Criptografia FIB

4. Modes d'operació

Anna Rio

Departament de Matemàtica Aplicada II • Universitat Politècnica de Catalunya

MODES D'OPERACIÓ

Recommendation for Block Cipher Modes of Operation
(SP 800-38A NIST 2001)

This recommendation defines five confidentiality modes of operation for use with an underlying symmetric key block cipher algorithm: Electronic Codebook (**ECB**), Cipher Block Chaining (**CBC**), Cipher Feedback (**CFB**), Output Feedback (**OFB**), and Counter (**CTR**). Used with an underlying block cipher algorithm that is approved in a Federal Information Processing Standard (FIPS), these modes can provide cryptographic protection for sensitive, but unclassified, computer data.

MODES D'OPERACIÓ

- Funció que xifra un bloc amb la clau k: E_k
- Algoritme per xifrar missatges: cal fixar la funció E_k i el mode d'operació

Igualment, podem distingir entre la funció D_k que desxifra un bloc i l'algoritme de desxifrar missatges

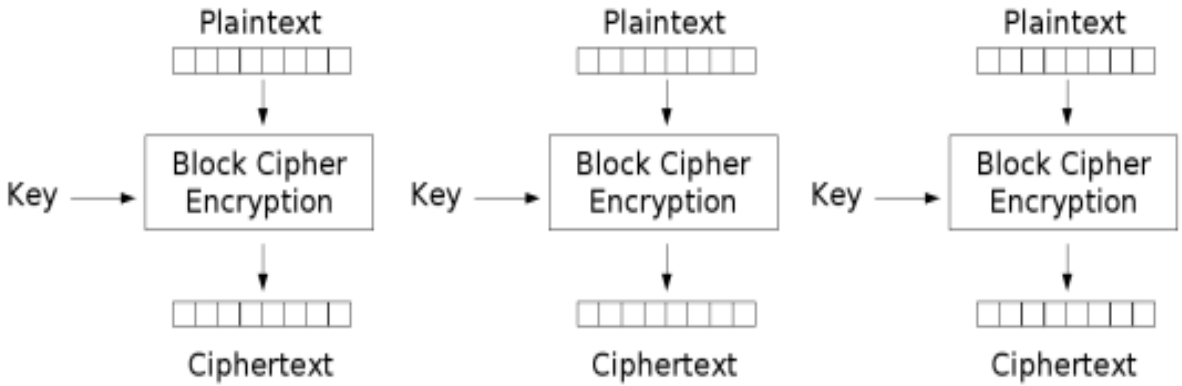
Els modes d'operació són vàlids per a qualsevol mètode simètric de xifrat en bloc

ECB: Electronic CodeBook

Missatge $= m_1 m_2 \ldots m_n$

Xifrat: $c_i = E_k(m_i)$ Desxifrat: $m_i = D_k(c_i)$

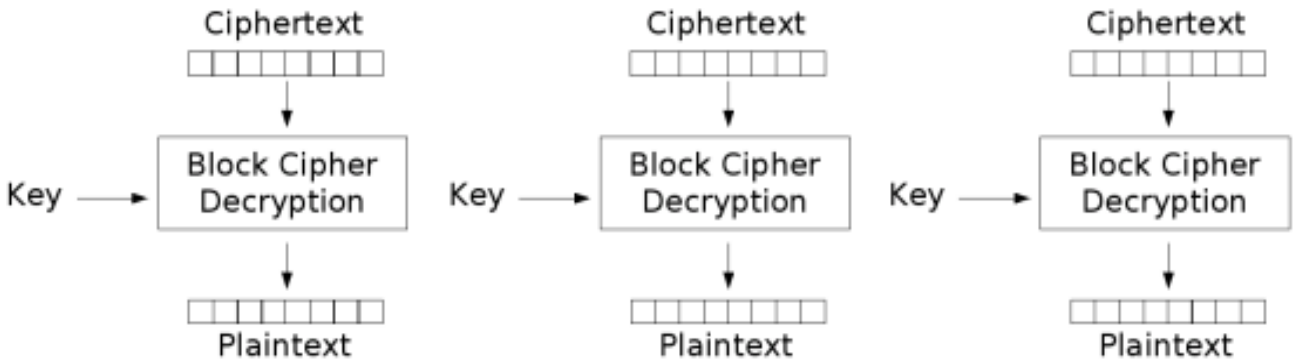
Criptograma $= c_1 c_2 \ldots c_n$



Electronic Codebook (ECB) mode encryption

ECB: Electronic CodeBook

- La funció de xifrat s'aplica directament i independentment a cada bloc del missatge (cal fer padding).
- La seqüència de blocs de sortida és el criptograma.
- Es pot fer computació en paral.lel.
- Donada una clau, un text sempre dóna lloc al mateix criptograma.



Electronic Codebook (ECB) mode decryption

ECB. Exemple

Suposem que tenim un fitxer de salaris

```
JOHN__105000
JACK__500000
```

i una funció que xifra blocs de 2 caràcters.

Xifrem en mode ECB:

```
Q9 2D FP VX C9 IO
LD AS FP C9 IO  IO
```

Repeticions en els criptograma provenen de repeticions en el missatge.
John coneix el seu salari, pot deduir el de Jack.

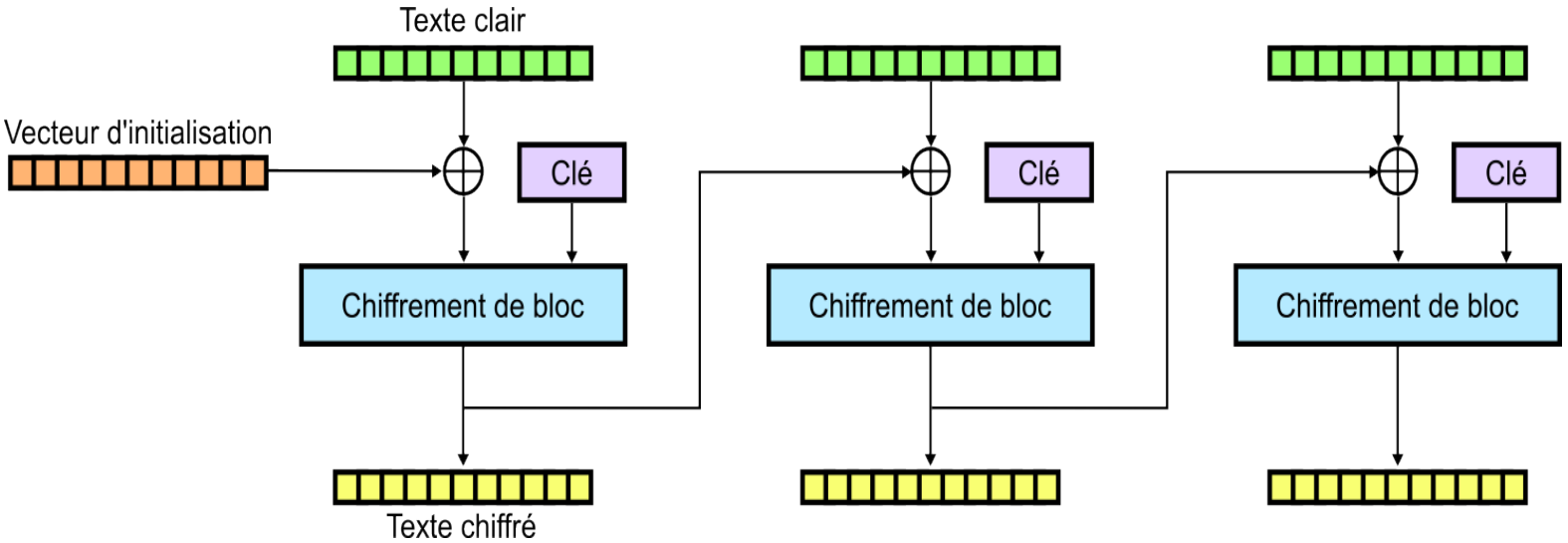
CBC: Cipher Block Chaining

S'inicialitza c_0 aleatori

$$\text{Xifrat:} \quad c_i = E_k(m_i \oplus c_{i-1})$$

Criptograma $= c_0 c_1 c_2 \ldots c_n$

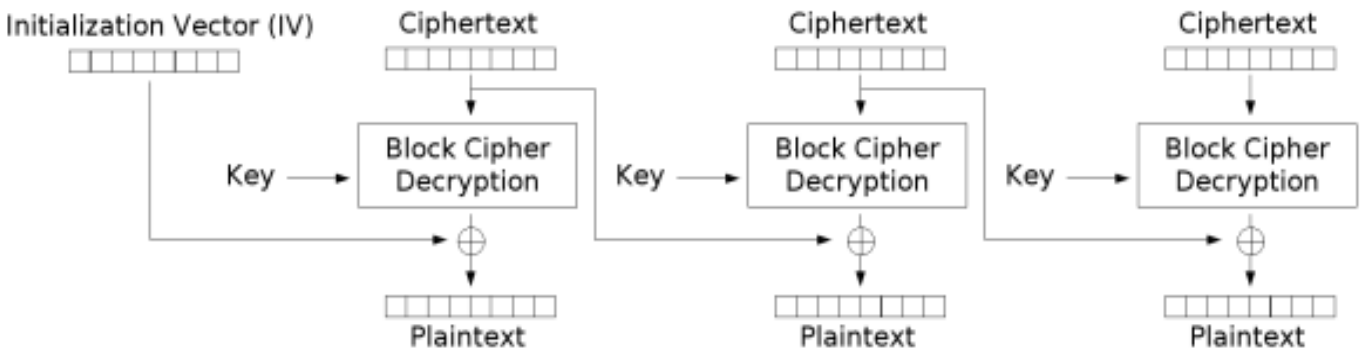
- Un mateix missatge dóna lloc a criptogrames diferents.



CBC: Cipher Block Chaining

Desxifrat: $m_i = D_k(c_i) \oplus c_{i-1}$

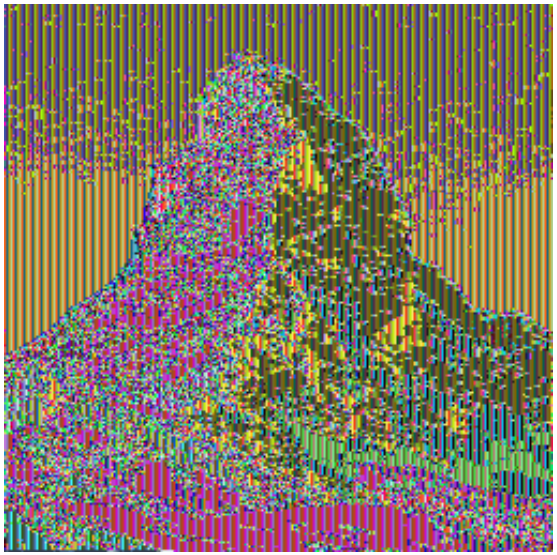
- En el desxifrat es pot fer computació en paral.lel.



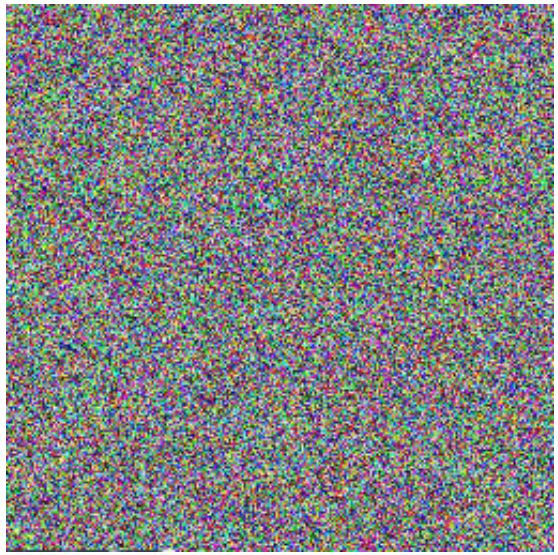
Cipher Block Chaining (CBC) mode decryption

Comparació

Original



ECB

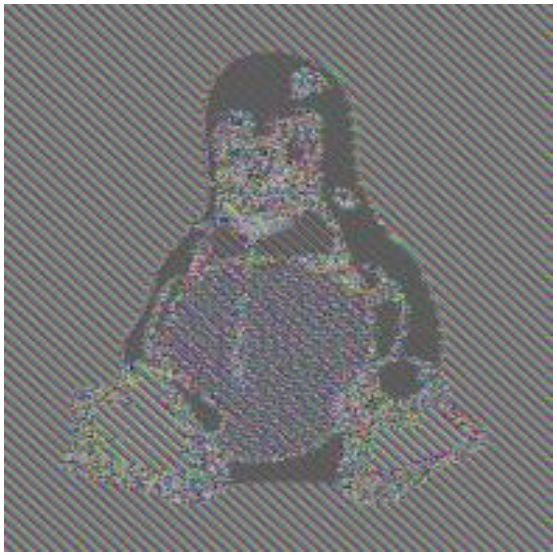


CBC

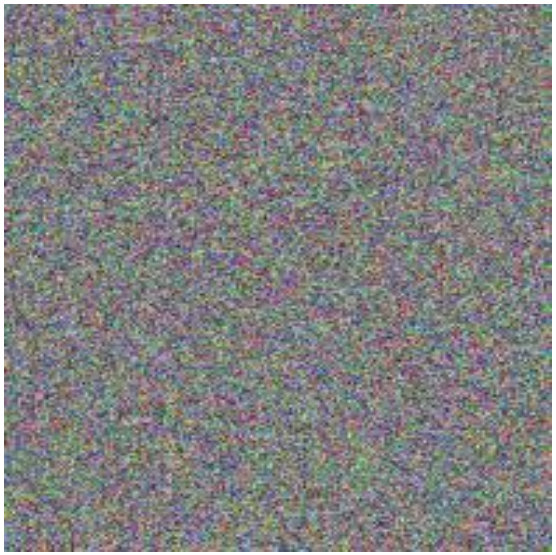
Blocs de 4 pixels

Comparació

Original



ECB

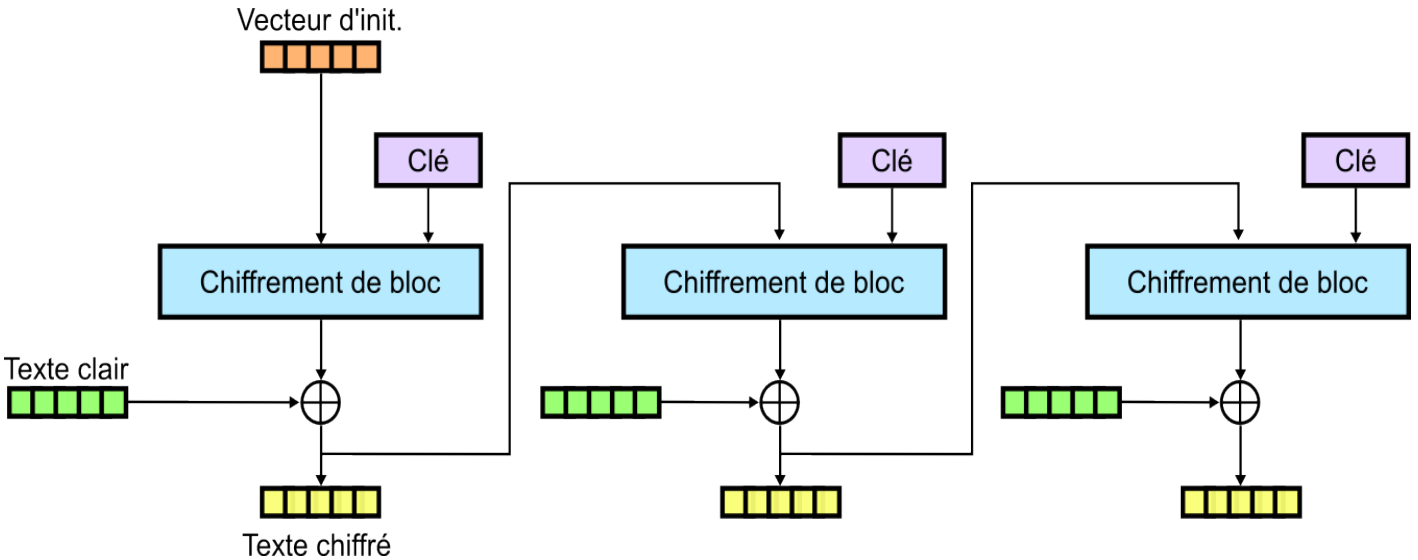


CBC

CFB: Cipher FeedBack

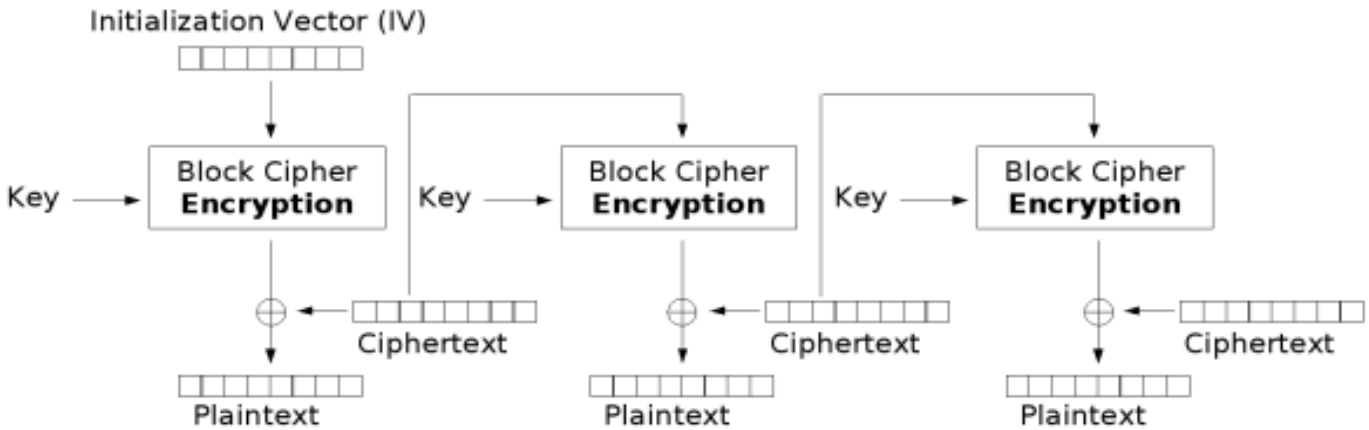
S'inicialitza c_0 aleatori

Xifrat: $c_i = m_i \oplus E_k(c_{i-1})$



CFB: Cipher FeedBack

Desxifrat: $m_i = c_i \oplus E_k(c_{i-1})$



Cipher Feedback (CFB) mode decryption

- No cal implementar la funció de desxifrat D_k
- El desxifrat es pot fer en paral.lel

s-bit CFB

- b indica la longitud de bloc per a la funció de xifrat
- El bloc d'inicialització s_0 té b bits
- El text es divideix en segments de s bits, amb $1 \leq s \leq b$

Xifrat:

$$\begin{aligned} c_i &= m_i \oplus MSB_s(E_k(s_{i-1})) \\ s_i &= LSB_{b-s}(s_{i-1})||c_i \end{aligned}$$

MSB_r indica els r bits més signicatius i LSB_r els r bits menys signicatius.

s-bit CFB

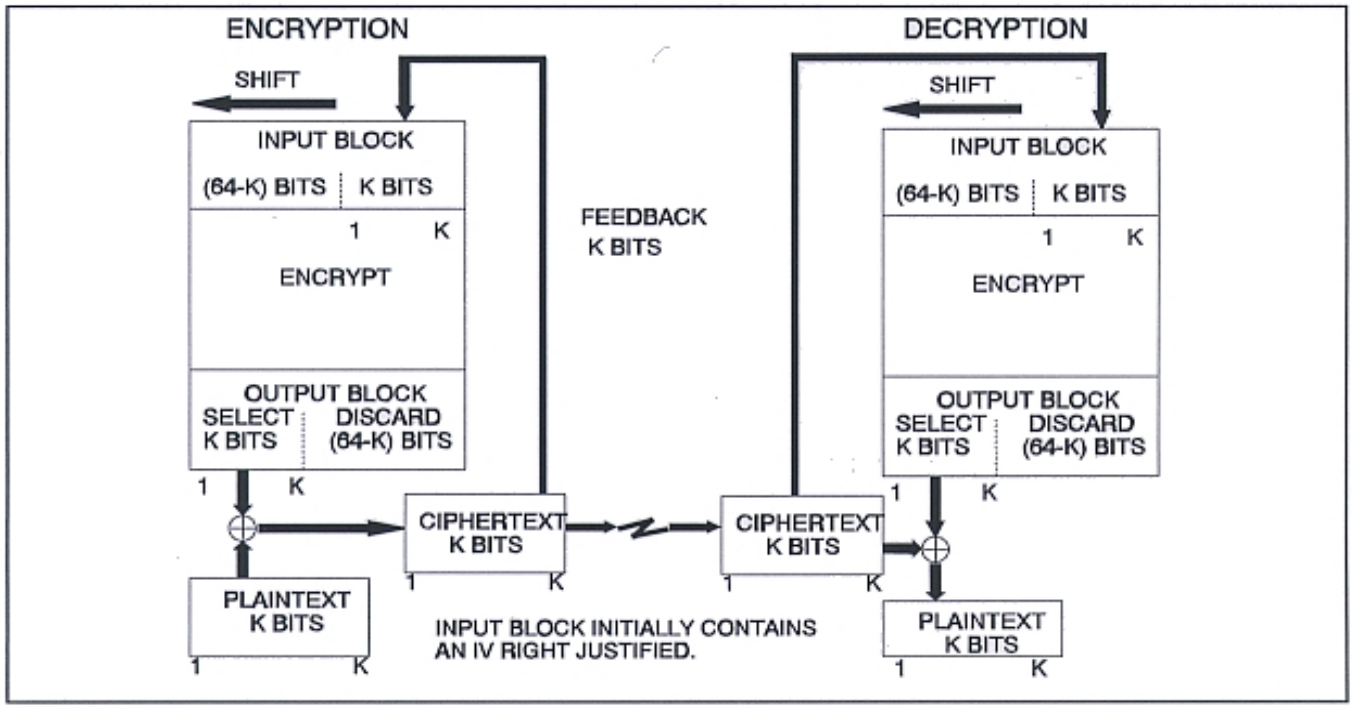


Figure 3: *k-bit Cipher Feedback (CFB) Mode*

Un cop calculats els s_i, el desxifrat es pot fer en paral.lel

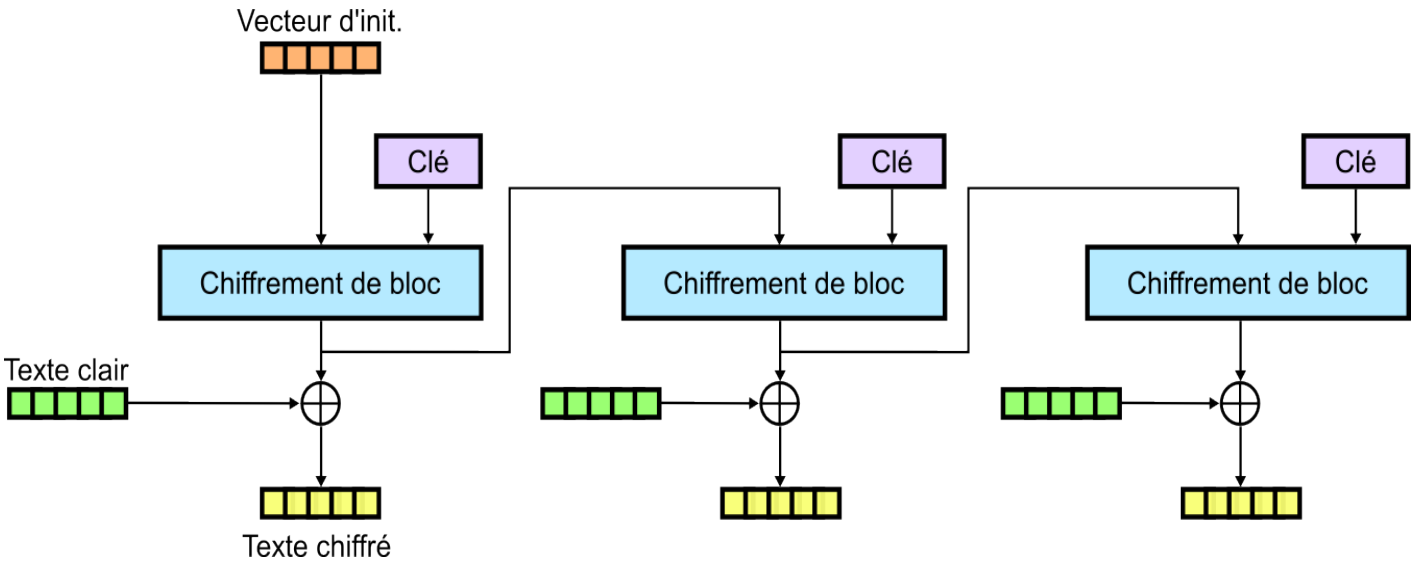
OFB: Output FeedBack

S'inicialitza s_0 aleatori. Xifrat:

$$\begin{aligned} s_i &= E_k(s_{i-1}) \\ c_i &= m_i \oplus s_i \end{aligned}$$

Desxifrat:

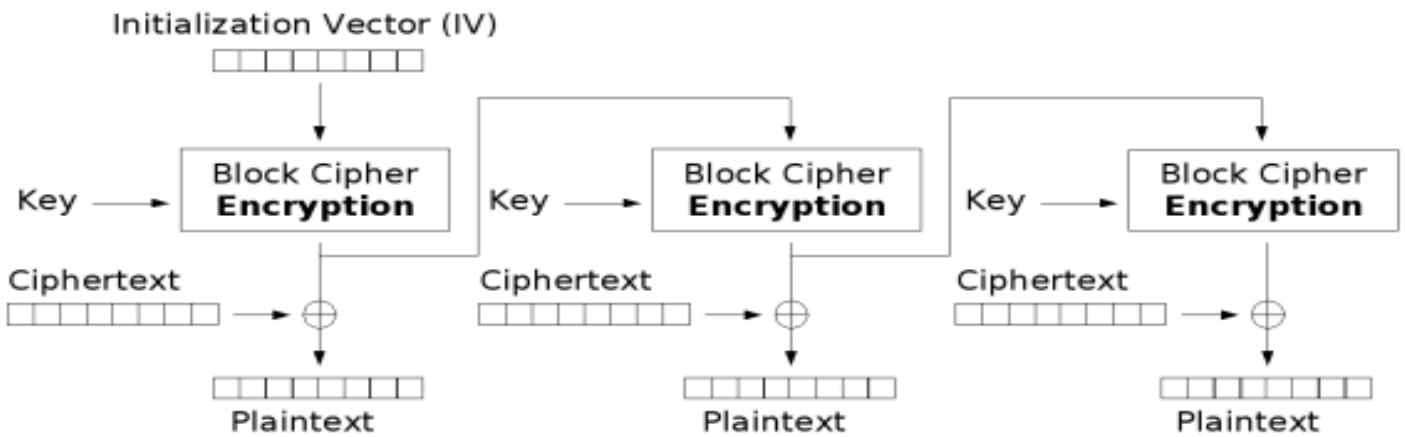
$$\begin{aligned} s_i &= E_k(s_{i-1}) \\ m_i &= c_i \oplus s_i \end{aligned}$$



OFB: Output FeedBack

Desxifrat:

$$\begin{aligned} s_i &= E_k(s_{i-1}) \\ m_i &= c_i \oplus s_i \end{aligned}$$



Output Feedback (OFB) mode decryption

OFB: Output FeedBack

- No cal implementar la funció de desxifrat D_k.
- Els s_i no depenen dels blocs de text.
- Fixada la clau, el vector inicial s_0 ha d'ésser diferent per a cada missatge.
- Per evitar la necessitat de fer padding, si el darrer "bloc"de missatge m_n té u bits, es pren

$$c_n = m_n \oplus MSB_u(E_k(s_{n-1}))$$

CTR: Counter

Per a cada missatge $m_1 \ldots m_n$, comptadors $T_1, \ldots, T_n$ (blocs).

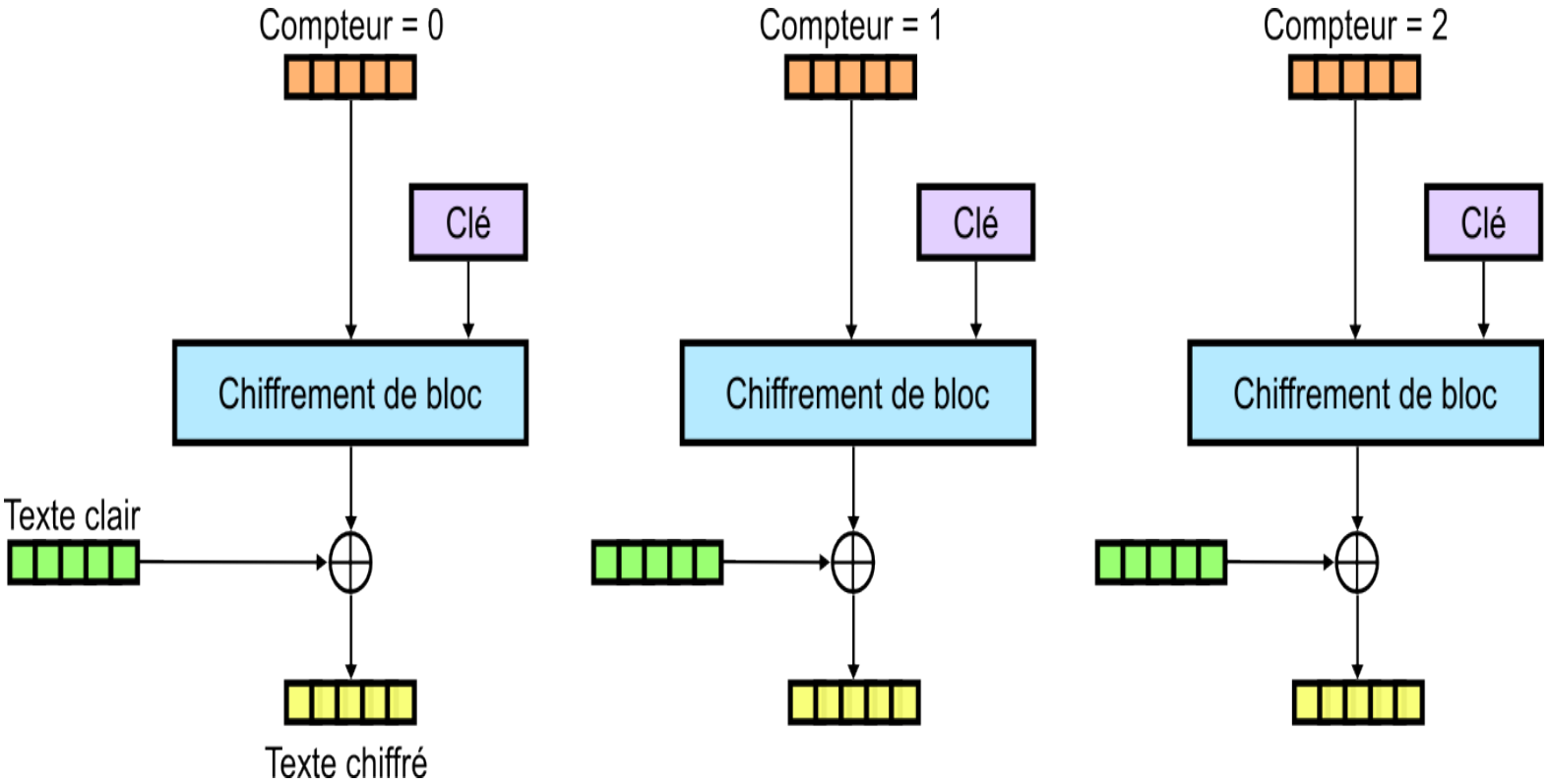
Xifrat

$$\begin{aligned} c_i &= m_i \oplus E_k(T_i) \\ c_n &= m_n \oplus MSB_u(E_k(T_n)) \end{aligned}$$

Desxifrat

$$\begin{aligned} m_i &= c_i \oplus E_k(T_i) \\ m_n &= c_n \oplus MSB_u(E_k(T_n)) \end{aligned}$$

CTR: Counter


Compteur = 0
Clé
Chiffrement de bloc
Texte clair
Texte chiffré
Compteur = 1
Clé
Chiffrement de bloc
Compteur = 2
Clé
Chiffrement de bloc

CTR: Counter

- No cal fer padding
- No cal usar l'algoritme de desxifrat D_k
- Els $E_k(T_i)$ es poden calcular abans de disposar de text o criptograma
- El xifrat/desxifrat de blocs es pot fer en paral.lel
- El desxifrat d'un bloc és independent del dels altres blocs, només cal el comptador corresponent

Comptadors

Fixat el missatge, els $T_1, \ldots, T_n$ han d'ésser diferents.

Mètode

Sobre un T_1 inicial, fem **increments parcials** successius:

- $m \leq b$ (longitud de bloc)
- Paraula de m bits $\sim$ enter $x < 2^m$
- Calculem $x + 1 \bmod 2^m$ i prenem els m bits corresponents. Iterem n vegades.
- Modifiquem els m bits menys significatius (o altres posicions fixades)

Comptadors

$b = 8 \qquad m = 5$

T_1	$***11110$	30
T_2	$***11111$	$31 \bmod 32$
T_3	$***00000$	$32 \bmod 32 = 0$
T_4	$***00001$	$33 \bmod 32 = 1$
T_5	$***00010$	$34 \bmod 32 = 2$
T_6	$***00011$	$35 \bmod 32 = 3$
	$\ldots$	

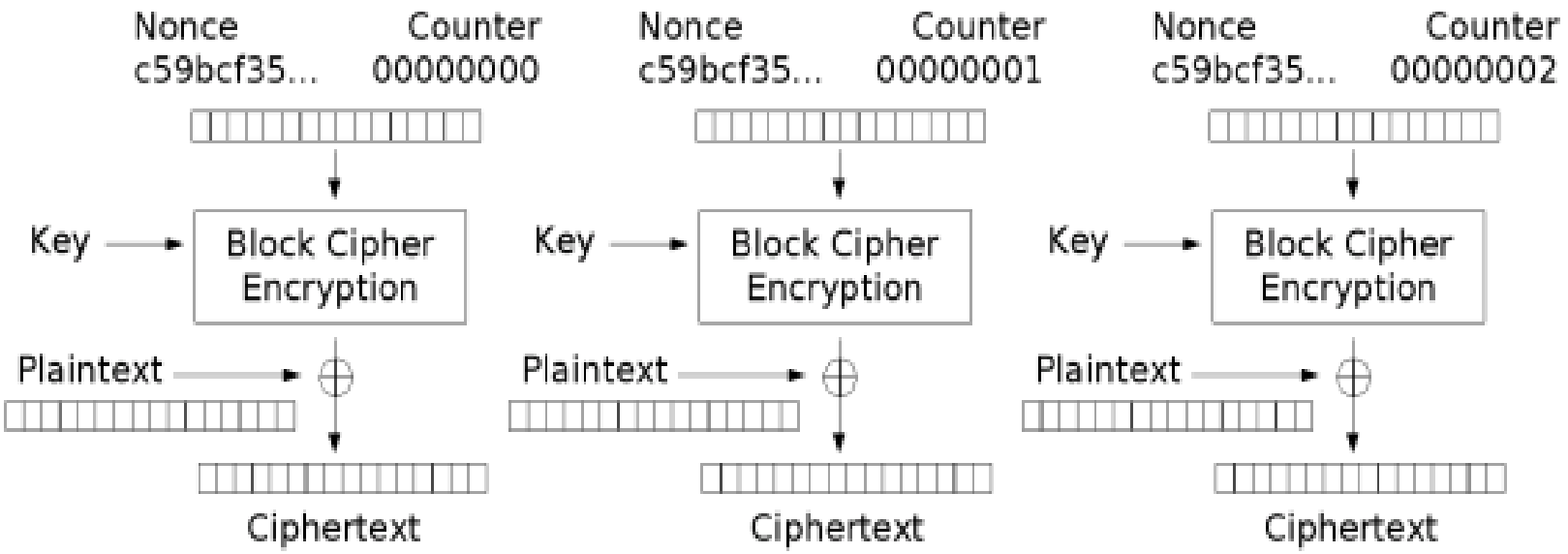
Si el nombre de blocs del missatge és $n \leq 2^m$,
tenim una seqüència $T_1, \ldots, T_n$ **sense repeticions**
(En la realitat, $b = 64, 128, 192, 256$)

Per a tots els missatges que es xifrin amb una mateixa clau, els comptadors han d'ésser diferents

Si usem un mètode com l'anterior, aquesta condició només depèn de l'elecció dels comptadors inicials

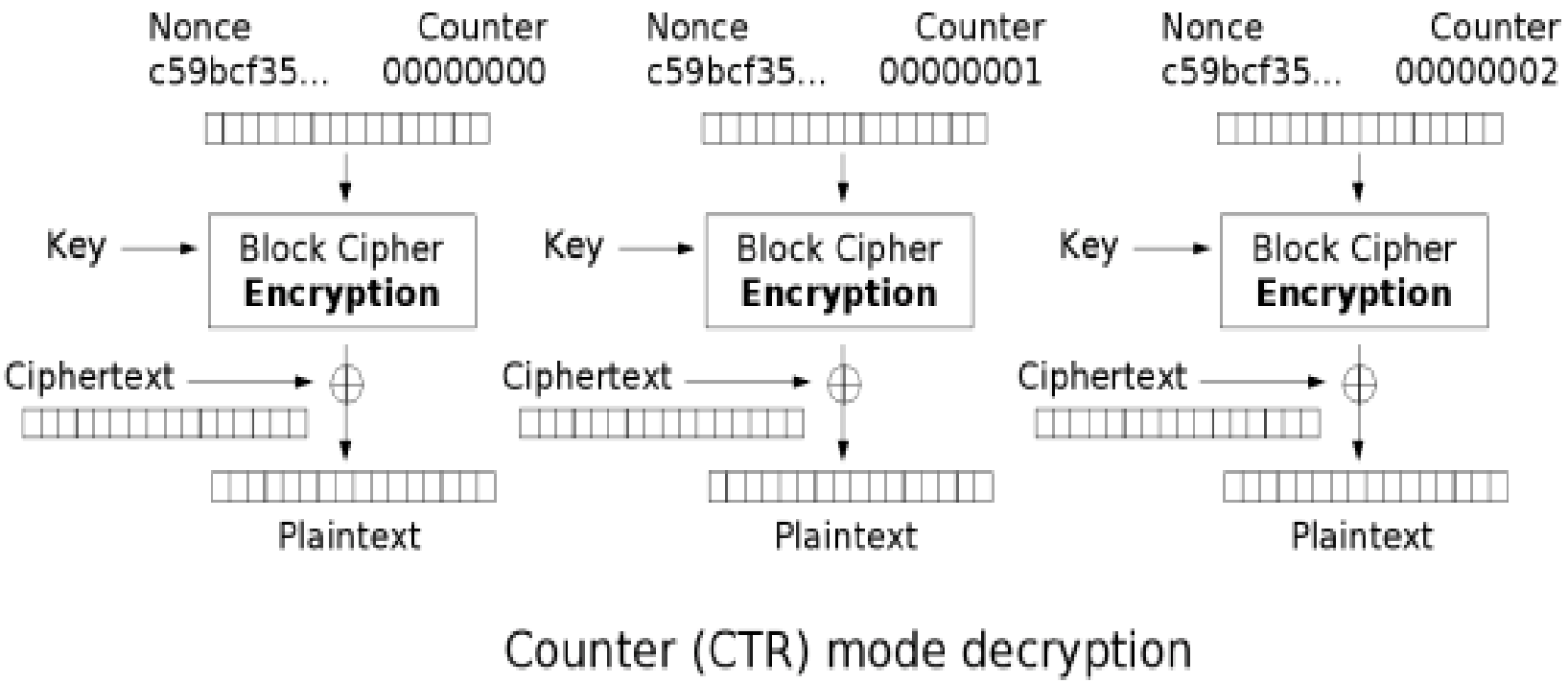
1. Model seqüencial de xifrat de missatges
   Per al primer missatge a xifrar, T_1 aleatori. Es calculen els $T_2, \ldots, T_n$. Per al segon missatge el comptador inicial serà el resultat d'aplicar la funció d'increment a T_n
   Cal que el nombre total de blocs de tots els missatges a xifrar amb una clau fixada sigui menor que 2^m
2. A cada missatge se li assigna una paraula de $b/2$ bits (**nonce**). Aquesta paraula s'incorpora a cada comptador del missatge. Per exemple, en els $b/2$ bits més significatius. (Sobre els $m = b/2$ restants es va fent l'increment).
   En aquest model, cal fixar una manera d'assignar nonces.

CTR: Counter. Xifrar



Counter (CTR) mode encryption

CTR: Counter. Desxifrar



Counter (CTR) mode decryption

CTR: Counter

- El mode COUNTER transforma un xifratge de bloc en un xifratge de flux
- És el mode recomenat per a l'AES