§4. Modes opératoires : Mise en œuvre d'un cryptosystème.

Le B-chiffrement, tel le DES, AES, 3-DES est un algorithme de cryptage de blocs de petite taille 8 byte ou 16 byte; alors qu'on cherche à chiffrer des e-mails, des fichiers de grande taille. On verra ici comment utiliser le B-cryptage pour cette tâche, et aussi des modes d'authentification (voir par ex. MAC.). On peut utiliser aussi le B-chiffrement pour le hachage (voir chap. privé), même si la cryptographie asymétrique est plus adaptée. On peut aussi exploiter le B-chiffrement pour construire des S-chiffrem

(4.1) Chiffrement avec le B-cryptage & modes opératoires.

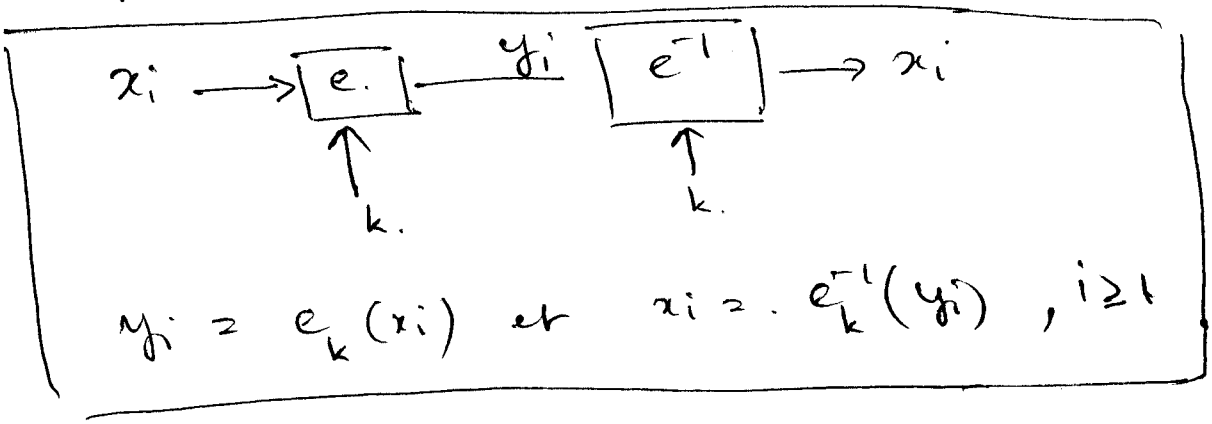
(4.1.1) Electronic Codebook Mode (ECB.)

Notons $e_k(x_i)$ le B-chiffrement du clair x_i par la clé k

$e_k^{-1}(y_i)$ l'opération de décryptage

des blocs de taille b. (Si le texte dépasse b, on le décompe en blocs de taille b, et on 'padde' si la taille $< b$).

ECB



$y_i = e_k(x_i)$ et $x_i = e_k^{-1}(y_i)$, $i \geq 1$