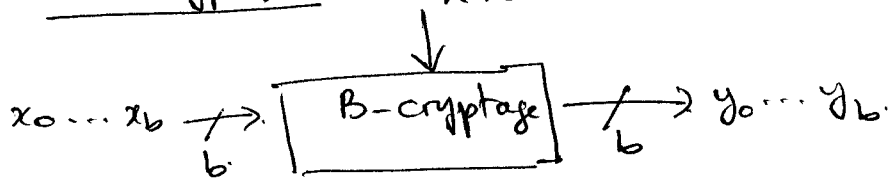
(2) B-cryptage : k : clé



on chiffre un bloc de bits, un à la fois avec la même clé k

Taille de bloc : 128 bits (16 bytes) pour AES
64 b. (8 bytes) " DES, 3DES

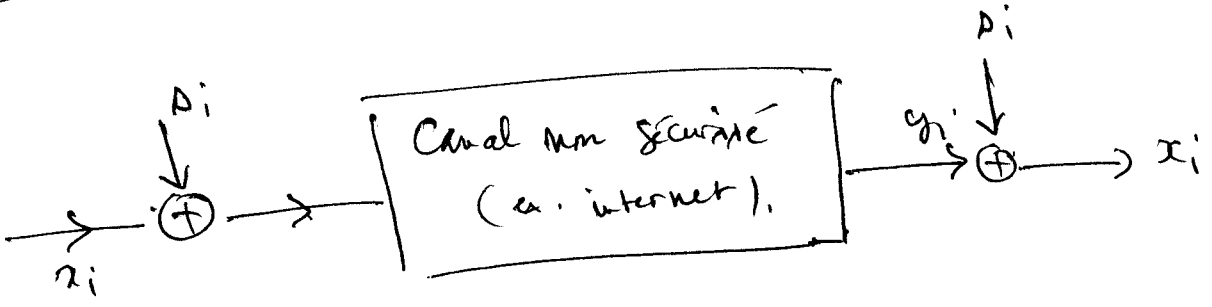
En pratique : ✓ B-cryptage plus utilisé que les-cryptage
✓ Mais le s-cryptage parfois rapide (ex. tél. cellulaire demandant moins de ressource

(3) • S-cryptage et décryptage :

entrée : $x_i, y_i, \Delta_i \in \{0,1\}$.

cryptage : $y_i = e_{\Delta_i}(x_i) = x_i + \Delta_i \mod 2$

décryptage : $x_i = d_{\Delta_i}(y_i) = y_i + \Delta_i \mod 2$.



→ rapide.

→ Comment obtenir la suite (Δ_i) ? C'est la base de la sécurité de ce système