MODES

ECB

Les blocs sont chiffrés indépendamment blocs par blocs
$C_i = DES_K(P_i)$
Usage : transmission sure de valeurs isolées

Sécurité :

- \- conservation des formats m=m' => c=c'
- \+ clé réutilisable
- \+ indépendance des blocs

Efficacité :

- \+ parallélisme possible
- \+ accès aléatoire possible
- \+ même vitesse de chiffrement
- \- pas de préprocessing
- \- nécessité de blocs complets de 8 bits

Propagation des erreurs :

- une erreur dans m_i (c_i) n'affecte que le m_i (c_i) correspondant
- la perte ou l'ajout d'un bit affecte tous les blocs suivants
- la perte d'un c_i n'affecte qu'un bloc

CBC

Les blocs sont liées entre-eux → chaînage → effet d'avalanche (un ci est dépendant de m_i et c_{i-1})
IV (vecteur d'initialisation) : un mot de passe, un timestamp, …
Usage : chiffrage de bloc, authentification

Sécurité :

- \+ effacement des formats (si IV différents)
- \+ il n'y a plus de risque de répétition de bloc
- \+ clé réutilisable (si IV différents)

Efficacité :

- \+ même vitesse de chiffrement
- \- pas de préprocessing
- \- pas de parallélisme
- \+ padding
- \- IV connu des 2 cotés

Propagation des erreurs :

+ la perte d'un c_i n'affecte qu'un bloc de M
+ une erreur dans m_i affecte tous les c_i suivants mais ne se retrouve que dans le m_i correspondant
- une erreur dans c_i affecte un bloc entier de mi et le bit correspondant dans m_{i+1}
- la perte ou l'ajout d'un bit de c_i affecte tous les blocs m_i, m_{i+1},… suivants (perte des limites de bloc)

CFB

Flux : ajout à la sorte du bloc chiffré, le résultat sert de feedback pour l'étape suivante
Nombre quelconque de bit pour le registre : 1, 8, 64 bits (le plus souvent 64)
Usage : chiffrement de flux, authentification

Sécurité :

+ même fonction pour le chiffrement et le déchiffrement
+ pas de répétition de bloc si IV différents
+ effacement du format standard

Efficacité :

+ même vitesse de chiffrement
- pas de préprocessing
- pas de parallélisme

Propagation des erreurs :

- une erreur dans ci affecte le mi correspondant et les 64/k blocs suivants
- perte ou ajout d'un bit de ci affecte mi correspondant plus le suivant
- la perte d'un bloc de ci : le synchronisme est récupéré dès que le ci est sorti du registre
- une erreur dans mi affecte les 64/k ci suivant mais uniquement le mi correspondant lors du déchiffrement

OFB

Le feedback est indépendant du message → mécanisme indépendant de mi et ci
Équivalent à un chiffrement de Vernam avec réutilisation de la clé et de l'IV
Usage : chiffrement du flux sur un canal bruyant

Sécurité :

+ IV unique et aléatoire
+ effacement du format de M
+ clé réutilisable
+ pas de répétition de blocs

Efficacité :

+ même vitesse de chiffrement
+ préprocessing
- pas de parallélisme

Propagation des erreurs :

+ une erreur dans c_i affecte uniquement le bit correspondant de m_i
- la perte ou l'ajout d'un bit de c_i affecte tout le bloc de m_i et le suivant
- pas de mécanisme de récupération de synchronisation

CTR

Usage : Réseaux grande vitesse
Un compteur et une clé différents pour chaque texte clair
Efficacité :

Parallélisme
Accès aléatoire possible
Sécurité démontrable