info607 : Mathématiques pour l'informatique
TD 4 : modes pour le chiffrement par bloc

Pierre Hyvernat

François Boussion

Laboratoire de mathématiques de l'université Savoie Mont Blanc

bâtiment Chablais, bureau 17, poste : 94 22

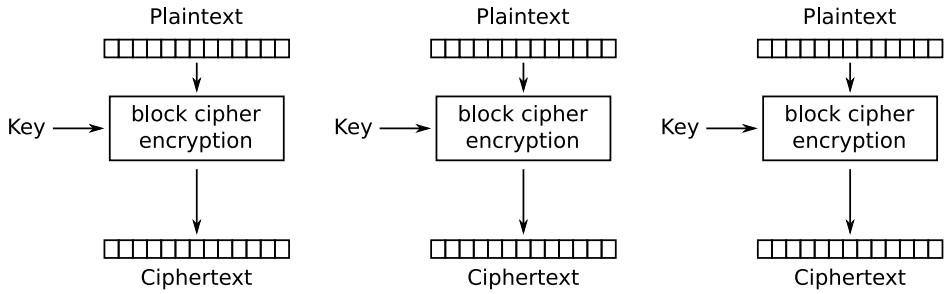
email : Pierre.Hyvernat@univ-smb.fr

www : http://www.lama.univ-smb.fr/~hyvernat/

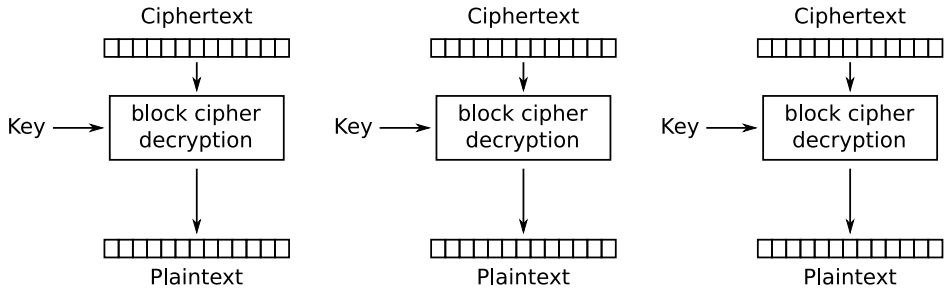
Dans tous ce qui suit, on suppose que l'on utilise un algorithme de chiffrement symétrique comme AES (blocs de 16 octets) ou DES (blocs de 8 octets). La clé secrète est nécessaire pour le chiffrement et le déchiffrement.

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 déchiffrement est fait de la même manière :



Formellement, si on note F_k pour la fonction de chiffrement (avec la clé k) et F_k^{-1} pour la fonction de déchiffrement (avec la clé k), on a

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

où B_i représente le i-ème bloc clair, C_i le i-ème bloc chiffré, et D_i le i-ème bloc déchiffré.

Les schémas montrent clairement que le chiffrement et le déchiffrement peuvent se faire en parallèle.

Question 1. Quel problème voyez vous avec ce mode de fonctionnement ?

Partie 2 : Mode CBC

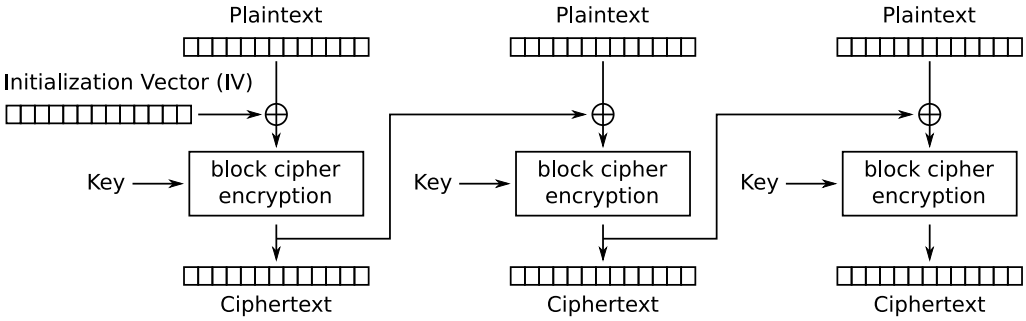
Le chiffrement du mode “CBC” (Cipher Block Chaining) est donné par
- $C_0 = IV$,
- $C_i = F_k(B_i \oplus C_{i-1})$,

et le déchiffrement par
- $D_i = F_k^{-1}(C_i) \oplus C_{i-1}$,

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

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

Question 2. Le schéma du chiffrement est donné par



Donnez le schéma correspondant pour le déchiffrement.

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

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

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

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

Partie 3 : mode CTR

Le mode “CTR” (CounTeR) marche de la manière suivante :
- $C_i = F_k(IV \cdot i) \oplus B_i$,

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 (constant pour tous les blocs d'un message) suivi d'un compteur (différent pour tous les blocs d'un message).

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

Question 2. Est-ce que cela pose problème si l'attaquant connait 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 déchiffrement F_k^{-1} ?

Question 4. Dessinez les schémas de chiffrement / déchiffrement correspondants.

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

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

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