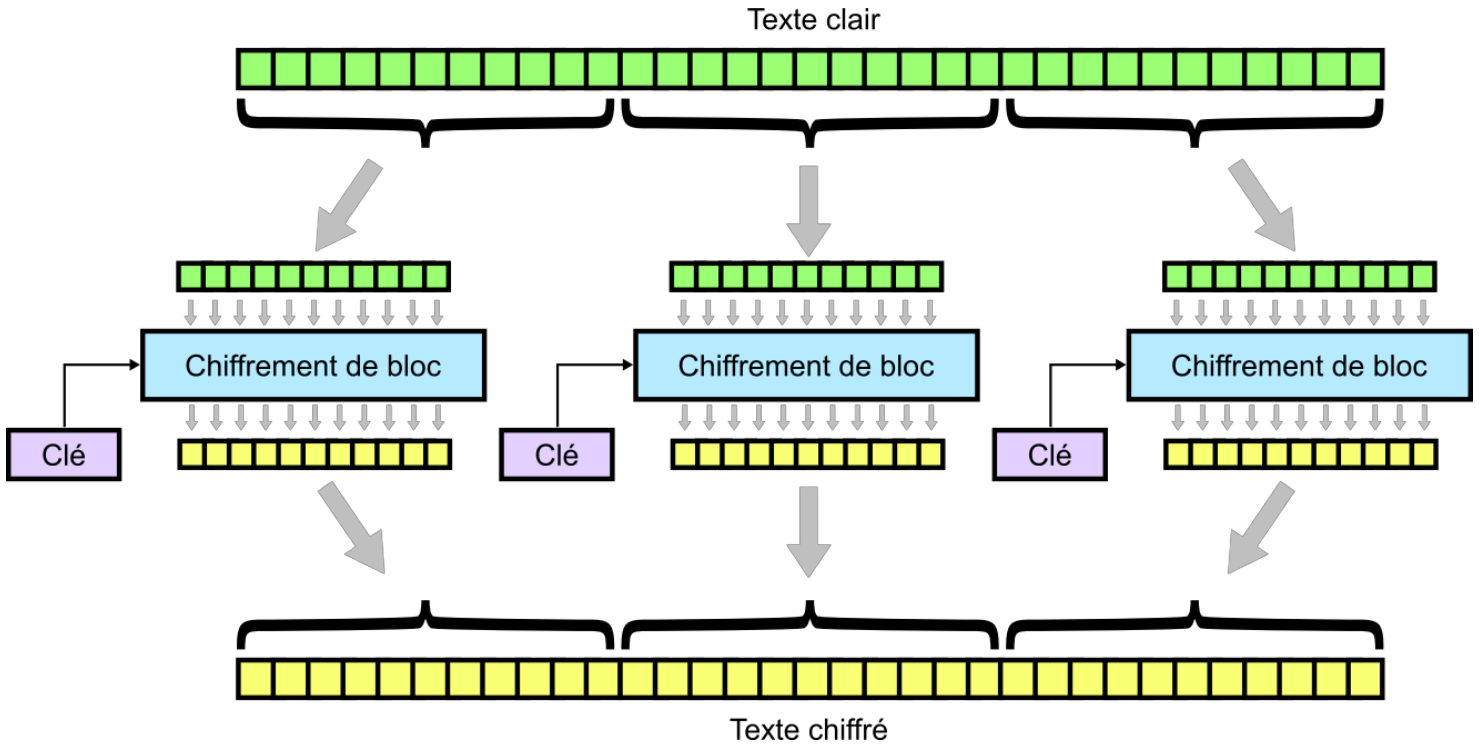
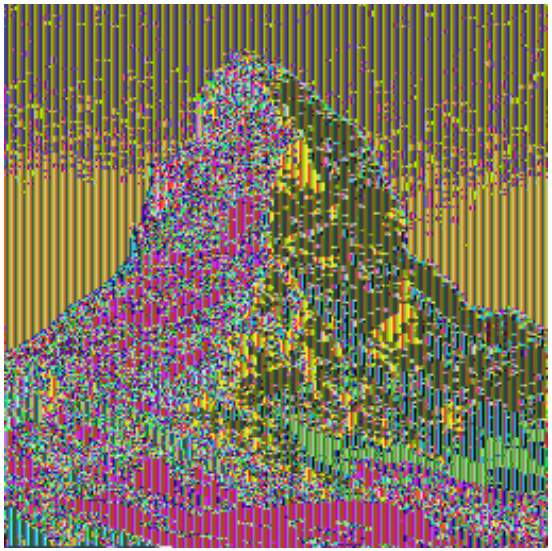
Modes opératoires des chiffrements par blocs

Mode ECB (Electronic Code Book)



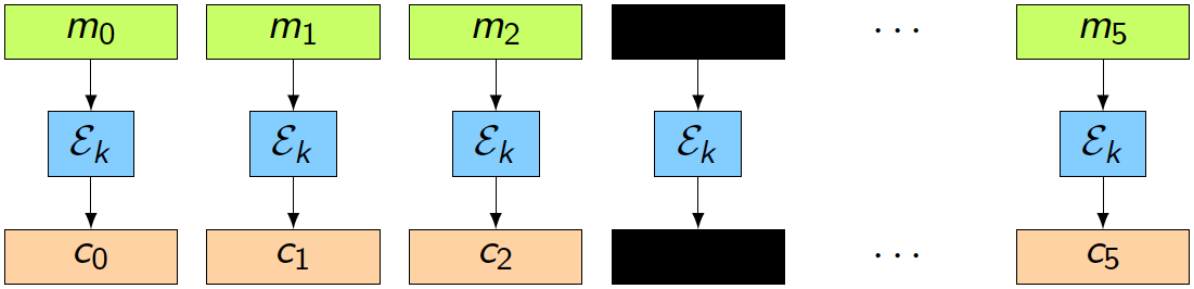
Mode ECB

- Inconvénients

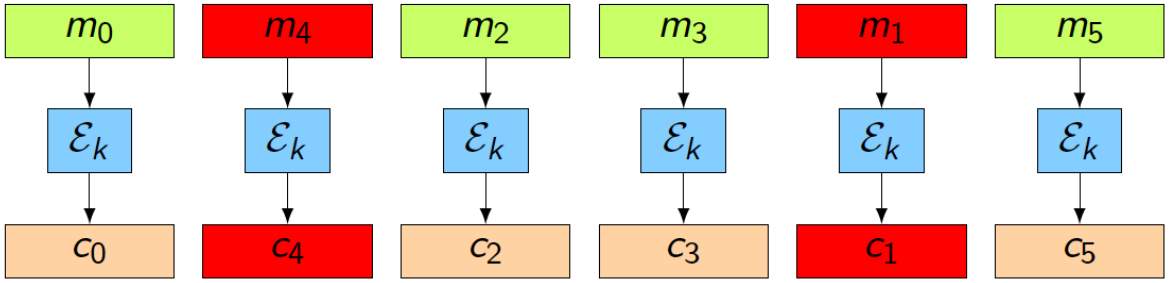


Mode ECB

- Inconvénients
  - Suppression d'un bloc

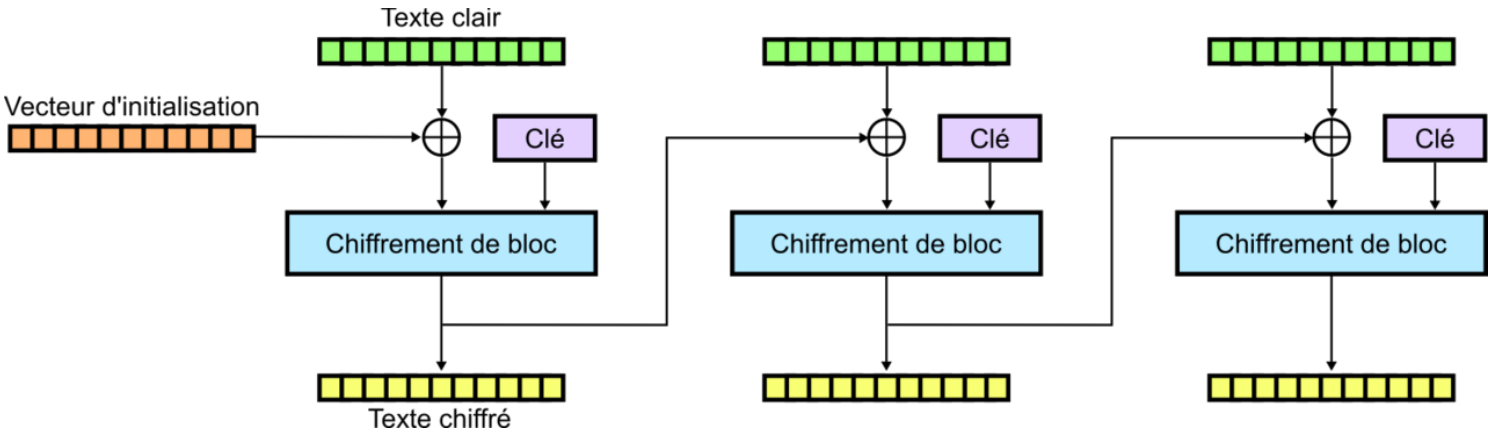


  - Echange de 2 blocs



- Mode à proscrire

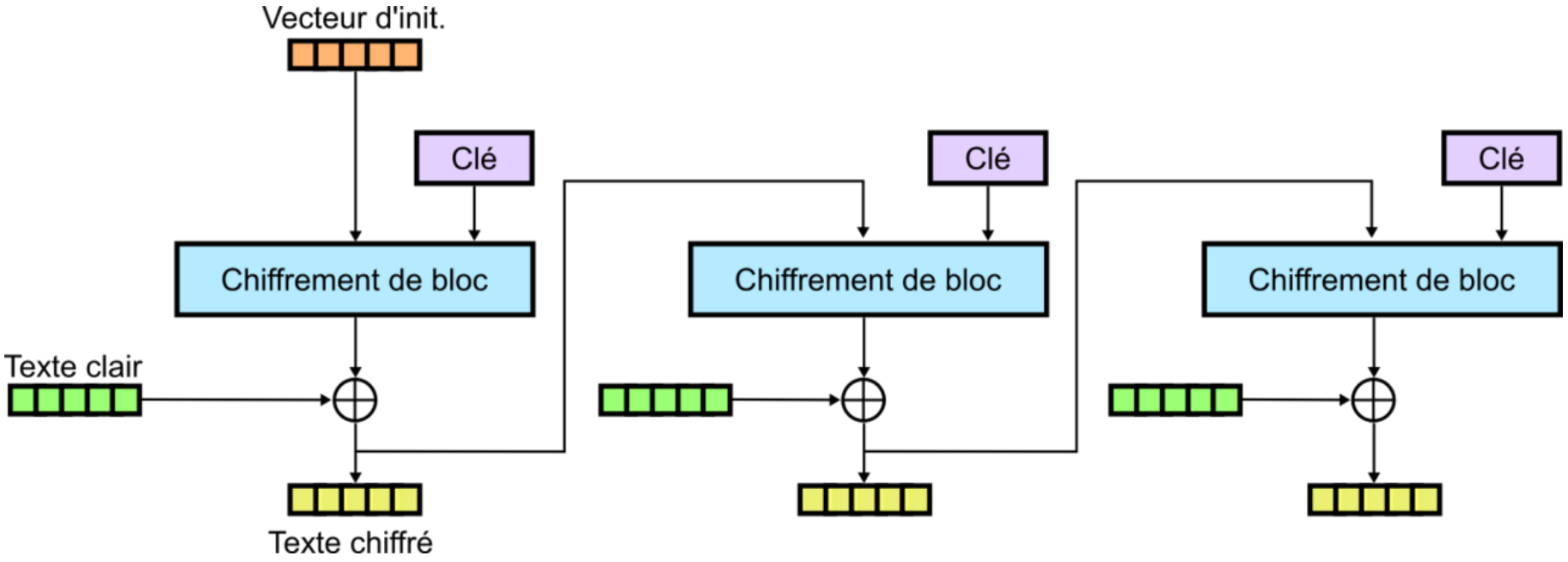
Mode CBC (Cipher Block Chaining)



- Un bloc dépend de tous les précédents
- Randomisé par le vecteur d'initialisation
- Inconvénient : chiffrement séquentiel (non parallélisable)

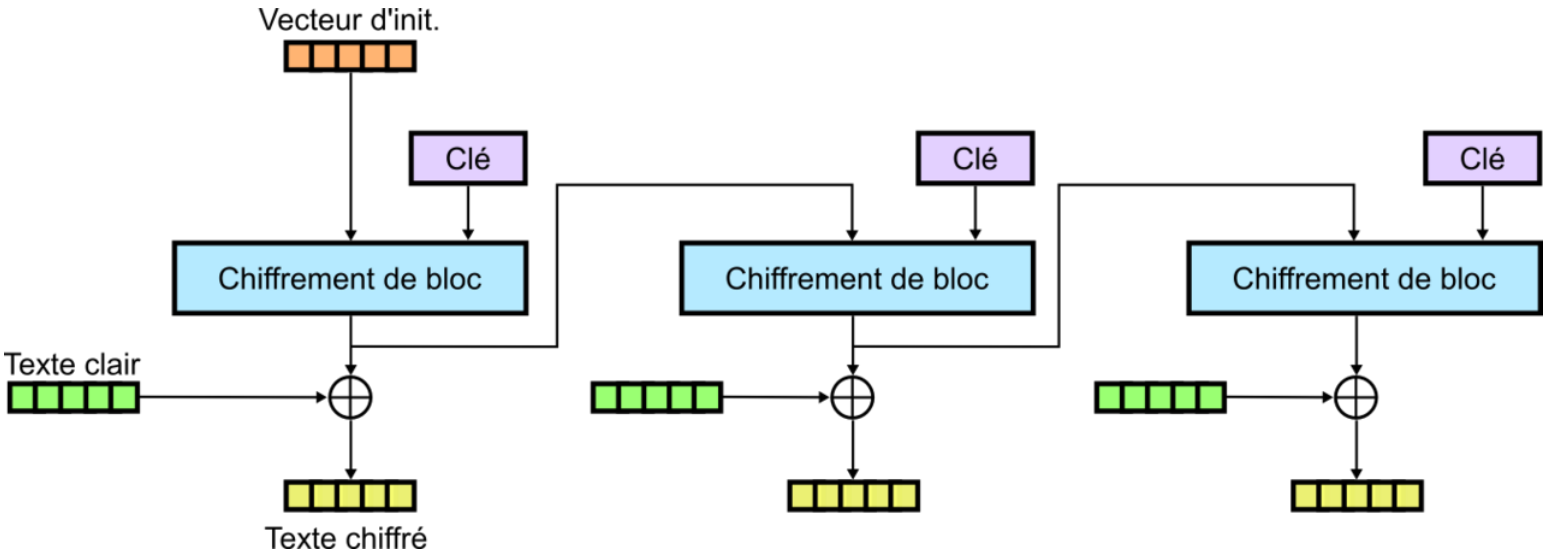
Mode CFB (Cipher Feedback)

- CFB est un chiffrement par flot (on génère un flux de clefs)
- Intérêt : il ne nécessite que la fonction de chiffrement. Le déchiffrement se fait avec la même fonction (exemple: AES).



Mode OFB (Output Feedback)

- Chiffrement de flot : mêmes avantages que CFB. De plus, il est possible de le précalculer les clefs. Il n'est donc sûr que si la fonction de chiffrement alliée à la clé forment une bonne suite pseudo-aléatoire.



- Pas de propagation d'erreurs

Mode CTR (Counter)

- Dans ce mode, le flux de clé est obtenu en chiffrant les valeurs successives d'un compteur.
- Nombreux avantages :
  - chiffrement par flot
  - précalculable
  - accès aléatoire aux données
  - parallélisable