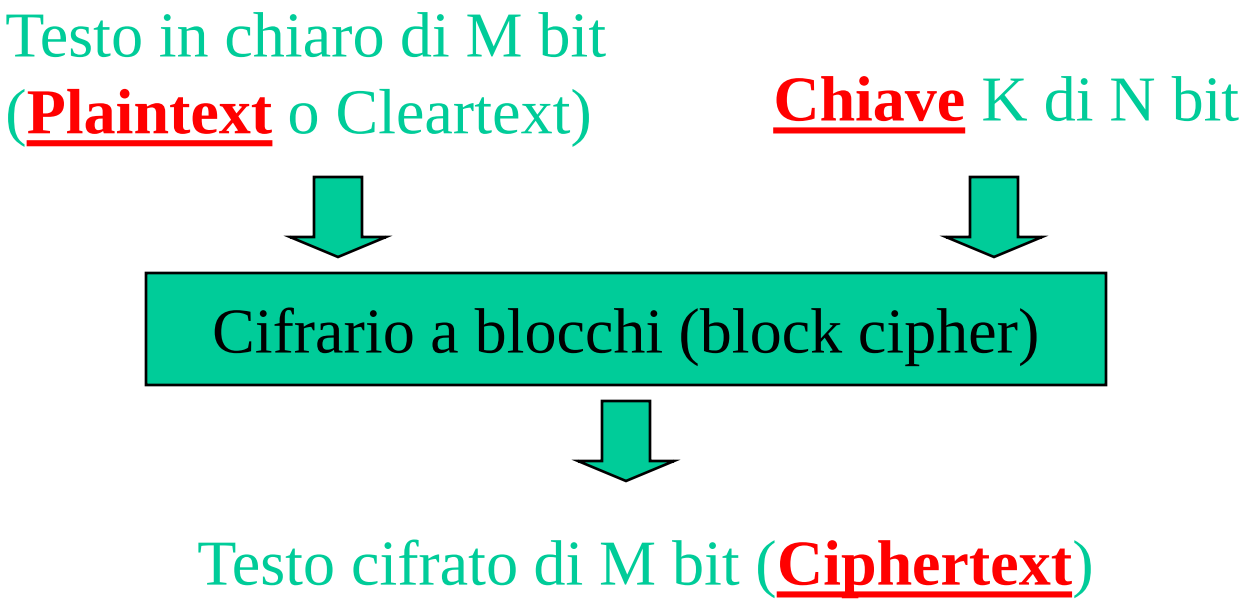
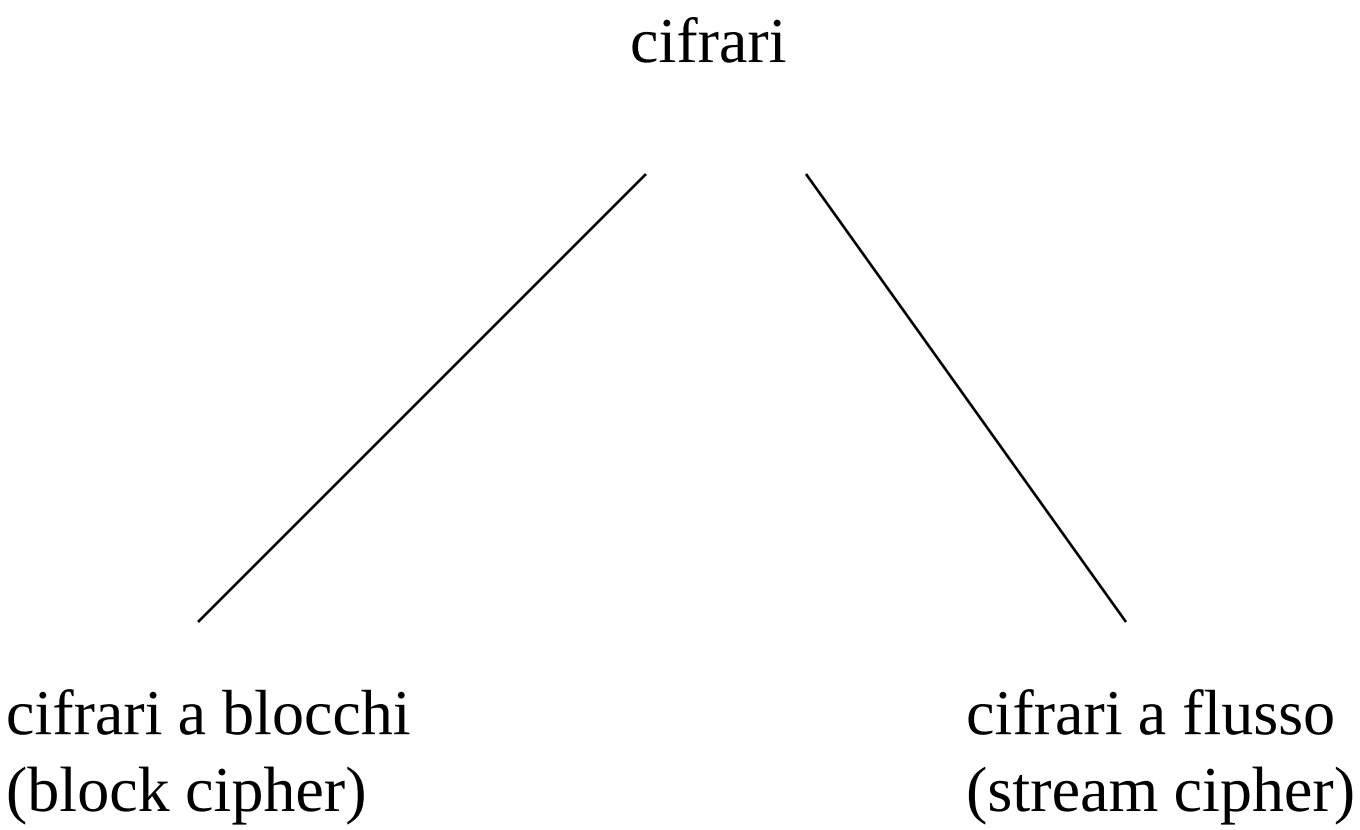
Utilizzi dei cifrari a blocchi

Prof. Francesco Bergadano

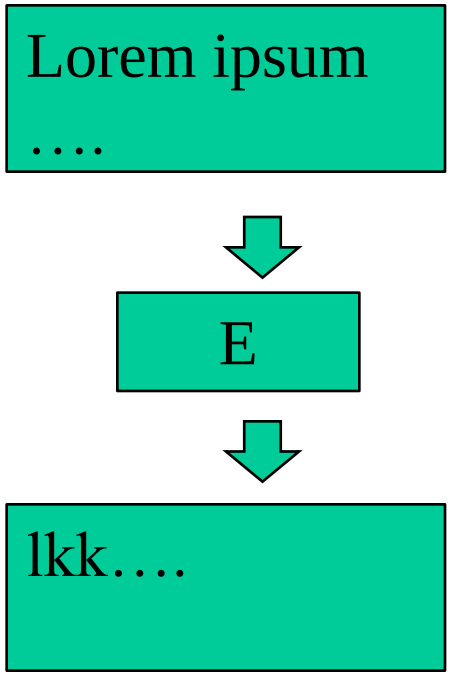
Dipartimento di Informatica
Università di Torino

Cifrari a blocchi

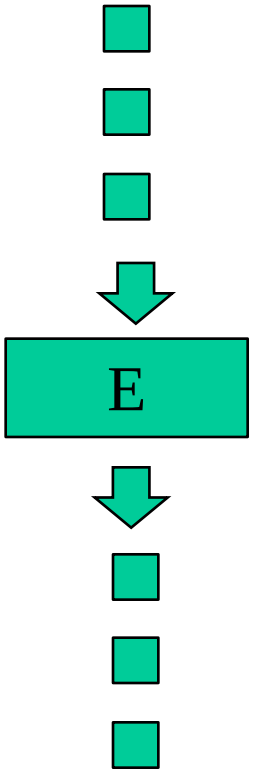



cifrari
cifrari a blocchi
(block cipher)
cifrari a flusso
(stream cipher)

cifrari a blocchi
(block cipher)



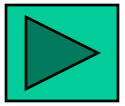
cifrari a flusso
(stream cipher)



Due problemi:

- Usare chiavi più lunghe
- Cifrare testi più lunghi

Chiavi più lunghe



Perché?

Chiavi più lunghe

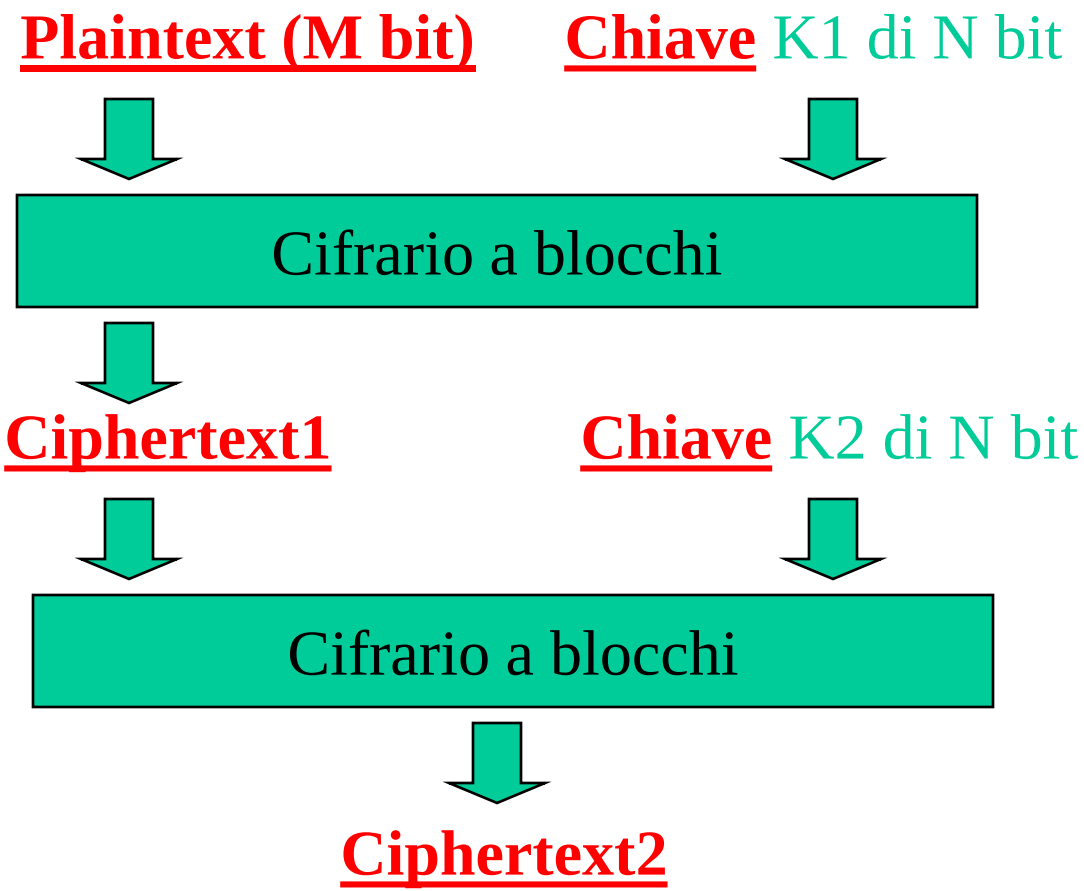
Perché una chiave corta rende il cifrario debole rispetto ad attacchi di tipo ‘forza bruta’.

Chiavi più lunghe

idea:

cifrare più volte,
ogni volta con una chiave diversa.

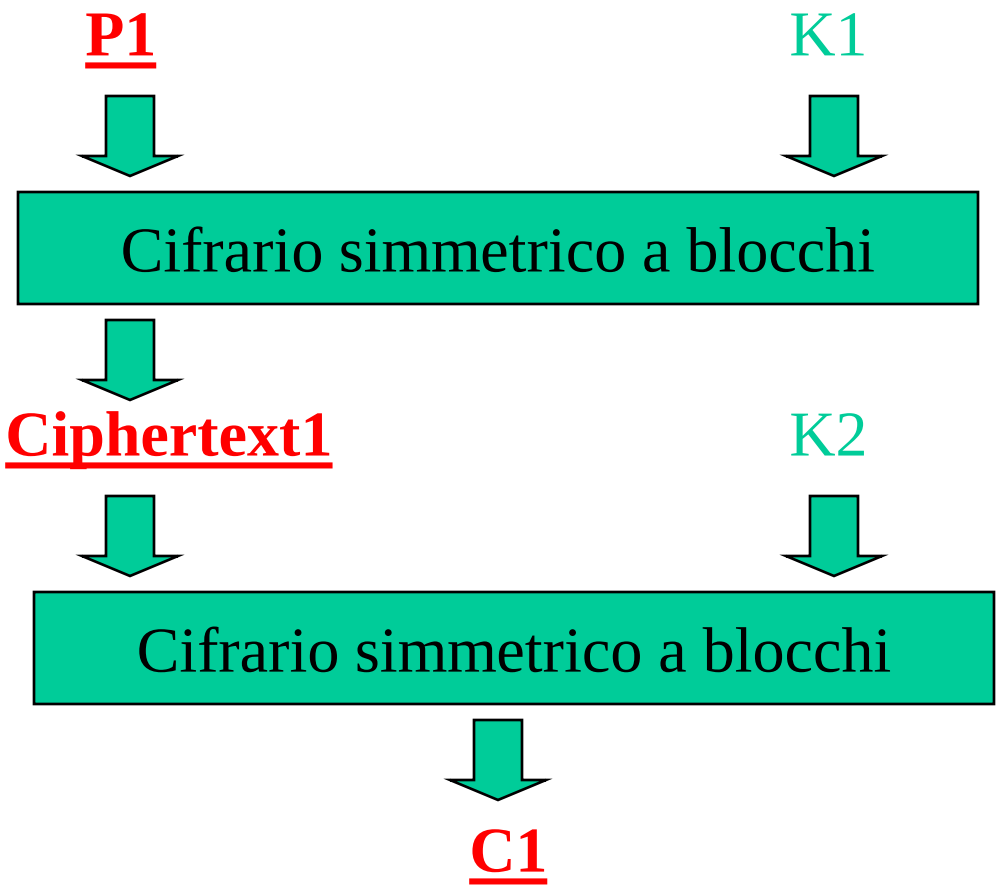
Cifratura a due fasi



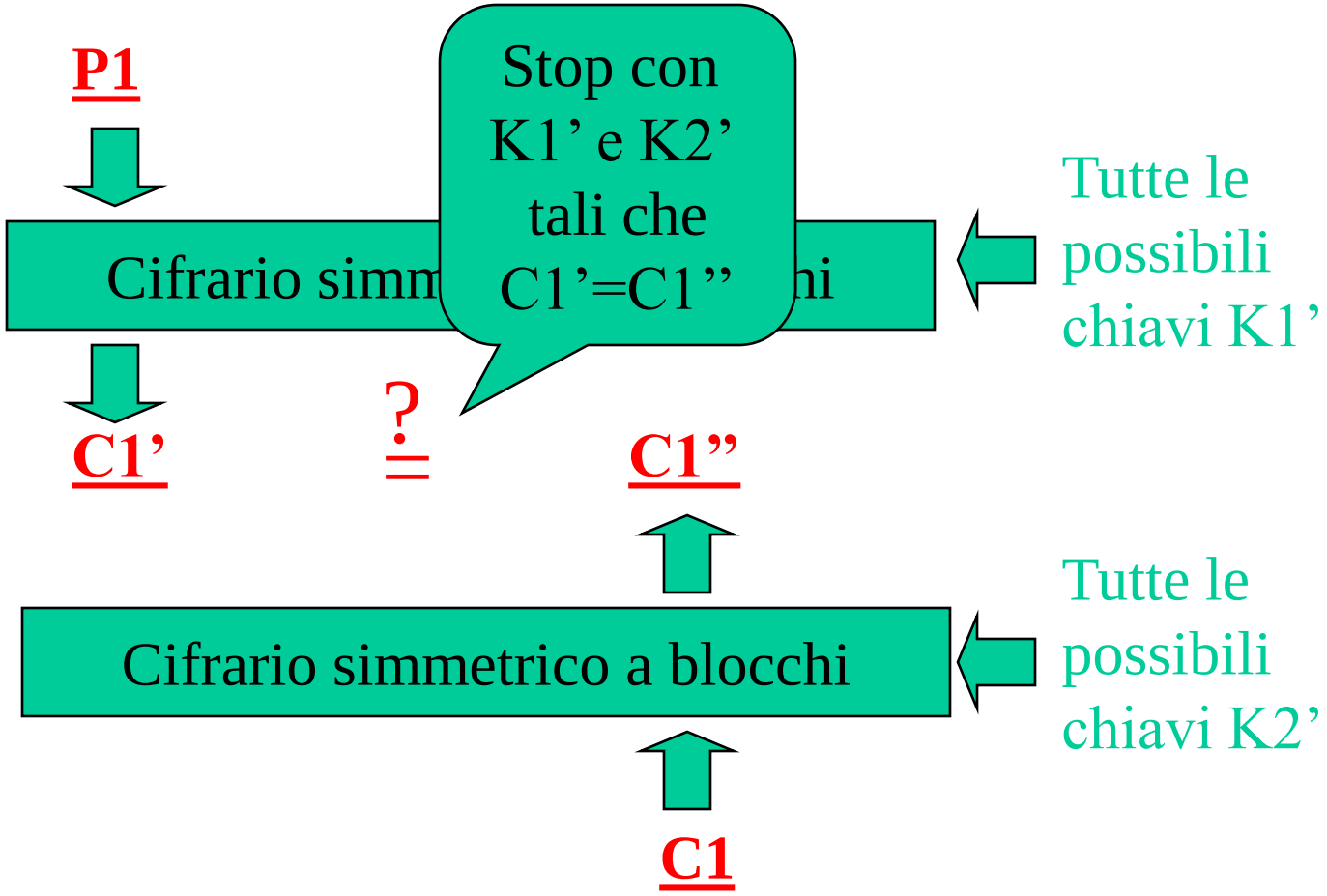
Problema della cifratura a 2 fasi attacco ‘meet in the middle’

Non è realmente più forte del cifrario a blocchi originario, a causa di un possibile attacco di tipo ‘forza bruta’ basato sul valore del testo cifrato intermedio Ciphertext1. Occorre conoscere almeno 2 coppie <P1,C1>, <P2,C2> prodotte con il cifrario.

Problemi della cifratura a due fasi



Problemi della cifratura a due fasi



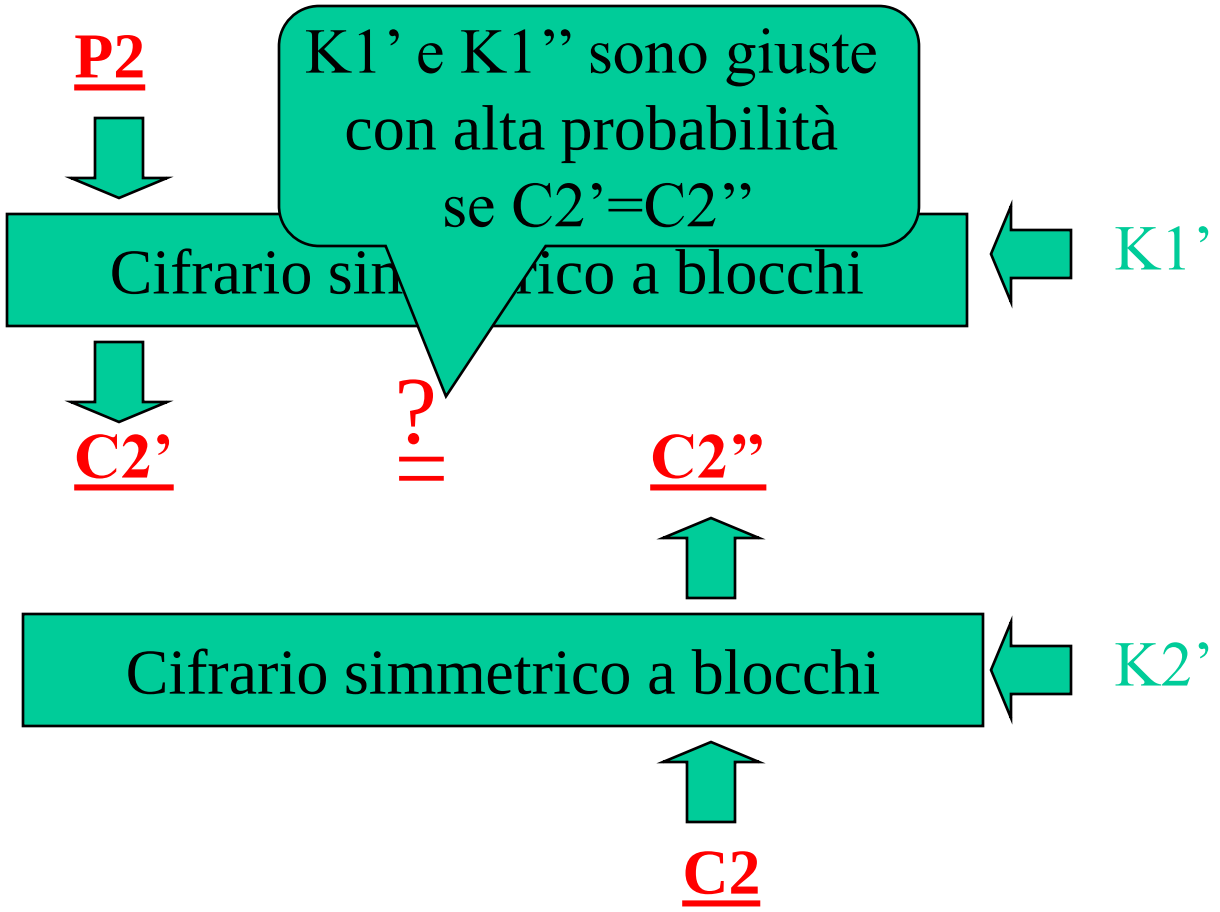
osservazione

Possibili coppie <k1,k2> sono 2^{2n}

Possili blocchi C1 sono 2^{M}

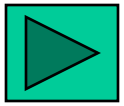
Se M < 2n ci sono più soluzioni

Problemi della cifratura a due fasi



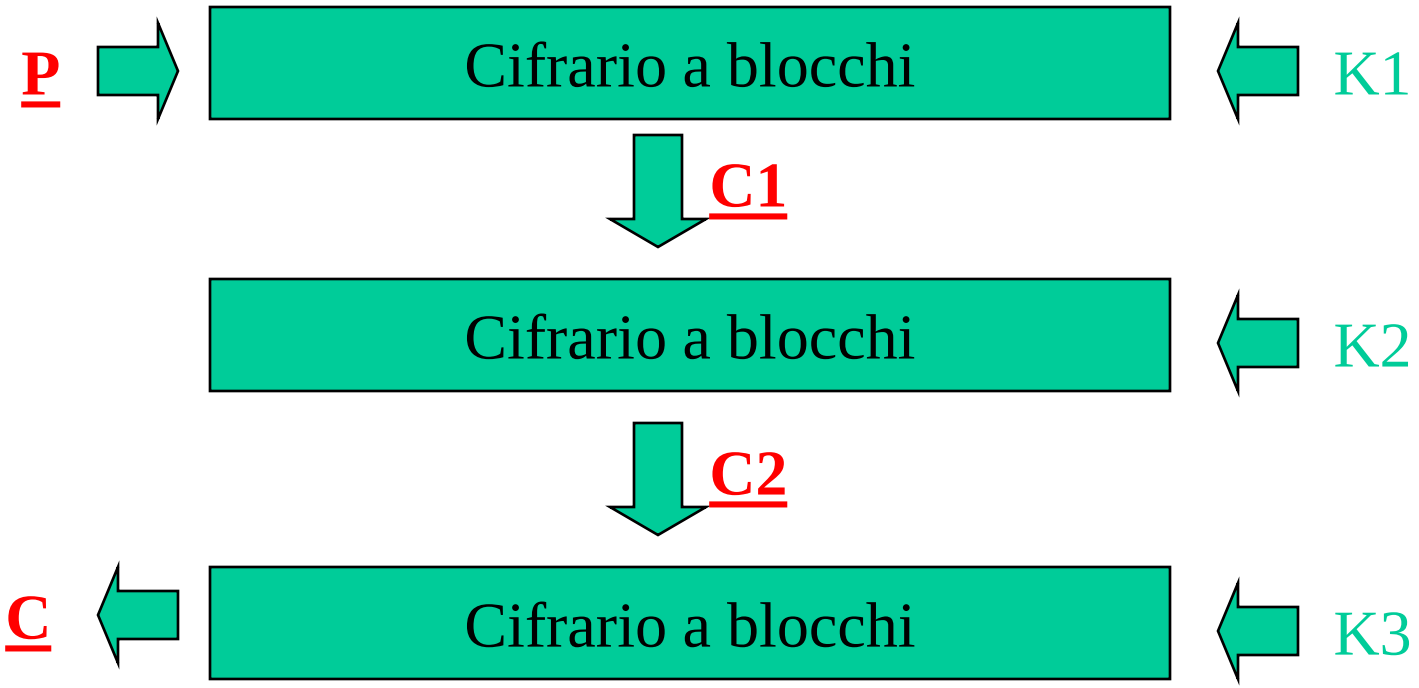
Problemi cifratura a 2 fasi

Soluzioni?



Cifratura a 3 fasi

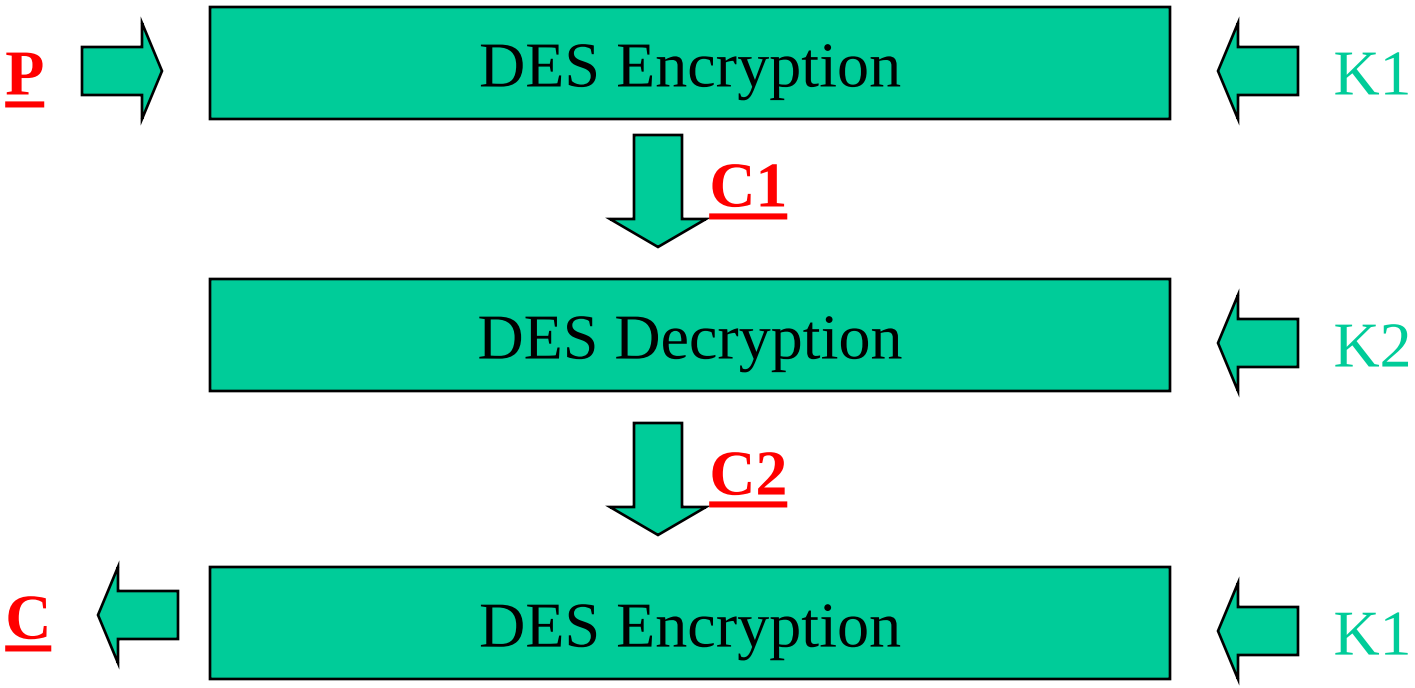
Cifratura a tre fasi



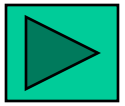
Cifratura a tre fasi

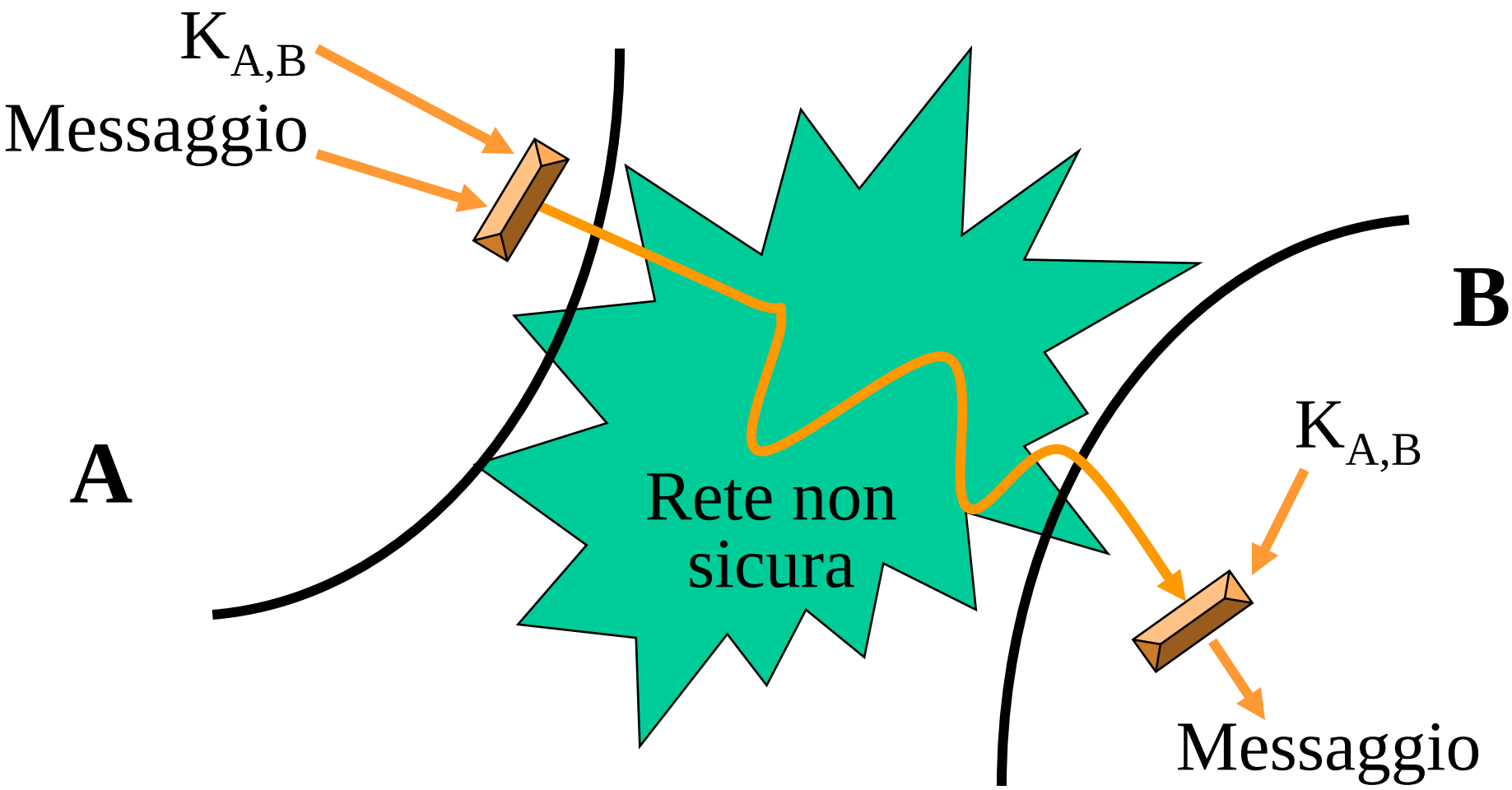
- Non ha i problemi delle 2 fasi
- Applicata al DES, produce il ‘triple DES’, usato spesso, anche nei Browser
- Triple DES è usato di solito con K1=K3, e con la seconda fase usata ‘all’inverso, ovvero in modalità ‘Decryption’ (3DES-EDE), questo affiché 3DES sia uguale a DES semplice per K1=K2=K3.

Triple DES (EDE)



Messaggi più lunghi

 Perché?



Il messaggio è solitamente di lunghezza variabile

Messaggi più lunghi

idea:

- dividere il testo in blocchi
- cifrare ogni blocco
- eventualmente usare il blocco cifrato precedente come input aggiuntivo.

Messaggi più lunghi

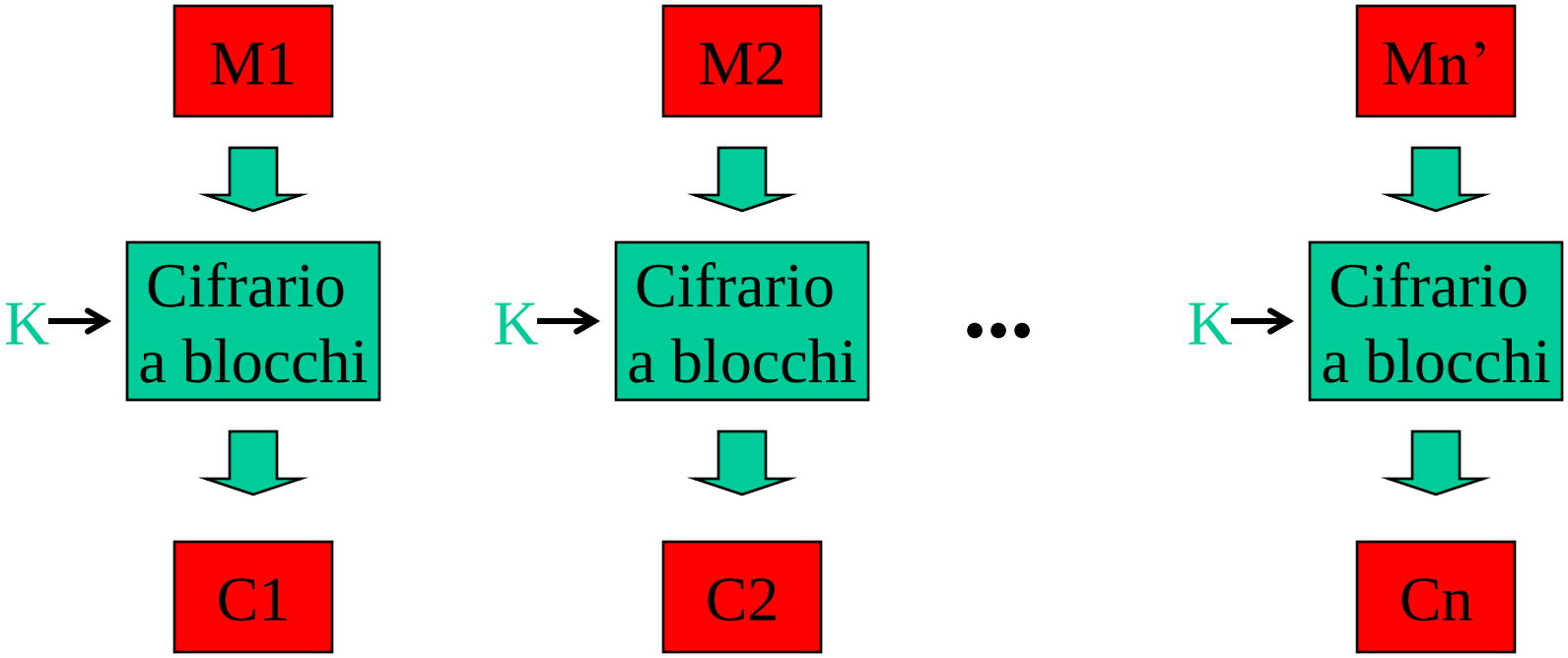
testo M di t bit, cifrario a blocchi di k bit
$n = \lfloor t/k \rfloor + 1$

M = M1 | M2 | … | Mn
dove ogni blocco Mi è lungo k bit e il blocco Mn è lungo al più k bit

Mn' = Mn con 'padding' di 0 fino a raggiungere k bit

Messaggi di lunghezza variabile

Electronic Codebook (ECB)



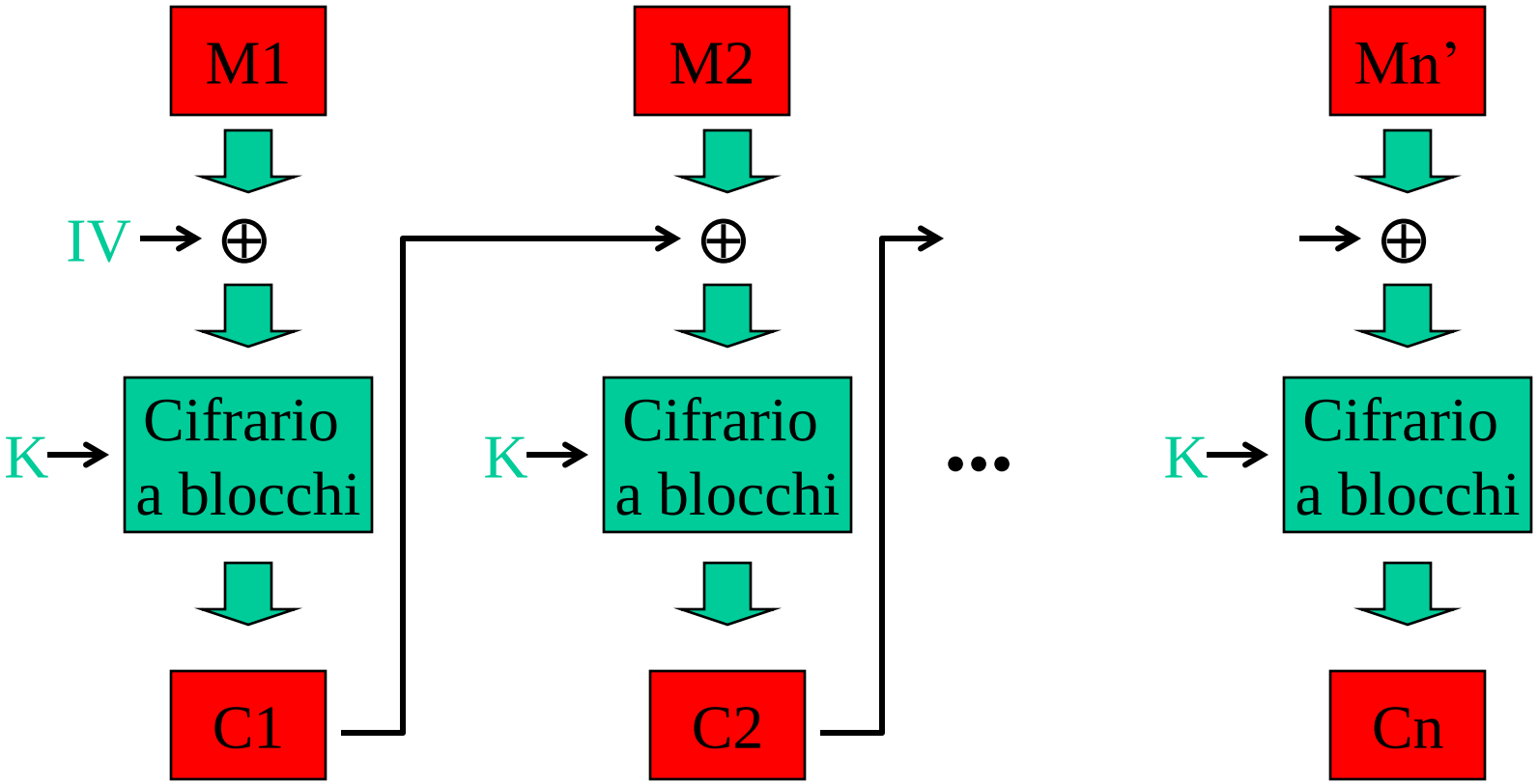
Problema di ECB

Un blocco ripetuto viene cifrato nello stesso modo, è quindi possibile una analisi statistica - in generale è possibile ottenere informazioni sul testo originario.

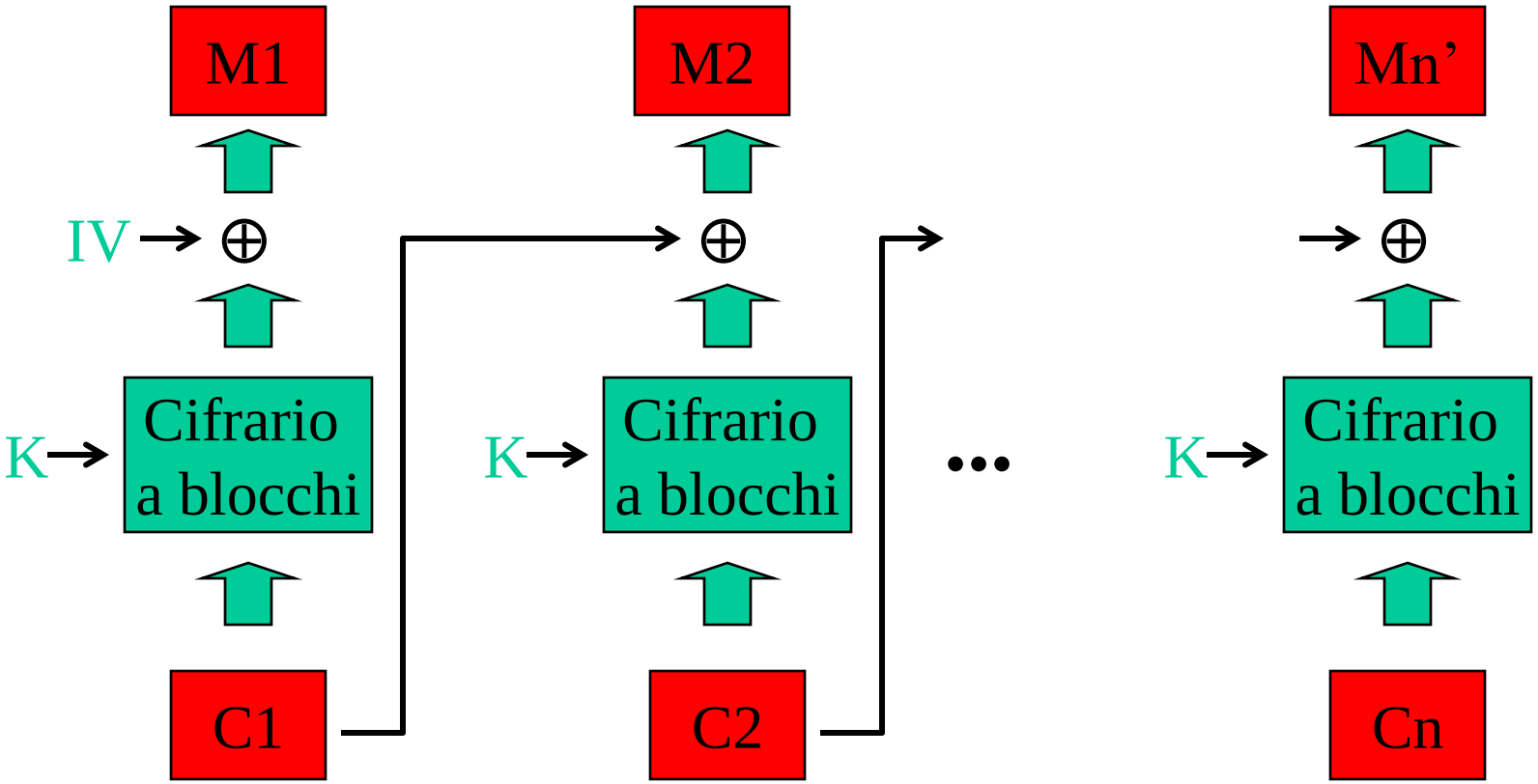
Non soddisfa il modello più restrittivo di sicurezza di un meccanismo di cifratura, può fornire un livello di sicurezza adeguato per messaggi corti.

Esercizio: inserire padding rimuovibile

Cipher Block Chaining (CBC)



Come decifrare con CBC



Cipher Block Chaining

E’ la modalità di cifratura (mode) più usata per un cifrario a blocchi. Non presenta i problemi di ECB, ed è altrettanto efficiente.

IV rappresenta un vettore di inizializzazione (Initialization Vector) lungo quanto un blocco.

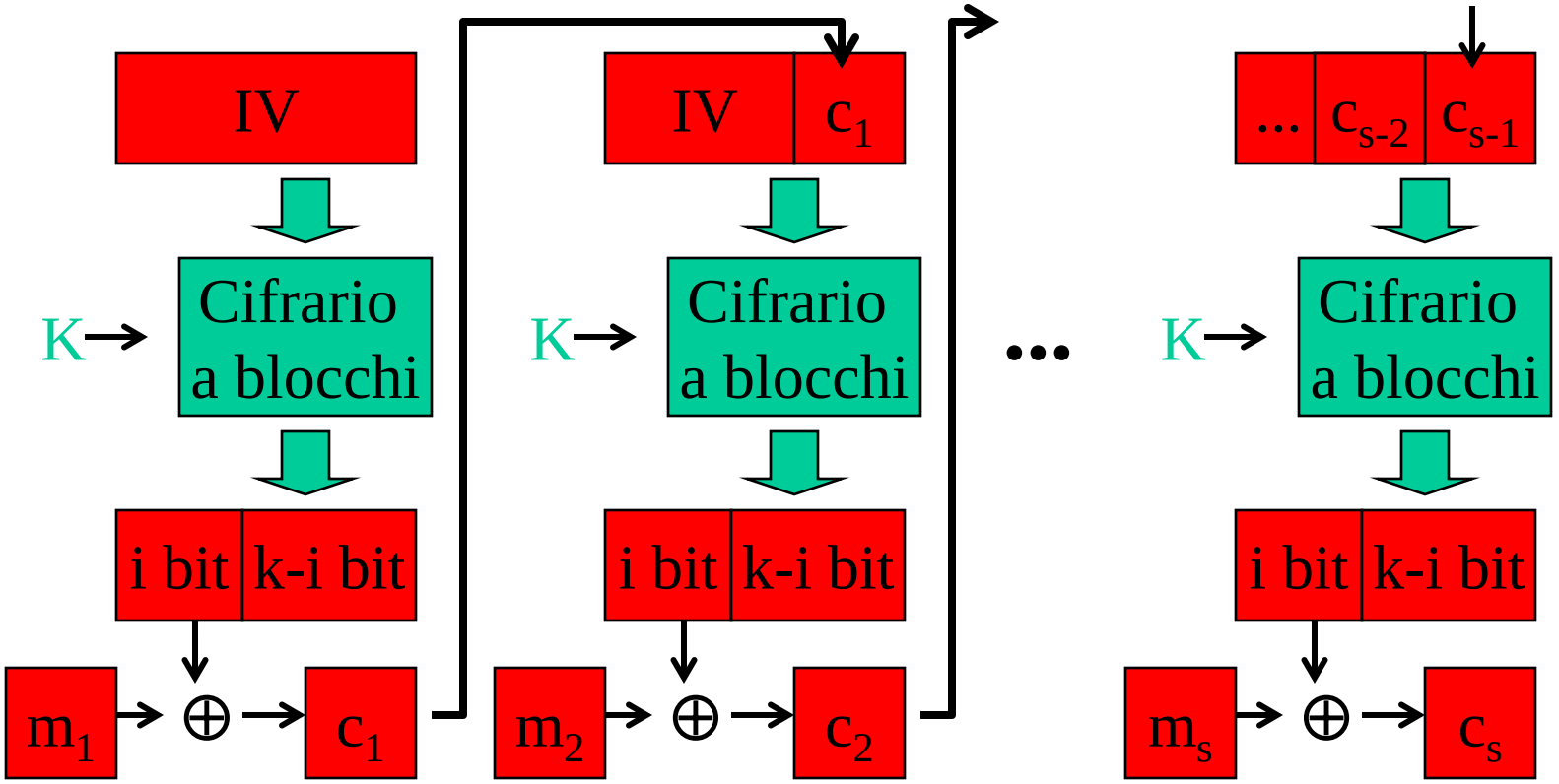
Ampiamente usato con DES (es. 3DES-EDE-CBC)

Problema di CBC

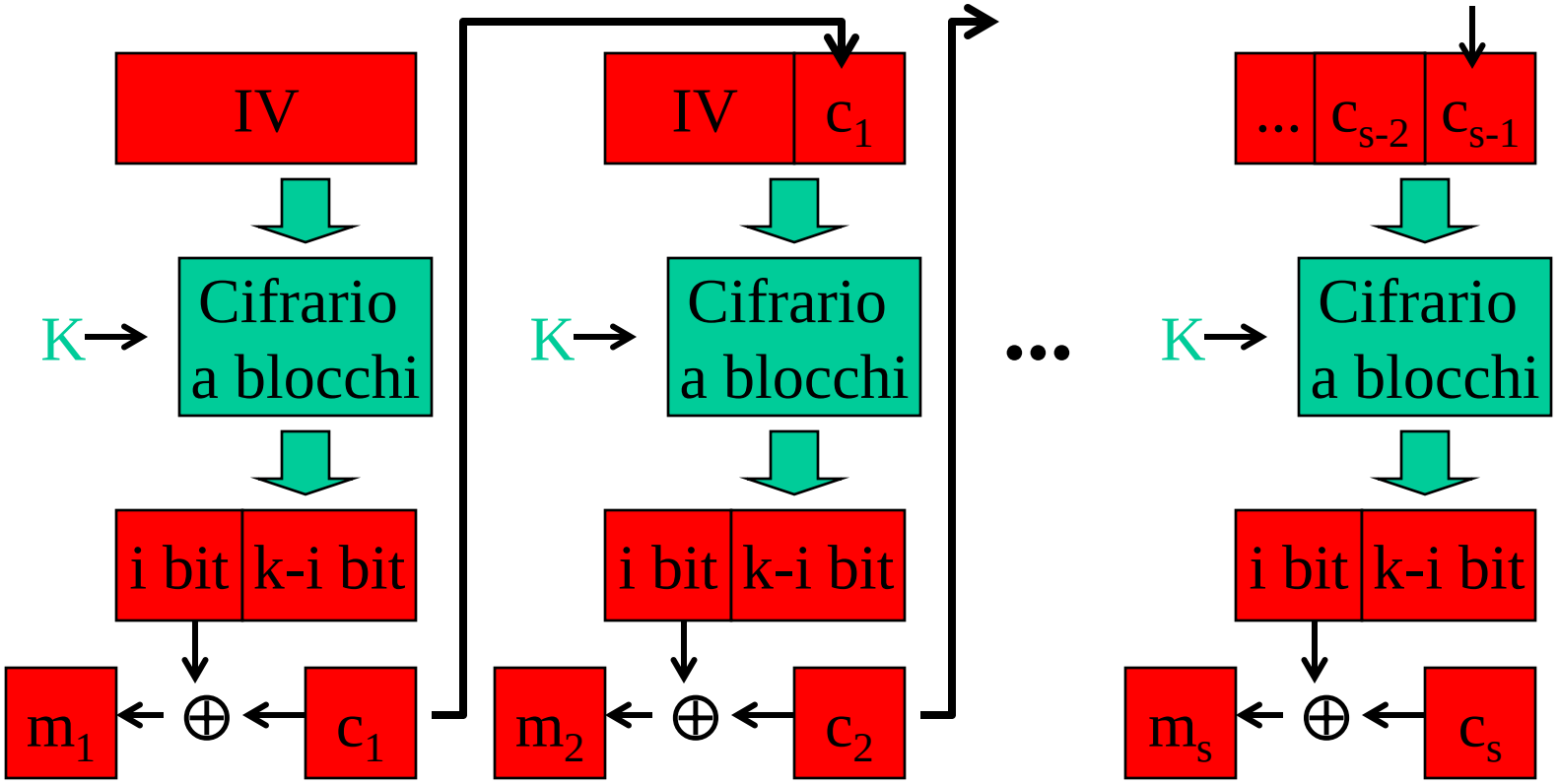
Un errore di trasmissione di un solo bit rende impossibile decifrare il corrispondente blocco e il blocco immediatamente successivo.

Inoltre prima di poter applicare il sistema di encryption a blocchi, devo avere a disposizione il testo in chiaro (possibile problema di efficienza).

Cipher Feedback (CFB)



Come decifrare con CFB



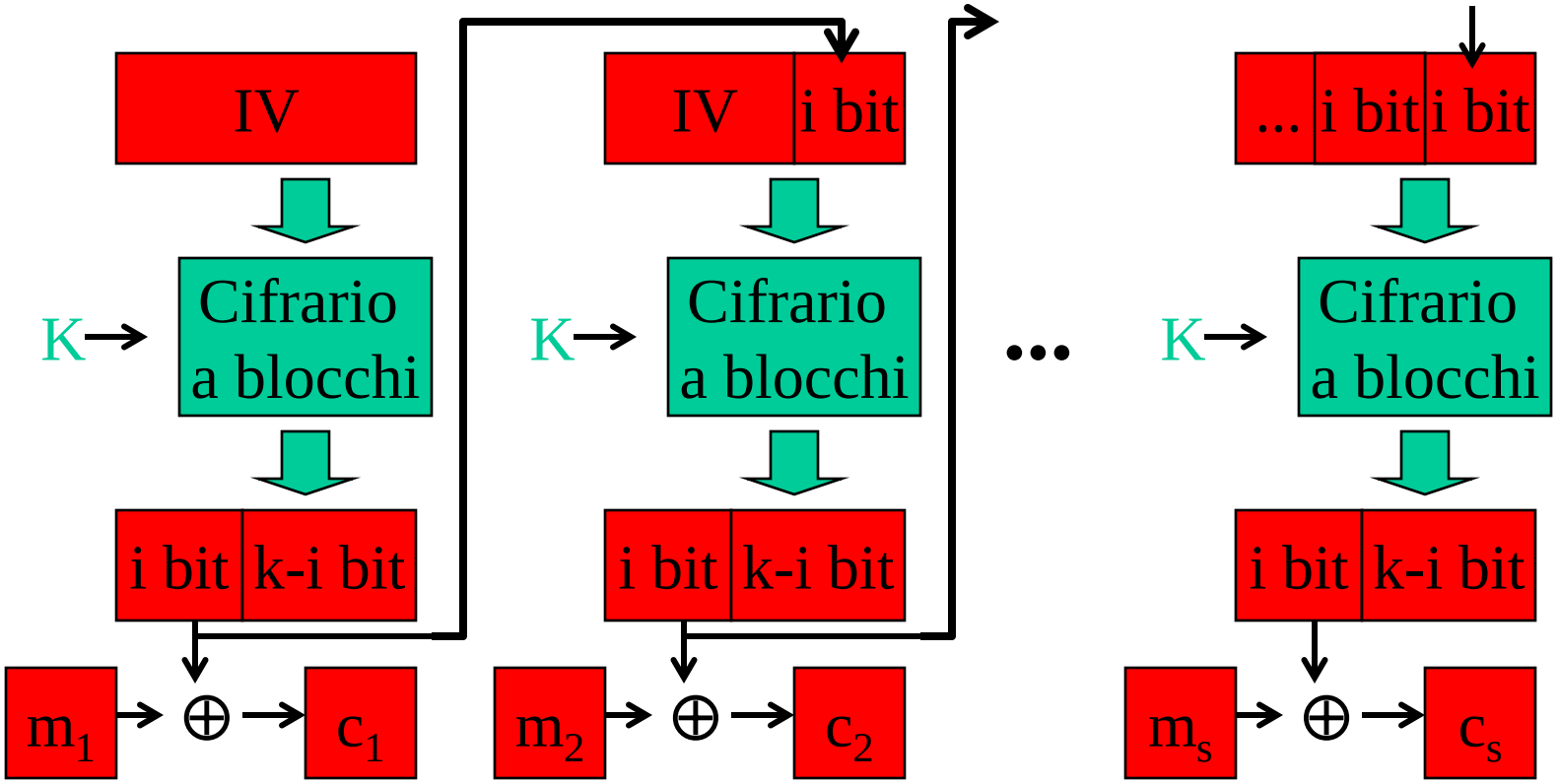
Modalità Cipher Feedback (CFB)

Traforma il cifrario a blocchi (block cipher) in cifrario a flusso (stream cipher).

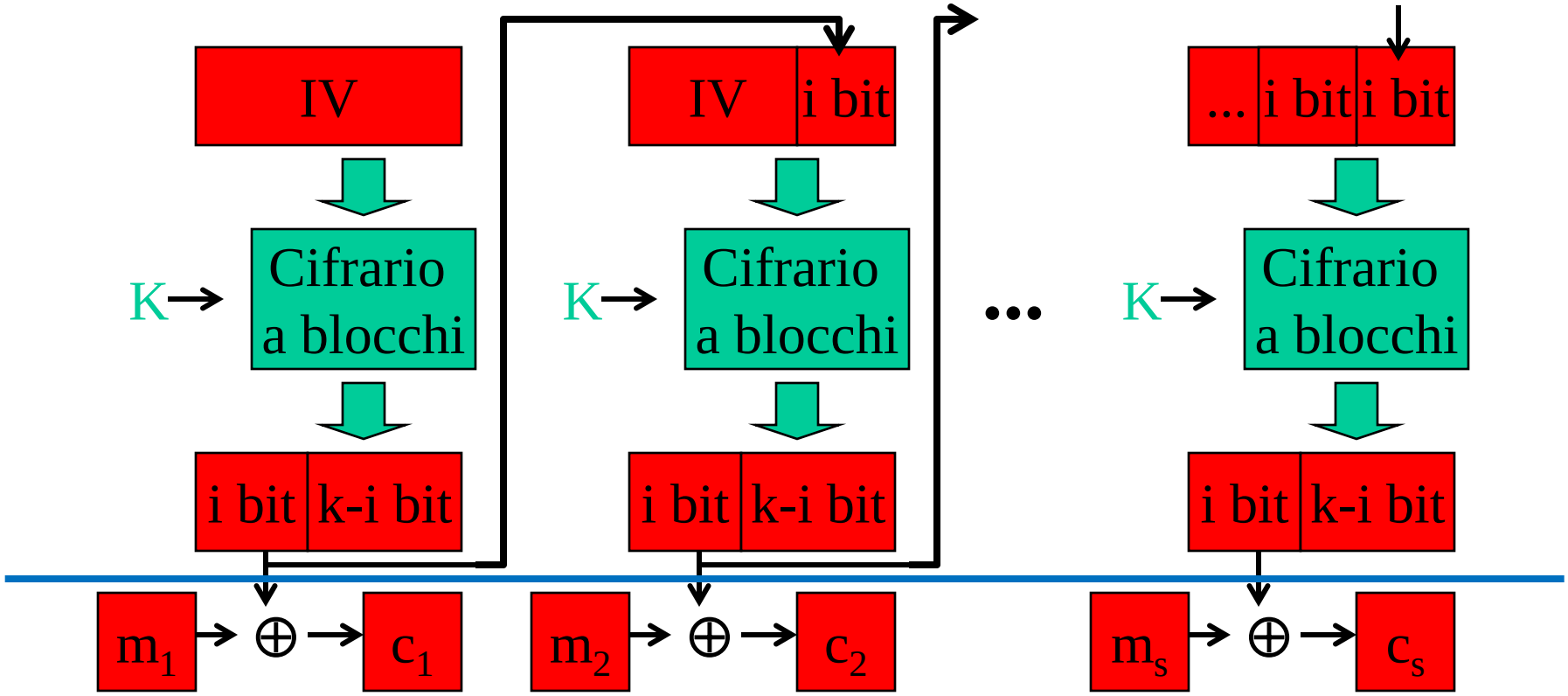
E’ meno efficiente di CBC.

Un errore di trasmissione di un bit nel testo cifrato si propaga per diversi blocchi, nel senso che risulteranno indecifrabili il blocco successivo e alcuni blocchi che lo seguono.

Output Feedback (OFB)



Output Feedback (OFB)



Modalità Output Feedback (OFB)

Traforma il cifrario a blocchi (block cipher) in cifrario a flusso (stream cipher).

E’ meno efficiente di CBC.

Un errore di trasmissione di un bit rende indecifrabile il solo gruppo di i bit locale, il resto del testo può essere decifrato.