(4.1.3) Mode OFB (Output Feedback Mode)

permet de construire des S-chiffrement.

Def OFB

$e(\ )$ B-cryptage de taille b ; x_i, y_i, s_i de long. b ;

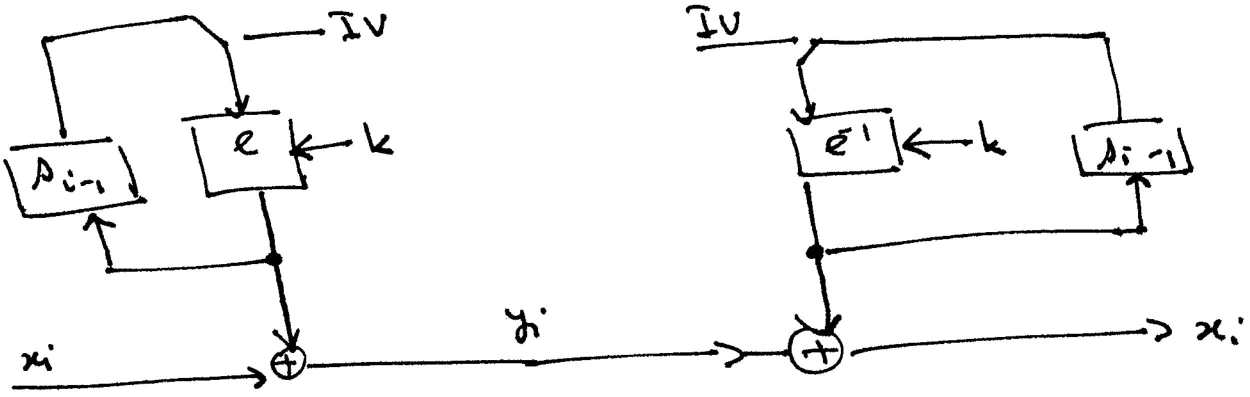
IV nonce de taille b ;

Cryptage (1er Bloc) : $s_1 = e_k(IV)$, $y_1 = s_1 \oplus x_1$

" (général) : $s_i = e_k(s_{i-1})$, $y_i = s_i \oplus x_i$, $i \geq 2$

Decryptage (1er bloc) : $s_1 = e_k(IV)$ $x_1 = s_1 \oplus y_1$

Decryptage (general) : $s_i = e_k(s_{i-1})$, $x_i = s_i \oplus y_i$, $i \geq 2$.



(4.1.4) Mode CFB (Cipher Feedback Mode).

ressemble OFB.

Def. C 1er bloc : $y_1 = e_k(IV) \oplus x_1$

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

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

D Général : $x_i = e_k(y_{i-1}) \oplus y_i$, $i \geq 2$

IV est un nonce qui peut être modifié.