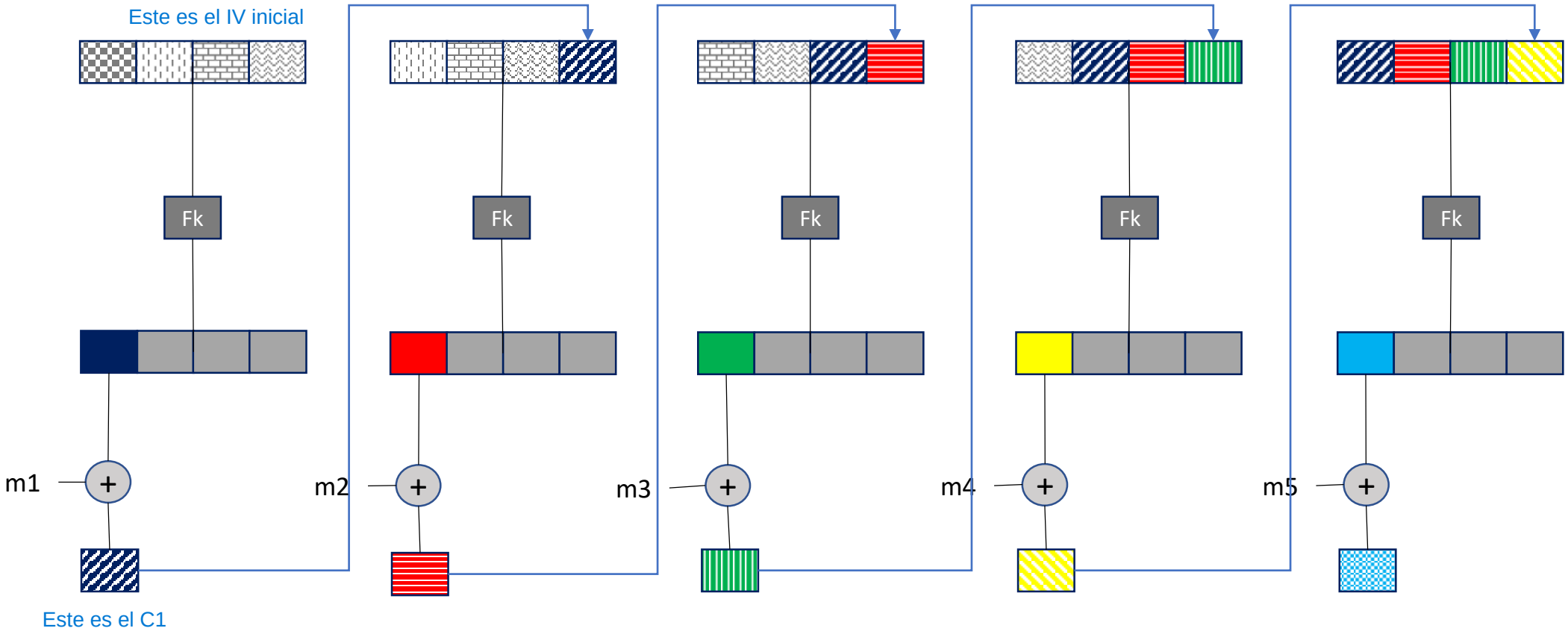
Cipher Feedback Mode

20 de marzo 2023

n: tamaño del IV, s: tamaño de bloque

Encripción

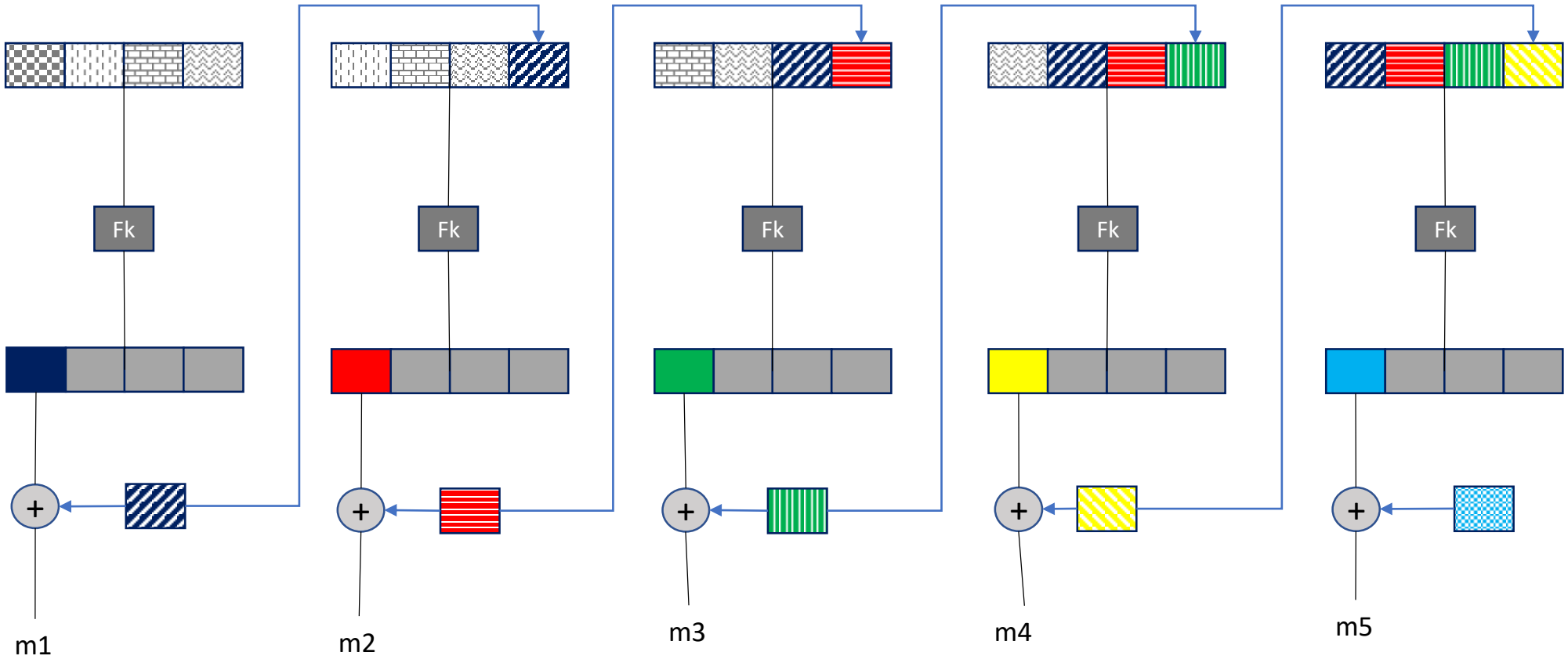
Ejemplo: n = 32; s=8



Desencripción correcta

(llegan ordenados y sin errores: c1, c2, c3, c4, c5, c6, c7, etc.)

Ejemplo: n = 32; s=8



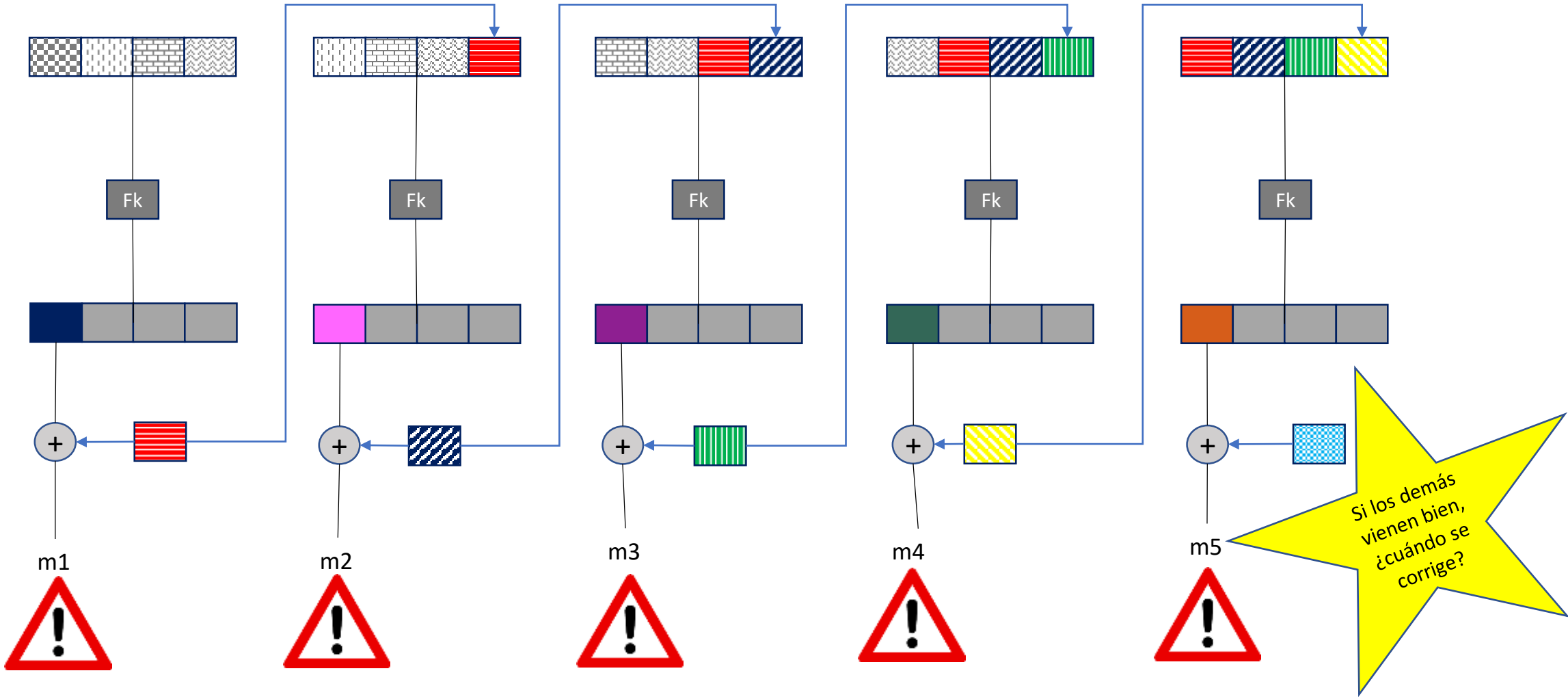
Desencripción incorrecta

(llegan mezclados: c2,c1,c3,c4,c5,c6,c7)

Ejemplo: n = 32; s=8

Primero llega c2, entonces no puedo obtener m1. Despues llega m1, y ya lo voy a descifrar mal. Voy a seguir descifrando mal los bloques hasta el sexto bloque (se tiene que vaciar todo el IV hasta que quede bien ordenado)

Aca yo tengo que tener primero el azul y despues el rojo, pero estan al reves. Voy a seguir descifrando mal los paquetes hasta que tanto el azul como el rojo se vayan del IV (en el 6to paquete).



Analizar: Desencripción incorrecta

(llega mal c1, o sea llega: c1*, c2,c3,c4,c5, ...)