

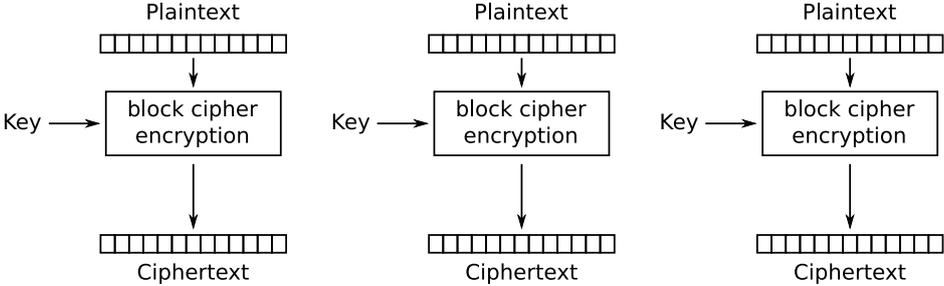
**info528 : Mathématiques pour l'informatique**  
**TD 5 : modes pour la cryptographie par bloc**

Pierre Hyvernât  
 Laboratoire de mathématiques de l'université de Savoie  
 bâtiment Chablais, bureau 22, poste : 94 22  
 email : Pierre.Hyvernât@univ-savoie.fr  
 www : <http://www.lama.univ-savoie.fr/~hyvernât/>

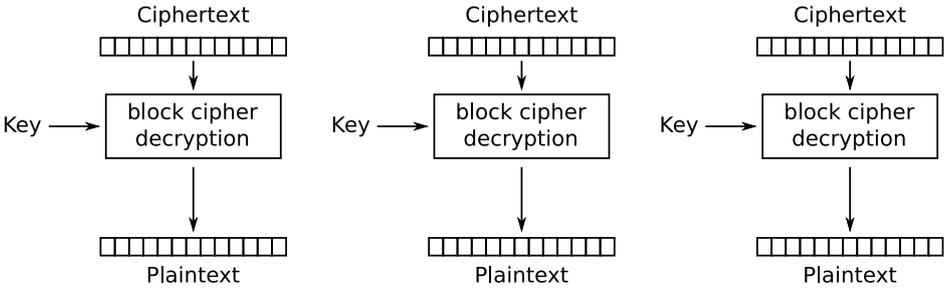
Dans tous ce qui suit, on suppose que l'on utilise un algorithme de cryptage symétrique (AES, DES, etc.) La clé secrète est nécessaire pour le cryptage et le décryptage.

**Partie 1 : Mode ECB**

Le mode "ECB" (Electronic CodeBook) fonctionne en codant chaque bloc de manière indépendante. On peut représenter ce mode de fonctionnement par le schéma suivant (Wikipédia) :



Le décryptage est fait de la même manière :



Formellement, si on note  $K$  pour la fonction de cryptage et  $K^{-1}$  pour la fonction de décryptage, on a

- $C_i = K(B_i)$ ,
- $D_i = K^{-1}(C_i)$ ,

où  $B_i$  représente le  $i$ -ème bloc clair,  $C_i$  le  $i$ -ème bloc crypté, et  $D_i$  le  $i$ -ème bloc décrypté. Les schémas montrent clairement que le cryptage et le décryptage peuvent se faire en parallèle.

**Partie 2 : Mode CBC**

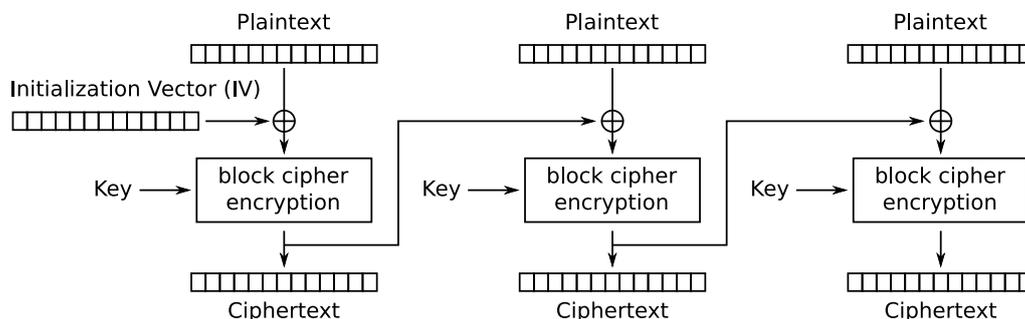
Le mode "CBC" (Cipher Block Chaining) est donné par :

- $C_0 = IV$ ,
- $C_i = K(B_i \oplus C_{i-1})$ ,
- $D_i = K^{-1}(C_i) \oplus C_{i-1}$ ,

où  $IV$  est un bloc aléatoire qui doit être changé à chaque communication.

Question 1. Vérifiez que le décryptage fonctionne, c'est à dire que  $D_i = B_i$ .

Question 2. Le schéma du cryptage est donné par



Donnez le schéma correspondant pour le décryptage.

Question 3. Est-ce que le cryptage peut être fait en parallèle ?

Est-ce que le décryptage peut être fait en parallèle ?

Est-il possible de crypter un bloc partiel ? (Il faut pouvoir crypter la suite du bloc lorsqu'elle est connue.)

Question 4. Que se passe-t'il si un attaquant modifie un bit dans un bloc crypté  $C_k$  ?

### Partie 3 : mode CTR

Le mode "CTR" (CouTeR) marche de la manière suivante :

$$- C_i = K(IV \cdot i) \oplus B_i,$$

où  $IV$  est un "morceau" de bloc aléatoire qui doit changer à chaque communication, et  $\cdot$  représente la concaténation. " $IV \cdot i$ " est donc un bloc qui se décompose en deux parties :  $IV$  suivi de la valeur d'un compteur.

Question 1. Pourquoi est-il important que  $IV$  soit différent à chaque communication ?

Question 2. Est-ce que cela pose problème si l'attaquant connaît  $IV$  à l'avance ?

Question 3. Donnez la formule qui permet de calculer  $D_i$  à partir de  $C_i$ .

À quoi sert l'algorithme de décryptage  $K^{-1}$  ?

Question 4. Dessinez les schémas de cryptage / décryptage correspondants.

Est-ce que le cryptage peut être fait en parallèle ?

Est-ce que le décryptage peut être fait en parallèle ?

Est-il possible de crypter un bloc partiel ? (Il faut pouvoir crypter la suite du bloc lorsqu'elle est connue.)