Mathématiques-Cryptographie

Anne Garcia-Sanchez

M2i cyber2 dev - CFA CCI Avignon

7 mai 2024

Chiffrements symétriques

chiffrements symétriques: une clé pour chiffrer et déchiffrer

- chiffrements par flot
- chiffrements par blocs

Chiffrements par blocs

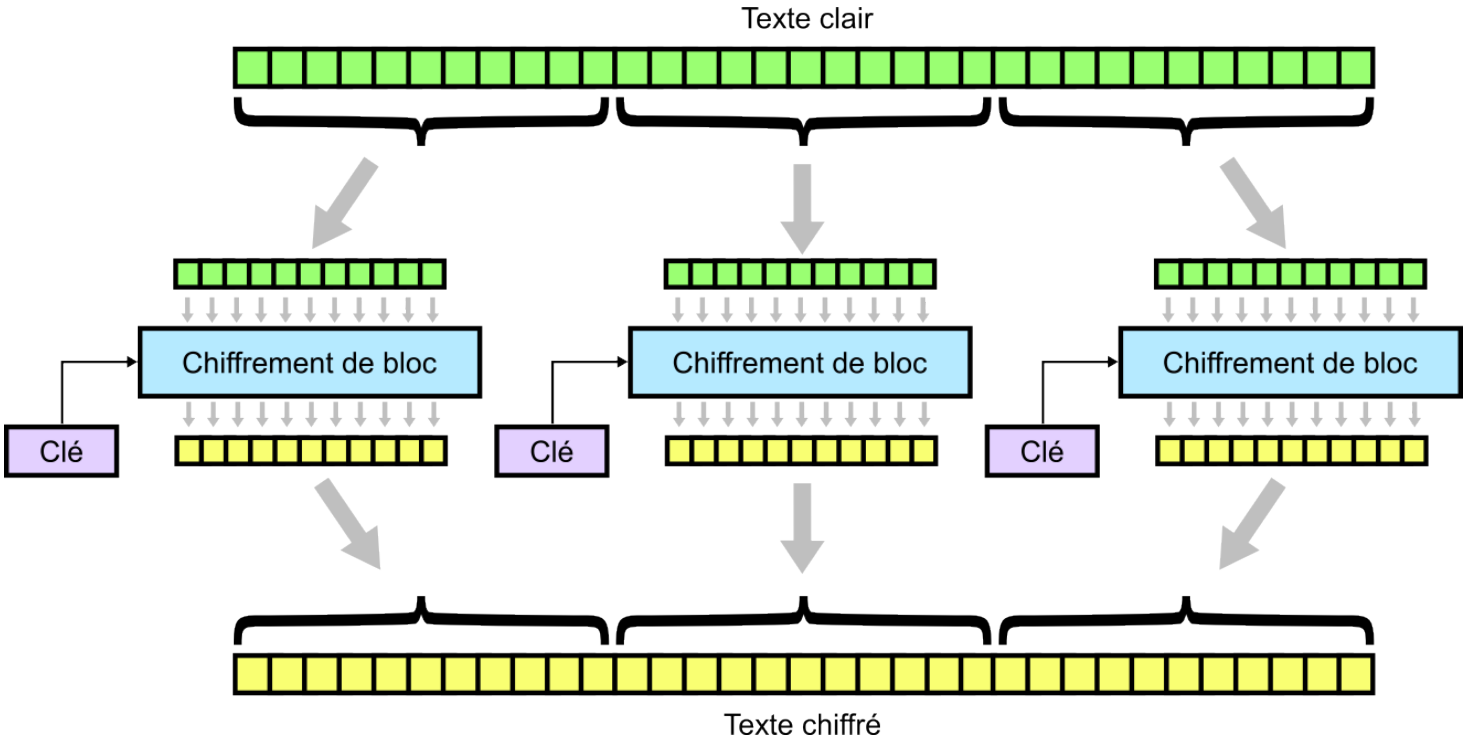
le message est découpé en blocs de longueur fixe.

modes opératoires: différentes façons d'enchaîner le chiffrement de plusieurs blocs.

Mode opératoire ECB

ECB = *Electronic Code Book*

blocs chiffrés indépendamment avec la même clé secrète.



Ce mode de chiffrement est le plus simple mais ne présente aucune sécurité et n'est normalement jamais utilisé en cryptographie.

Mode opératoire ECB

Un bloc de message m est toujours chiffré de la même façon.
Exemple illustrant le problème: ECB penguin

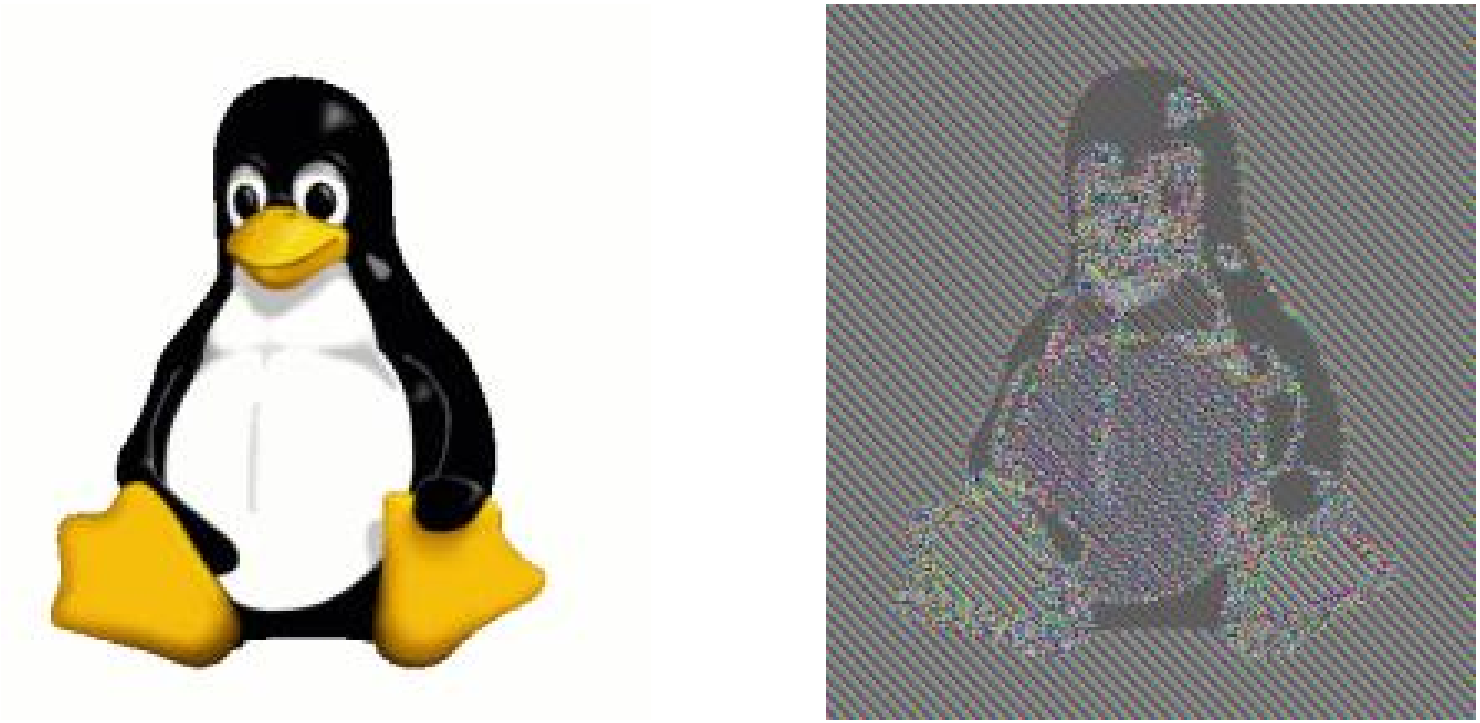


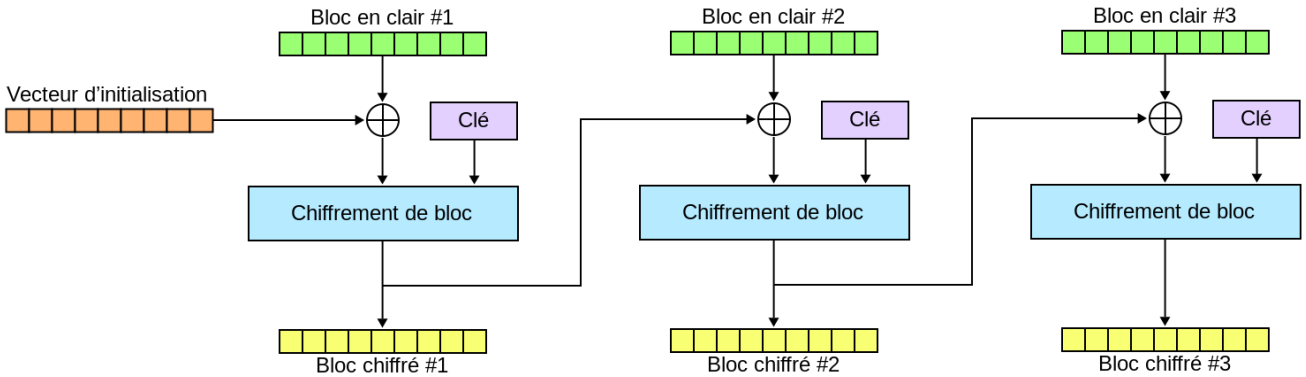
Figure: Image originale (Larry Ewing) et image chiffrée en mode ECB

Mode opératoire CBC

CBC = *Cipher Block Chaining*

ou exclusif avec le chiffré du bloc précédent.

pour le premier bloc:
vecteur d'initialisation (IV) = bloc de données aléatoires.
Ce vecteur ne doit jamais être réemployé avec la même clé.



source: wikipedia

Mode opératoire CBC

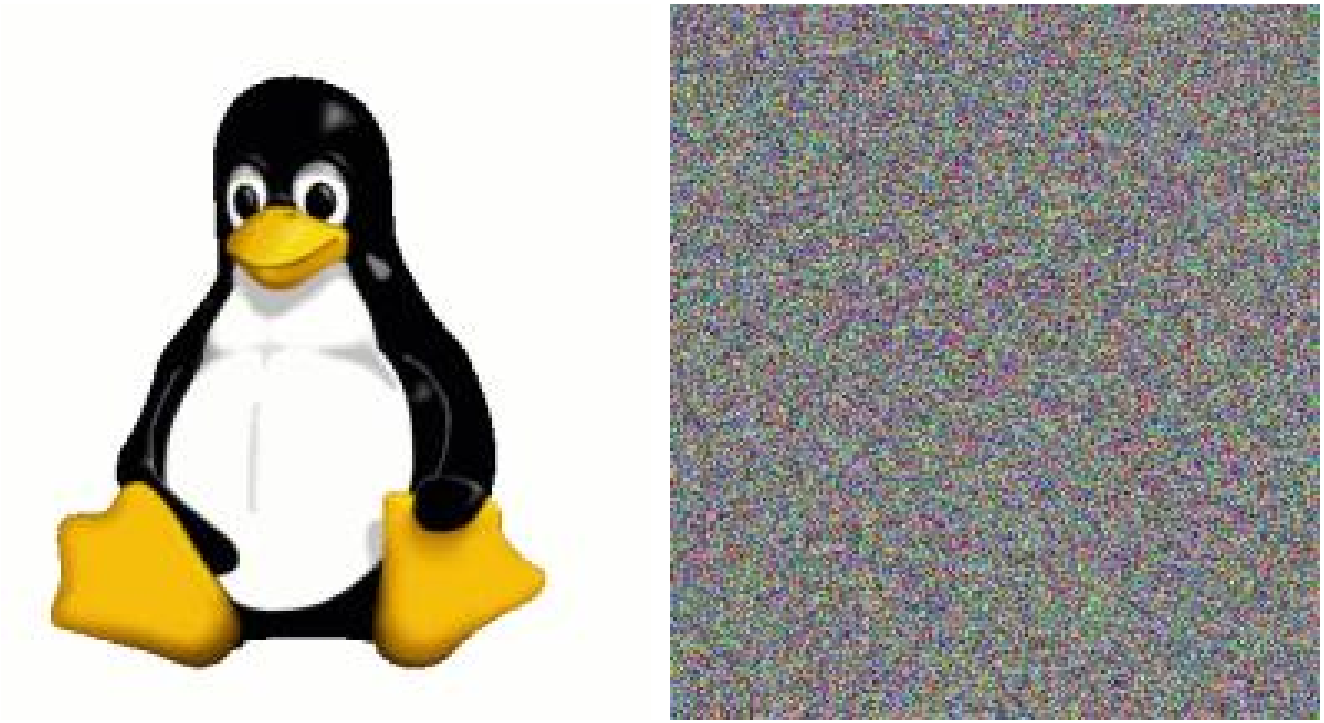


Figure: Image originale (Larry Ewing) et image chiffrée en mode CBC

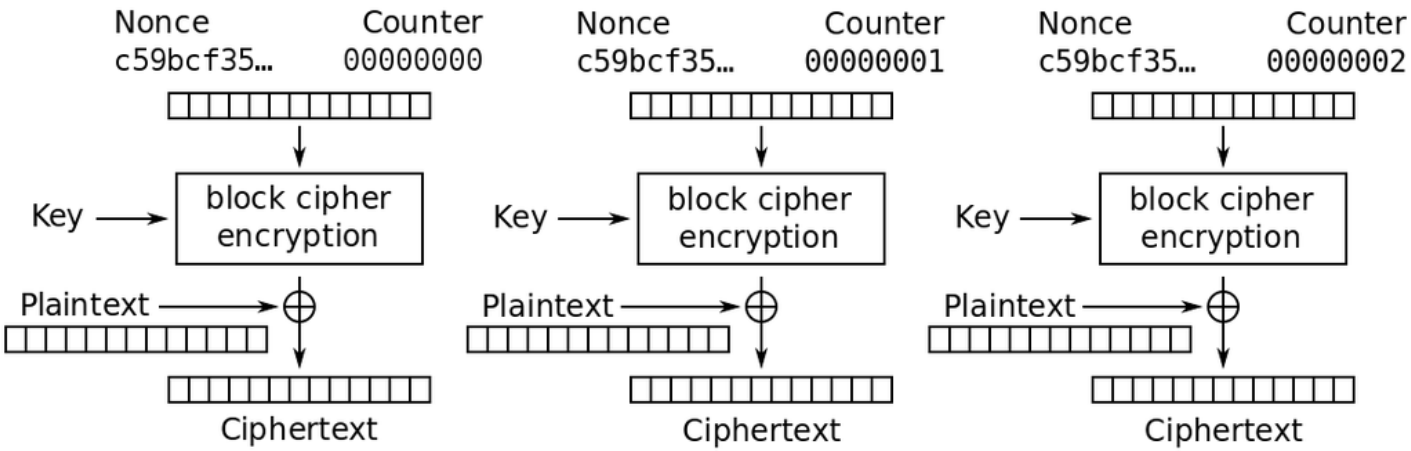
Problème CBC: non parallélisable, vulnérabilités (padding attack)

Mode opératoire CTR

CTR = *Counter*

vecteur d'initialisation (nonce) concaténé avec un compteur puis chiffré : produit un bloc pseudo-aléatoire utilisé comme masque jetable.

Le vecteur d'initialisation ne doit jamais être réutilisé avec la même clé.



Mode opératoire GCM

GCM *Galois counter mode*

version plus élaborée de CTR

permet d'assurer l'intégrité et l'authenticité des données

mode opératoire largement adopté pour ses performances

Remplissage - bourrage - *padding*

chiffrements par bloc permettent de chiffrer des blocs de n bits

modes opératoires: permettent de chiffrer des messages dont la longueur est un multiple de n.

pour des messages de taille quelconque: processus de remplissage ou de bourrage ou *padding* pour obtenir un message dont la longueur est un multiple de n en complétant le dernier bloc.

Padding ANSI X9.23

Le bloc est complété avec des octets aléatoires ou des 00 selon les versions.

Le dernier octet indique le nombre d'octets ajoutés.

Exemple pour une taille de bloc de 8 octets en hexadécimal:
... | DD DD DD DD DD DD DD DD | DD DD DD DD **00 00 00 04** |

Padding PKCS#7

La valeur de chaque octet ajouté est le nombre d'octets qui sont ajoutés.

Exemple pour une taille de bloc de 8 octets en hexadécimal:

... | DD DD DD DD DD DD DD DD | DD DD DD DD **04 04 04 04** |

Attaque d'oracle de bourrage/remplissage - Padding attack
S. Vaudenay a proposé en 2002 une attaque contre ce processus de bourrage avec le mode opératoire CBC.

Padding ISO/IEC 7816-4

Le premier octet est un octet obligatoire de valeur "80" suivi, si nécessaire, d'octets de valeur "00", jusqu'à ce que la fin du bloc soit atteinte.

Exemple pour une taille de bloc de 8 octets en hexadécimal:

... | DD DD DD DD DD DD DD DD | DD DD DD DD **80 00 00 00** |

Confusion et diffusion

Claude Shannon: *Communication Theory of Secrecy Systems* - 1949

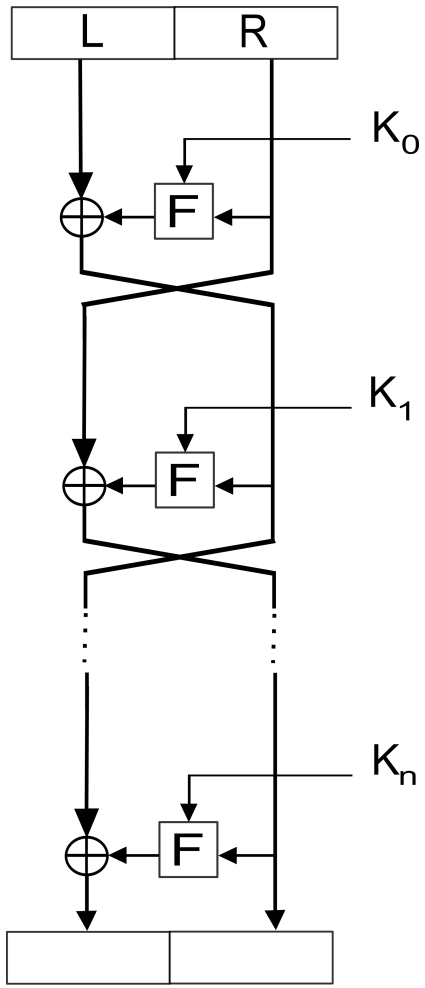
propriétés fondamentales pour assurer la sécurité d'un système de chiffrement

confusion: liens entre texte clair et texte chiffré trop compliqués pour être exploités par un attaquant

diffusion: chaque bit du texte clair et chaque bit de la clé influencent chaque bit du texte chiffré

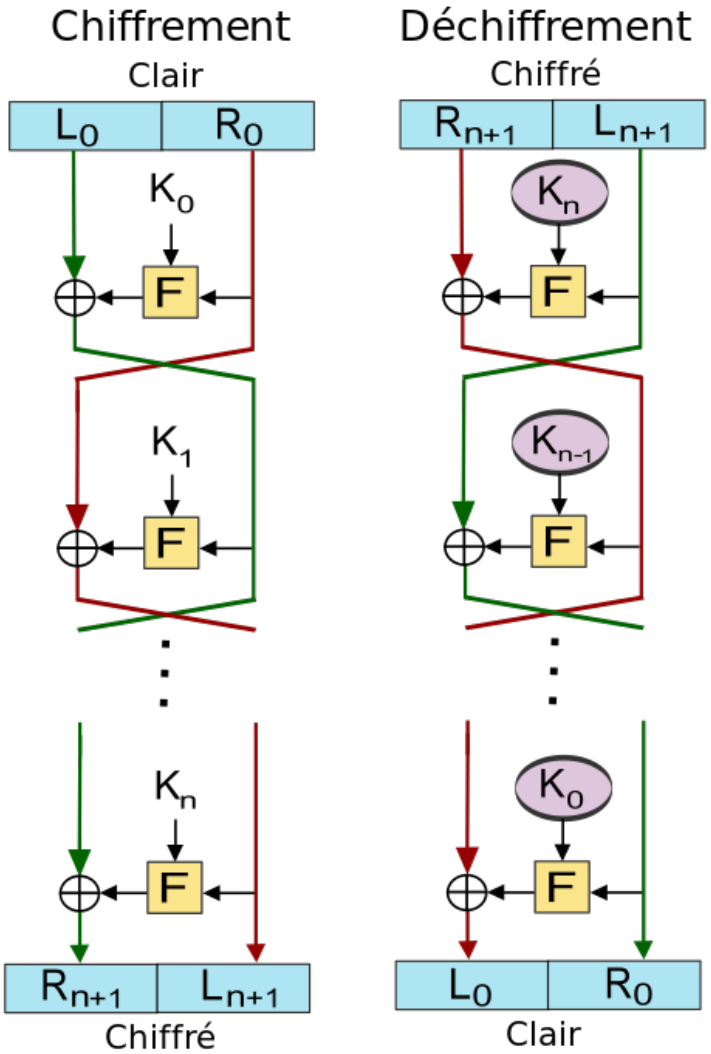
Shémas de Feistel

1970 cryptographe américain Horst Feistel



Shémas de Feistel

Quelle que soit la fonction F utilisée, le déchiffrement fonctionne.



Shémas de Feistel

Quelle que soit la fonction F utilisée, le déchiffrement fonctionne.