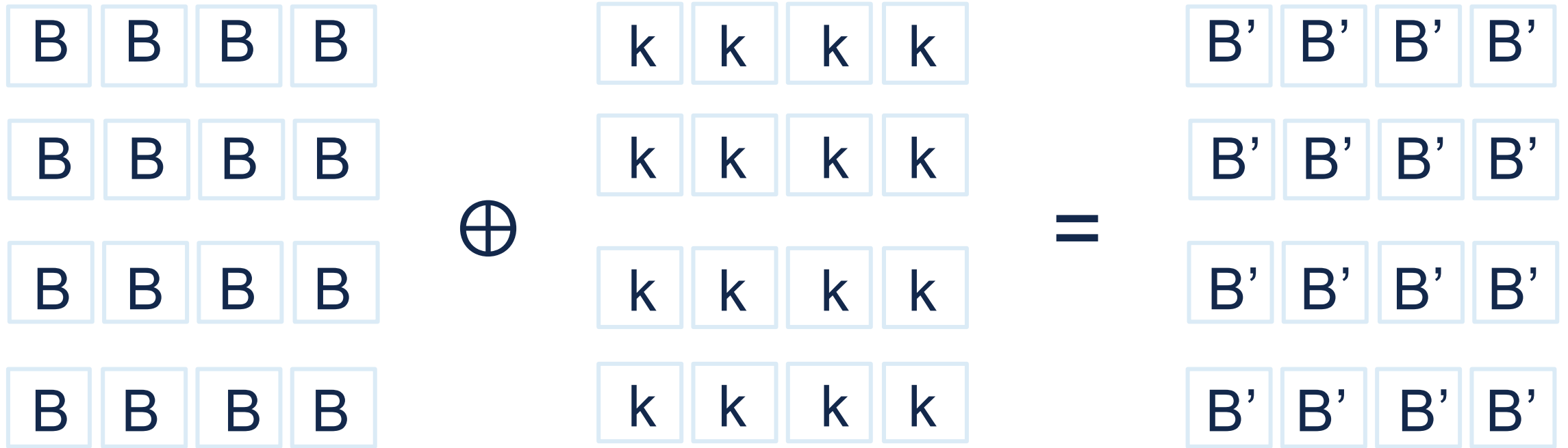


A	B	C	D
F	G	H	E
K	L	I	J
P	M	N	O

MixColumns

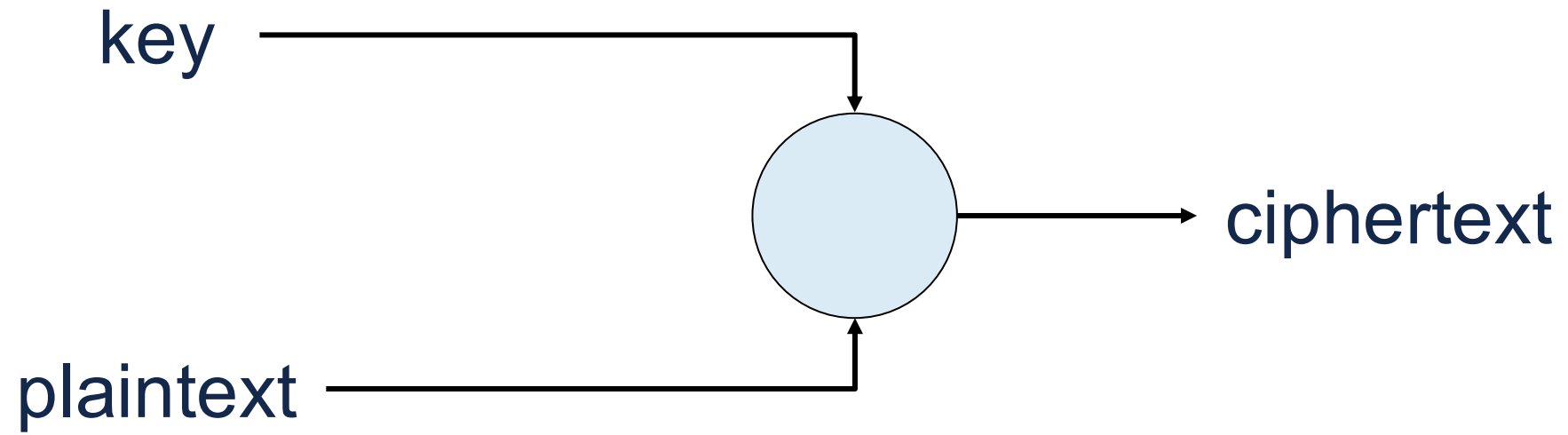


AddRoundKey

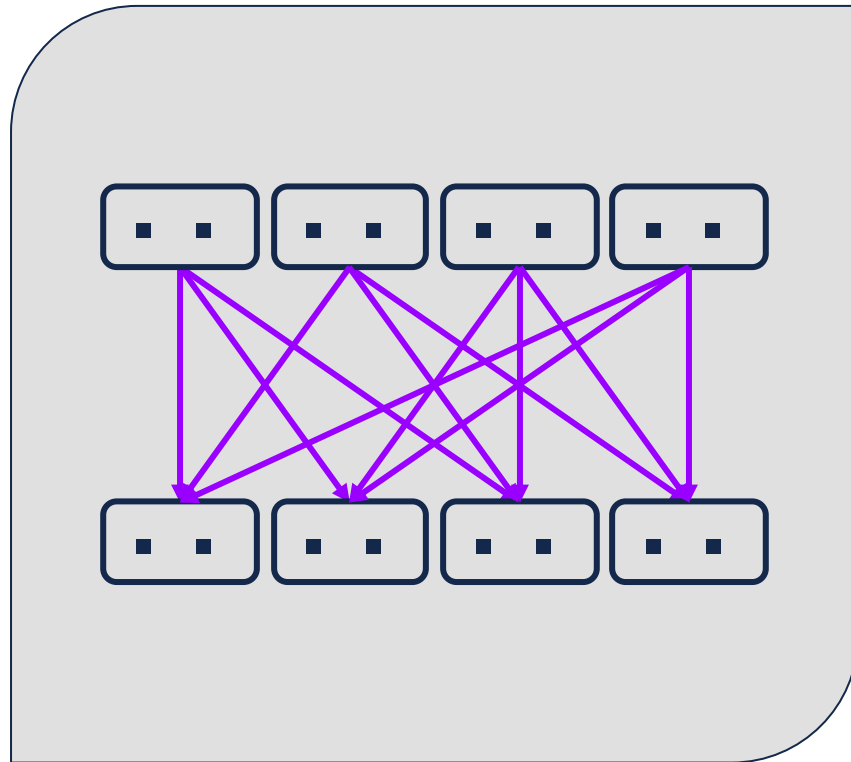




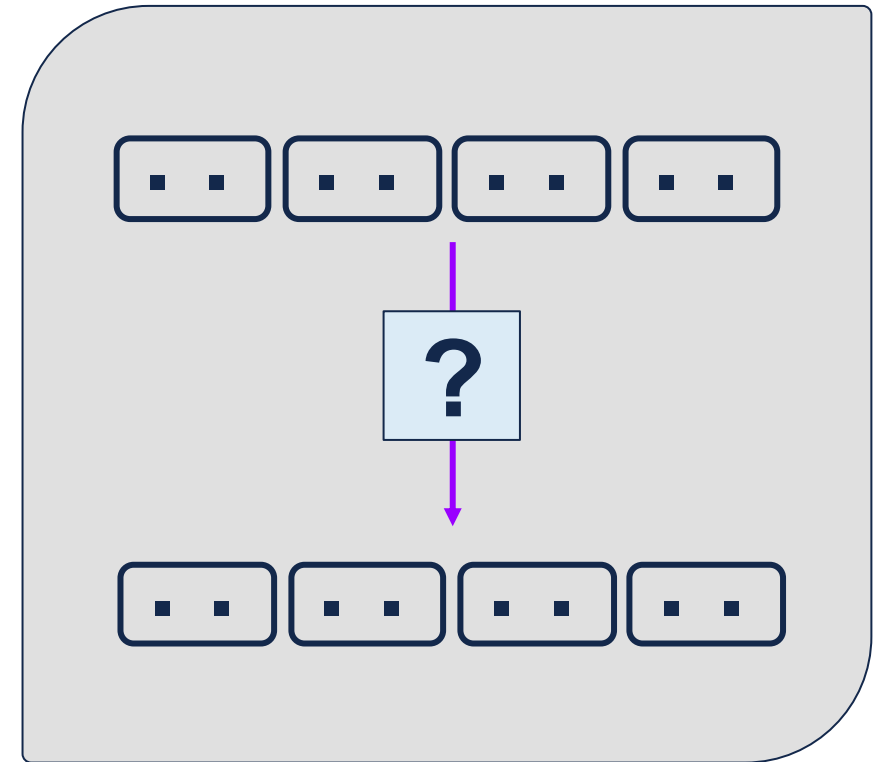
Properties of strong symmetric ciphers



Properties of Strong Symmetric Ciphers



Diffusion

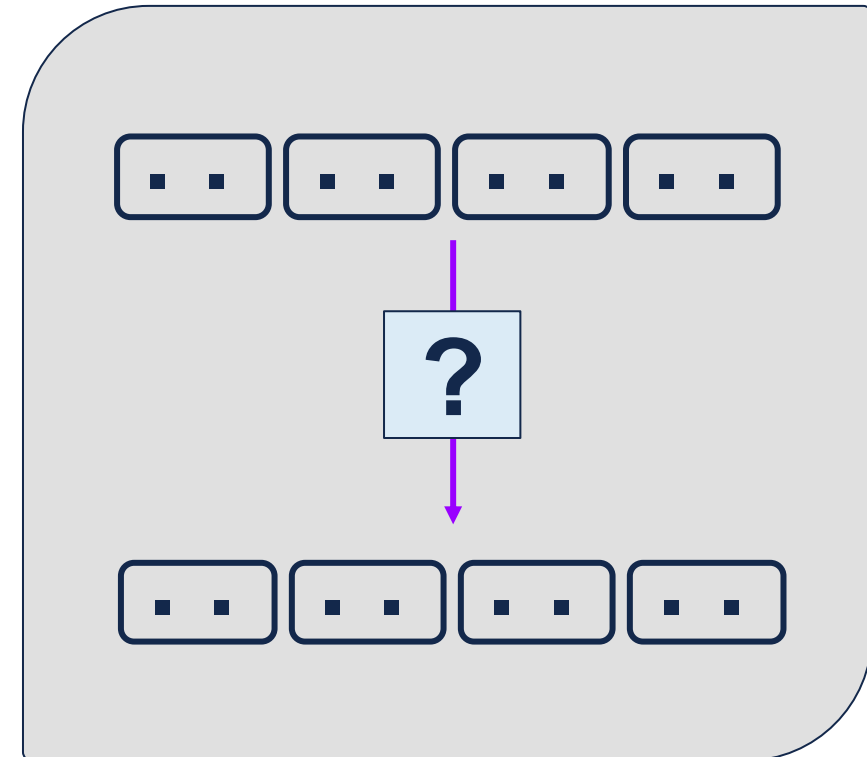


Confusion

Confusion



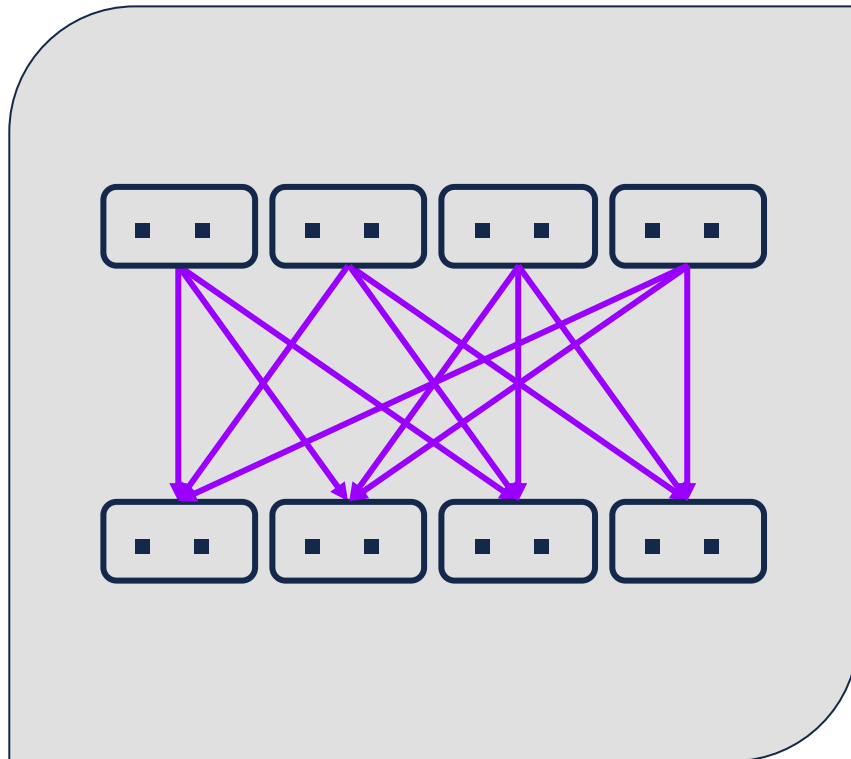
Def'n: obscure the relationship between key and ciphertext



Diffusion



Def'n: spread the plaintext statistics across the ciphertext



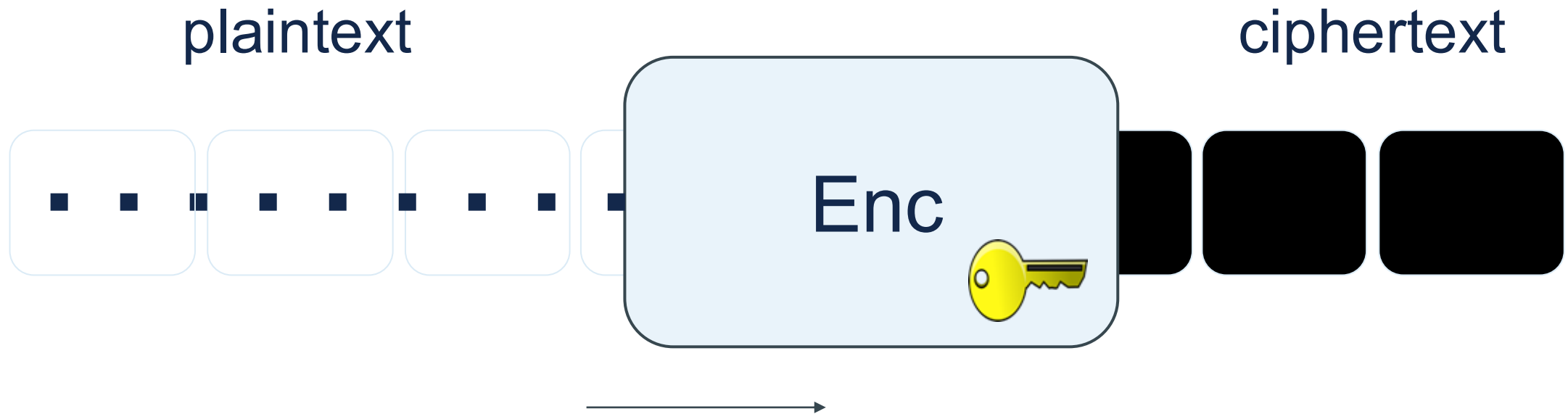
Lec22 Worksheet 😊 -- The Back!



Block Cipher

Modes of Operation

Block Ciphers



Modes of Operation



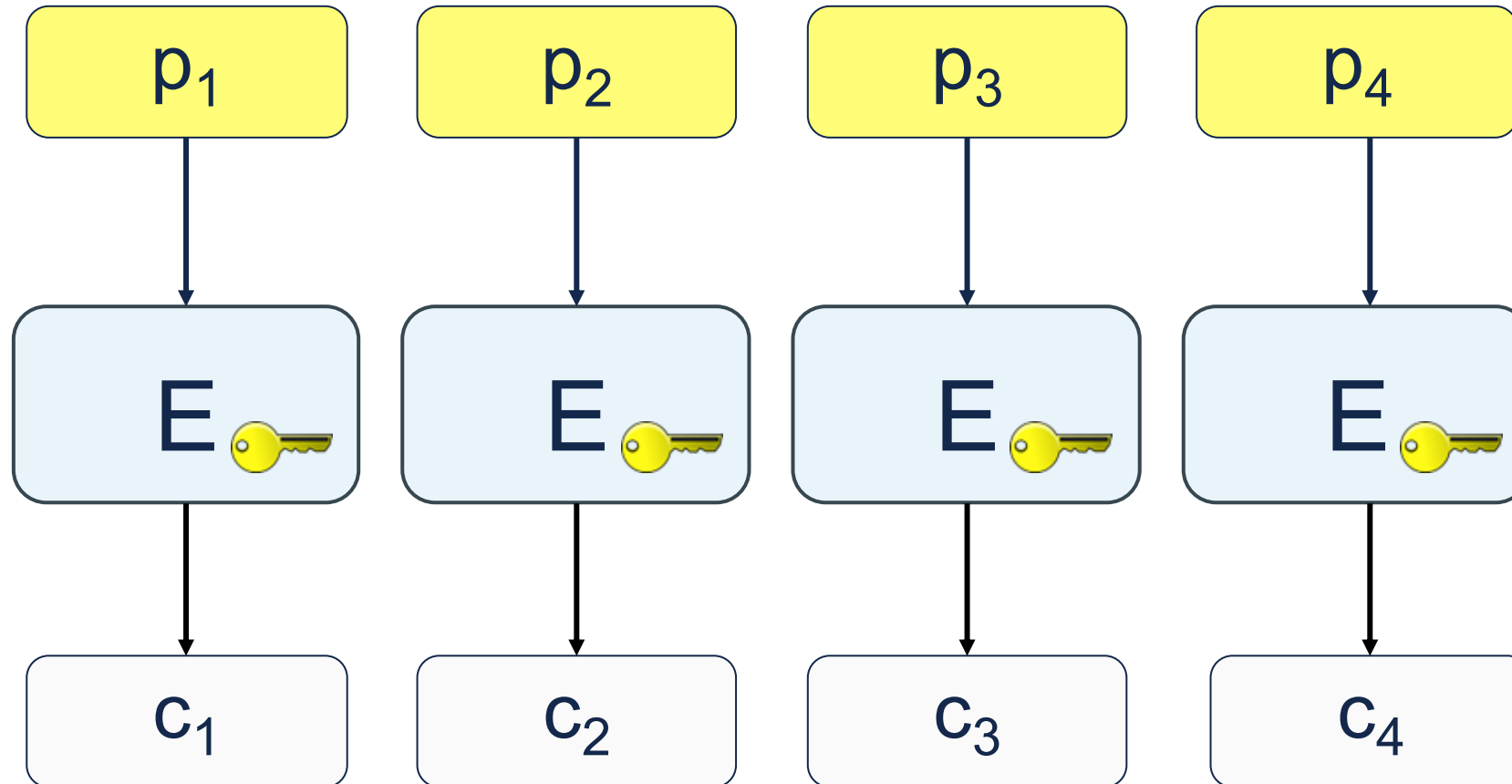
Electronic
Code Book
Mode

Cipher
Block
Chaining
Mode

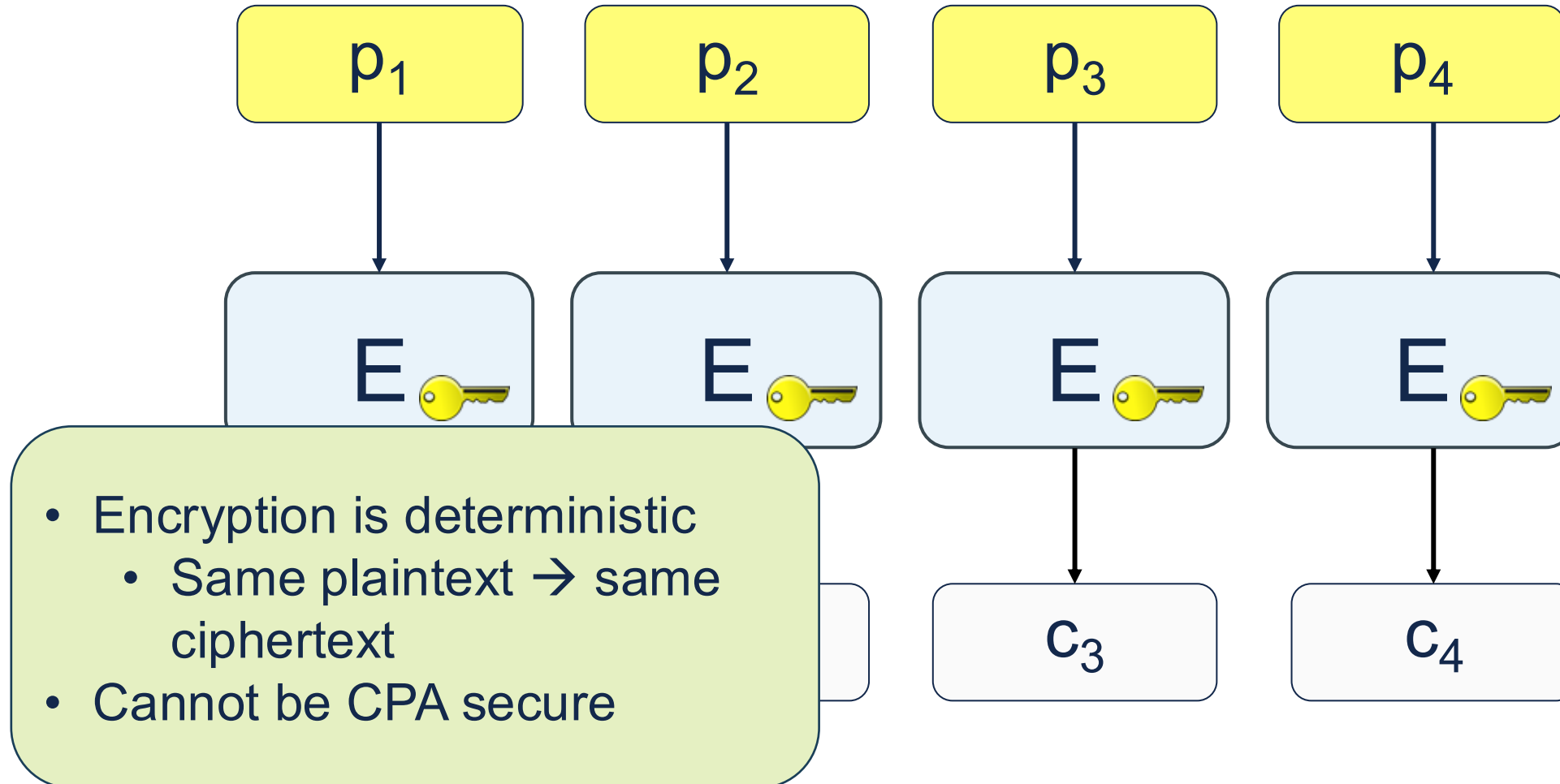
Output
Feedback
Mode

Counter
Mode

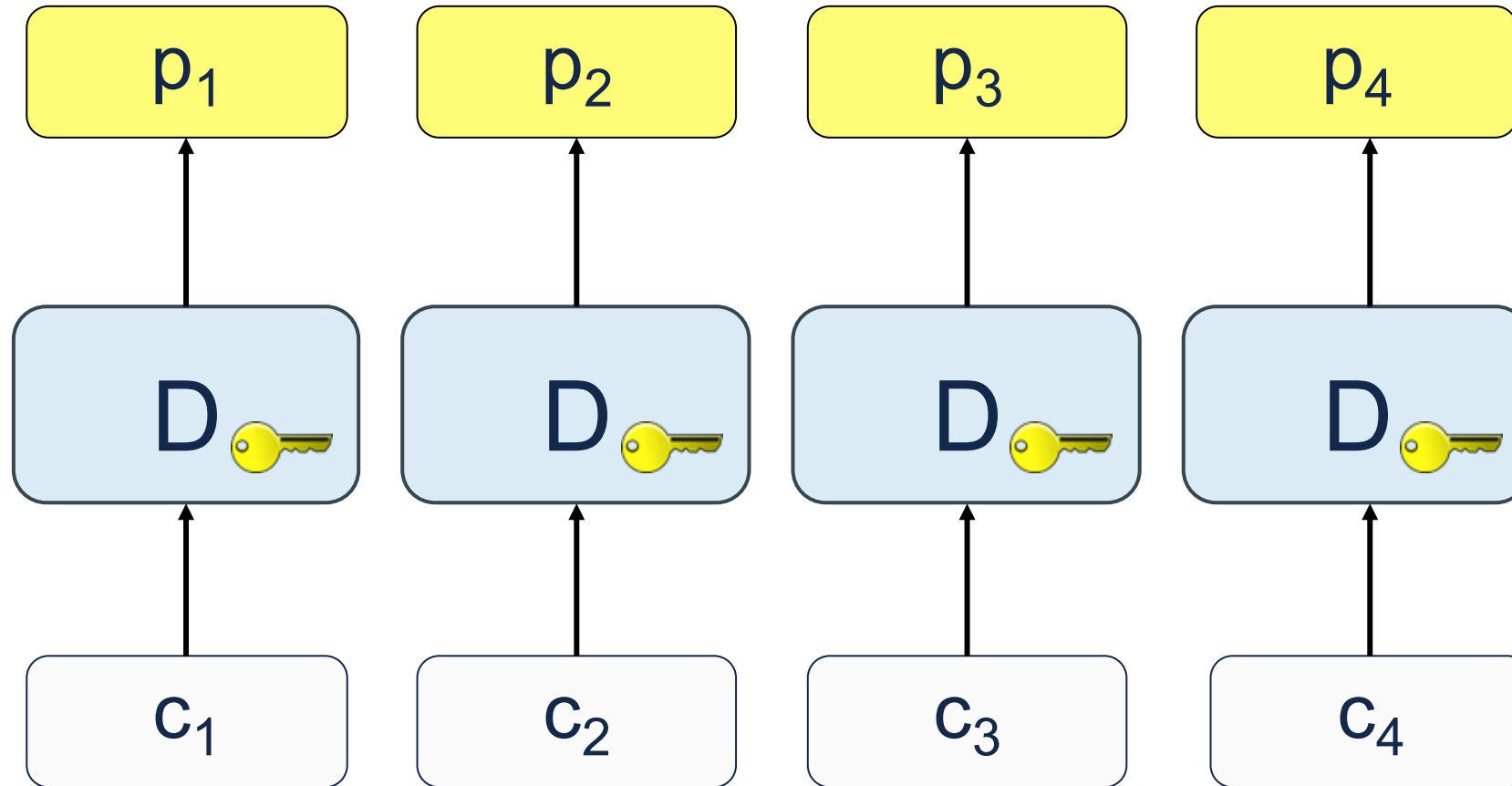
Electronic Code Book (ECB) Mode: Encryption



Electronic Code Book (ECB) Mode: Encryption



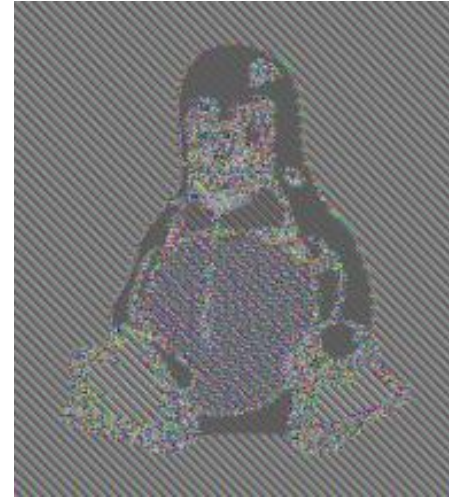
Electronic Code Book (ECB) Mode: Decryption



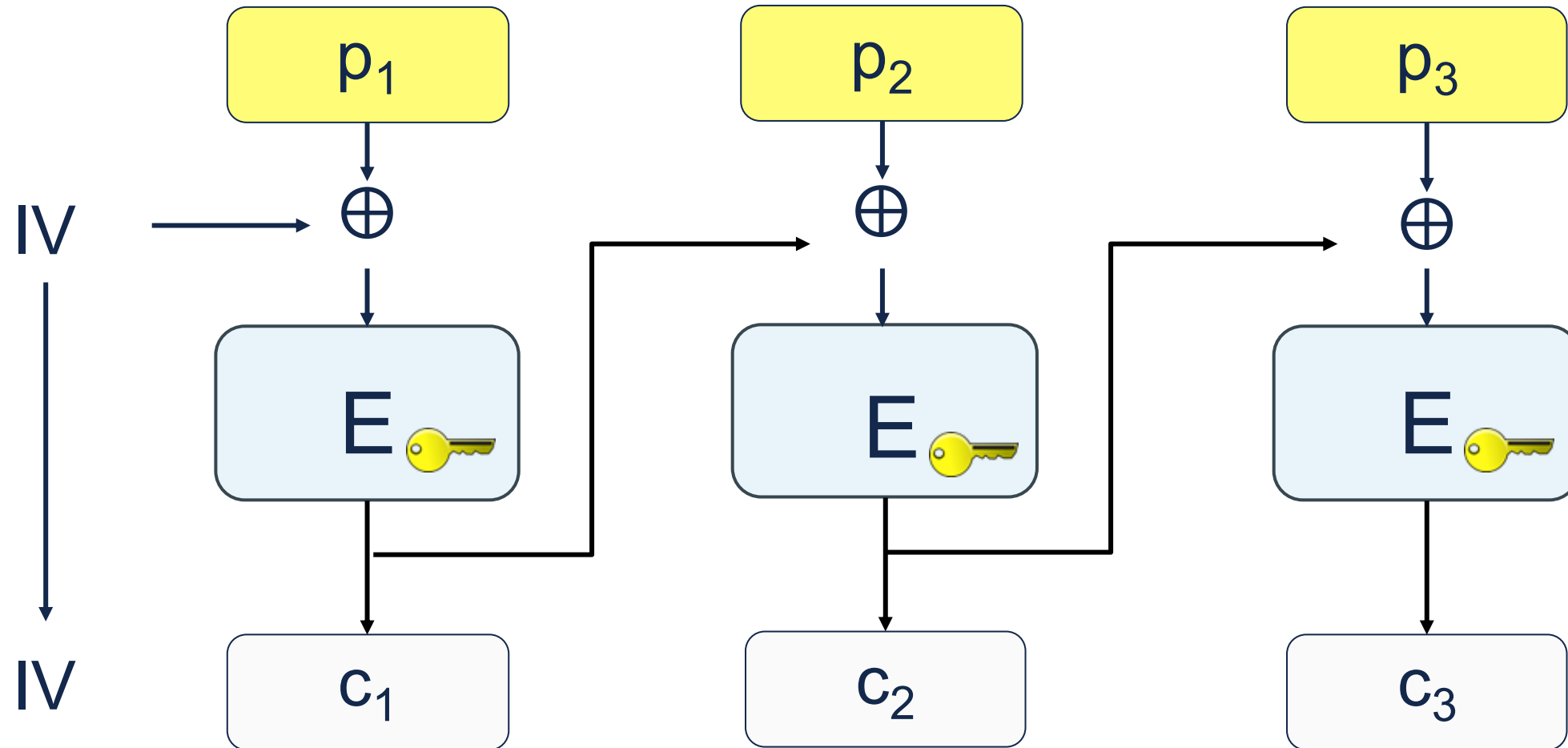
Securely Encrypted



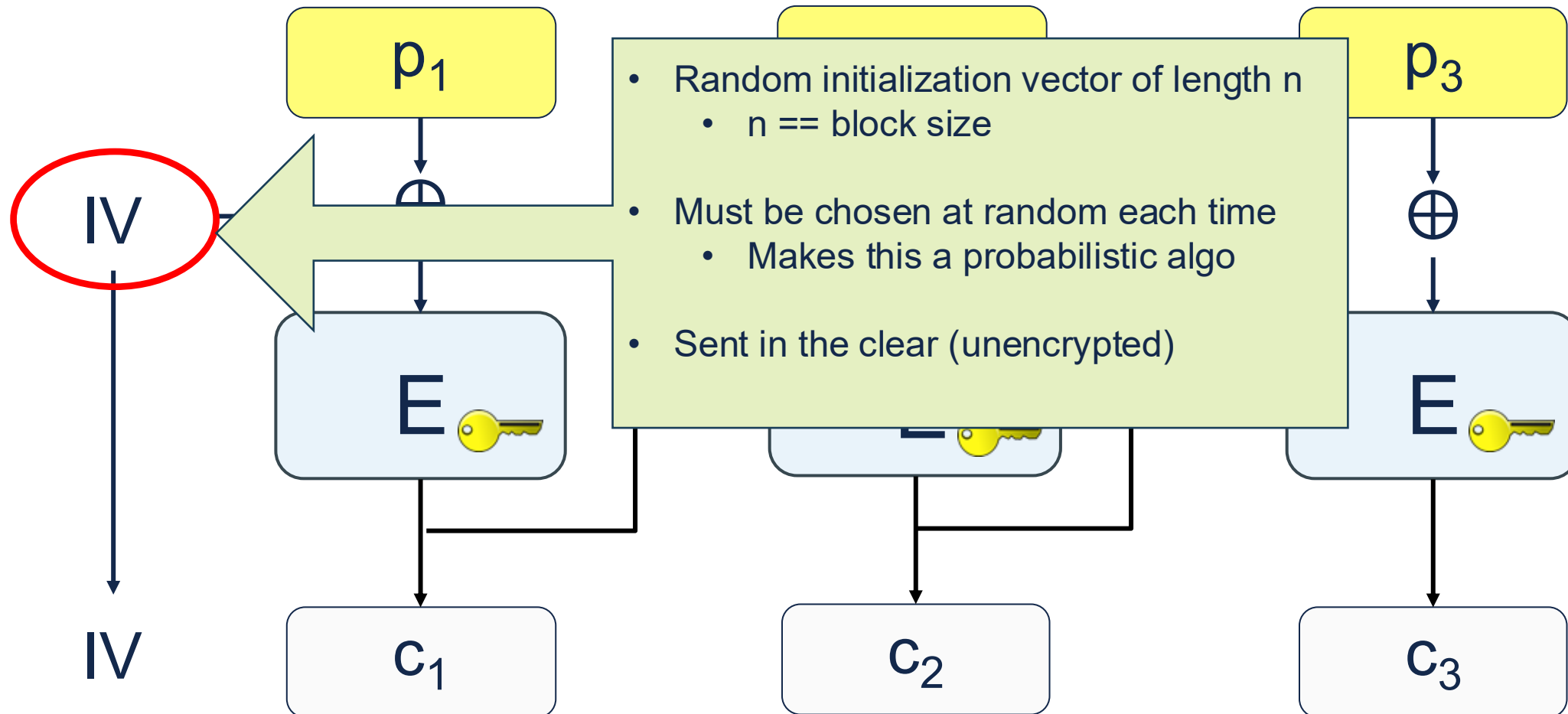
Electronic Code Book (ECB) Mode



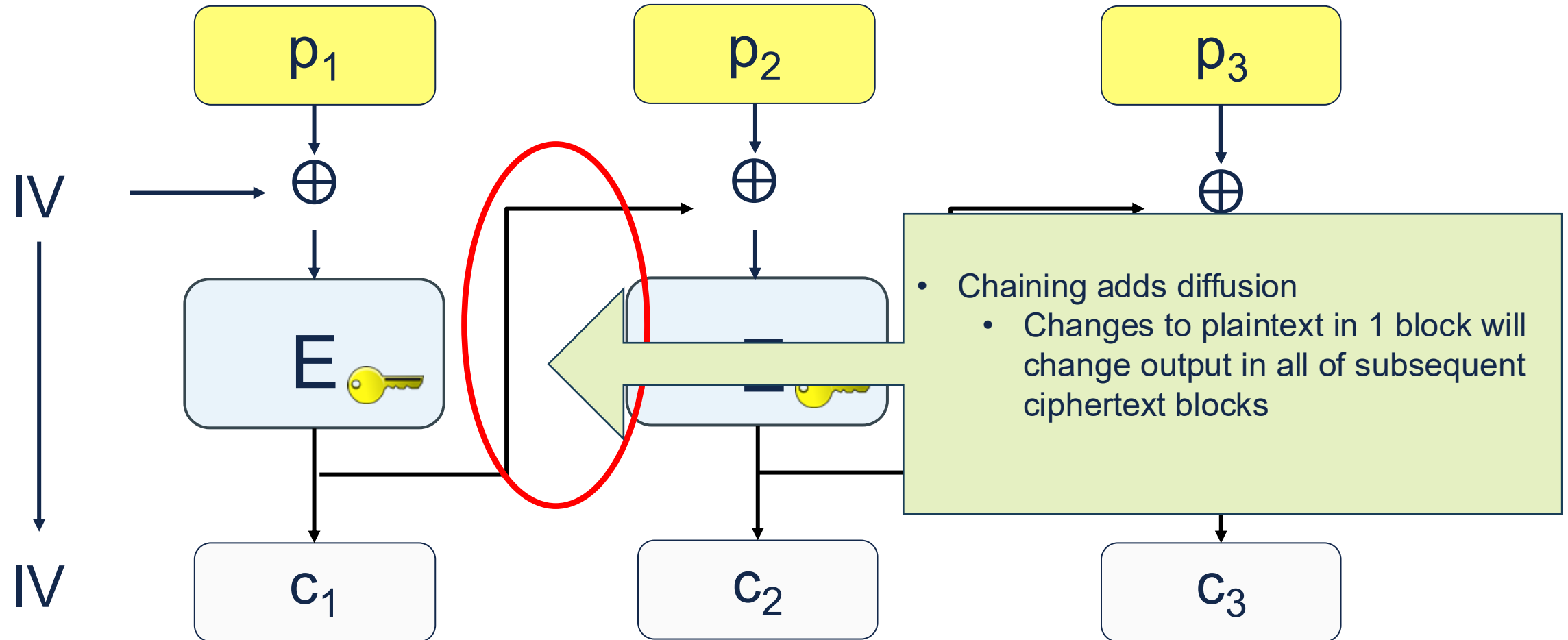
Cipher Block Chaining (CBC) Mode: Encryption



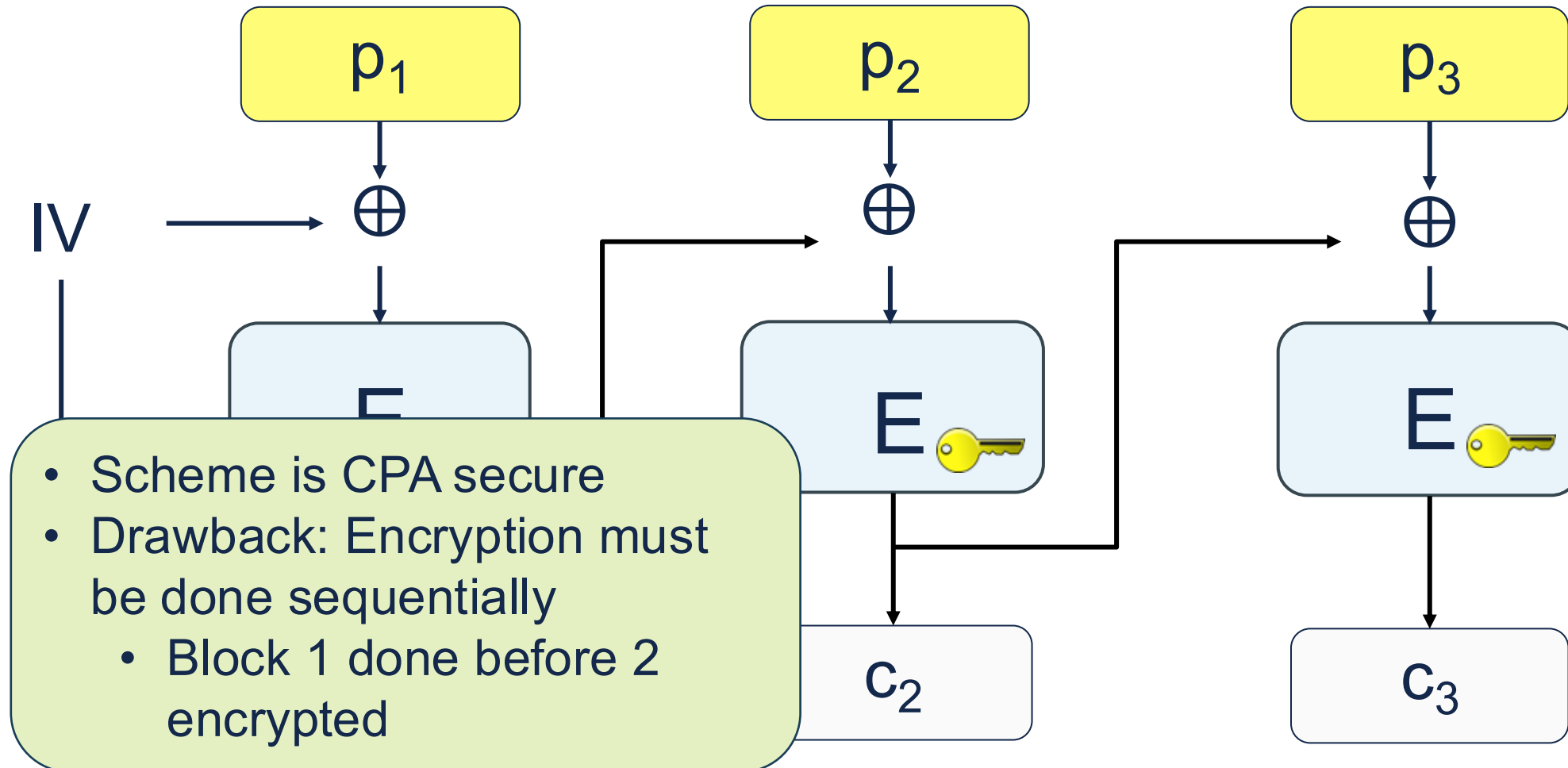
Cipher Block Chaining (CBC) Mode: Encryption



Cipher Block Chaining (CBC) Mode: Encryption

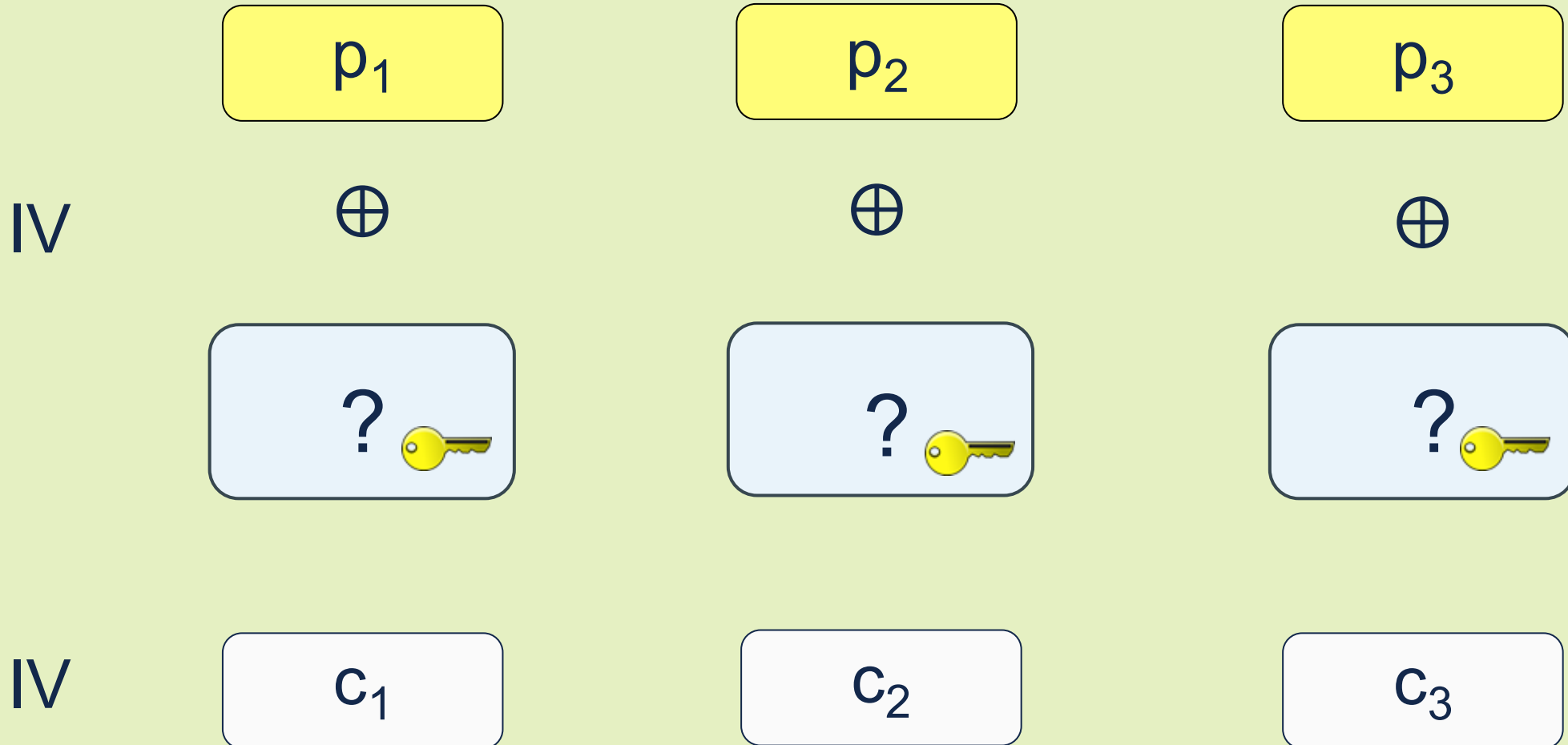


Cipher Block Chaining (CBC) Mode: Encryption

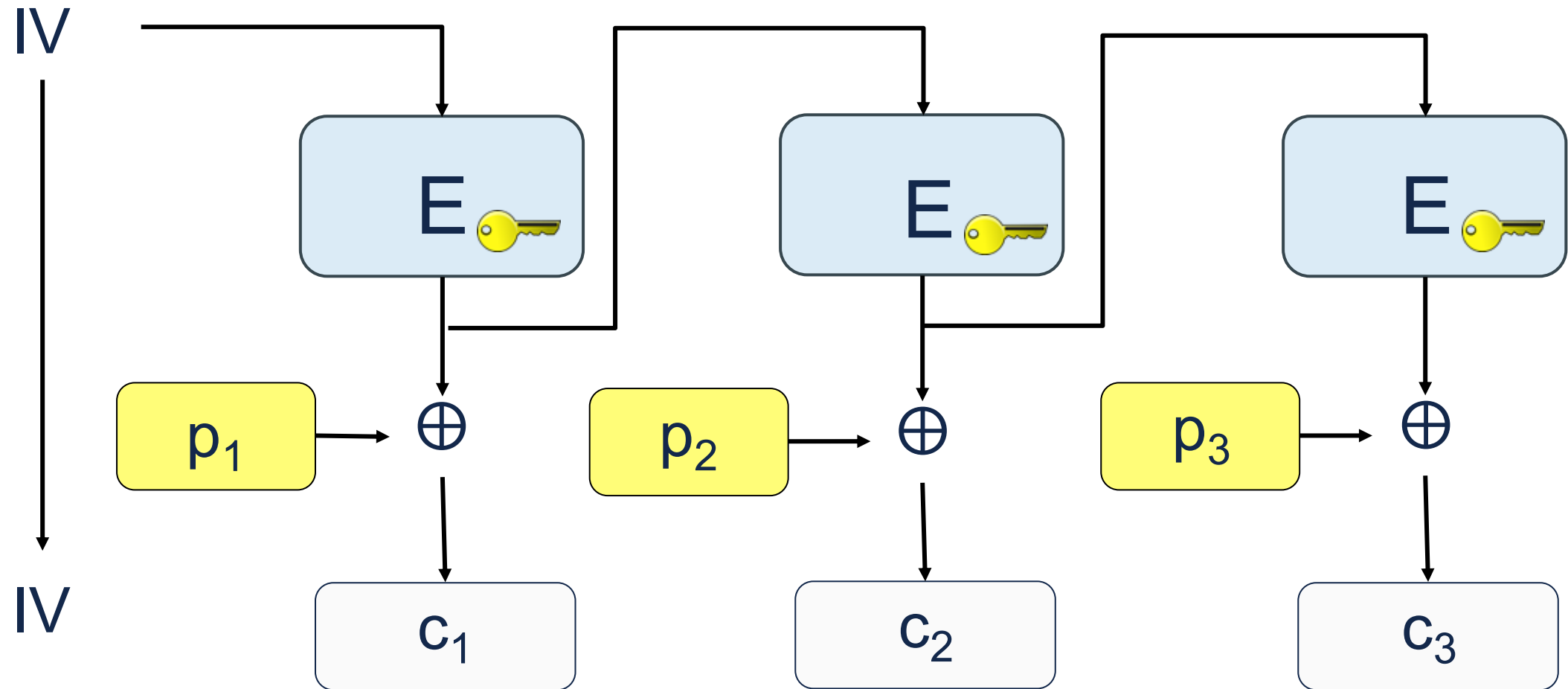


Decryption?

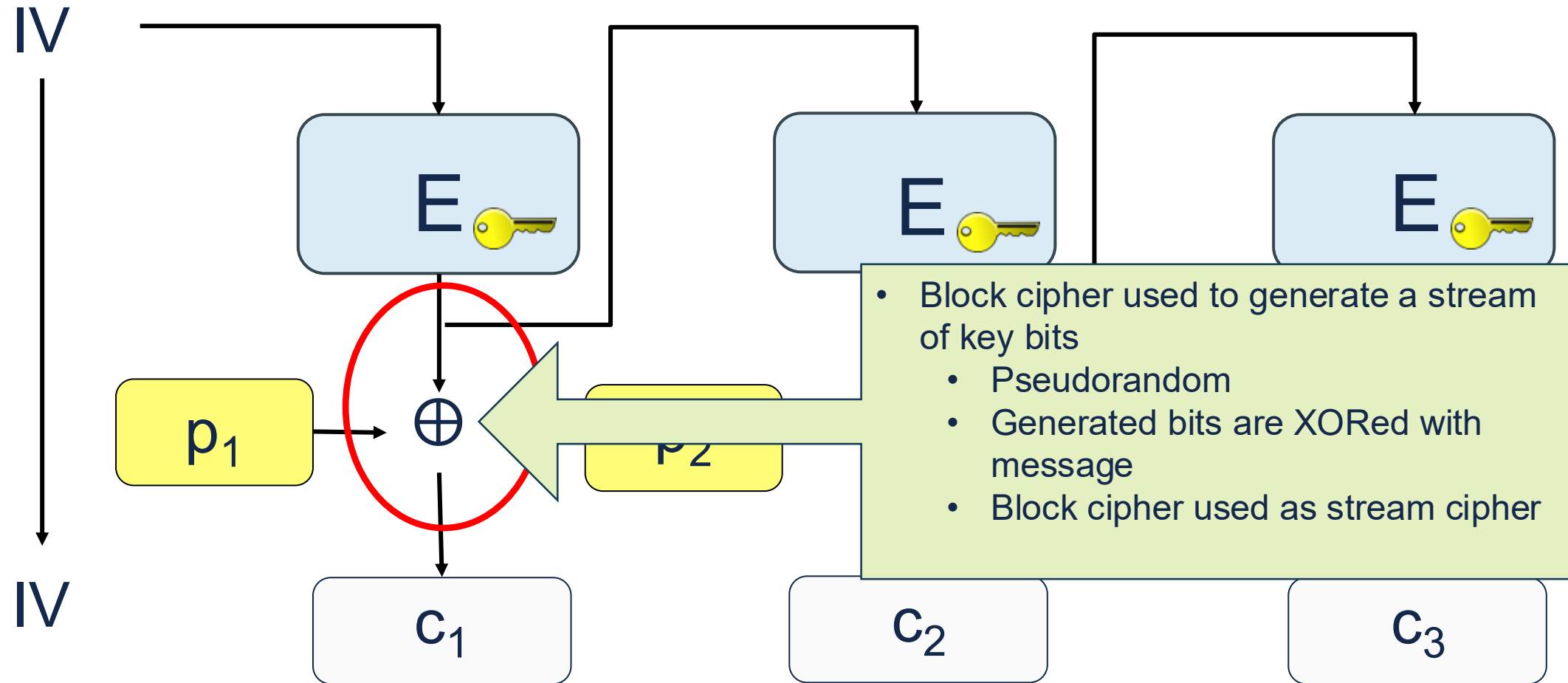
1. Draw the corresponding figure for decryption
2. Must decryption be done sequentially?



Output Feedback (OFB) Mode: Encryption

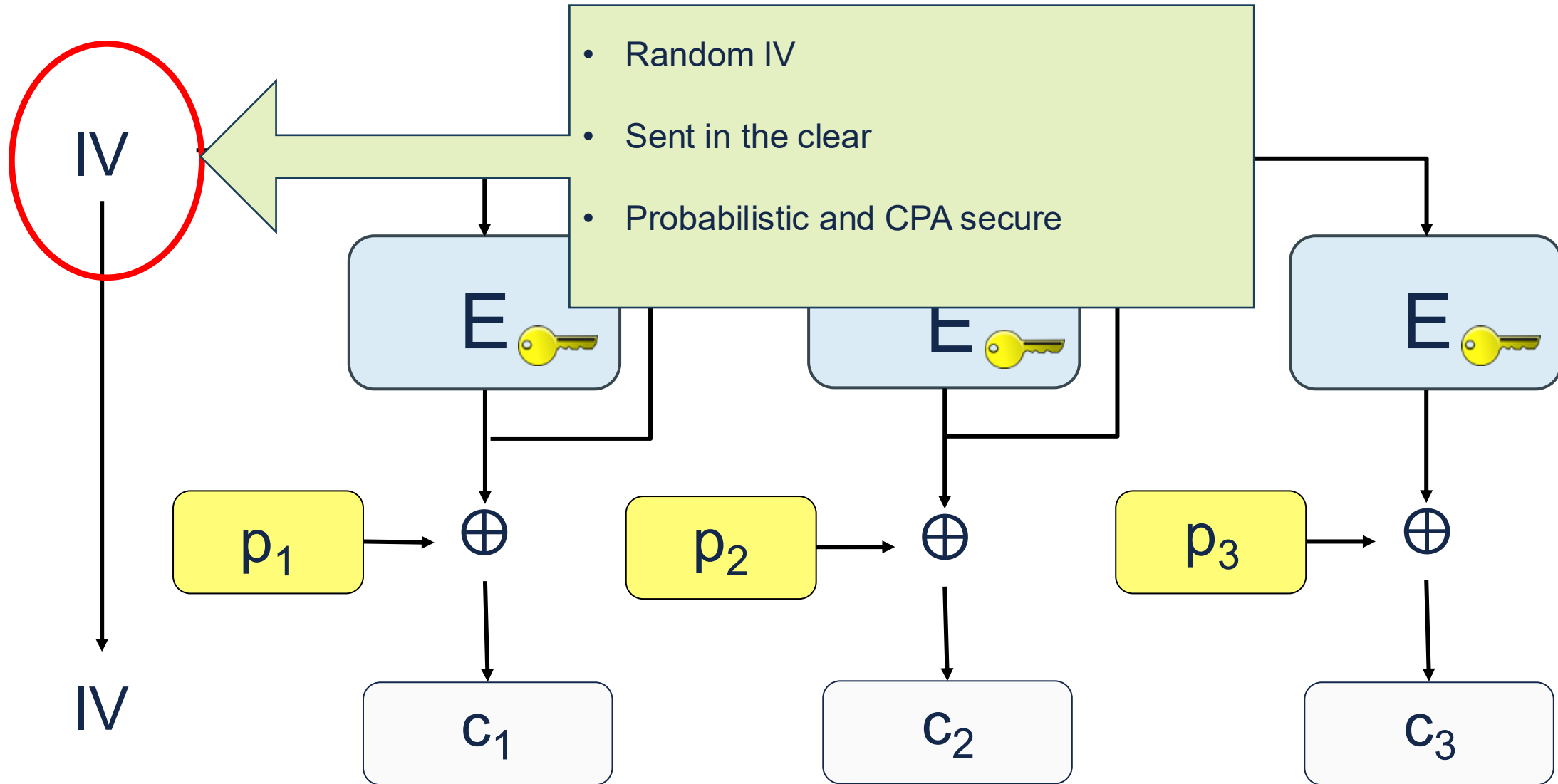


Output Feedback (OFB) Mode: Encryption



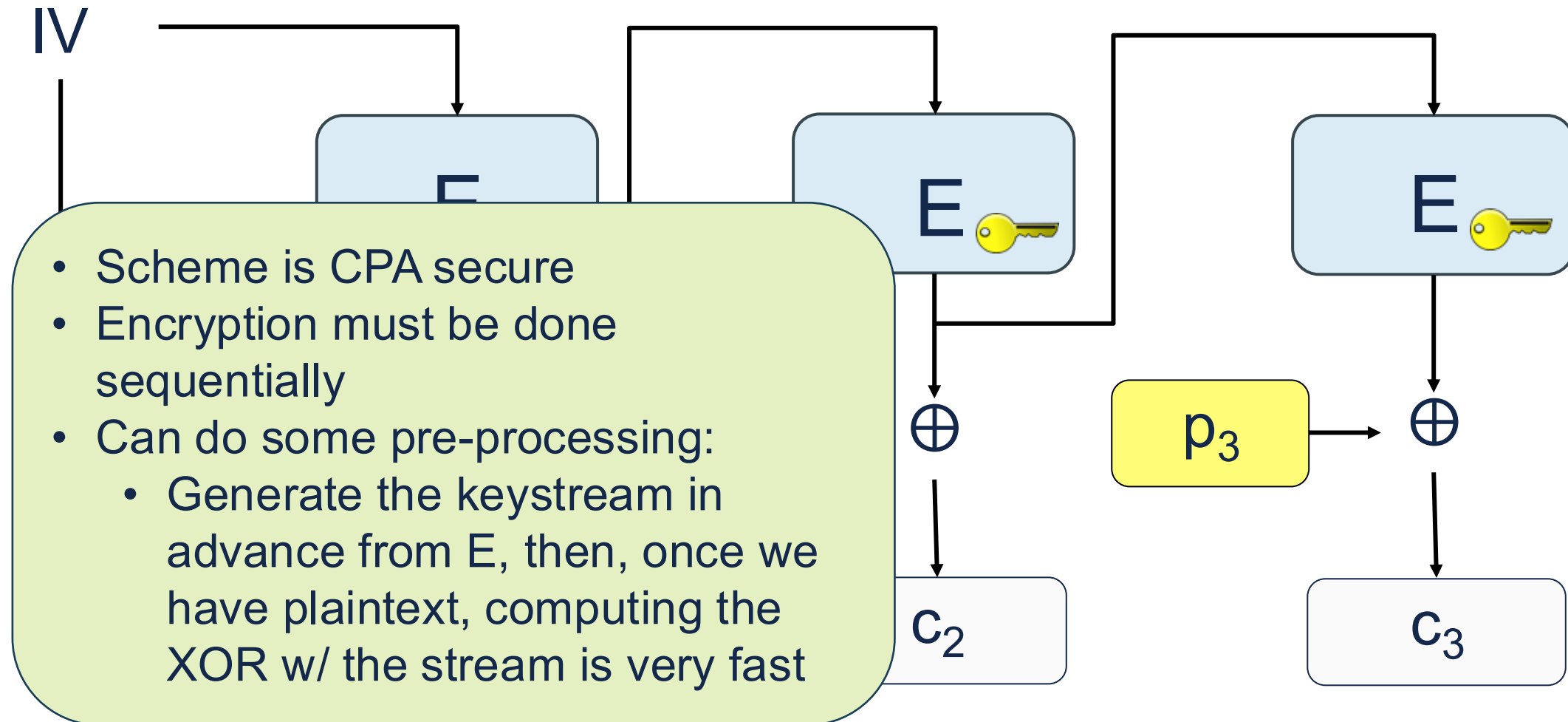


Output Feedback (OFB) Mode: Encryption





Output Feedback (OFB) Mode: Encryption

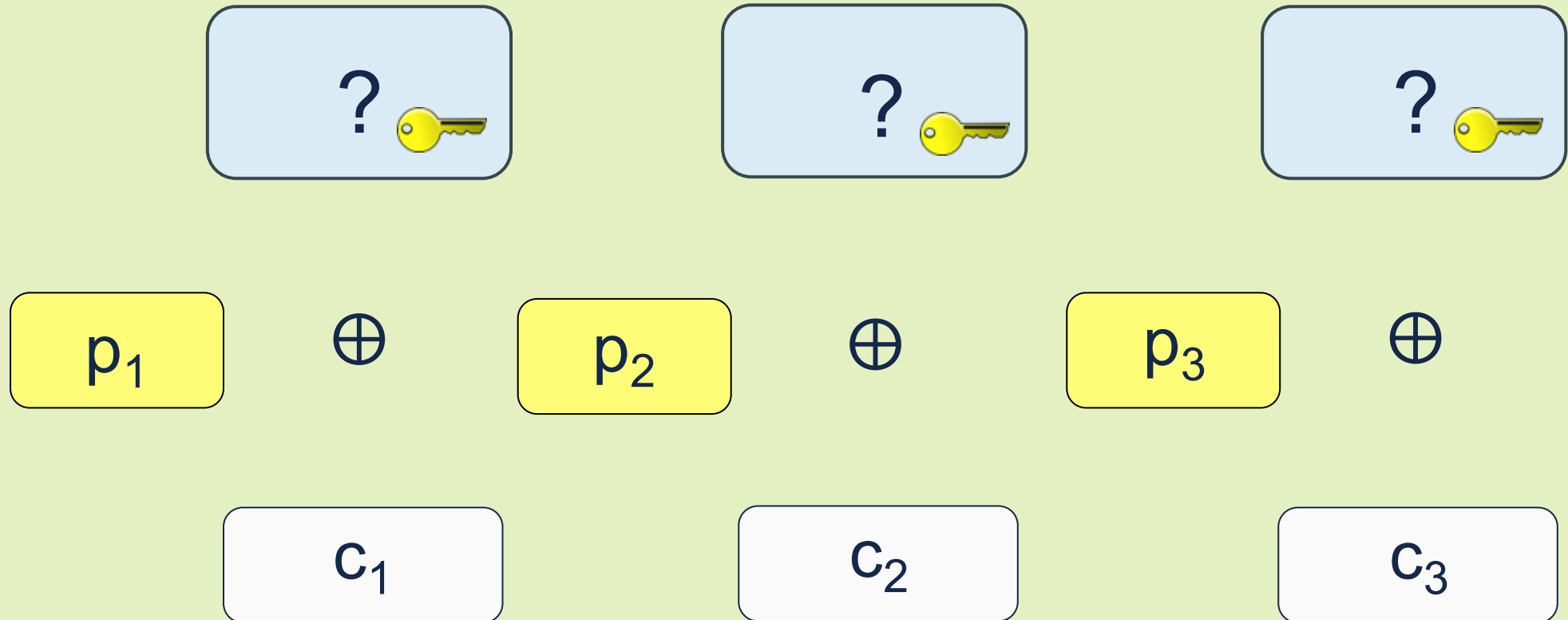


Decryption?

1. Draw the corresponding figure for decryption
2. Why is pre-processing not an option for the message receiver?

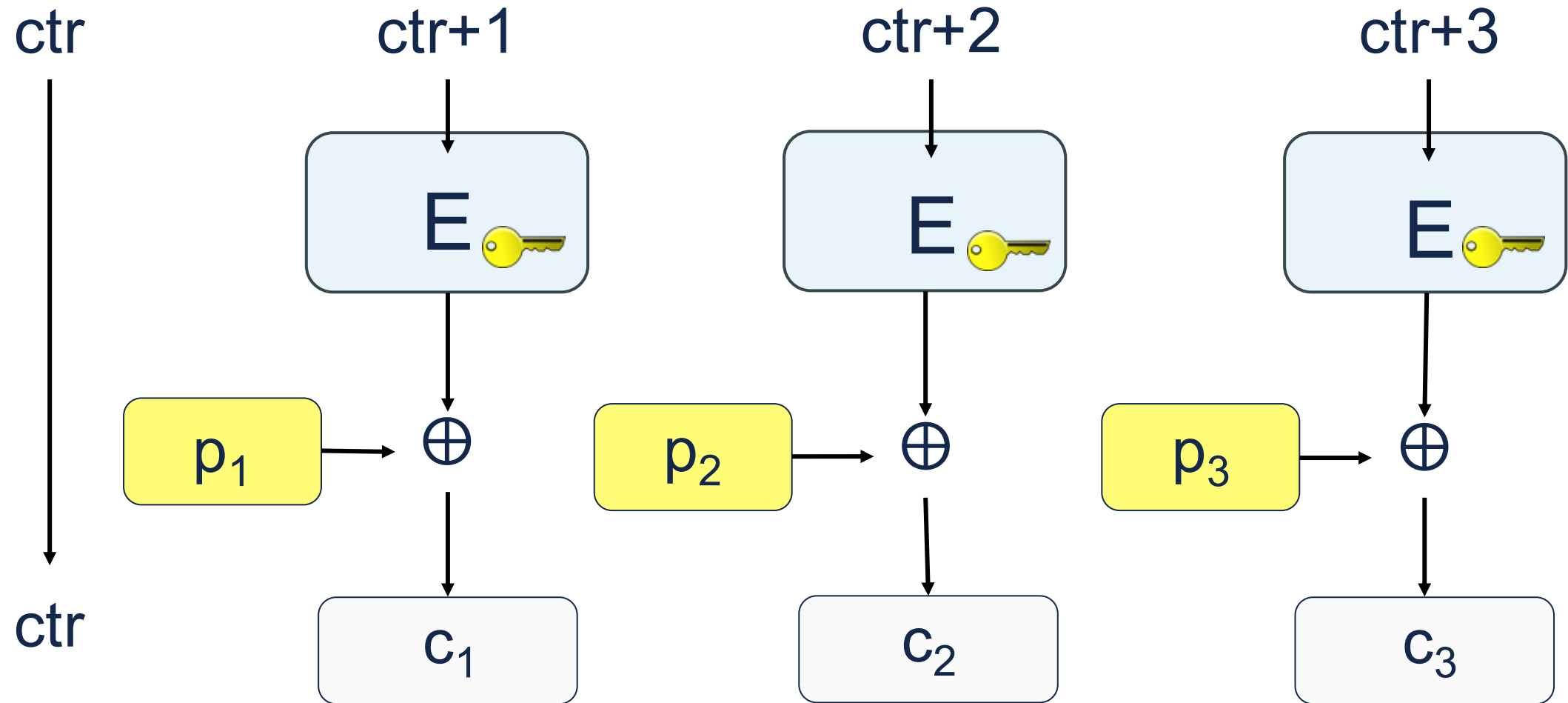


IV

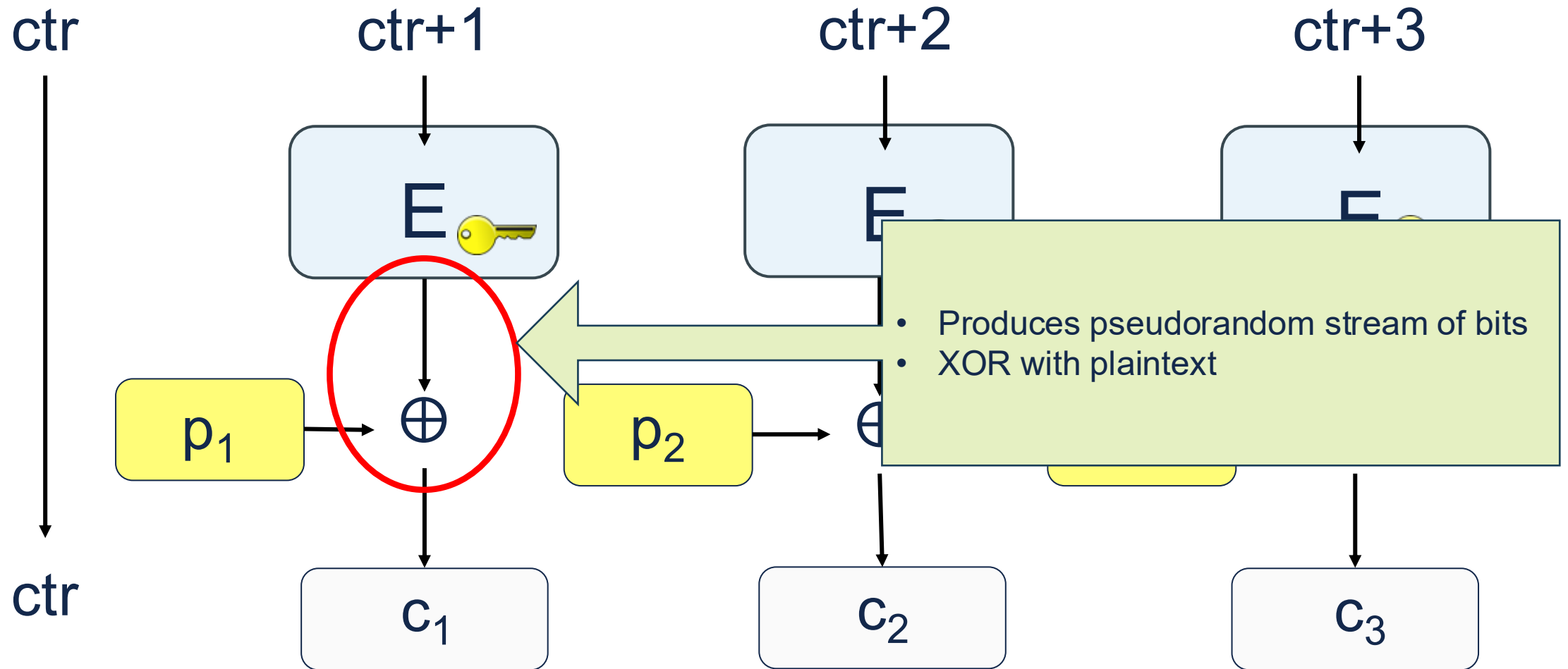


IV

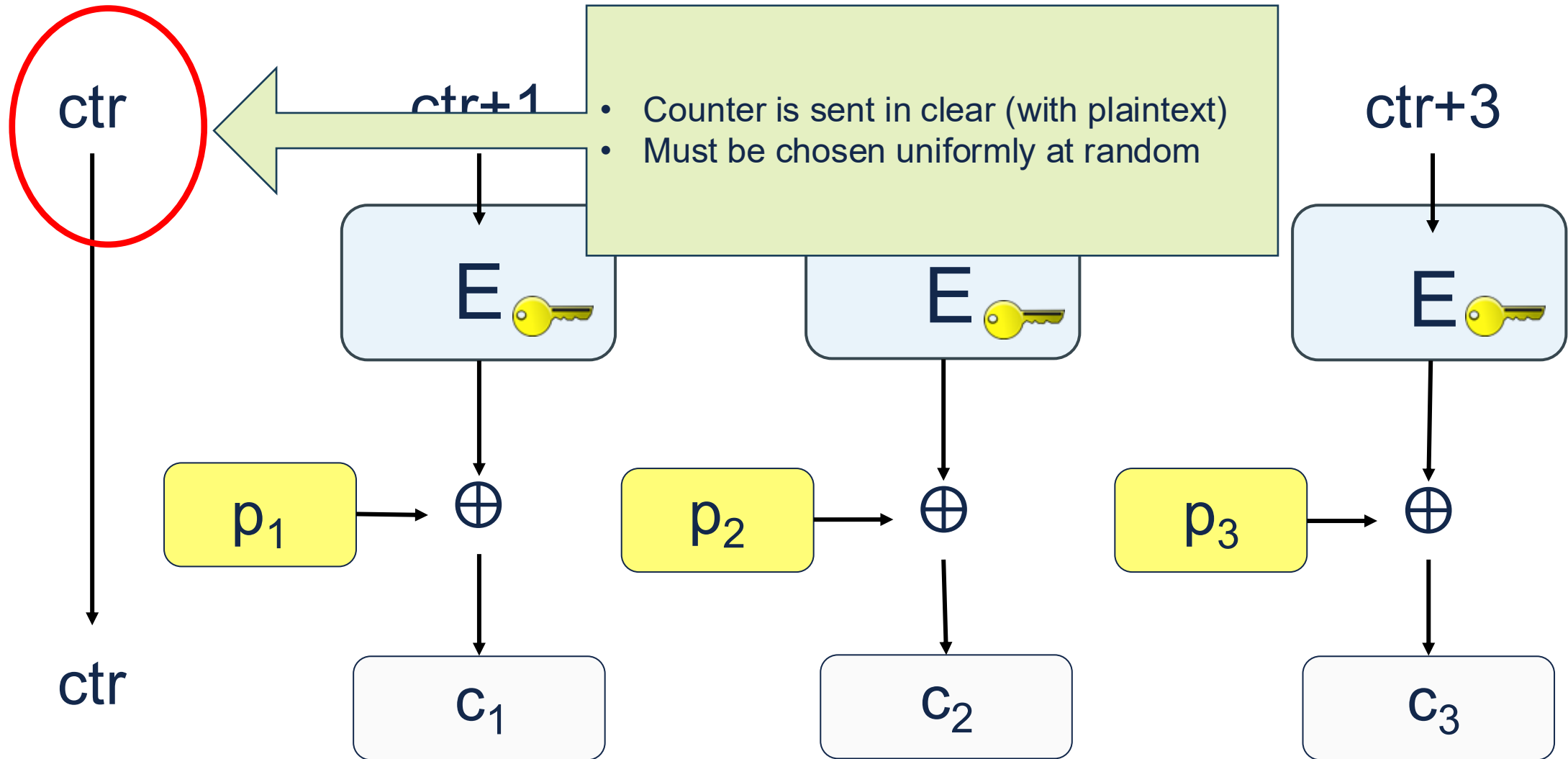
Counter (CTR) Mode: Encryption



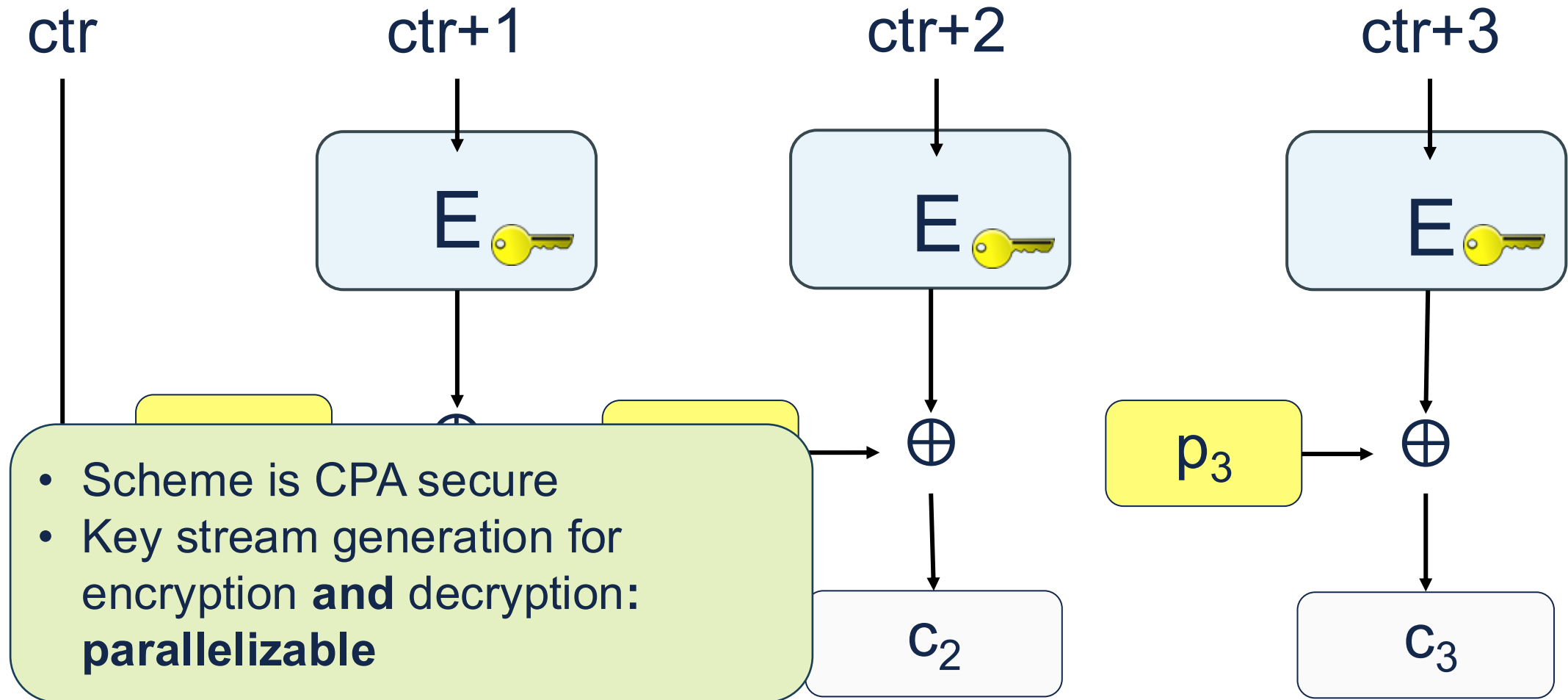
Counter (CTR) Mode: Encryption



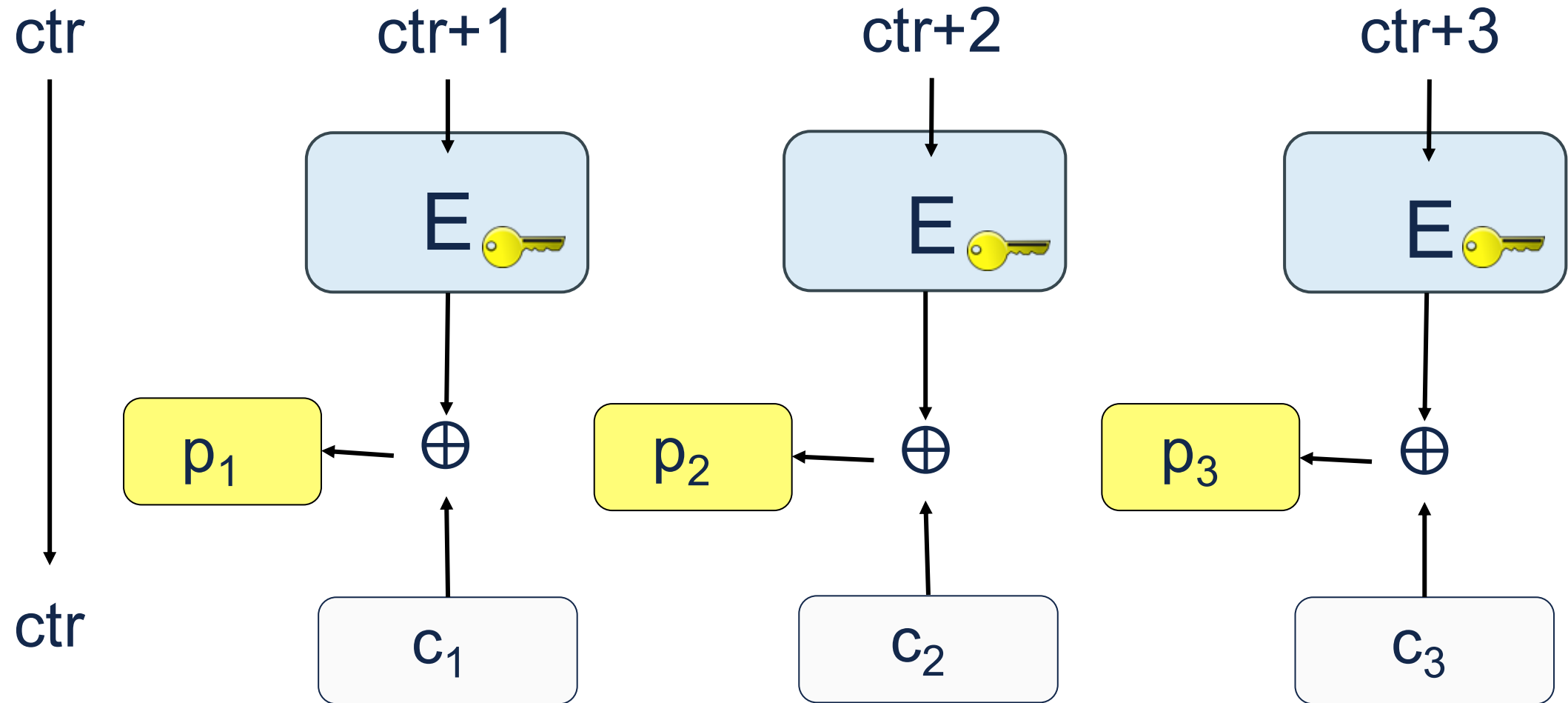
Counter (CTR) Mode: Encryption



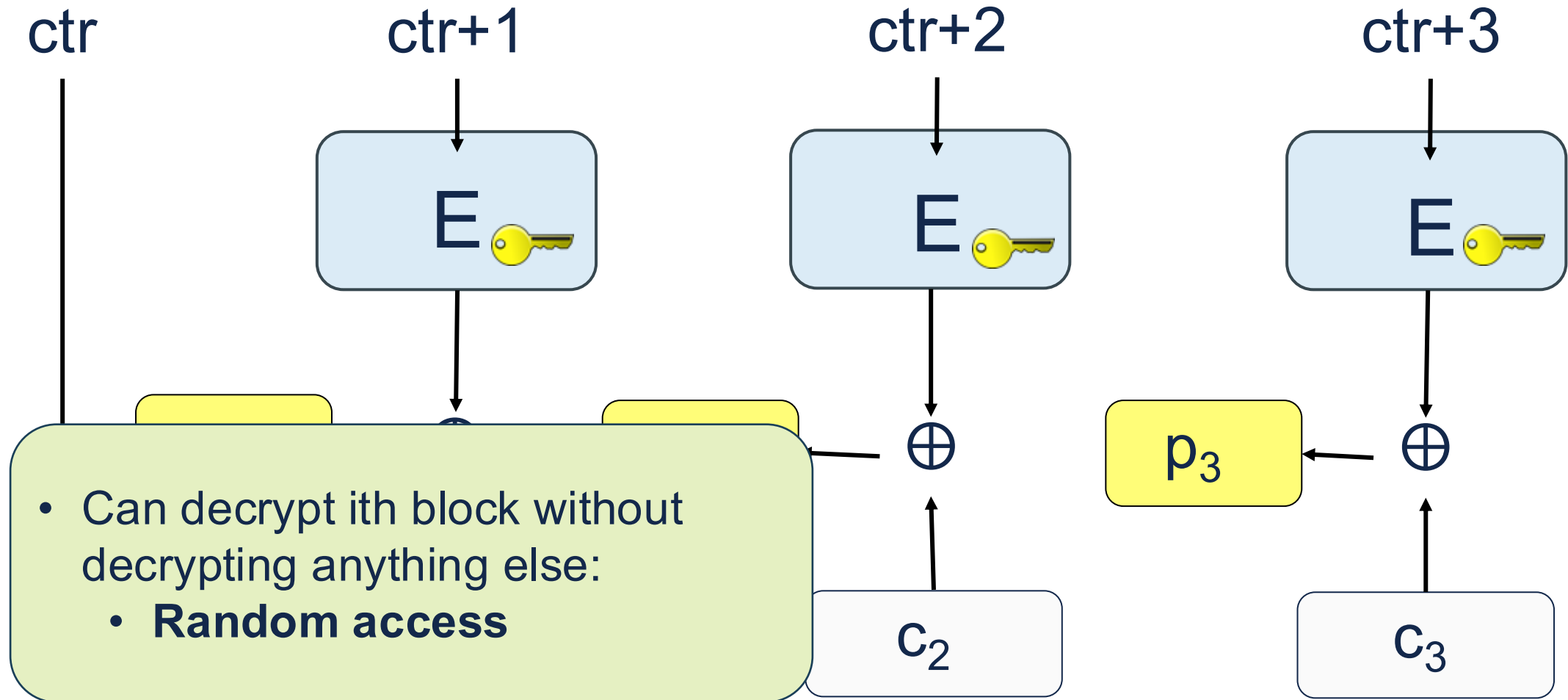
Counter (CTR) Mode: Encryption



Counter (CTR) Mode: Decryption



Counter (CTR) Mode: Decryption



Electronic Code Book Mode

- Deterministic
- Not secure

Cipher Block Chaining Mode

- Probabilistic
- IV chosen UatR
- Encrypt sequentially, decrypt in parallel
- CPA secure

Output Feedback Mode

- Probabilistic
- IV chosen UatR
- Encrypt, decrypt sequentially
- Builds a stream cipher
- CPA secure

Counter Mode

- Probabilistic
- ctr chosen UatR
- Encrypt, decrypt in parallel
- Builds a stream cipher
- Random access
- CPA secure

