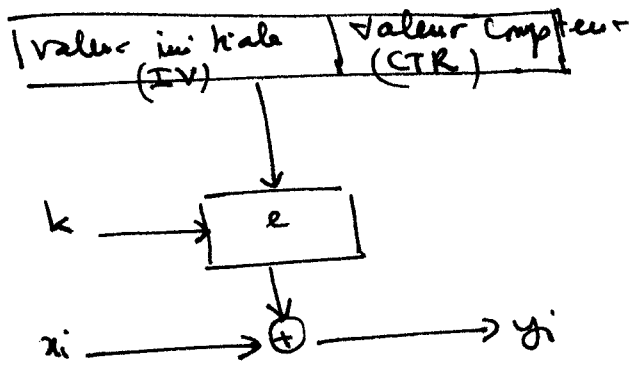
(4.1.5) CTR mode (Counter Mode)



Def. CTR mode.

$(IV \| CTR_i)$ Concaténation de IV et CTR_i de longueur b.

Cryptage : $y_i = e_k(IV \| CTR_i) \oplus x_i \quad i \geq 1$

Décryptage $x_i = e_k(IV \| CTR_i) \oplus y_i \quad , i \geq 1.$

- Alice et Bob peuvent s'échanger la valeur initiale $(IV \| CTR_1)$ publique et à chaque chiffrement le Compteur est incrémenté (qui peut être un LSFR de taille maximum).

(4.1.6) GCM (Galois Counter Mode)

→ Il permet de calculer aussi un MAC (Message Authentification Code) en plus de la fonction de cryptage avec le mode CTR.

→ Alice calcule un MAC rajouté à la fin de son message crypté. Bob calcule son 'MAC' et le compare à celui d'Alice : si égalité authentique.

En plus, le message est intègre (personne ne l'a manipulé en cours de la transmission).