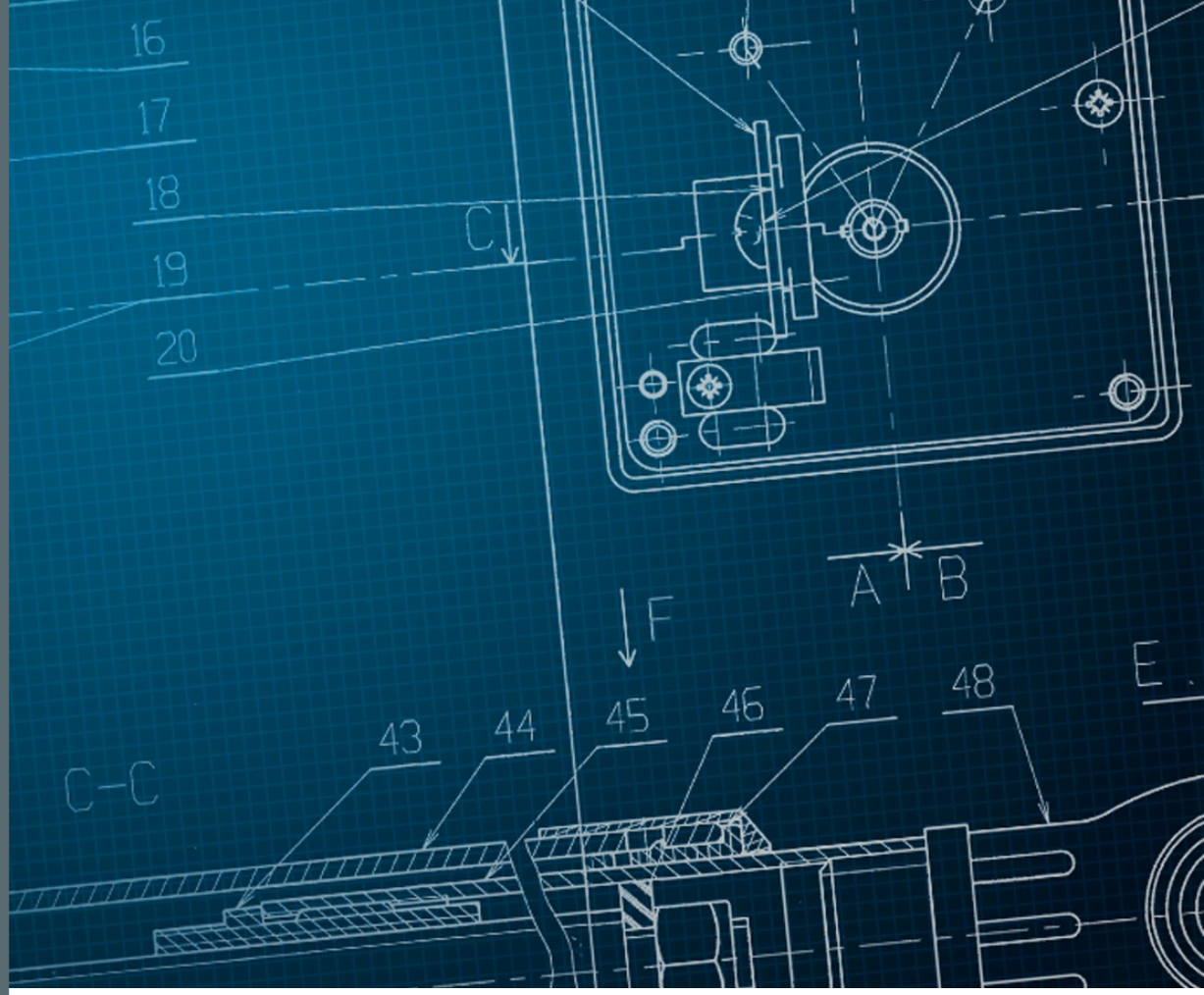
THIERRY MEYER
SÉCURITÉ INFORMATIQUE



2

Les principaux systèmes cryptographiques

Les concepts fondamentaux de la cryptographie appliquée

Extrait étudiants

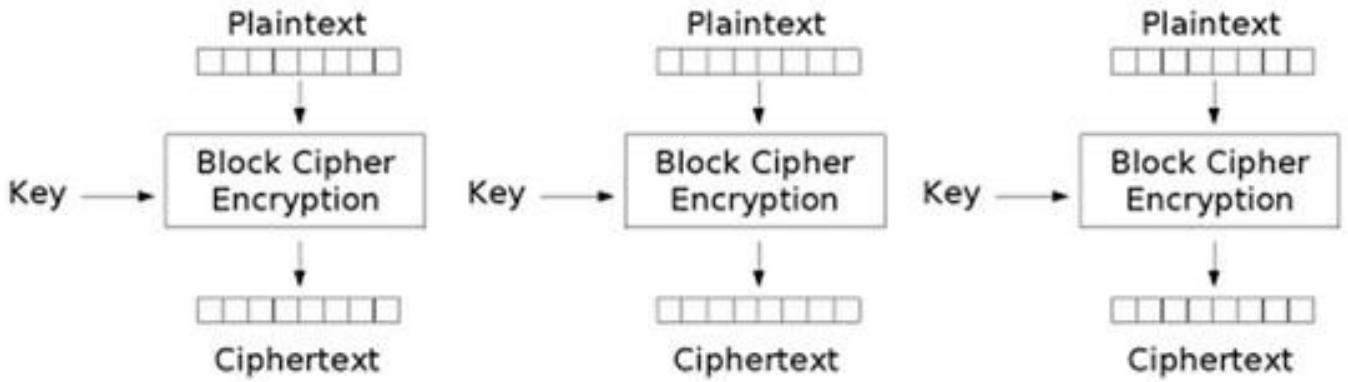
PLAN DU COURS

II. Les principaux systèmes cryptographiques :

- Les fonctions de hachage (One Way Hash Functions)
- La cryptographie symétrique
- Le cryptographie asymétrique (Ou à clef publique)

> Le mode d'opération ECB (Electronic Codebook)

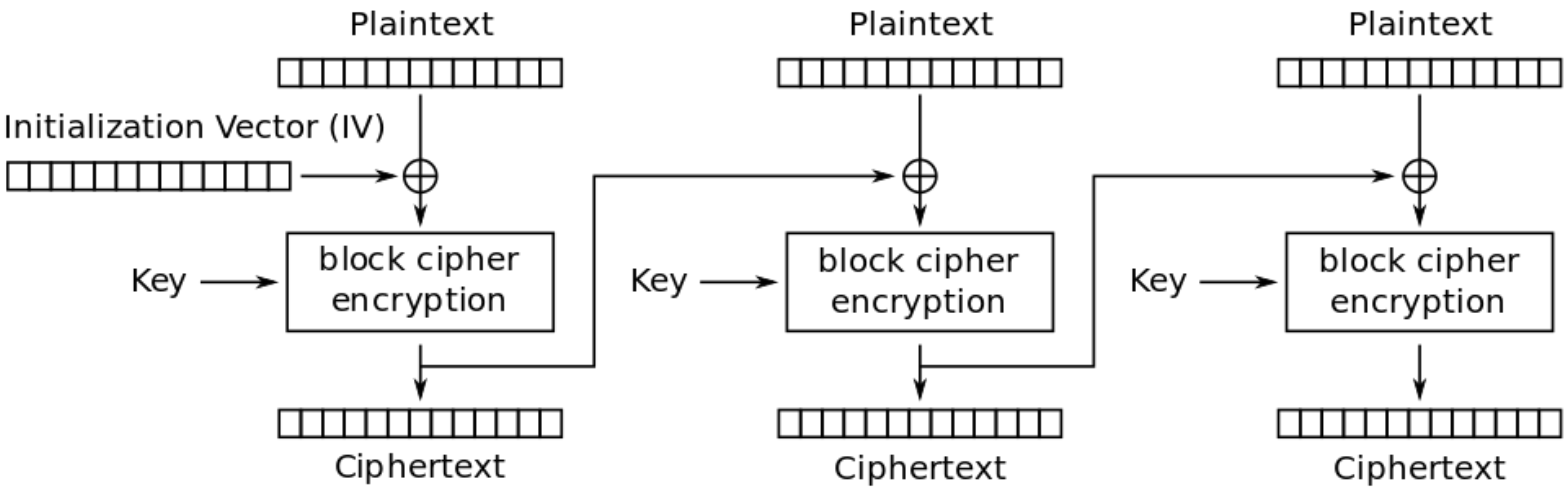
- Chiffrement (déchiffrement) :



Electronic Codebook (ECB) mode encryption

> Le mode d'opération CBC (Cipher Block Chaining)

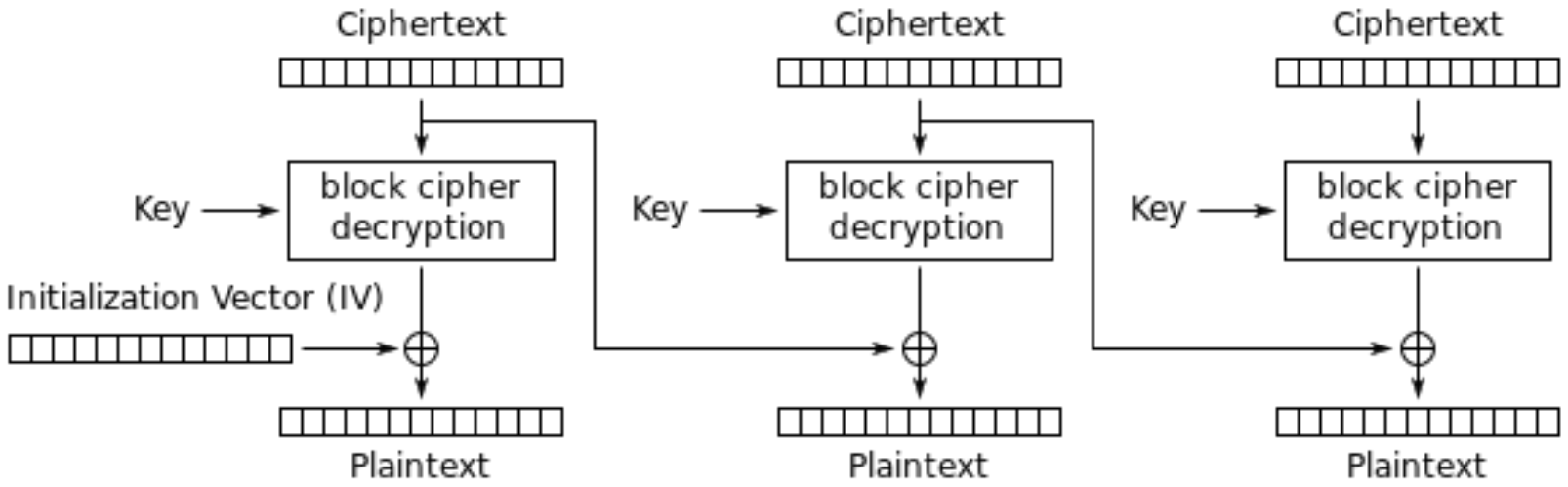
- Chiffrement :



Cipher Block Chaining (CBC) mode encryption

> Le mode d'opération CBC (Cipher Block Chaining)

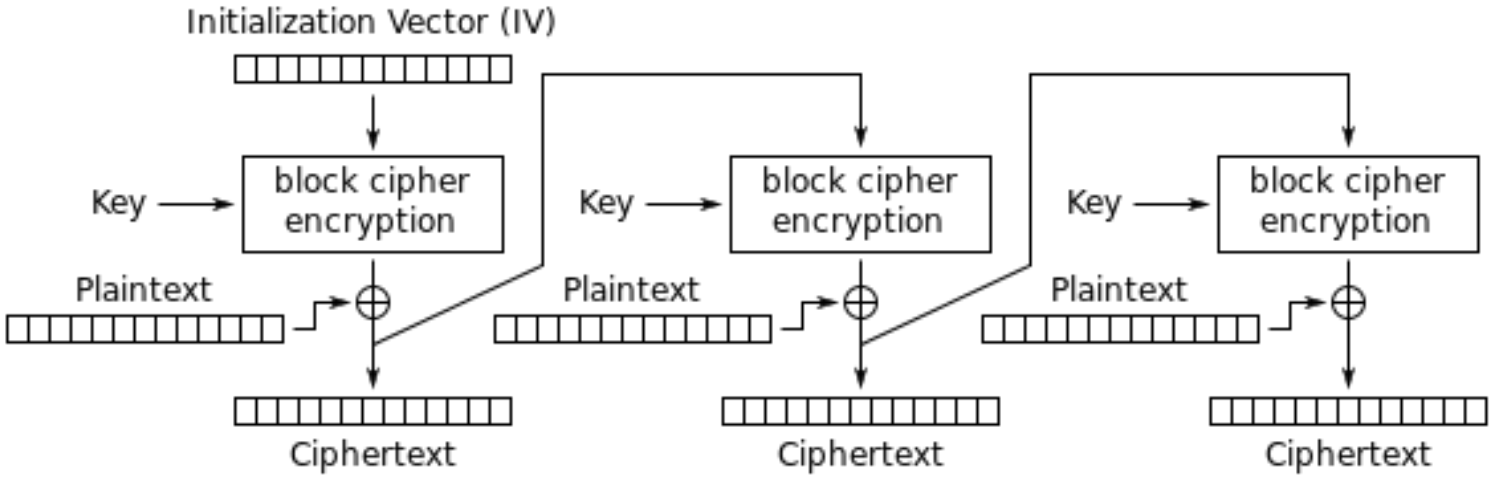
- Déchiffrement :



Cipher Block Chaining (CBC) mode decryption

> Le mode d'opération CFB (Cipher Feedback)

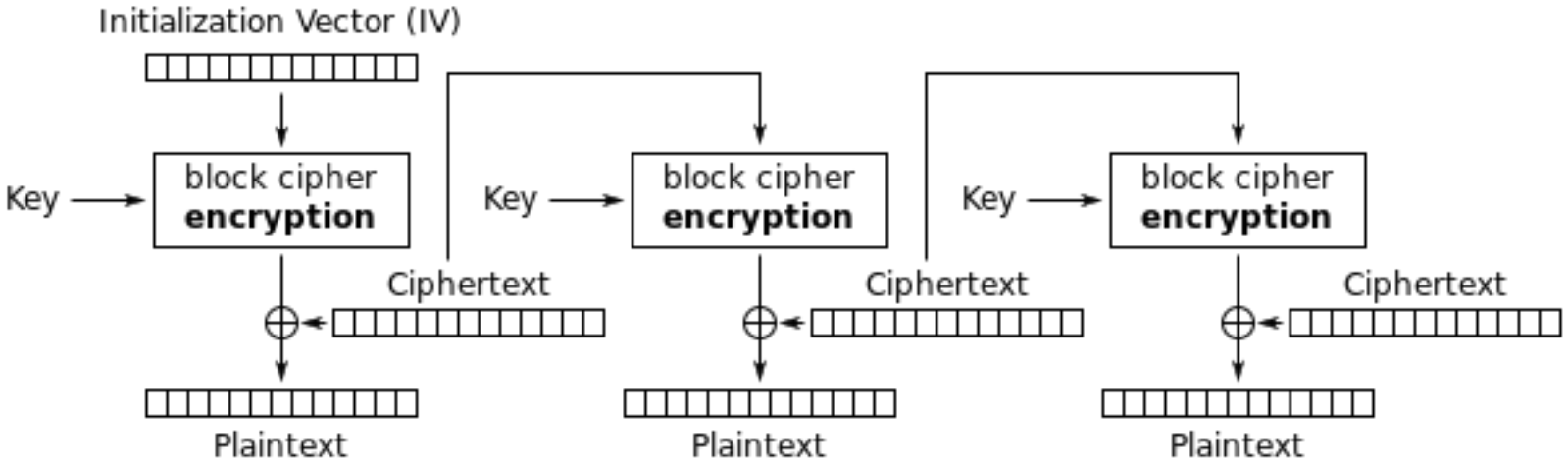
- Chiffrement :



Cipher Feedback (CFB) mode encryption

> Le mode d'opération CFB (Cipher Feedback)

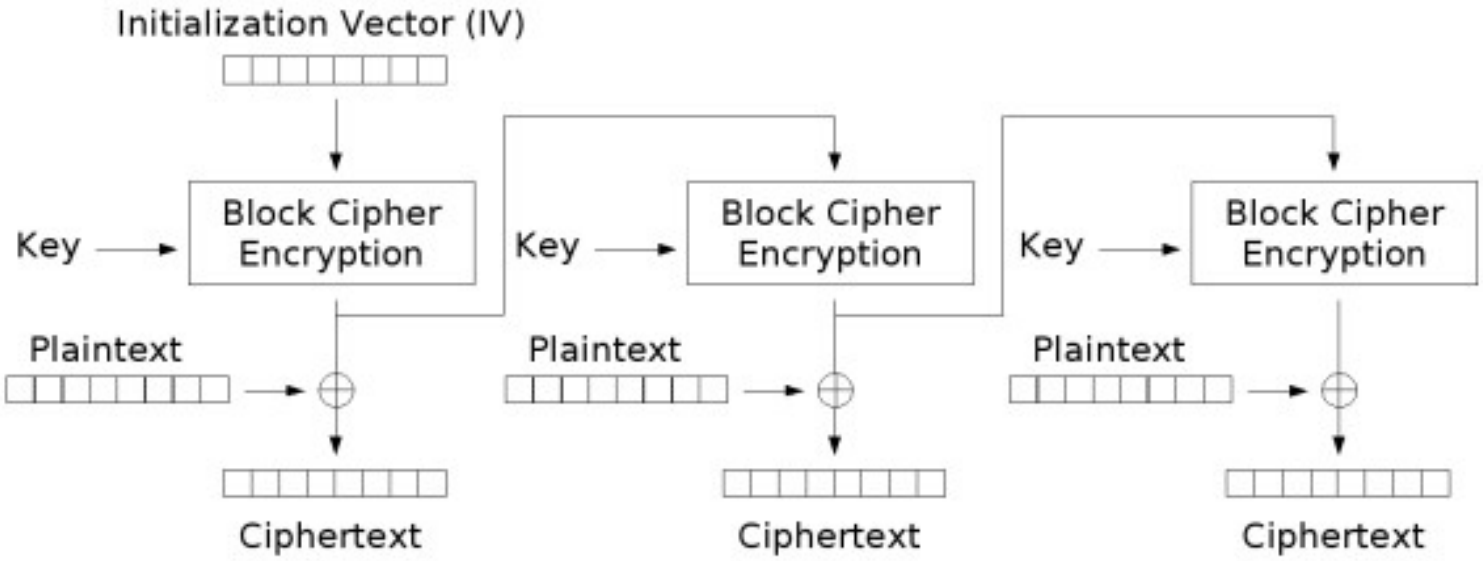
- Déchiffrement :



Cipher Feedback (CFB) mode decryption

> Le mode d'opération OFB (Output Feedback)

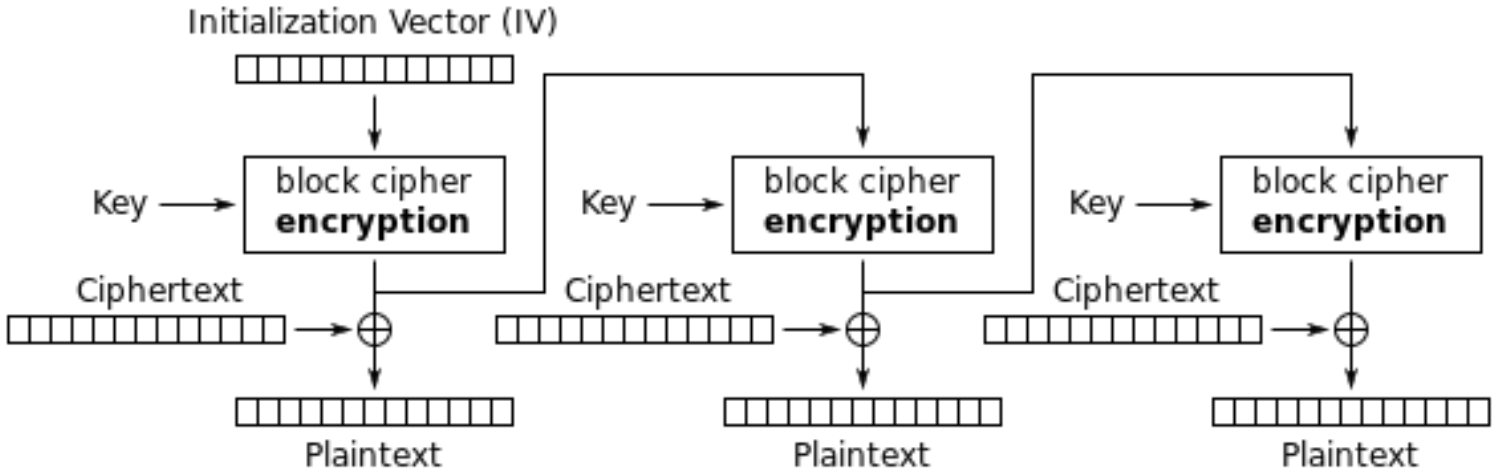
- Chiffrement :



Output Feedback (OFB) mode encryption

> Le mode d'opération OFB (Output Feedback)

- Déchiffrement :



Output Feedback (OFB) mode decryption

LES PRINCIPAUX SYSTÈMES CRYPTOGRAPHIQUES

> Des questions ?

LES PRINCIPAUX SYSTÈMES CRYPTOGRAPHIQUES

Thierry MEYER Consultants, est un cabinet de conseil, audit, et expertise technique spécialisé en sécurité des systèmes d'information depuis sa création en 2005.

contact@tm-consultants.fr

@Th1tux