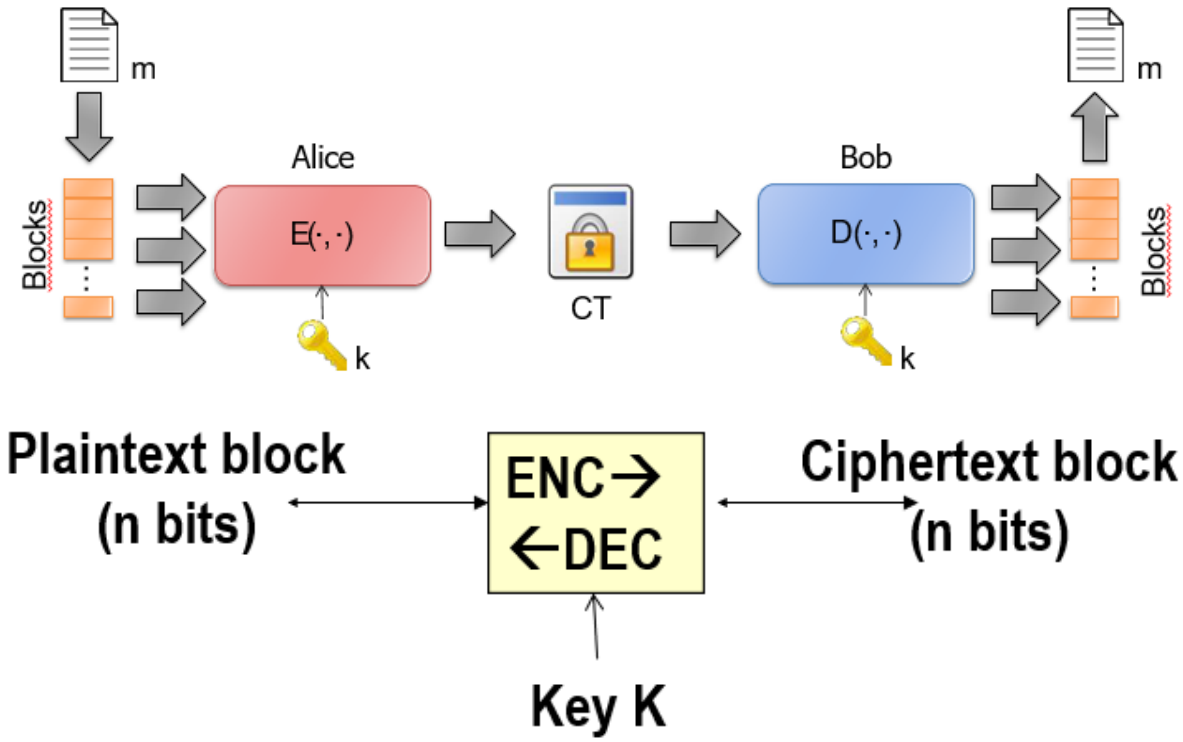
Revisione dei Cifrari a Blocchi e Modalità di Funzionamento

Introduzione ai Cifrari a Blocchi

L'obiettivo dei cifrari a blocchi è quello di "generalizzare" i cifrari a sostituzione su blocchi di testo in chiaro di lunghezza fissa n bit, producendo blocchi di testo cifrato della stessa dimensione n bit.

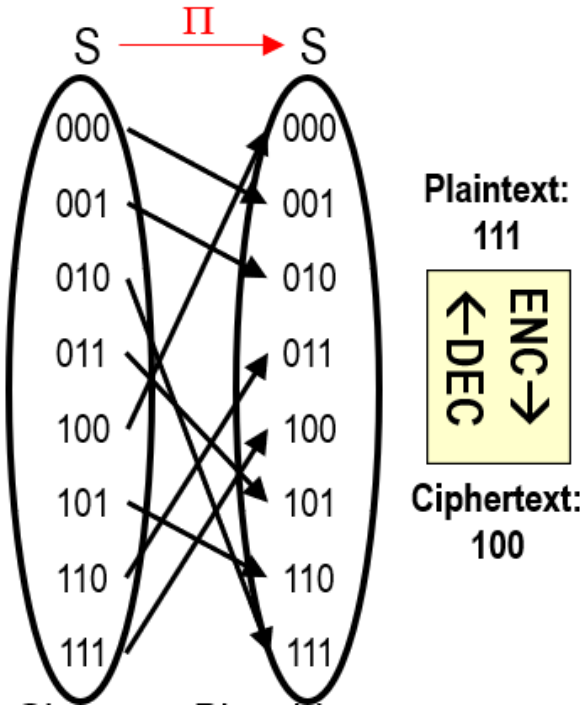


L'algoritmo a blocchi deve implementare una *Pseudo Random Permutation* (PRP), ovvero una permutazione pseudocasuale.

In pratica, la chiave permette di selezionare solo fra 2^{keysize} permutazioni.

Pseudo Random Permutation (PRP)

Sia S l'insieme di tutti i possibili testi in chiaro di n bit, con $|S| = 2^n$. La permutazione $P : S \to S$ deve essere una funzione biiettiva (1-a-1). Una mappatura non reversibile non è valida.



Un cifrario a blocchi PRP dovrebbe selezionare uniformemente una delle possibili permutazioni dell'insieme, selezionata dalla chiave segreta K.

Problema della quantità di permutazioni: La quantità di permutazioni possibili per n bit è $(2^n)!$. Per esempio:

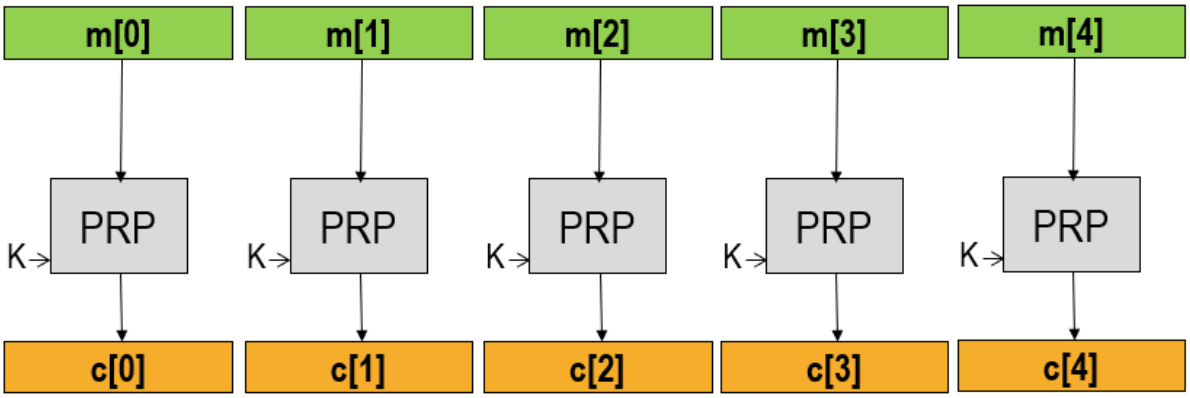
- $n = 3$: $8! = 40320$
- $n = 8$: $256! \approx 8.58 \times 10^{506}$ (un numero estremamente grande)

Nel caso di AES con $n = 128$, il numero di permutazioni teoriche è $2^{128}! \approx 2^{2135}$, un numero incredibilmente grande.

Le chiavi AES possono essere di 128, 192 o 256 bit, dunque il numero reale di permutazioni AES è molto minore rispetto a quello ideale, ma comunque accettabile per la sicurezza pratica.

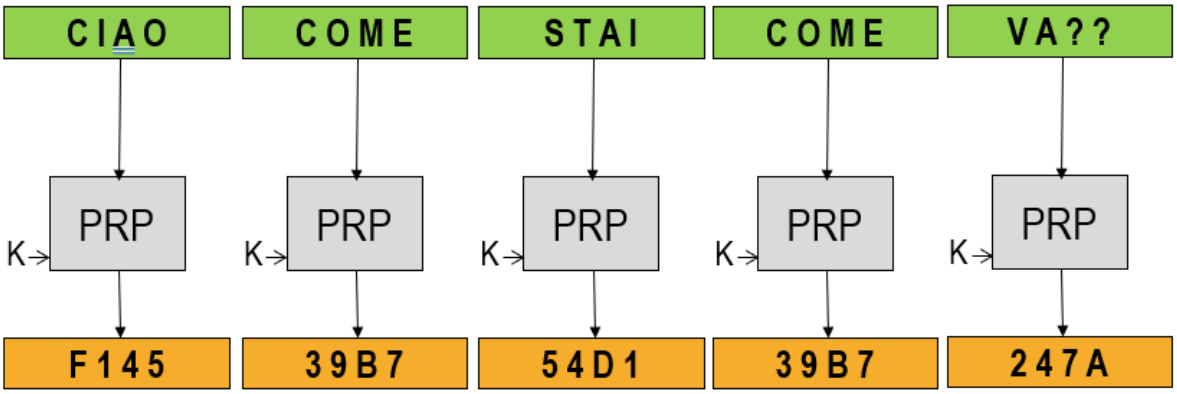
Modalità di Funzionamento dei Cifrari a Blocchi

Quando il messaggio in chiaro è più lungo della dimensione di blocco, il testo viene suddiviso in blocchi di n bit e ciascun blocco è cifrato indipendentemente, modalità nota come *Electronic Code Book* (ECB).



Tuttavia, ECB presenta gravi problemi:

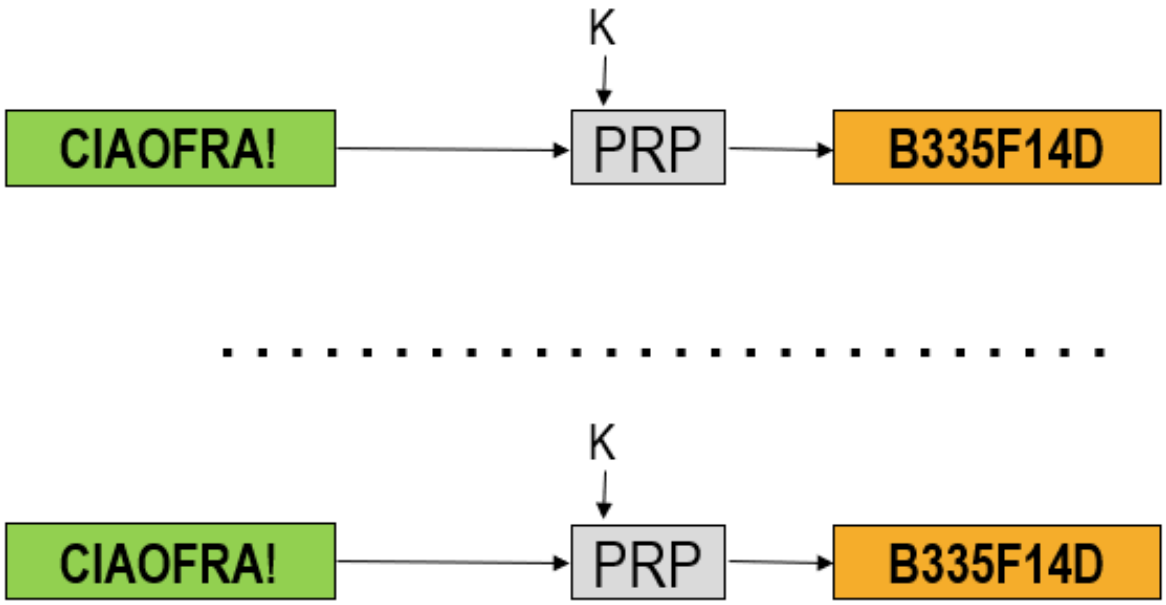
- Blocchi di testo uguali producono blocchi cifrati uguali.
- Non garantisce sicurezza semantica.
- Facilmente vulnerabile al criptoanalisi triviale.



Ricorda: mai utilizzare la modalità ECB in applicazioni reali!

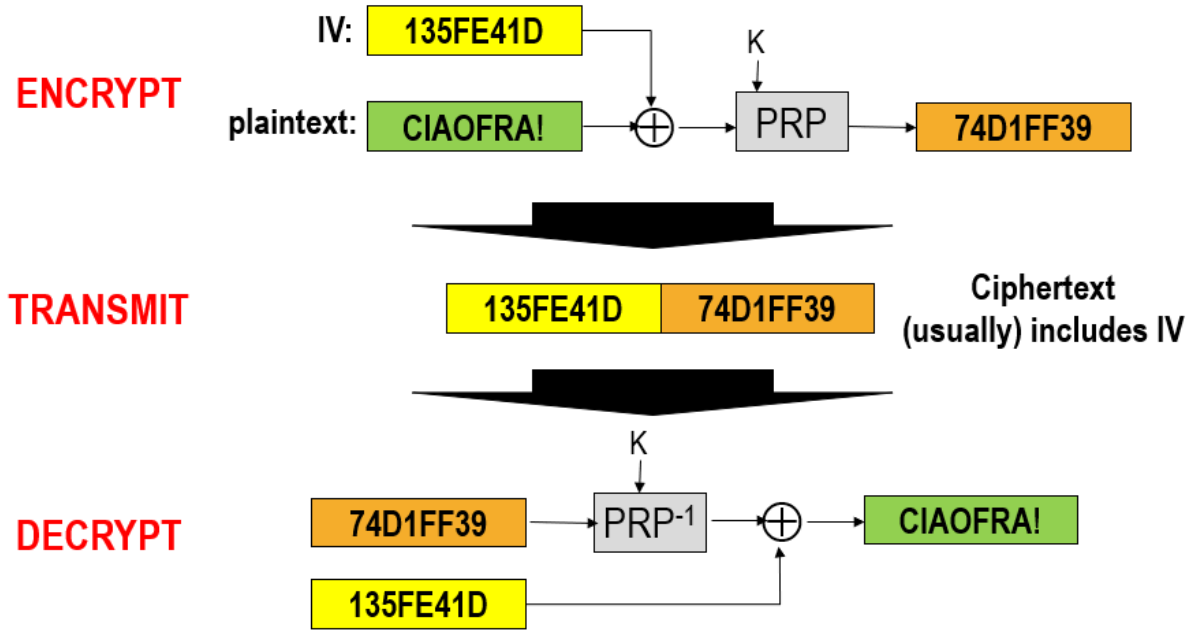
Problemi di Riutilizzo e Vettori di Inizializzazione (IV)

Se si cifra due volte lo stesso messaggio con la stessa chiave, si ottiene lo stesso testo cifrato, analogamente ai cifrari a flusso.



Per ovviare, si utilizza un vettore di inizializzazione (IV) fresco e casuale per ogni cifratura. L'IV deve essere anche imprevedibile per garantire la sicurezza.

Il testo cifrato di solito include l'IV. L'IV non deve mai ripetersi e deve essere scelto in modo imprevedibile.



Modalità di Cifratura Sicure e Usuali

Le modalità di cifratura a blocchi più usate sono:

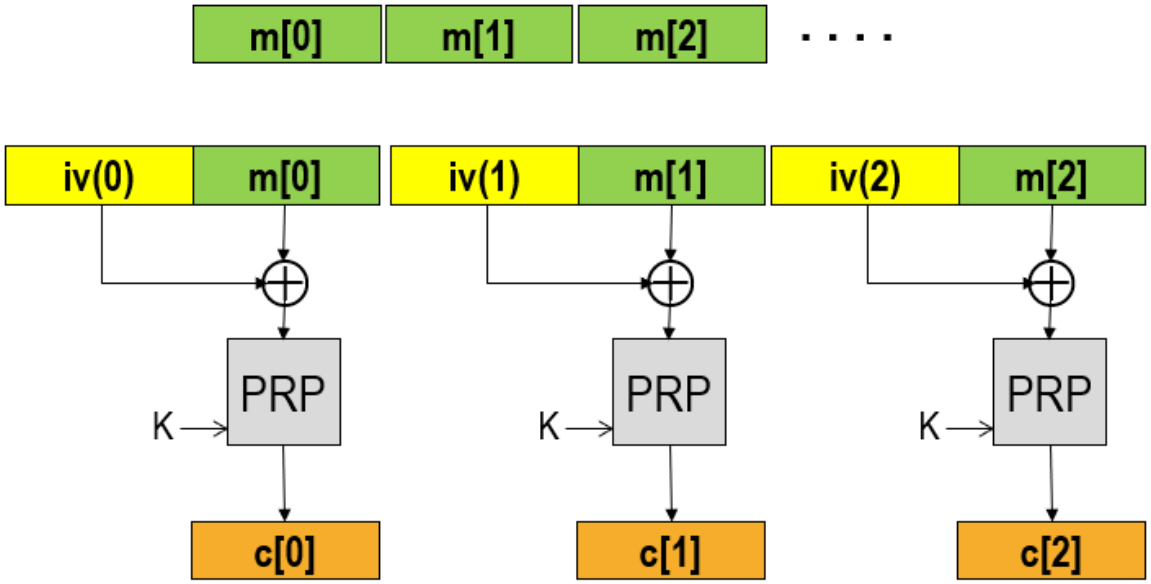
- Cipher Block Chaining (CBC)
- Counter Mode (CTR)
- Cipher Feedback Mode (CFB)

- Output Feedback Mode (OFB)
- Galois Counter Mode (GCM) per cifratura autenticata

NIST ha raccomandato queste modalità nel documento del 2001, anche se alcune (come CBC) sono più usate di altre.

Sicurezza Semantica

La sicurezza semantica (IND-CPA) si ottiene se tutti gli IV sono casuali e indipendenti, anche se questo comporta un overhead di dimensione (circa il doppio per l'IV).

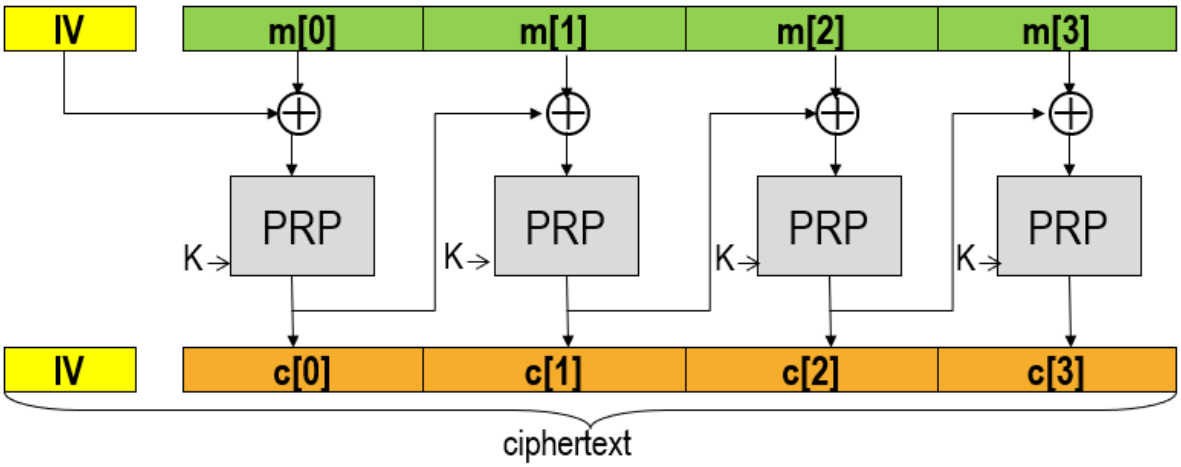


Cipher Block Chaining (CBC)

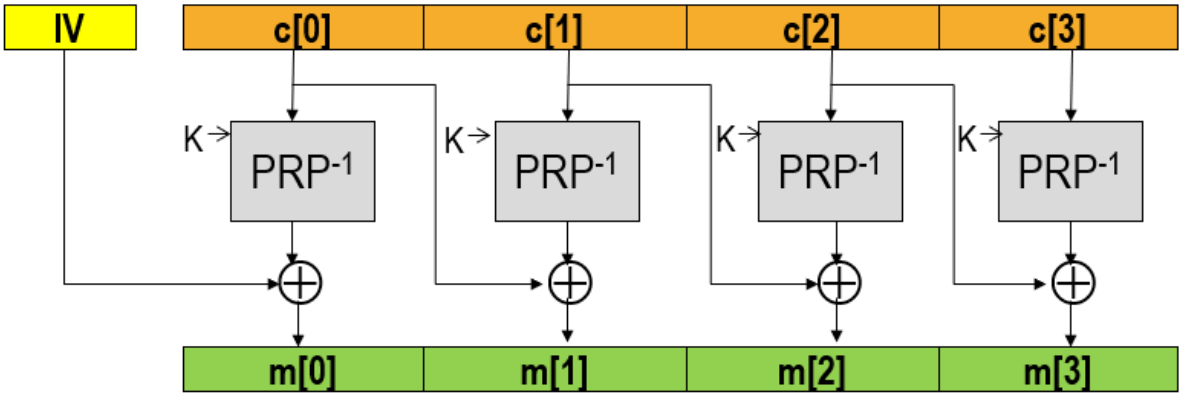
CBC sfrutta la proprietà che il blocco cifrato precedente viene usato come IV per il blocco successivo:

$$c_0 = \mathrm{ENC}_K(IV \oplus m_0)$$
$$c_i = \mathrm{ENC}_K(c_{i-1} \oplus m_i)$$

Il testo cifrato ha un overhead minimo dovuto solo all'IV iniziale.



La decrittazione in CBC è parallellizzabile, mentre la cifratura deve essere sequenziale, limitando le prestazioni hardware.



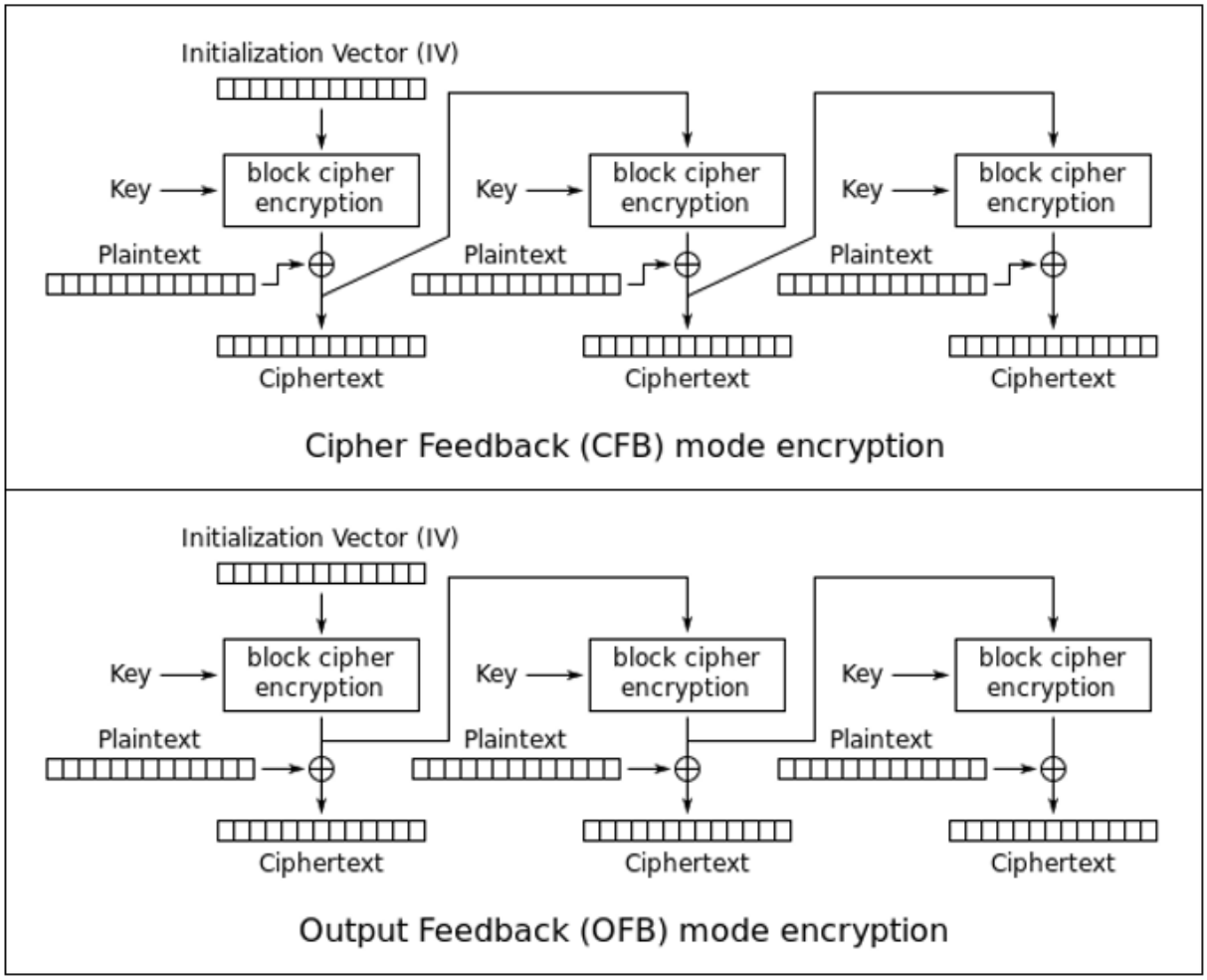
Importante: CBC è sicuro solo se l'IV è casuale e non prevedibile. IV prevedibili possono portare a attacchi CPA, come il BEAST exploit su TLS 2011.

Padding

Poiché il testo deve essere multiplo della dimensione del blocco, si usa il padding (ad esempio PKCS7) per riempire gli spazi.

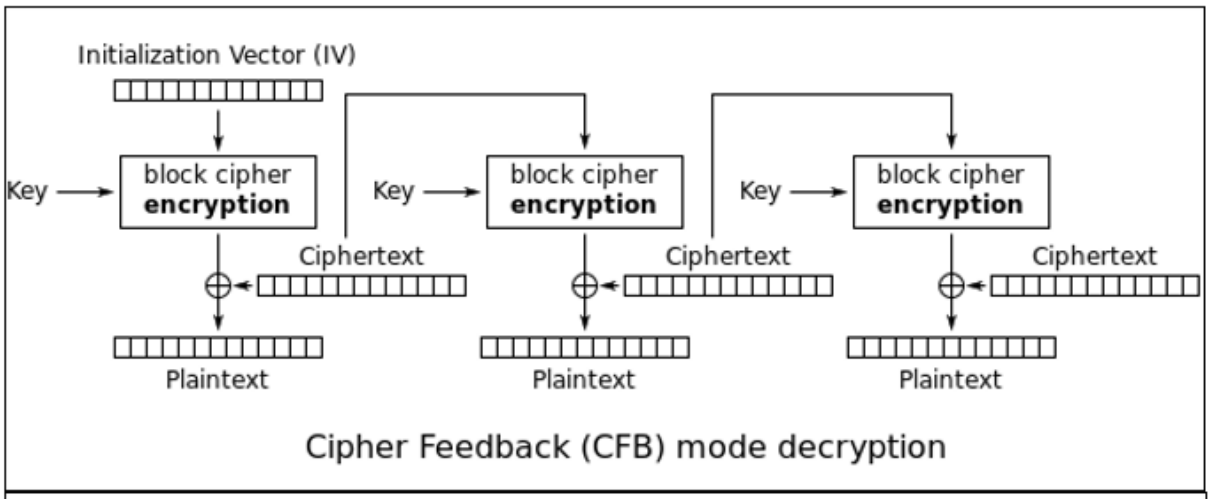
Modalità CFB e OFB

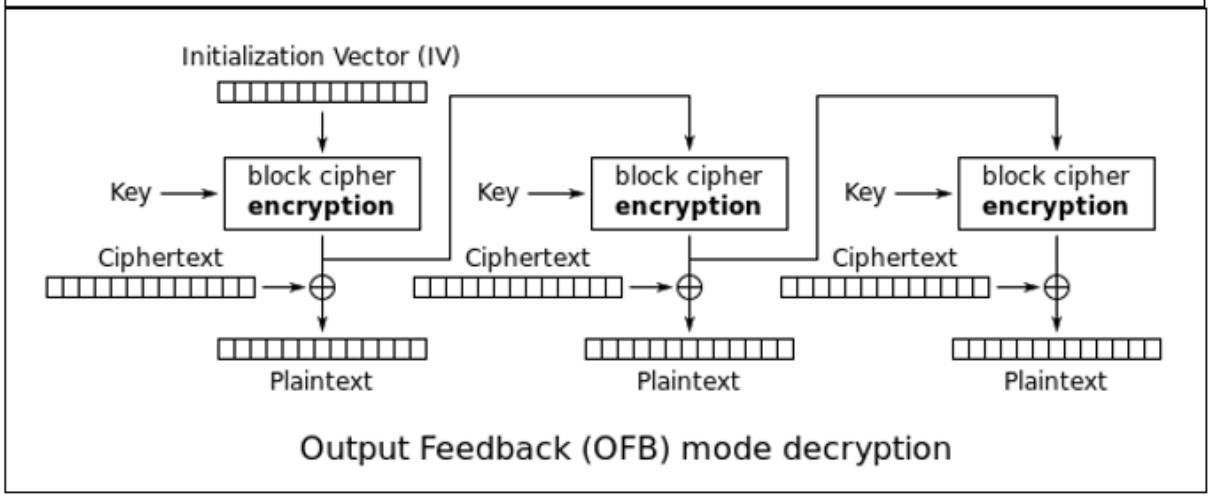
CFB e OFB utilizzano il cifrario a blocchi come cifrario a flusso, cifrando mediante XOR del plaintext con un flusso generato.



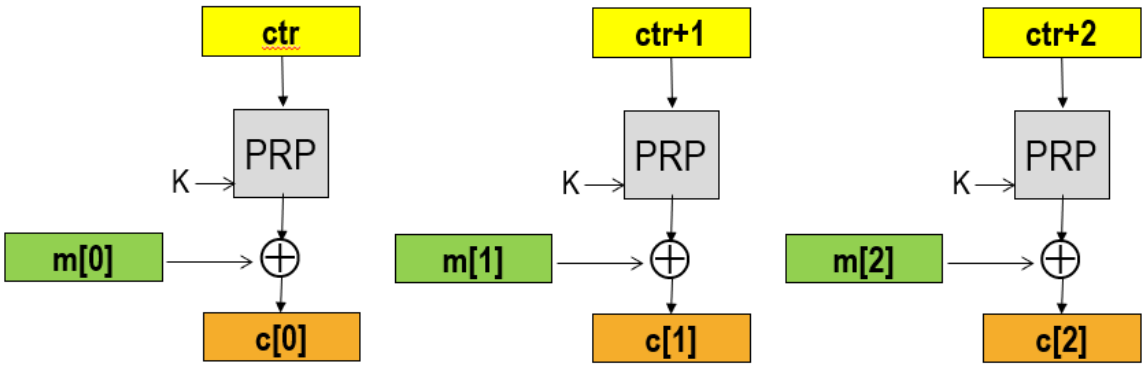
Queste modalità non richiedono padding e OFB permette il preprocessing per migliorare le prestazioni.

La decrittazione in CFB è parallellizzabile, mentre OFB è seriale.





Counter Mode (CTR)



CTR è particolarmente semplice ed efficiente:

- Si inizializza un contatore che viene incrementato ad ogni blocco.
- Si cifra il contatore e si effettua l'XOR con il blocco di testo in chiaro.

È possibile precomputare la cifratura del contatore indipendentemente dal testo. CTR combina i vantaggi di CFB e OFB, consentendo:

- Crittografia e decrittografia parallele.

- Accesso casuale ai blocchi.
- Nessun problema di cicli brevi se il contatore è usato correttamente.
- Richiede solo la cifratura, non la decifratura inversa.

Con un'appropriata gestione del contatore, CTR assicura sicurezza e alta efficienza.