- Avantages : facile à implémenter et parallélisable
- Inconvénients : clé fixée ; faible devant attaques par substitution ⇒ Intégrité détruite

(4.1.2) Mode CBC (Chiffer Block chaining Mode).

- Chainage des blocs tq y_i dépend aussi des clairs précédents ($x_{i-1}, x_{i-2}, \cdots$).
- Rendu aléatoire en utilisant un vecteur d'initialisation (IV).

Définition CBC

$e(\cdot)$ cryptage bloc de taille b ; x_i, y_i de taille b ;

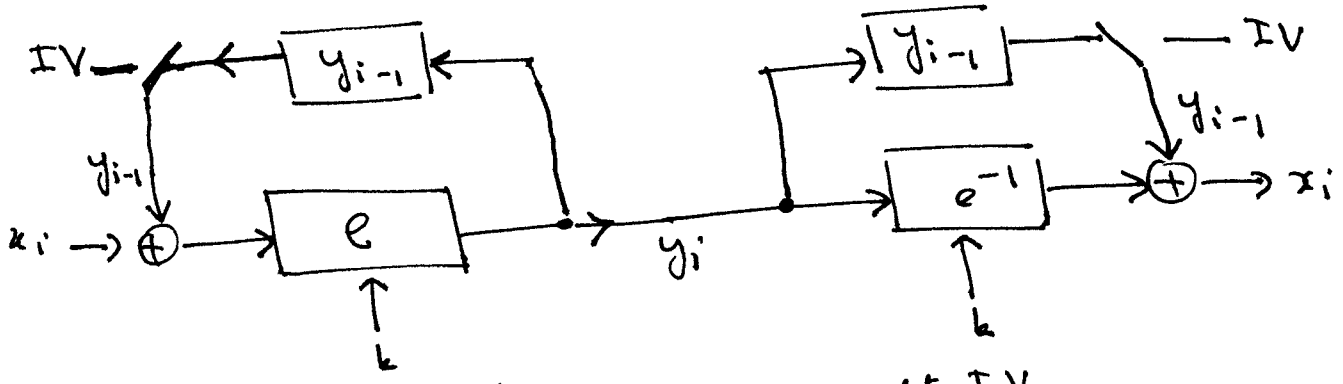
IV nonce (number used once) de long. b.

Cryp, 1er bloc : $y_1 = e_k(x_1 \oplus IV)$

Cry, En général : $y_i = e_k(x_i \oplus y_{i-1})$ $i \geq 2$.

Dec, 1er bloc : $x_1 = e_k^{-1}(y_1) \oplus IV$

Dec, En général : $x_i = e_k^{-1}(y_i) \oplus y_{i-1}$, $i \geq 2$.



⇒ y_i dépend de $x_1, \cdots, x_{i-1}$ et IV