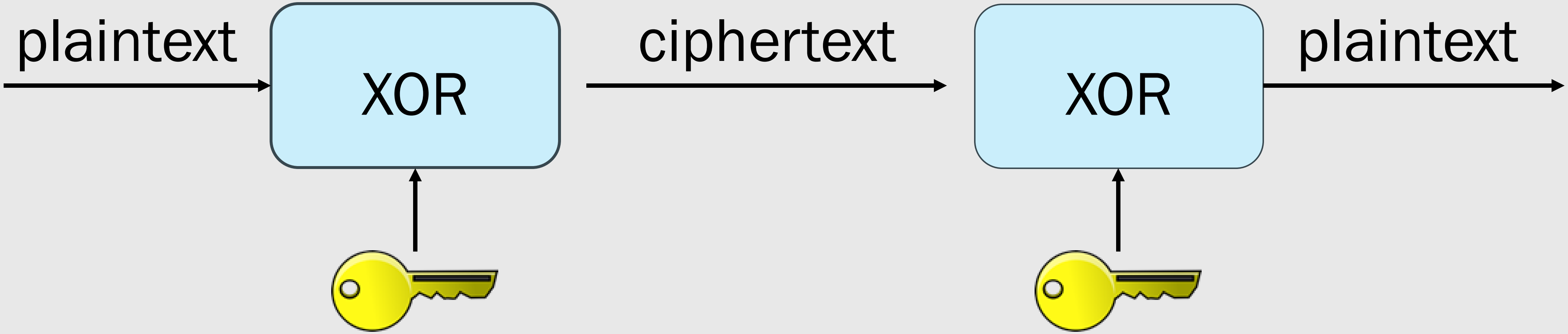
COMP435: *SECURITY CONCEPTS!*

Lecture 6: One Time Pad, Symmetric Encryption

tinyurl.com/comp435-fa25

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): Encryption

plaintext		0	1	0	0	0	0	0	1
key	⊕	0	1	0	1	0	1	0	1
ciphertext		0	0	0	1	0	1	0	0

One Time Pad (Vernam Cipher): Decryption

ciphertext		0	0	0	1	0	1	0	0
key	⊕	0	1	0	1	0	1	0	1
plaintext		0	1	0	0	0	0	0	1

One Time Pad

- *Symmetric encryption algorithm* ← single key used for encryption and decryption
- Stream cipher
- Substitution cipher

One Time Pad

- 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

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

each unit of the plaintext is replaced with a unit of ciphertext

One Time Pad Keys

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

uniformly at random

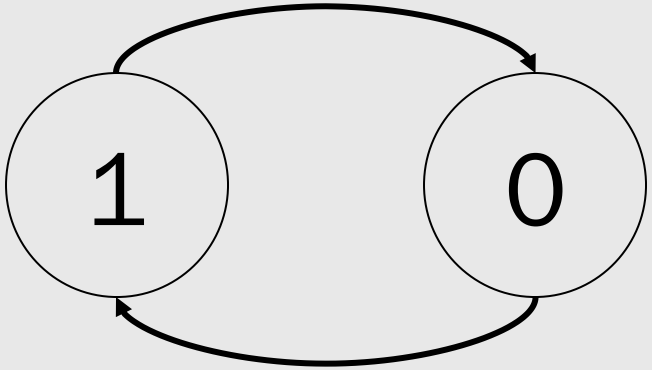
sampled from a uniform distribution

uniformly at random

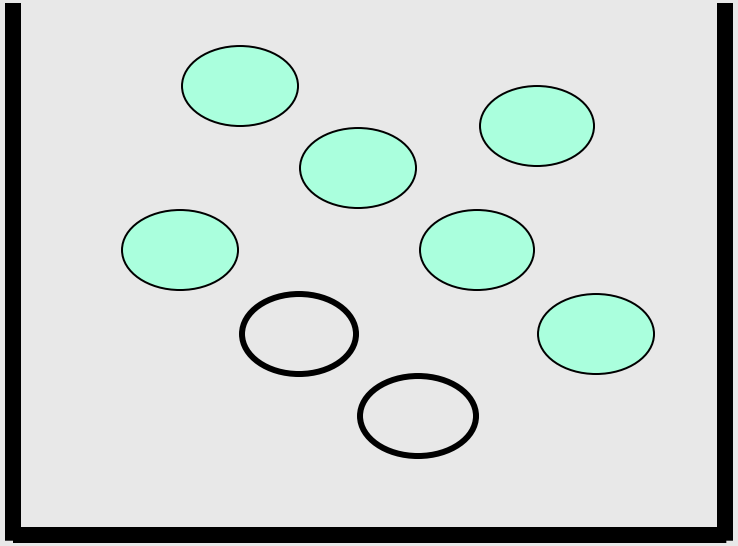
without bias

nondeterministic

Unbiased, Deterministic



Biased, Nondeterministic



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***

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

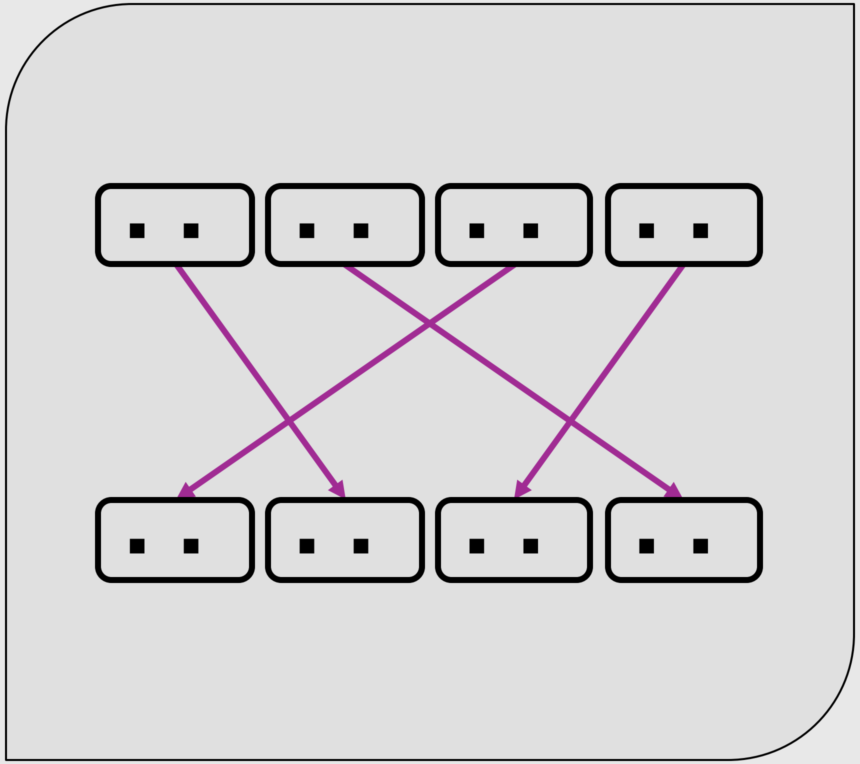
Worksheet 6 Q2-5

OTP

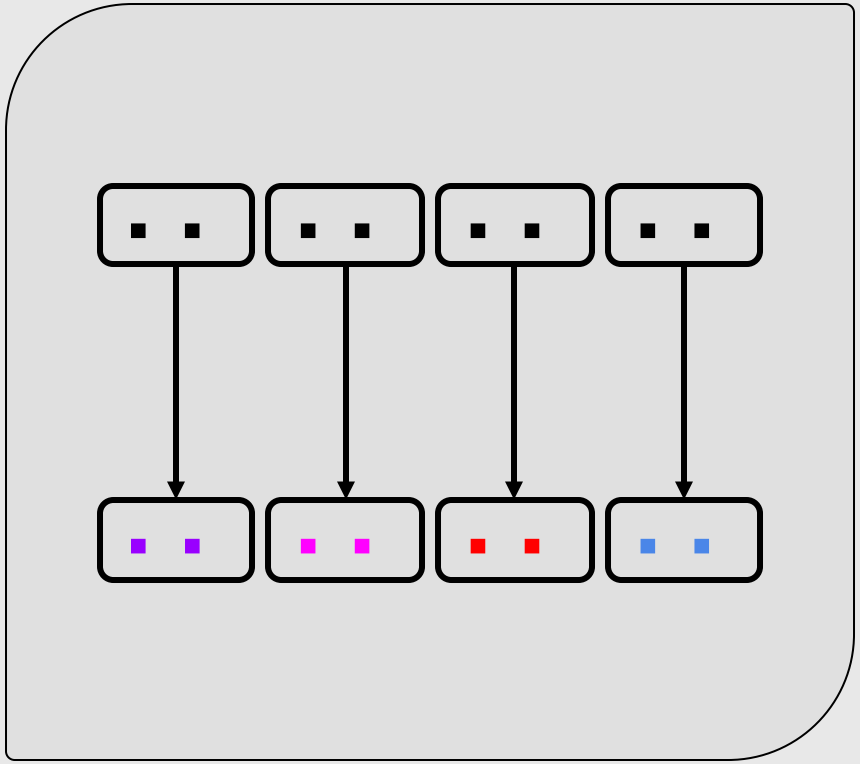
- Provides **perfect secrecy**
- Does not provide integrity
- Difficult to use in practice

SYMMETRIC ENCRYPTION

Building Blocks of Symmetric Encryption Ciphers

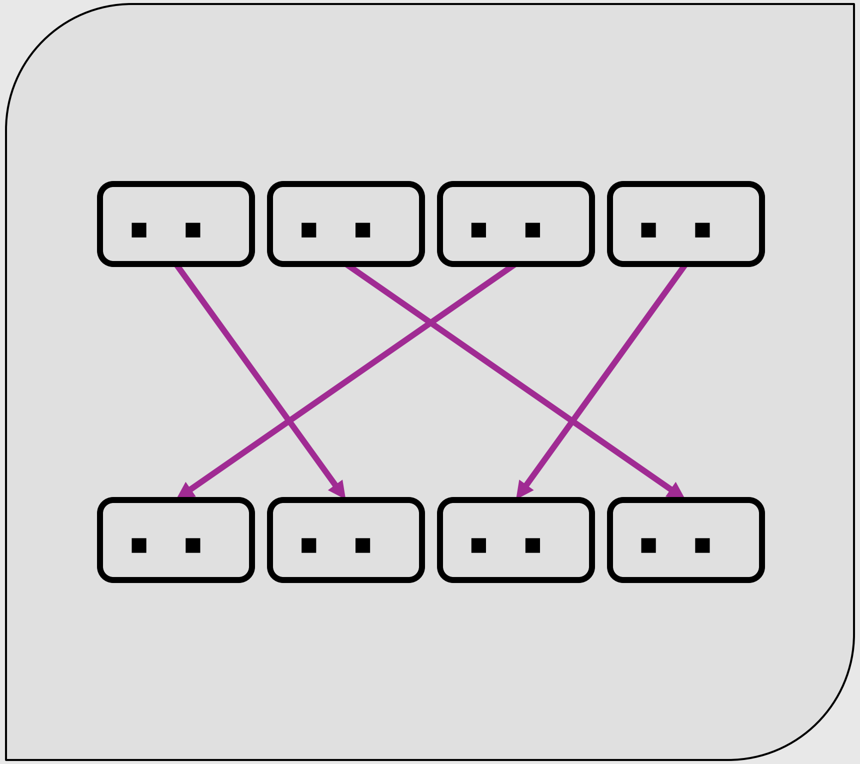


Transposition



Substitution

Transposition



Transposition

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

E.g., security → 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 xzmamvbibqwv bpmzm izm uivg atqlma. Qn gwc ow bpzwcop itt bpm atqlma, gwc eqtt amm bpm kwuxtmbm xzmamvbibqwv.

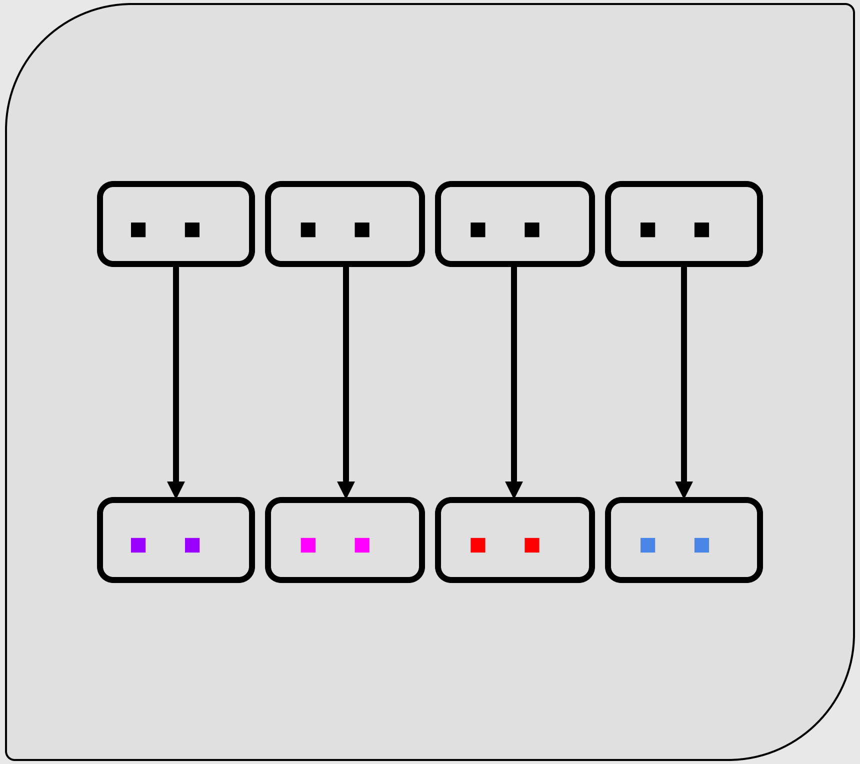
Without Transposition

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

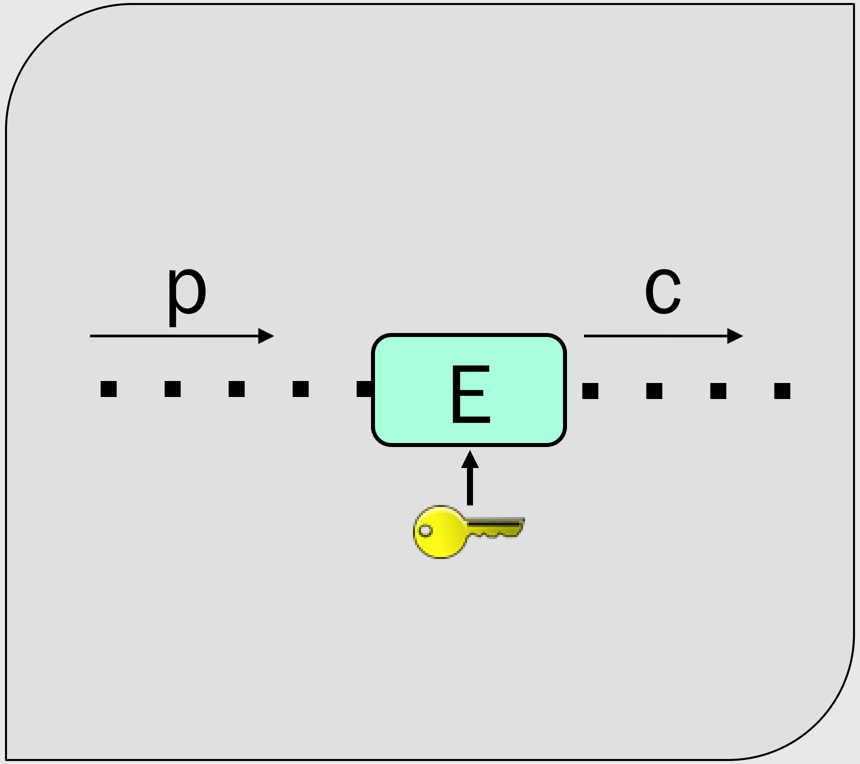
Yvd, yvd, yvd fvby ivha,

Nluasf kvdu aol zaylht.

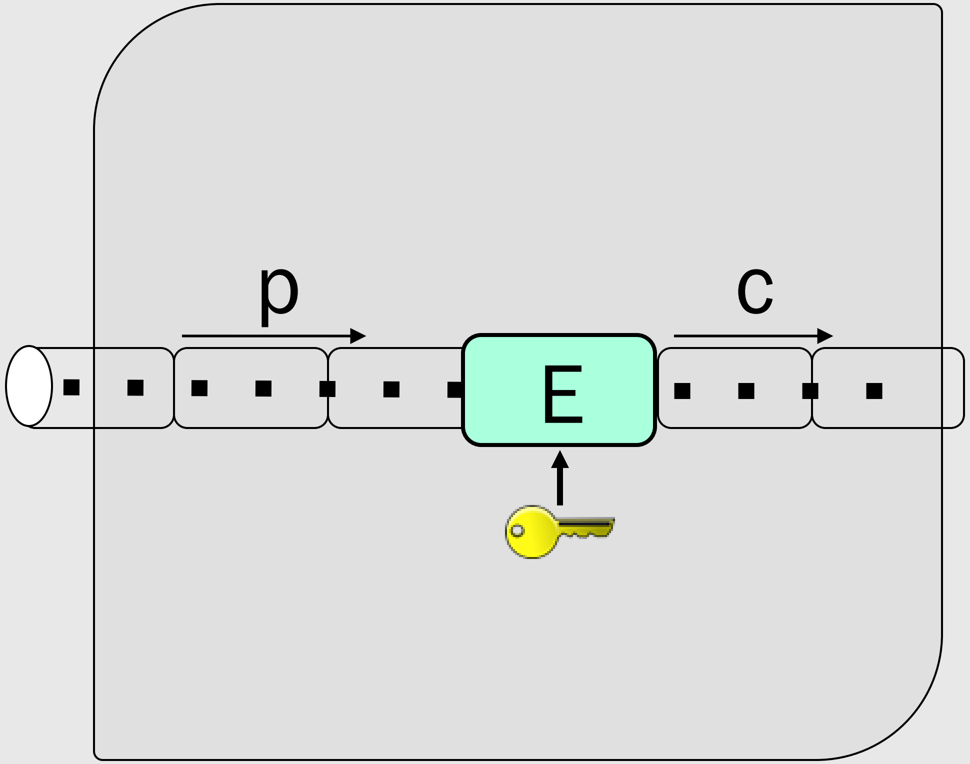
Tlyypsf, tlyypsf, tlyypsf, tlyypsf,

Spml pz iba h kylht.

Symmetric Encryption Algorithms

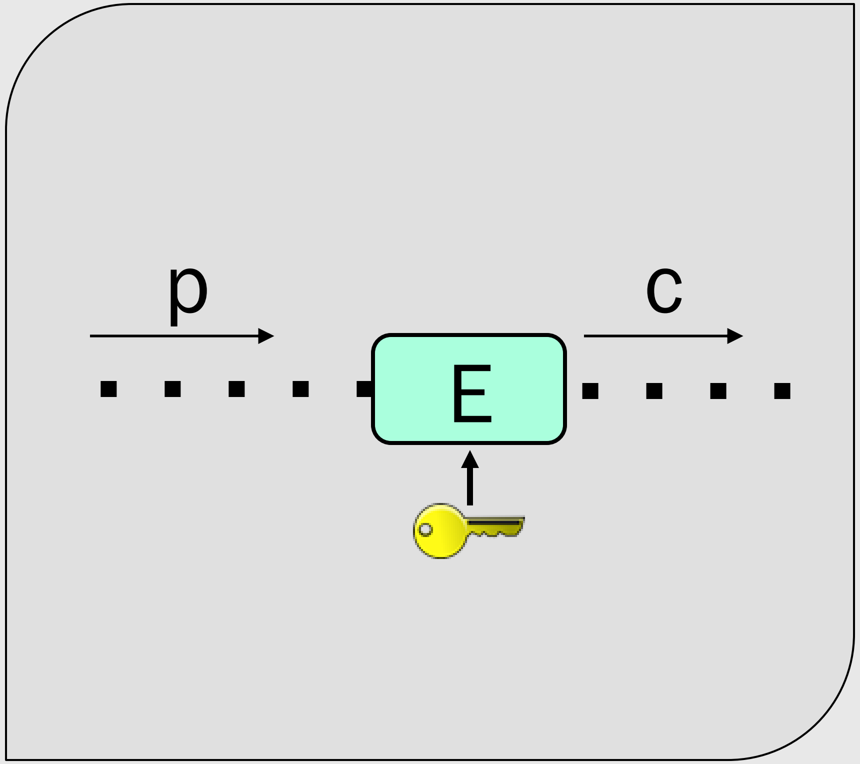


Stream Ciphers



Block Ciphers

Stream Ciphers

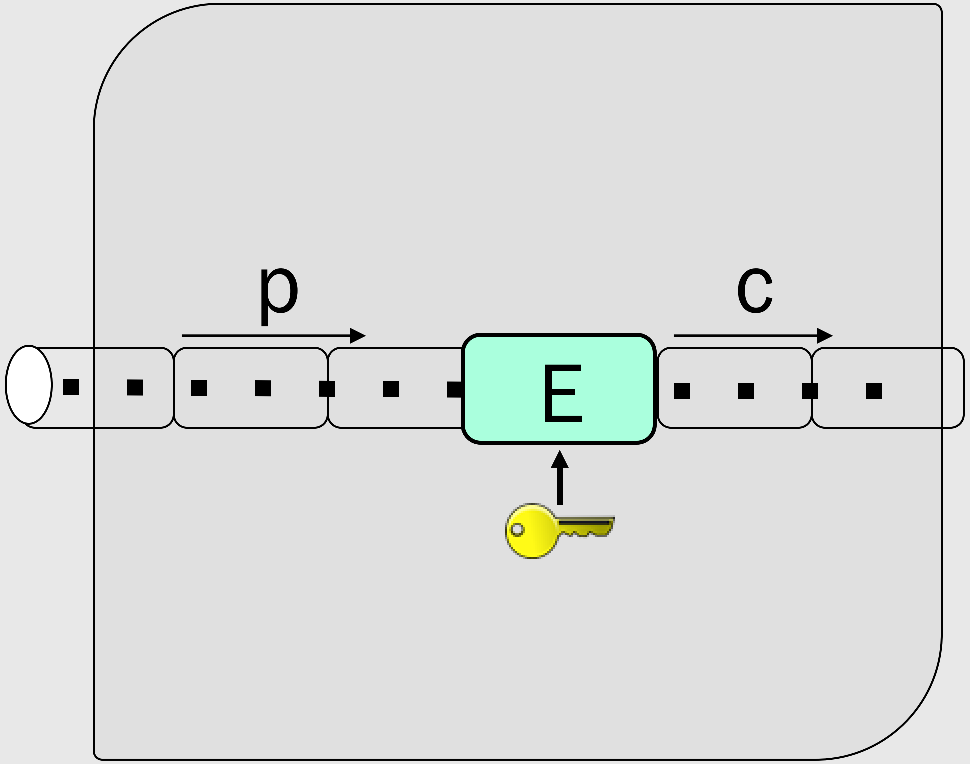


Stream Cipher

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

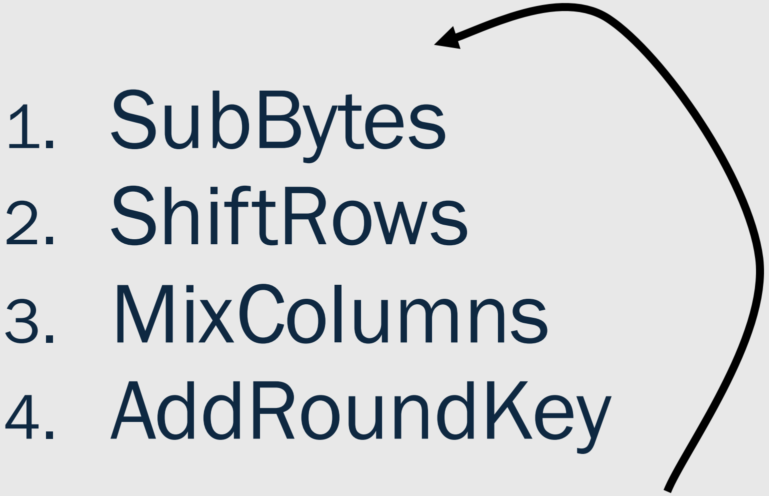
Def’n: groups of symbols are encrypted together as a single block

E.g., AES, DES, 3DES

AES

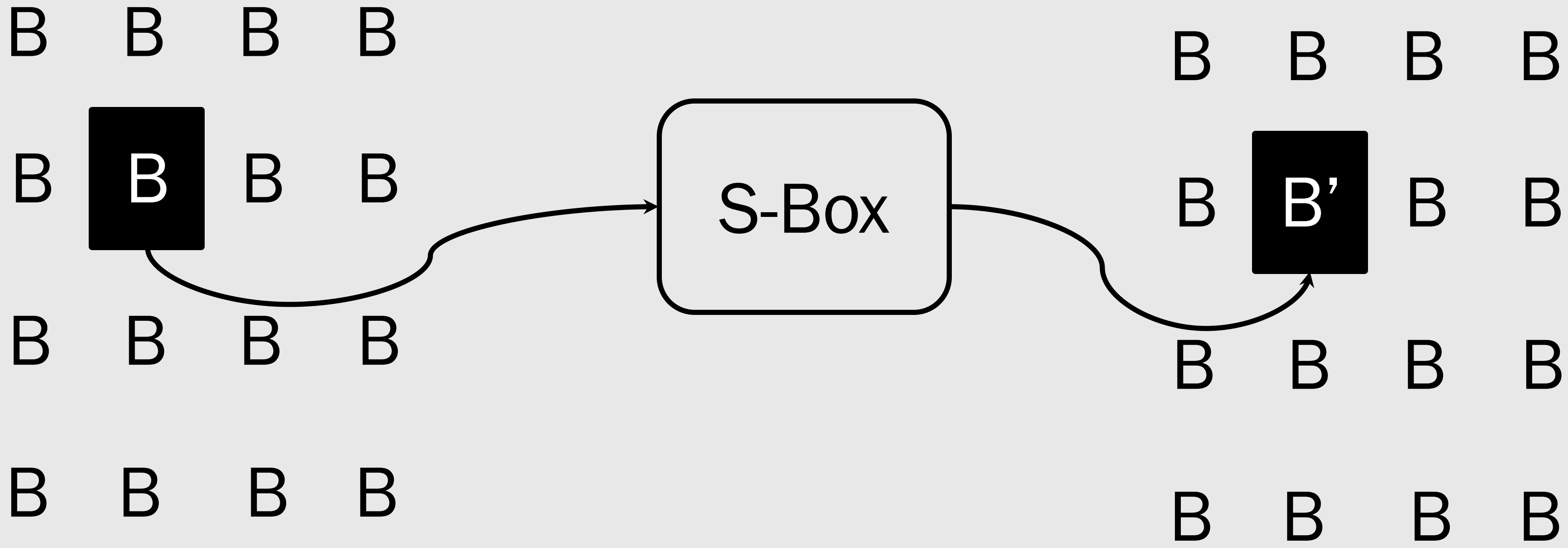
- Developed in 1997 in open call from NIST
- Replacement for DES
- Rijndael algorithm
- 128-bit block; 128-, 192-, or 256-bit keys

AES



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

SubBytes



B B B B
B B B B
B B B B
B B B B

S-Box

B B B B
B B' B B
B B B B
B B B B

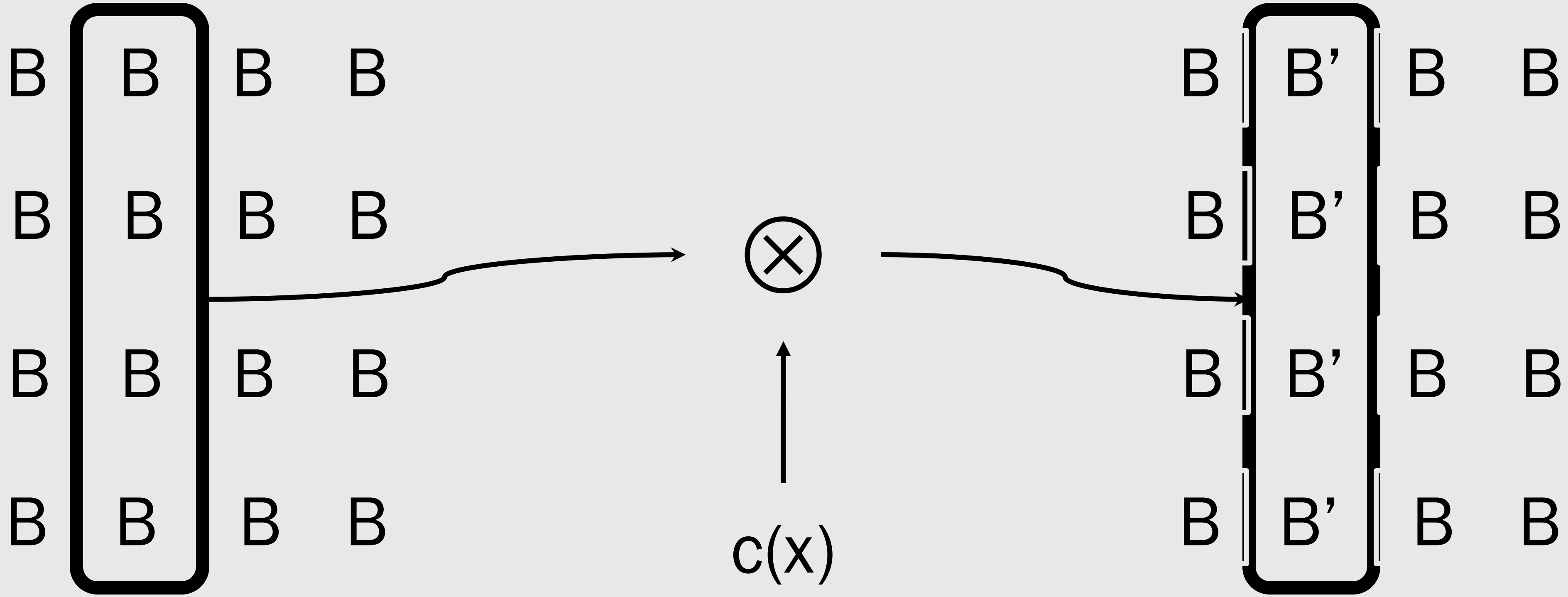
ShiftRows

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



B B B B

B B B B

B B B B

B B B B

⊗

c(x)

B B' B B

B B' B B

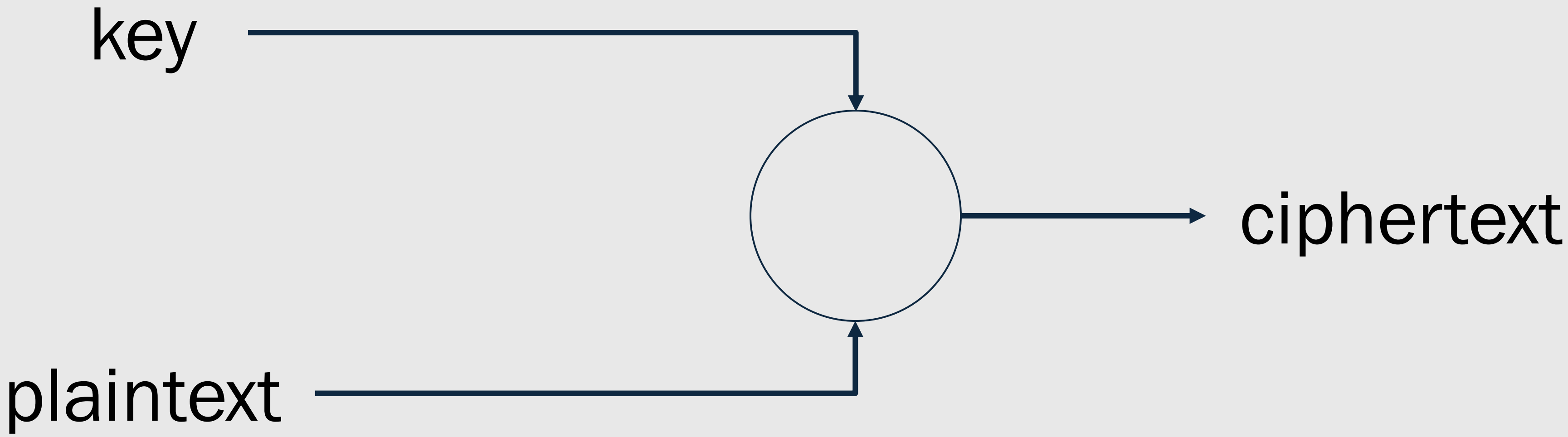
B B' B B

B B' B B

AddRoundKey

$$\begin{matrix} B & B & B & B \\ B & B & B & B \\ B & B & B & B \\ B & B & B & B \end{matrix} \oplus \begin{matrix} k & k & k & k \\ k & k & k & k \\ k & k & k & k \\ k & k & k & k \end{matrix} = \begin{matrix} B' & B' & B' & B' \\ B' & B' & B' & B' \\ B' & B' & B' & B' \\ B' & B' & B' & B' \end{matrix}$$

PROPERTIES OF STRONG SYMMETRIC CIPHERS

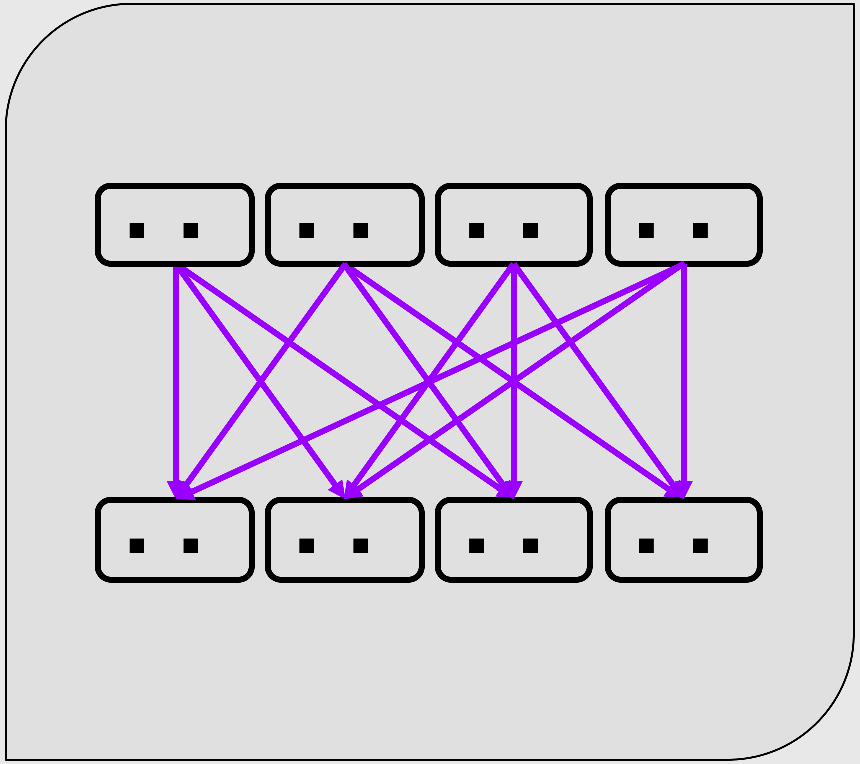


key

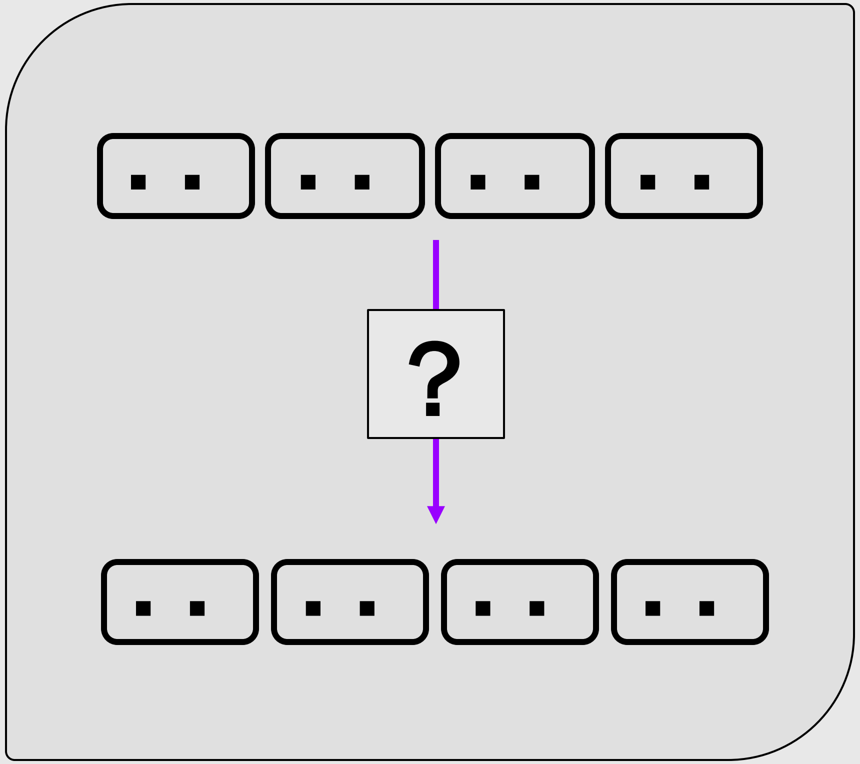
plaintext

ciphertext

Properties of Strong Symmetric Ciphers



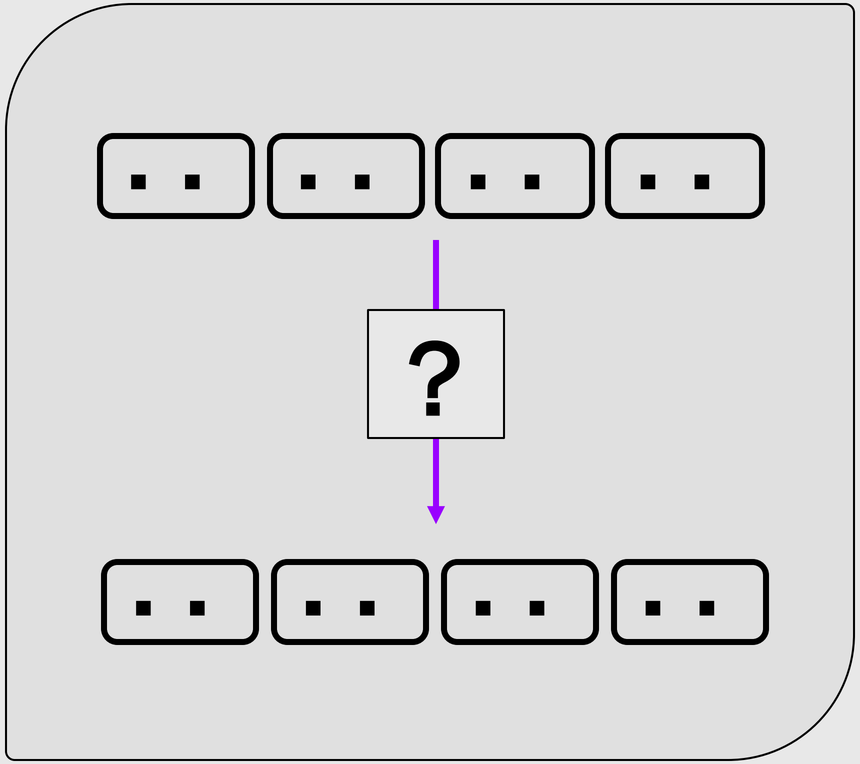
Diffusion



Confusion

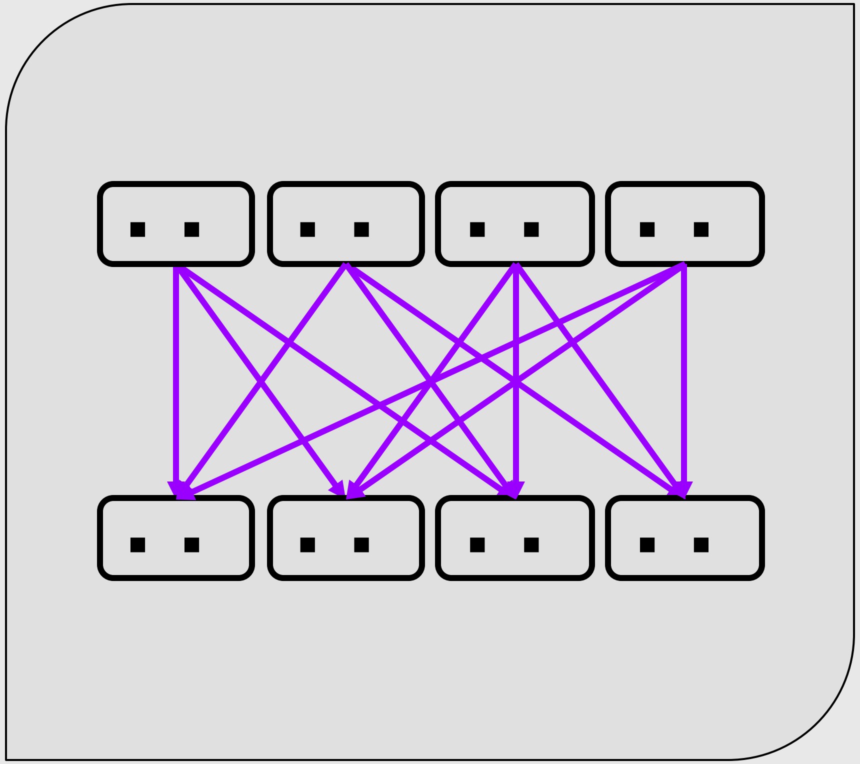
Confusion

Def’n: obscure the relationship between key and ciphertext



Diffusion

Def’n: spread the plaintext statistics across the ciphertext



Stream Ciphers and Block Ciphers

+ Low latency
- No diffusion
+ High confusion

Stream Ciphers

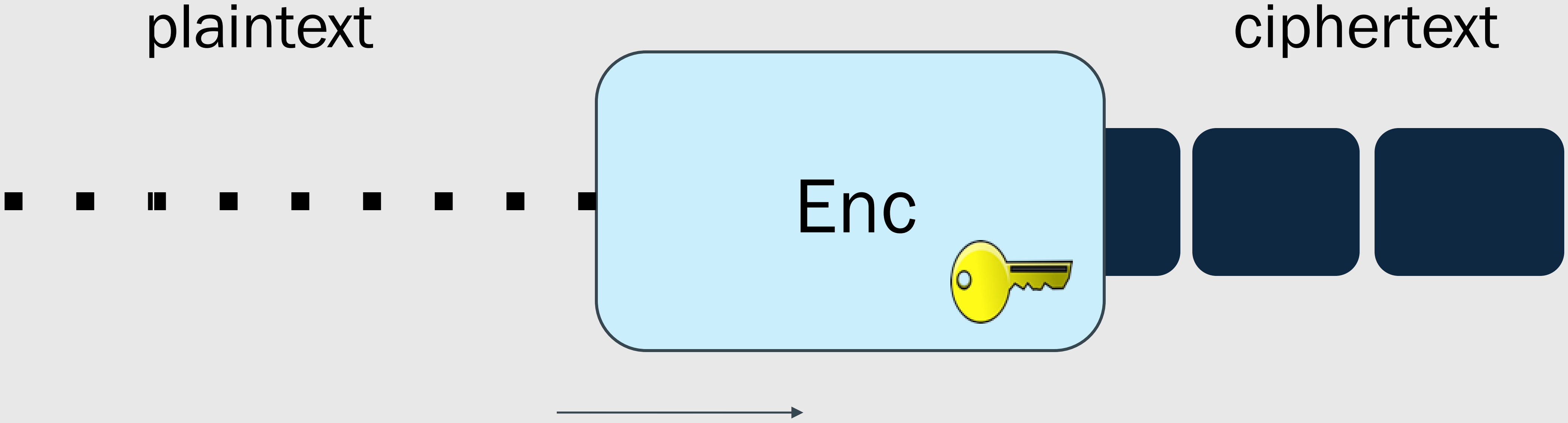
- Higher latency
+ High diffusion
+ High confusion

Block Ciphers

Worksheet 7 Q1-5☺

BLOCK CIPHER MODES OF OPERATION

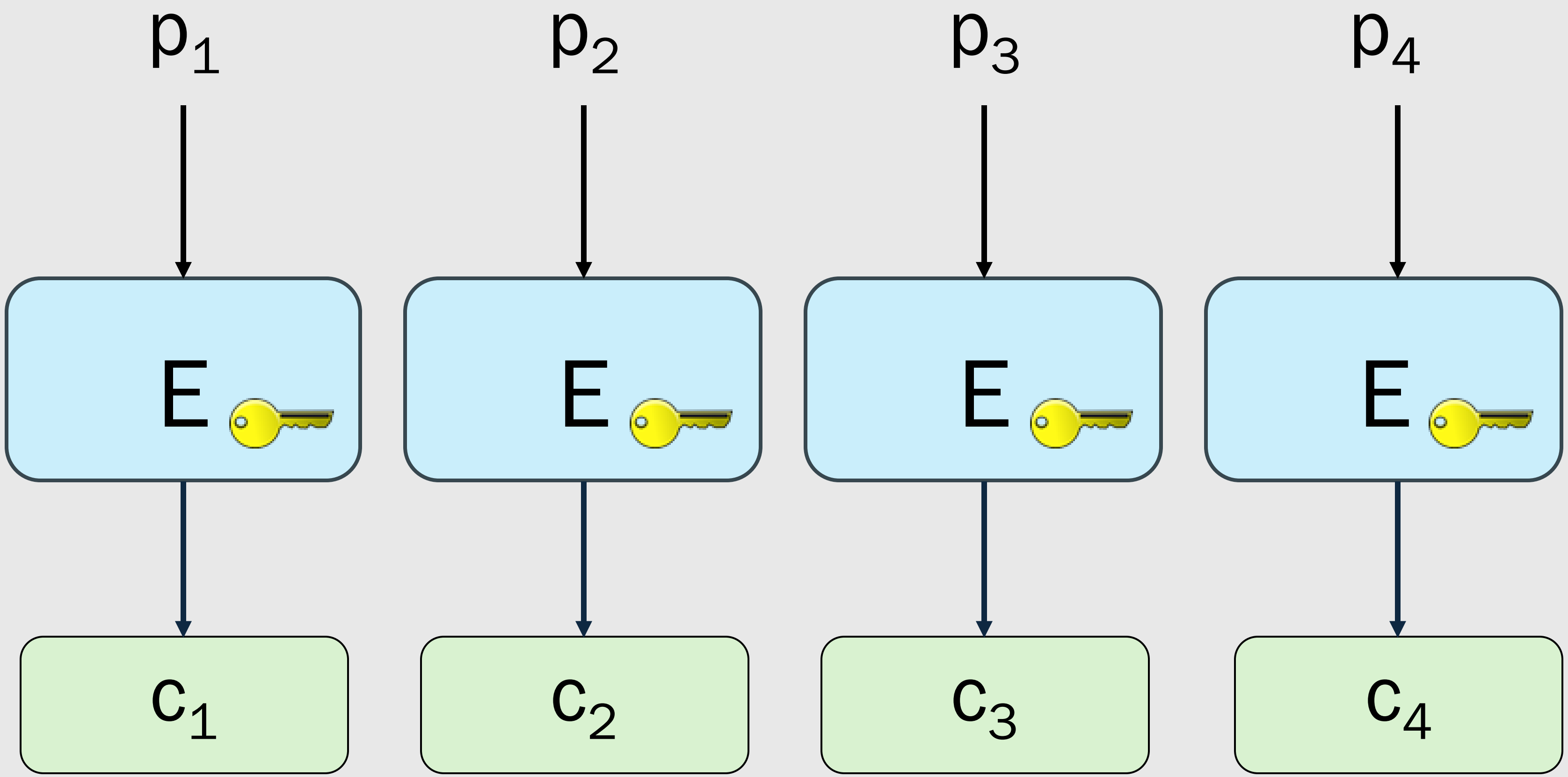
Block Ciphers



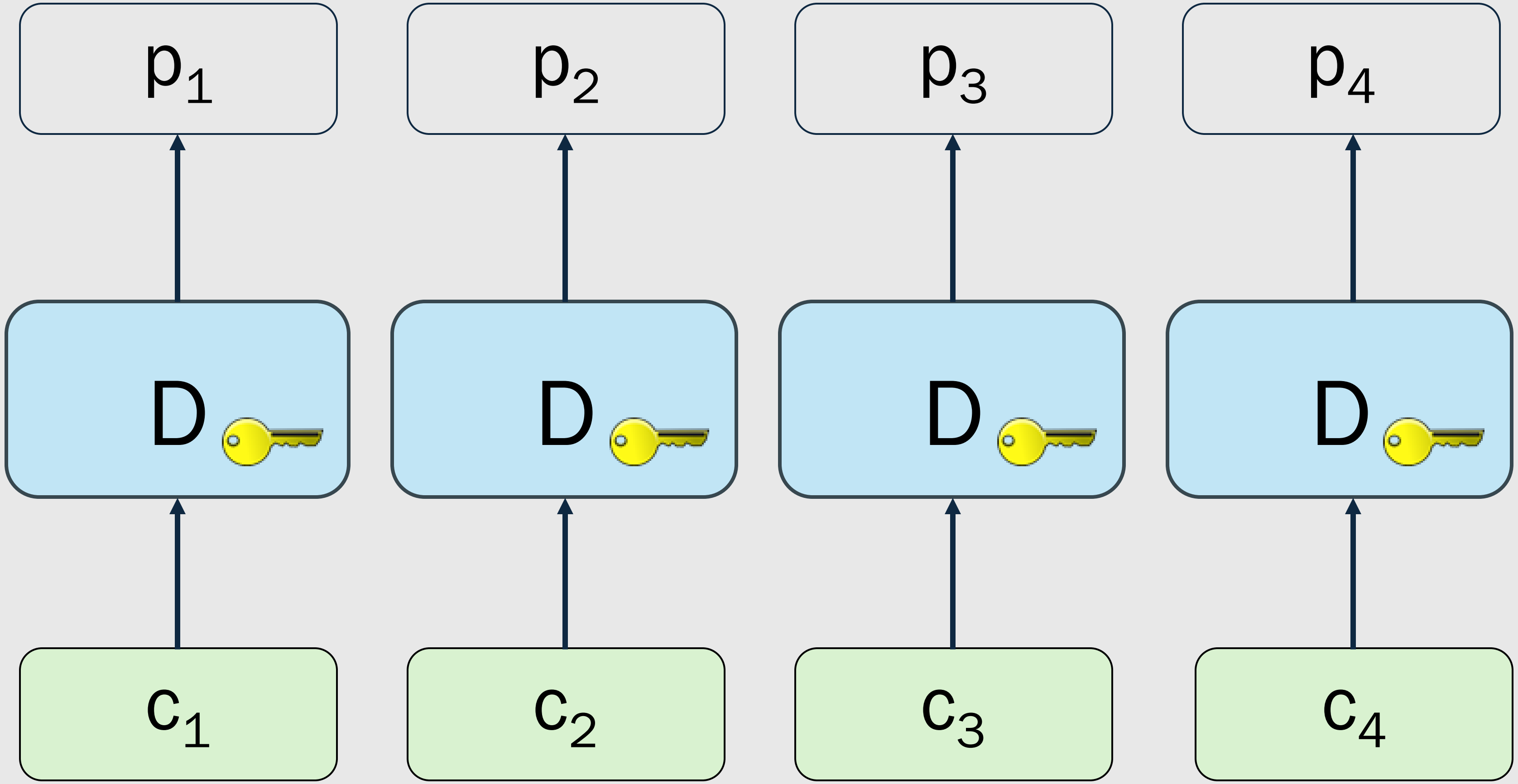
Modes of Operation

- Electronic Code Book Mode
- Cipher Block Chaining Mode
- Output Feedback Mode
- Counter Mode

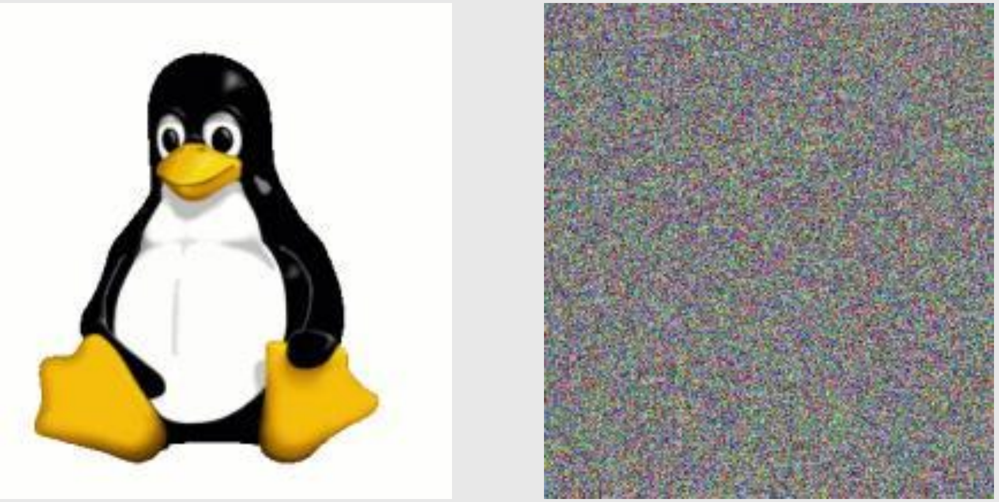
Electronic Code Book (ECB) Mode: Encryption



Electronic Code Book (ECB) Mode: Decryption

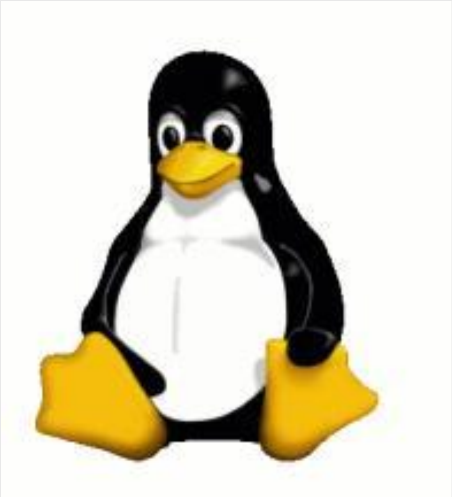


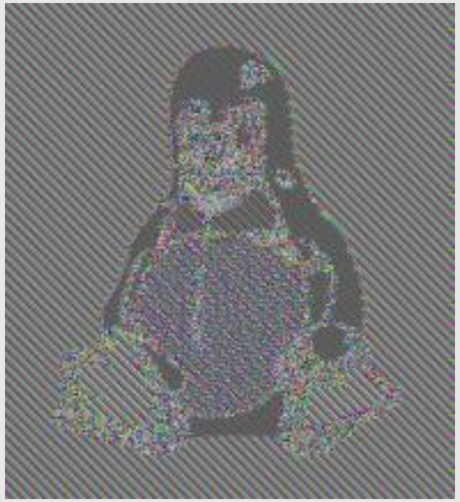
Securely Encrypted



https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

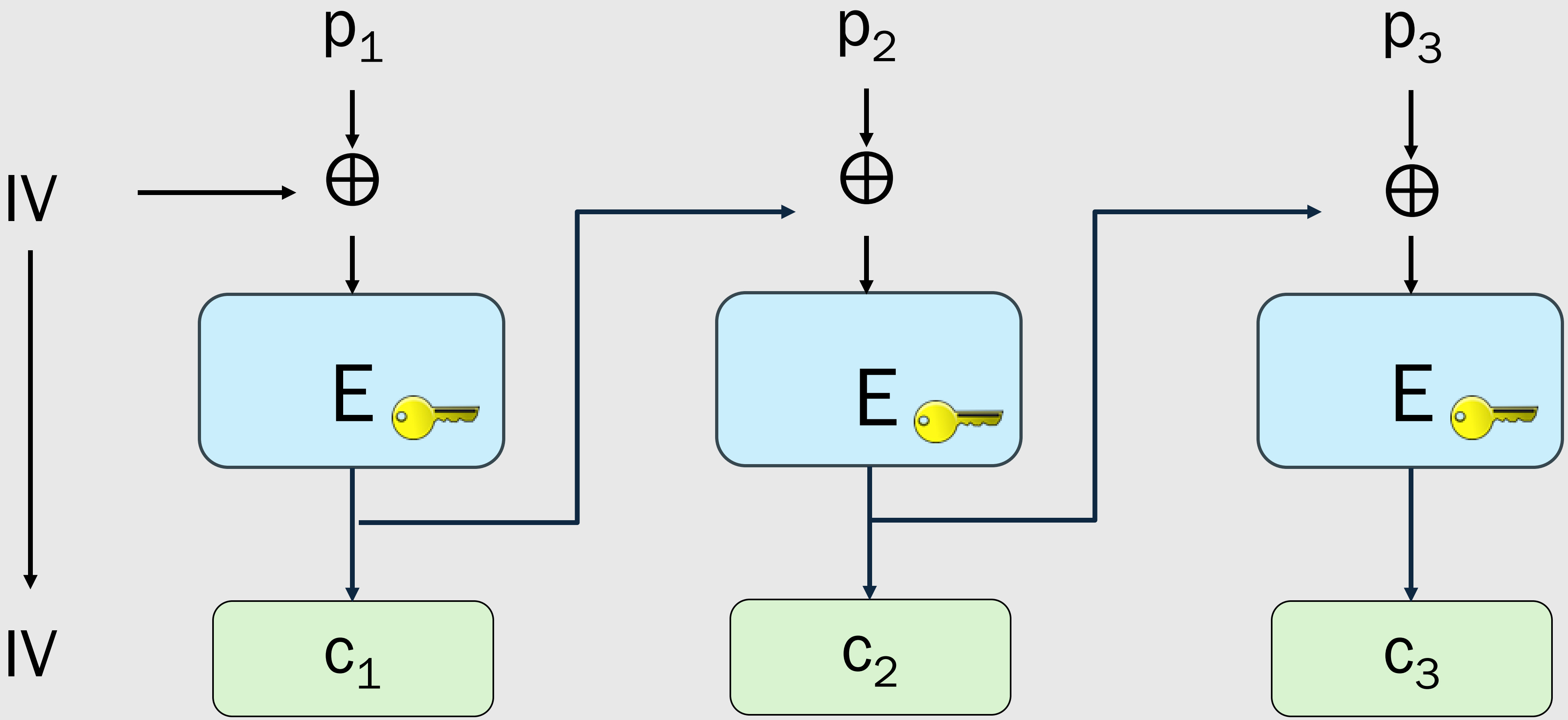
Electronic Code Book (ECB) Mode





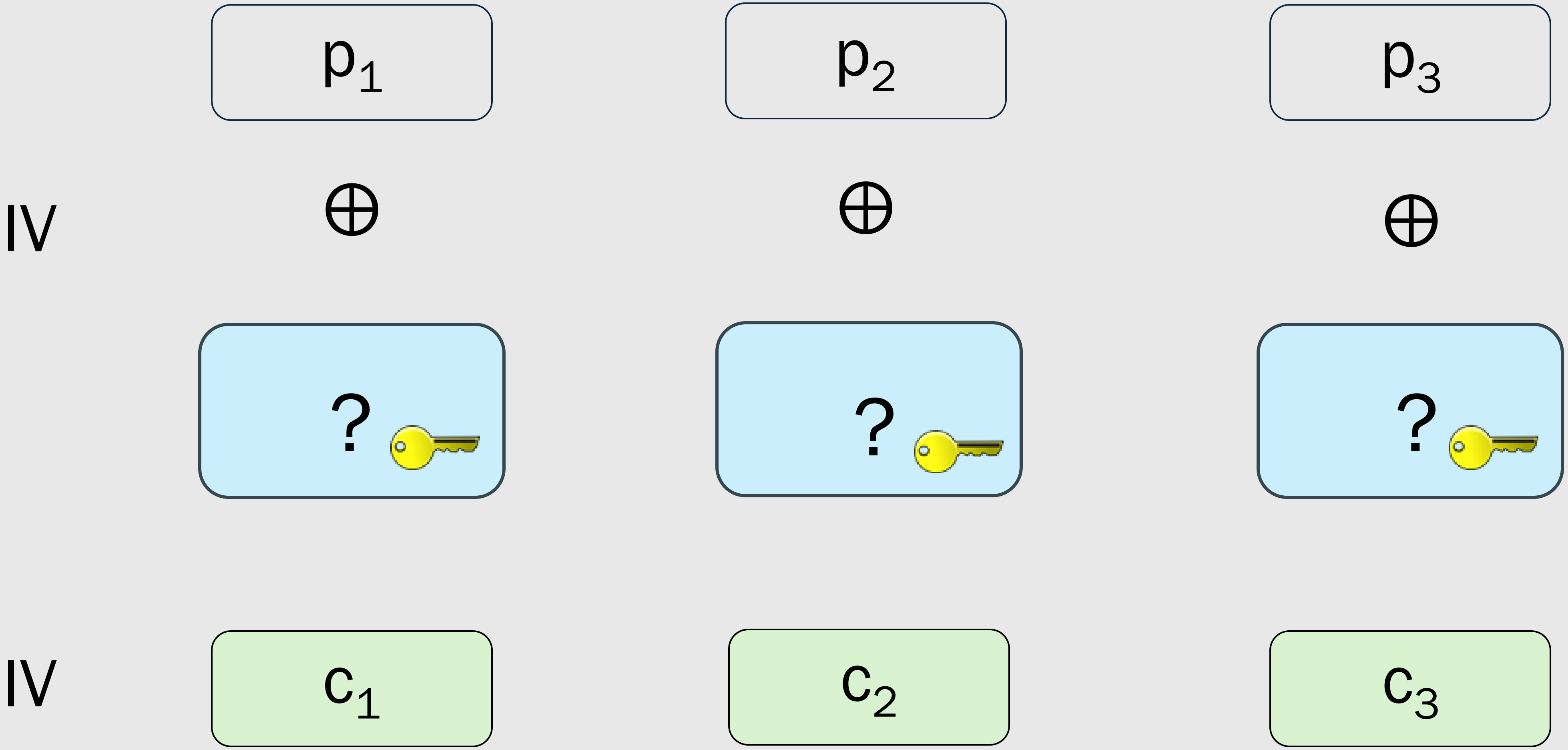
https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

Cipher Block Chaining (CBC) Mode: Encryption

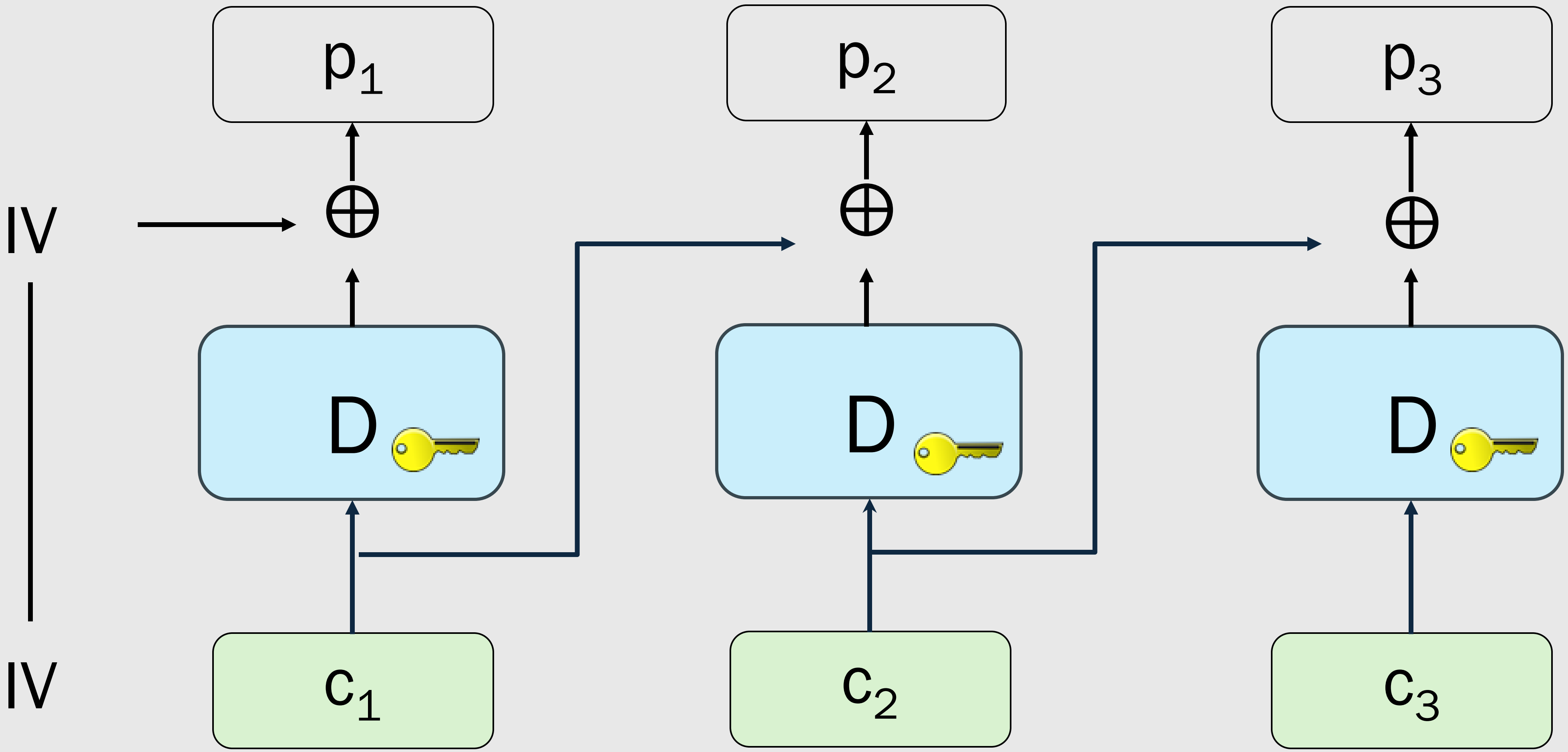


Decryption?

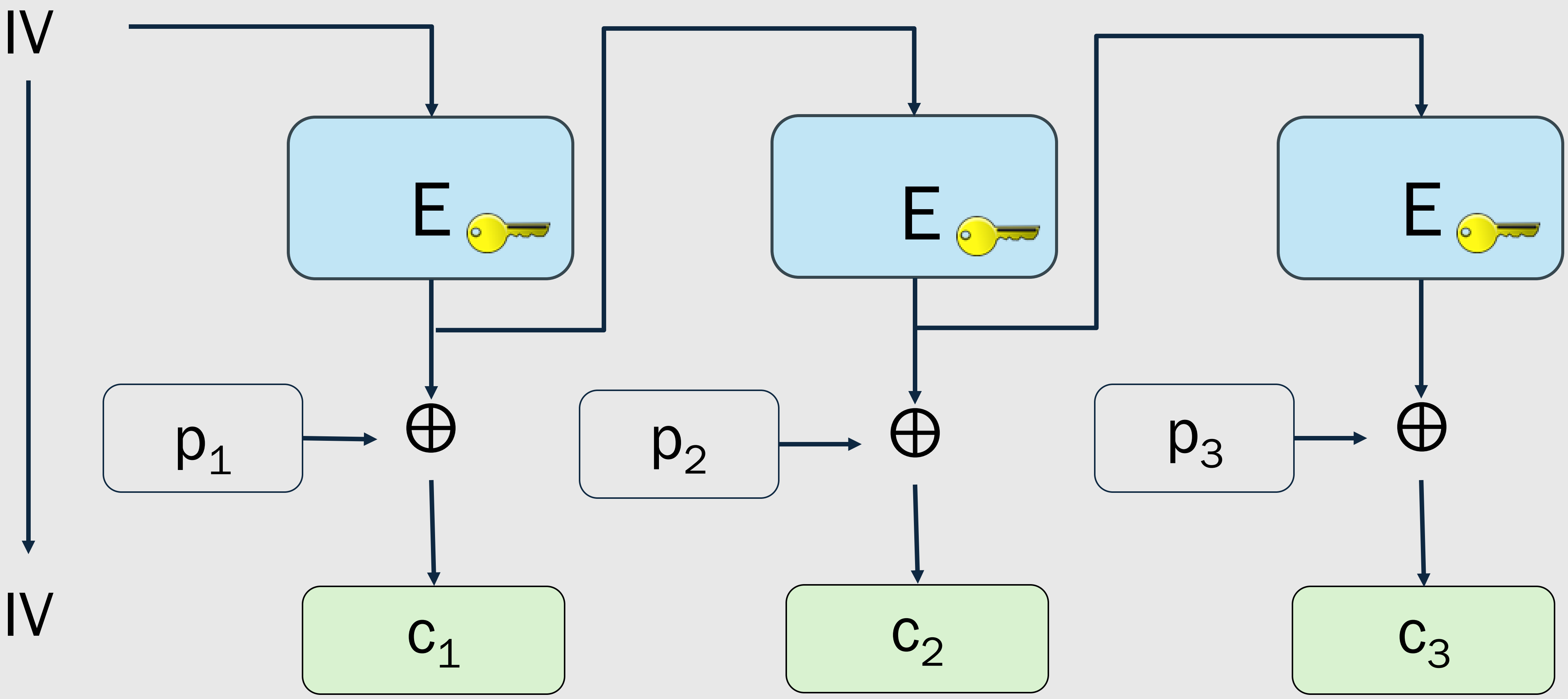
1. Draw the corresponding figure for decryption
2. Must decryption be done sequentially?



CBC Mode Decryption

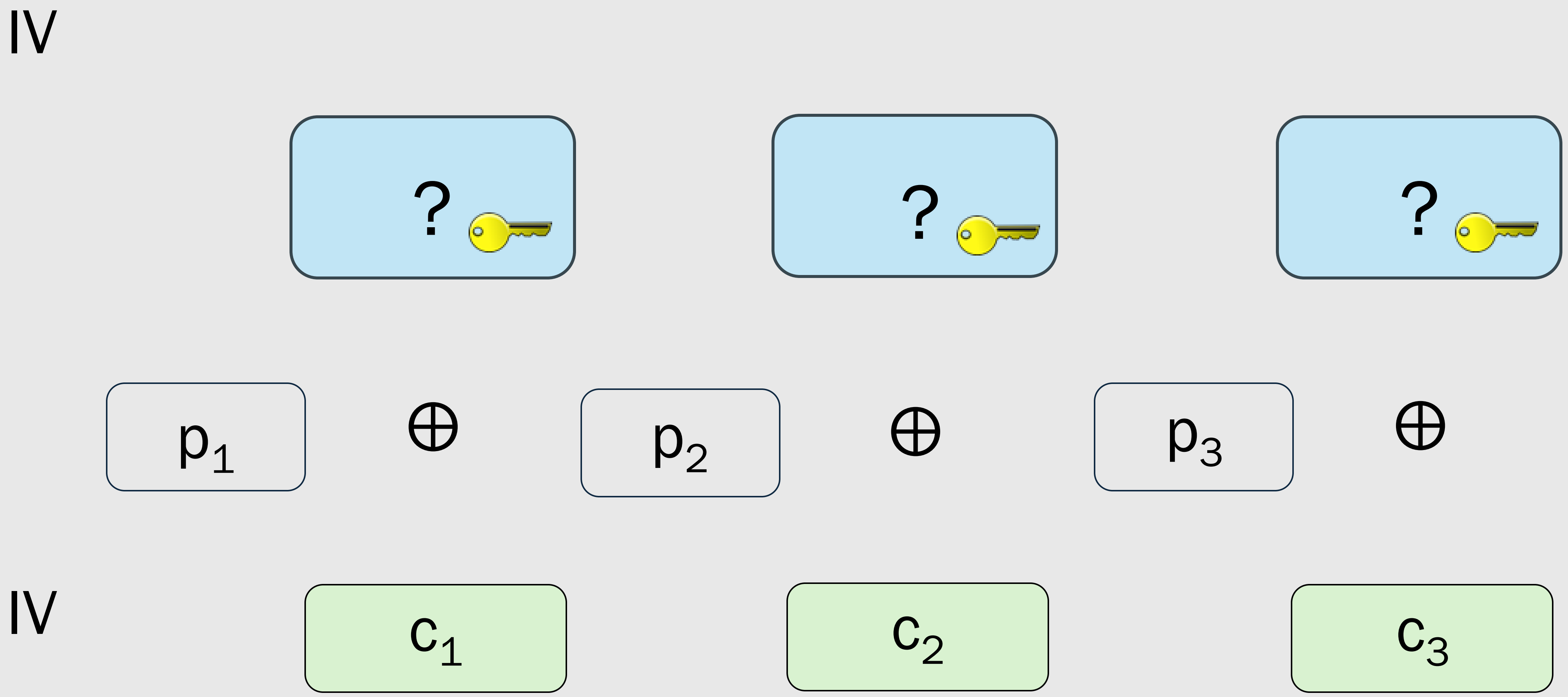


Output Feedback (OFB) Mode: Encryption

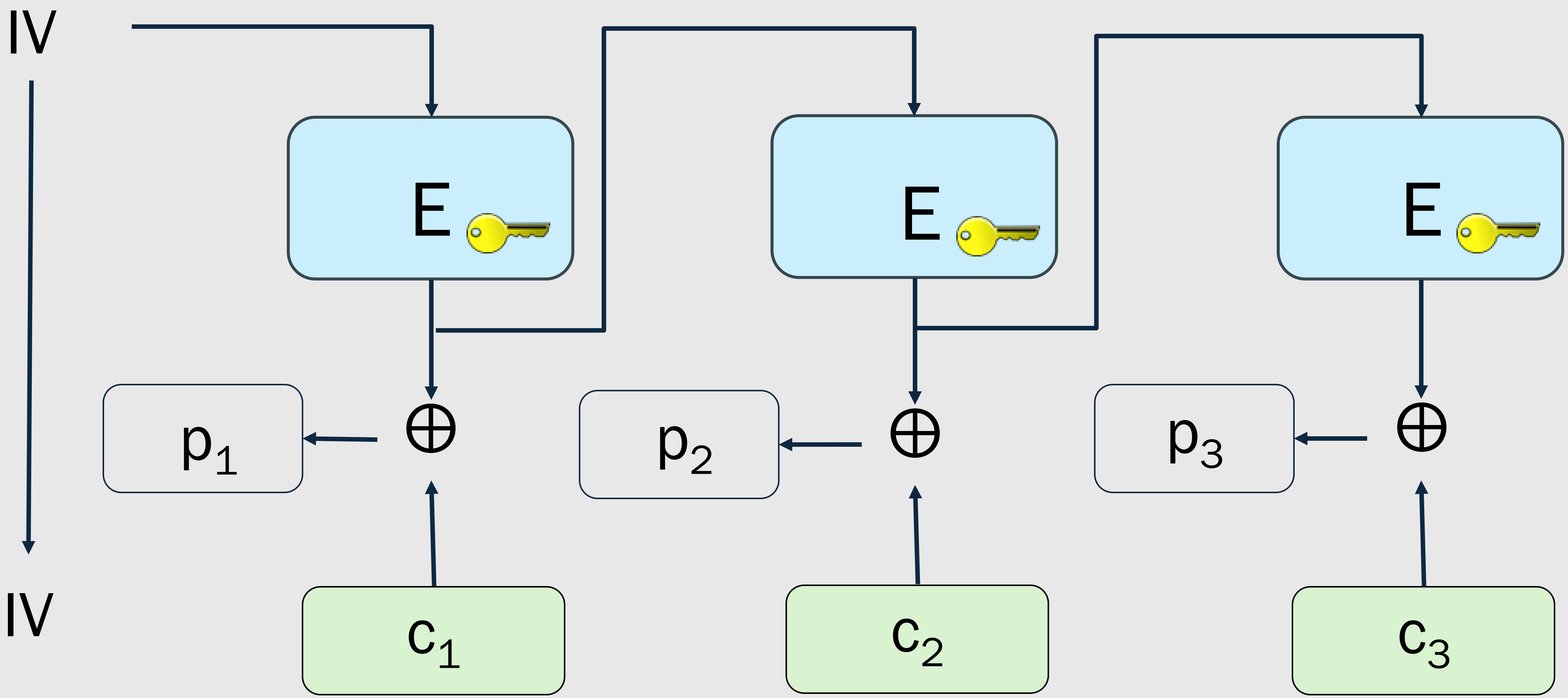


Decryption?

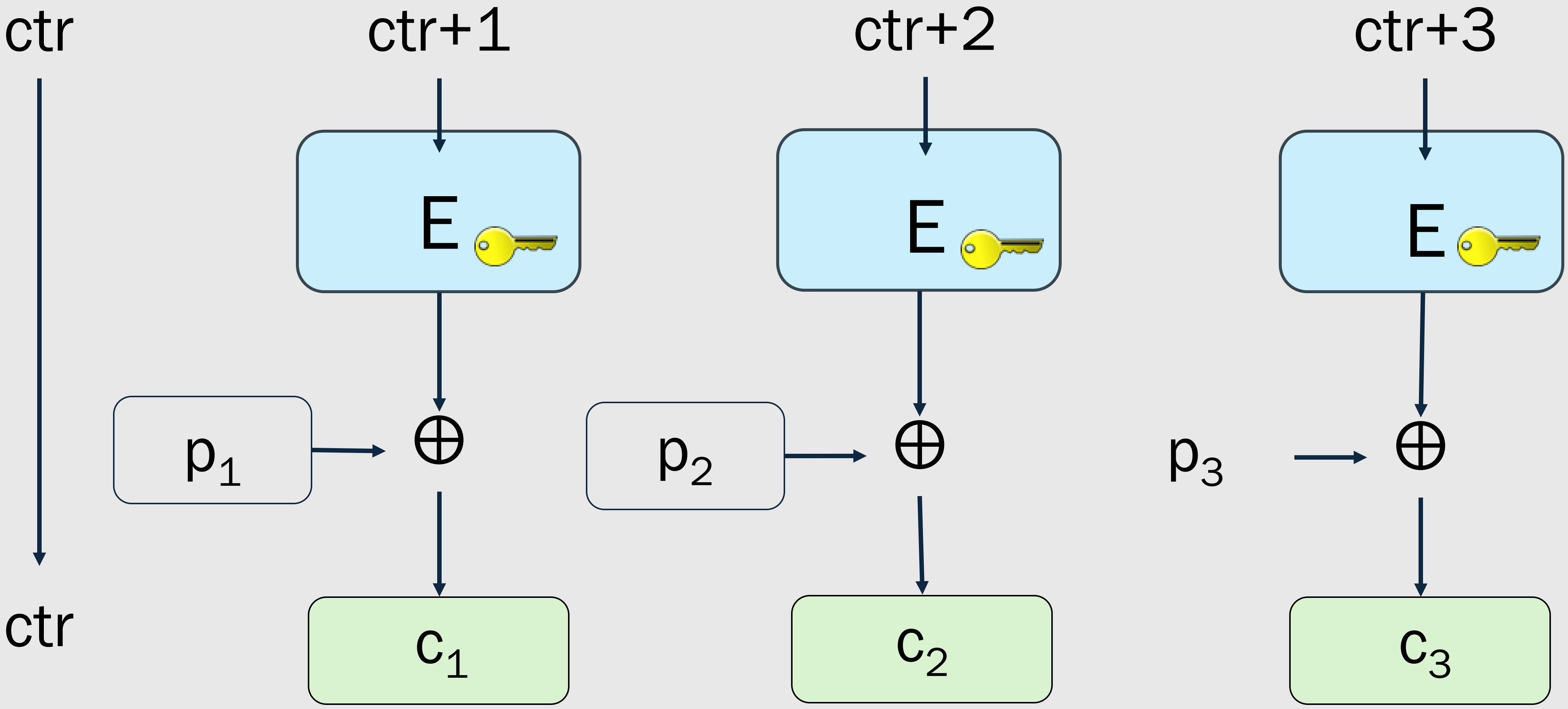
1. Draw the corresponding figure for decryption
2. Why is pre-processing not an option for the message receiver?



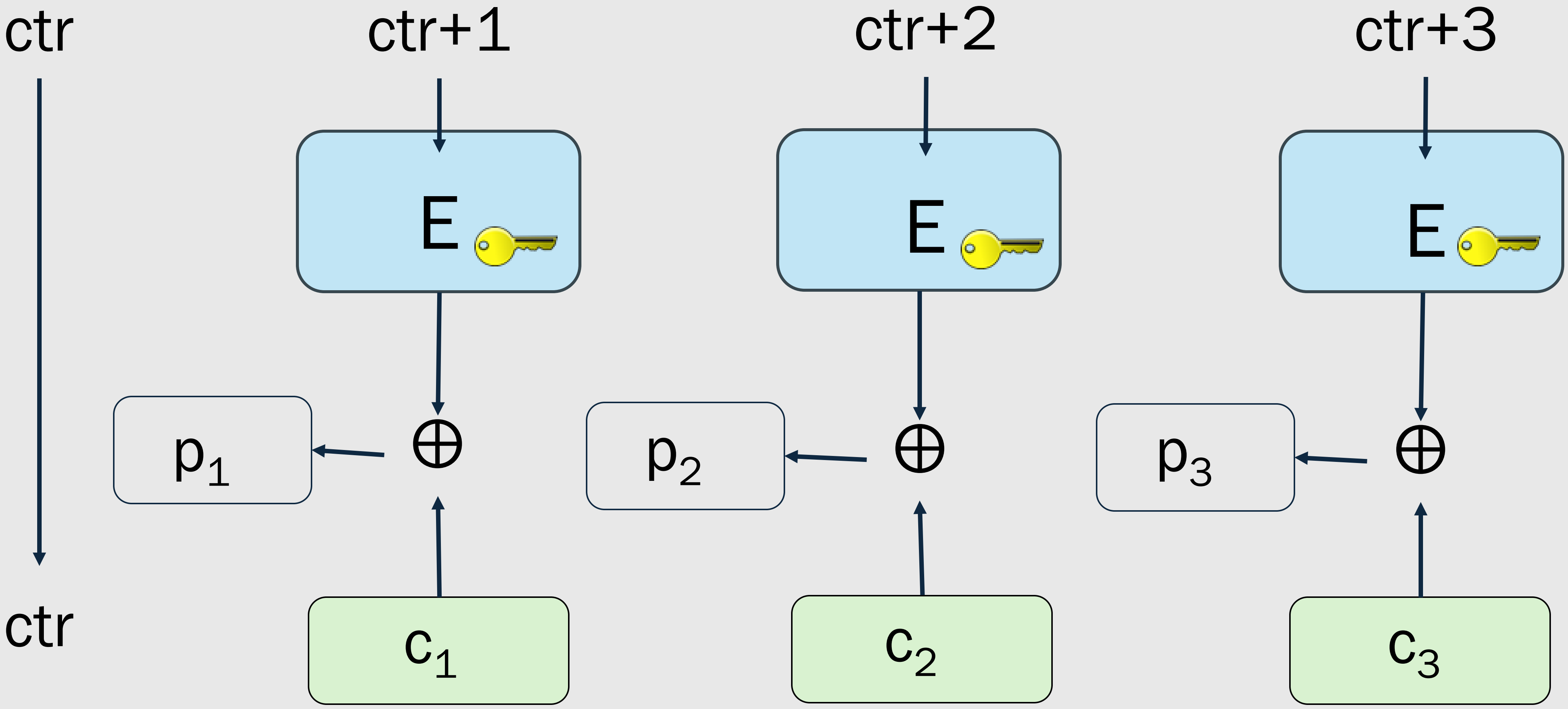
Output Feedback (OFB) Mode: Decryption



Counter (CTR) Mode: Encryption



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