mécanismes de la crypto symmetrique par bloc

Gueguen David

Jeudi 21 Avril 2016

'références'

Article -wiki-

- https://en.wikipedia.org/wiki/Block_cipher
- https://en.wikipedia.org/wiki/Substitution-permutation_network
- https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

Book -dispo en ligne-

- Applied crytpography - Bruce Schneier
- The block cipher companion - Lars R. Knudsen

au programme

Crypto symétrique & la théorie de l'information

'Data Encryption Standard' - 1975

Modes d'opérations

Questions a trancher

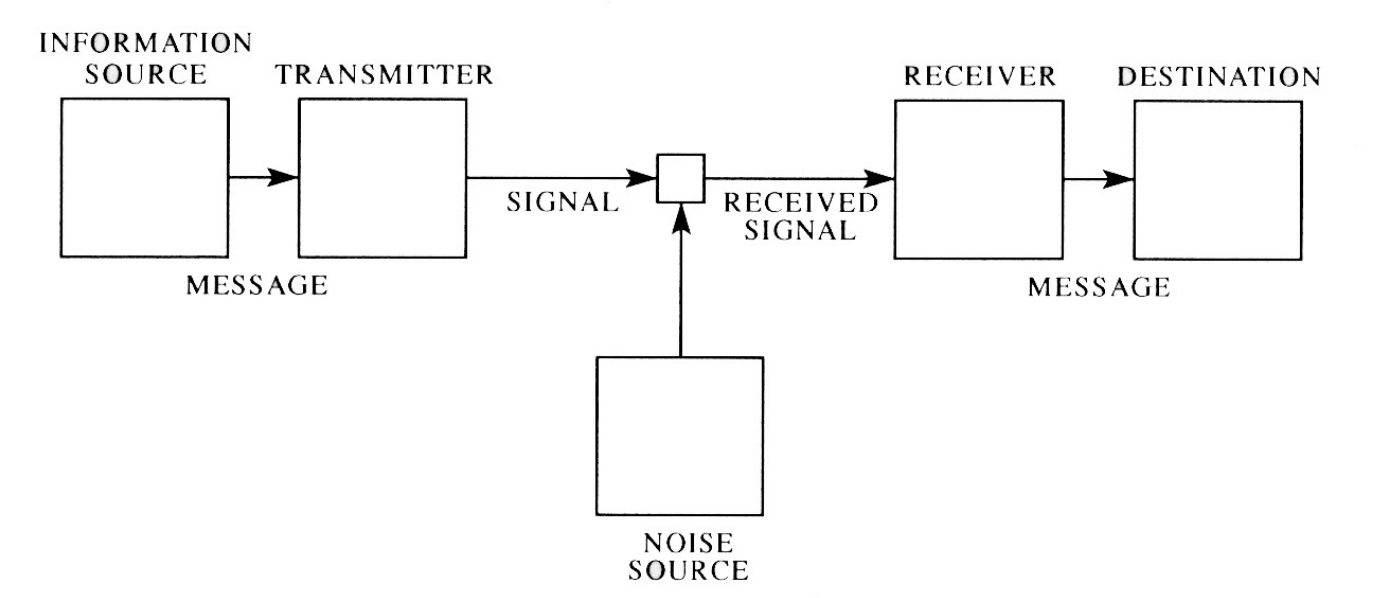
crypto symétrique & la théorie de l'information

theorie de l'information in a nutshell

- Fondation: *Theorie de l'Information*

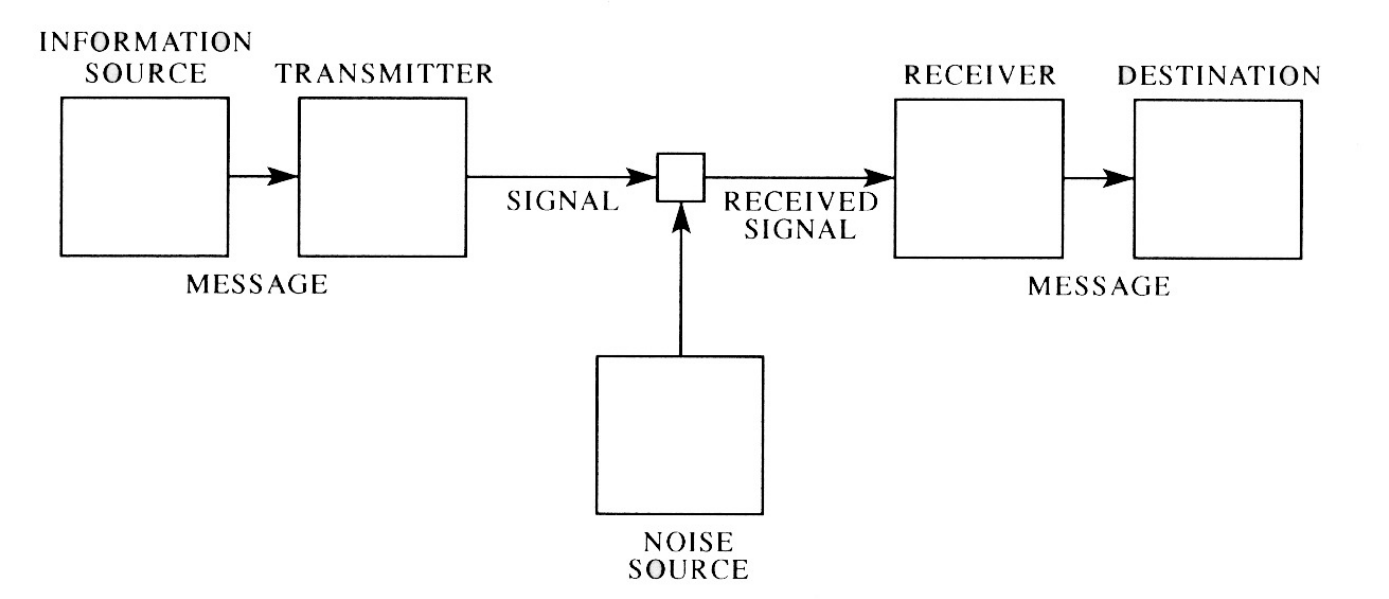
theorie de l'information in a nutshell

- Fondation: *Theorie de l'Information*



theorie de l'information in a nutshell

- Fondation: *Theorie de l'Information*

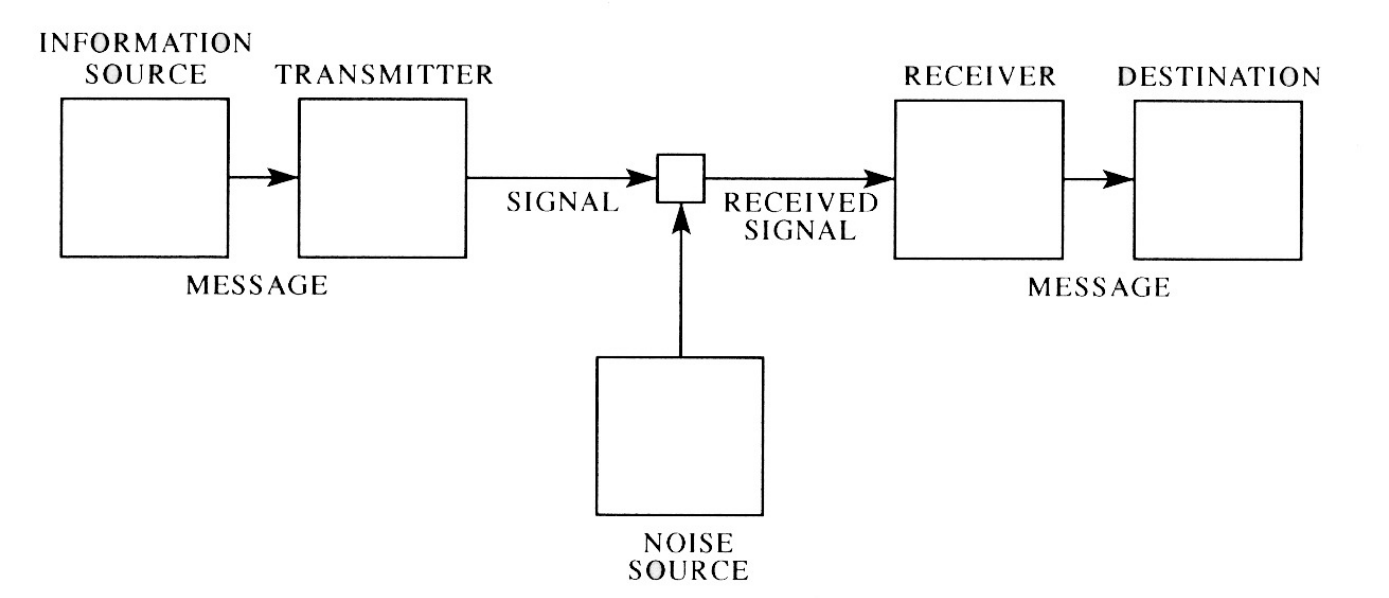


Quantifie la quantité d'information d'un canal.

Concepts clefs: Entropie, capacité du canal, code correcteur

theorie de l'information in a nutshell

- Fondation: *Theorie de l'Information*



Résultat

'On peut communiquer sans perte meme a travers un canal bruité'

'ideal block cipher'

Un chiffrement par bloque doit:

- se comporter comme une famille de 'permutations pseudo-aléatoire' paramétré par l'espace des clés

/!\mais ceci n'est pas mesurable,vérifiable /!\
En conséquence, on espère des trucs genres:

$$\forall A, Adv^{PRP}_{F_k K}(A) \approx 1/|K|$$

fondation crypto symetrique

Fondation de la cryptographie moderne

- 'Diffusion':
  'chaque bit du clair changé, influence la moitiee du chiffre'
  obfusque les relations clair/chiffre.
- 'Confusion':
  'chaque bit du chiffre doit dependre de differents bits de la cle'
  obfusque les relations clé/chiffre
  chaque bit de clé, influence chaque bit du chiffre.

fondation crypto symetrique

Fondation de la cryptographie moderne

- 'Diffusion':
  'chaque bit du clair changé, influence la moitiee du chiffre'
  obfusque les relations clair/chiffre.
- 'Confusion':
  'chaque bit du chiffre doit dependre de differents bits de la cle'
  obfusque les relations clé/chiffre
  chaque bit de clé, influence chaque bit du chiffre.

Wikipédia: 'Substitution-permutation network'
permutation comme diffuseur
substitution comme confuseur.

fondation crypto symetrique

Wikipédia: 'Substitution-permutation network'

permutation comme diffuseur

substitution comme confuseur.

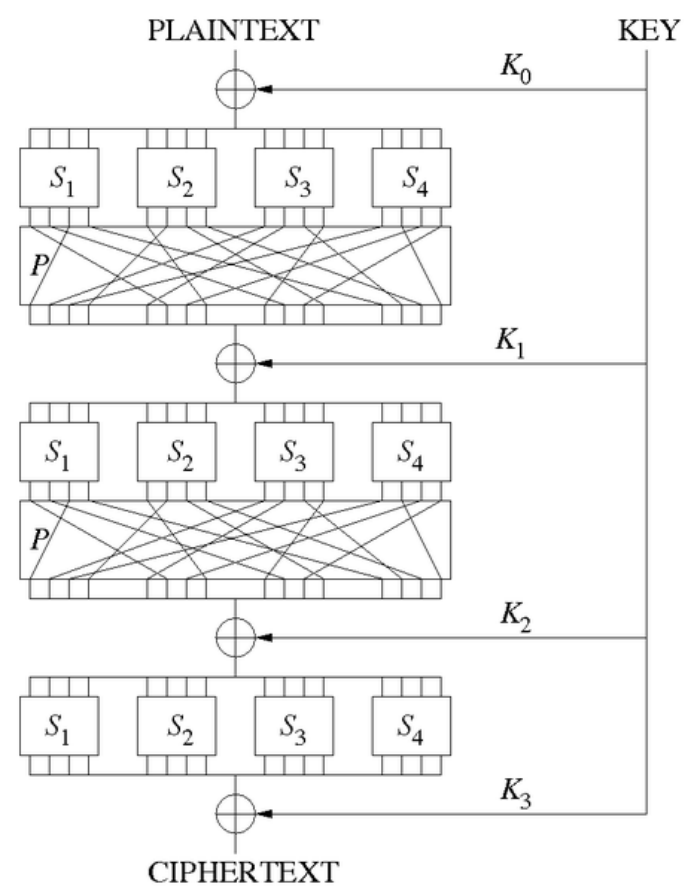


illustration effet avalanche

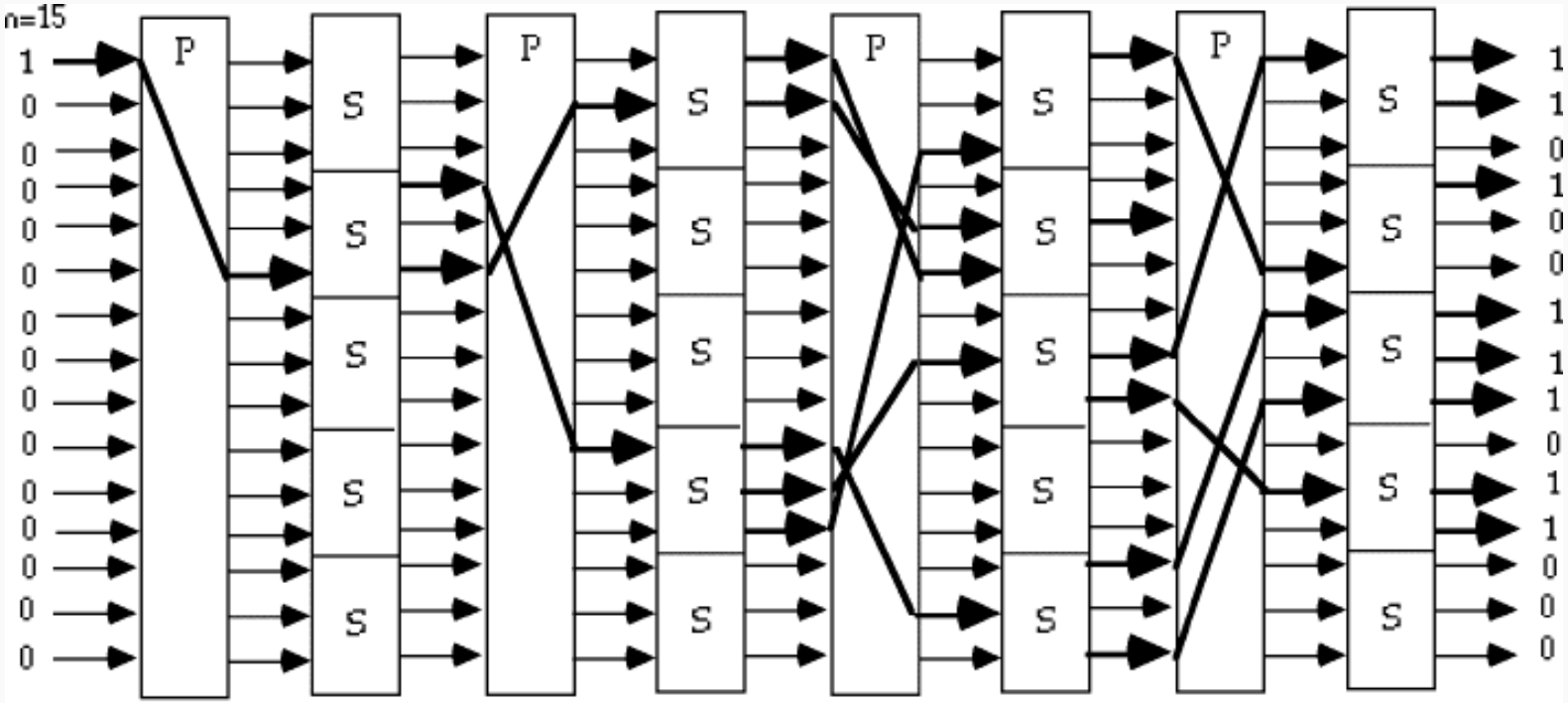
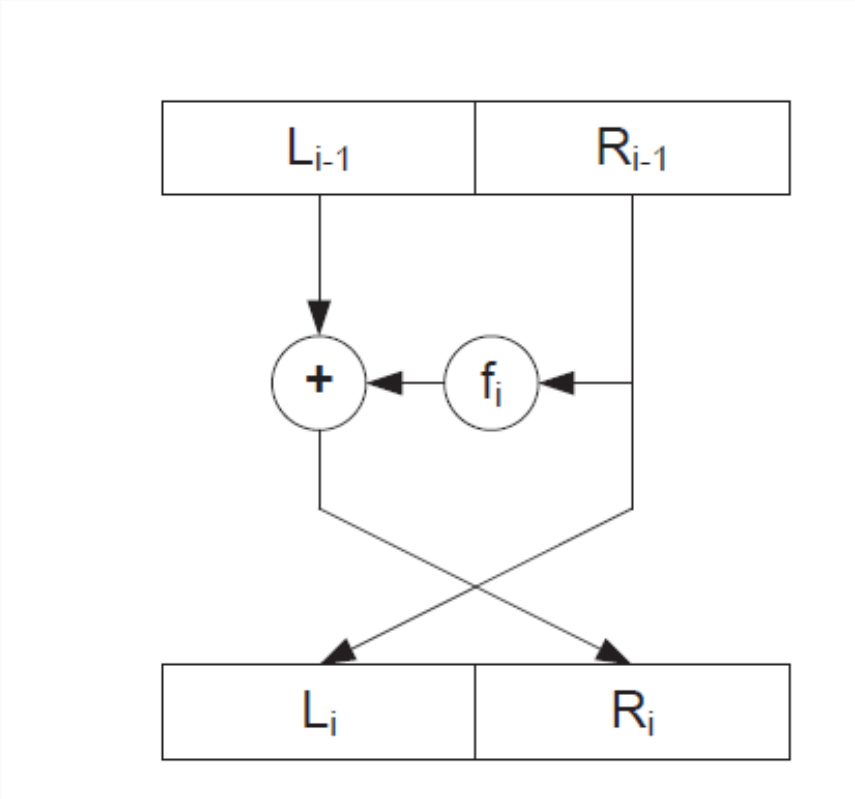


Fig 2.3 - Substitution-Permutation Network, with the Avalanche Characteristic

schéma de feistel-coppersmith

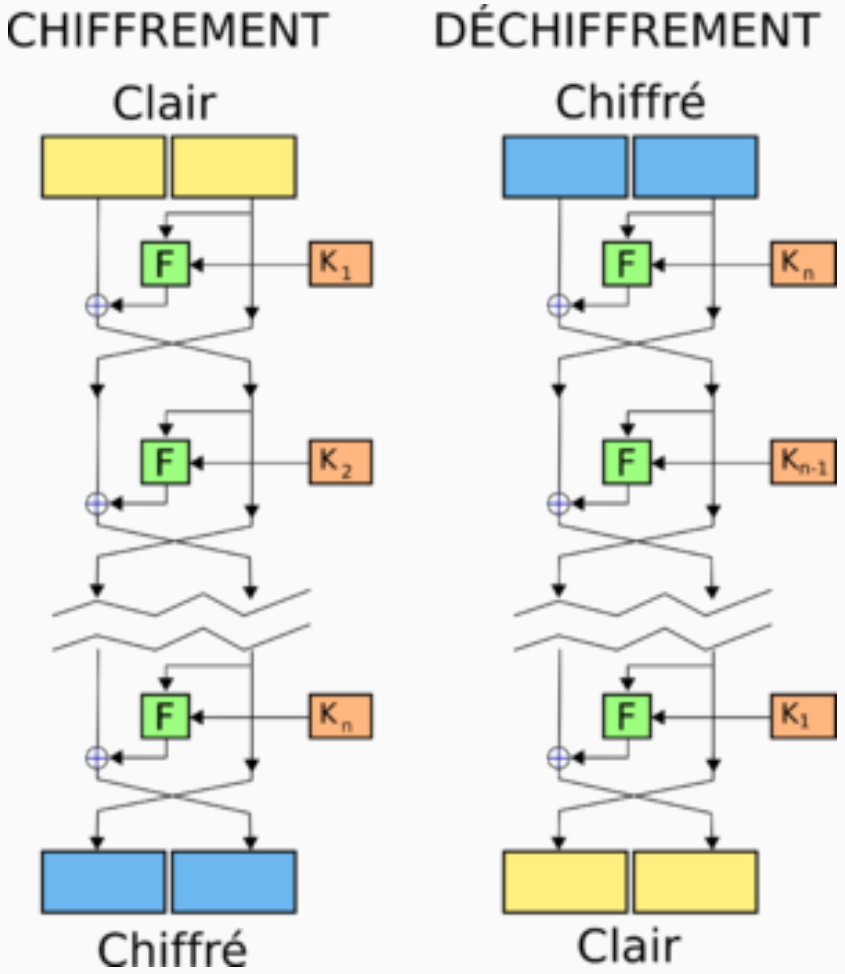


théorème luby-rackoff

'Reduit le problème de construction de *permutations pseudo aleatoire* a celui de *fonctions pseudo aleatoire*'

'Un schema de Feistel-Coppersmith, avec n d'entrée/sortie, et 4 rounds ou plus, est indistinguable d'une permutation réellement aléatoire pour m requêtes, $m << 2^n$'

schema de feistel-coppersmith



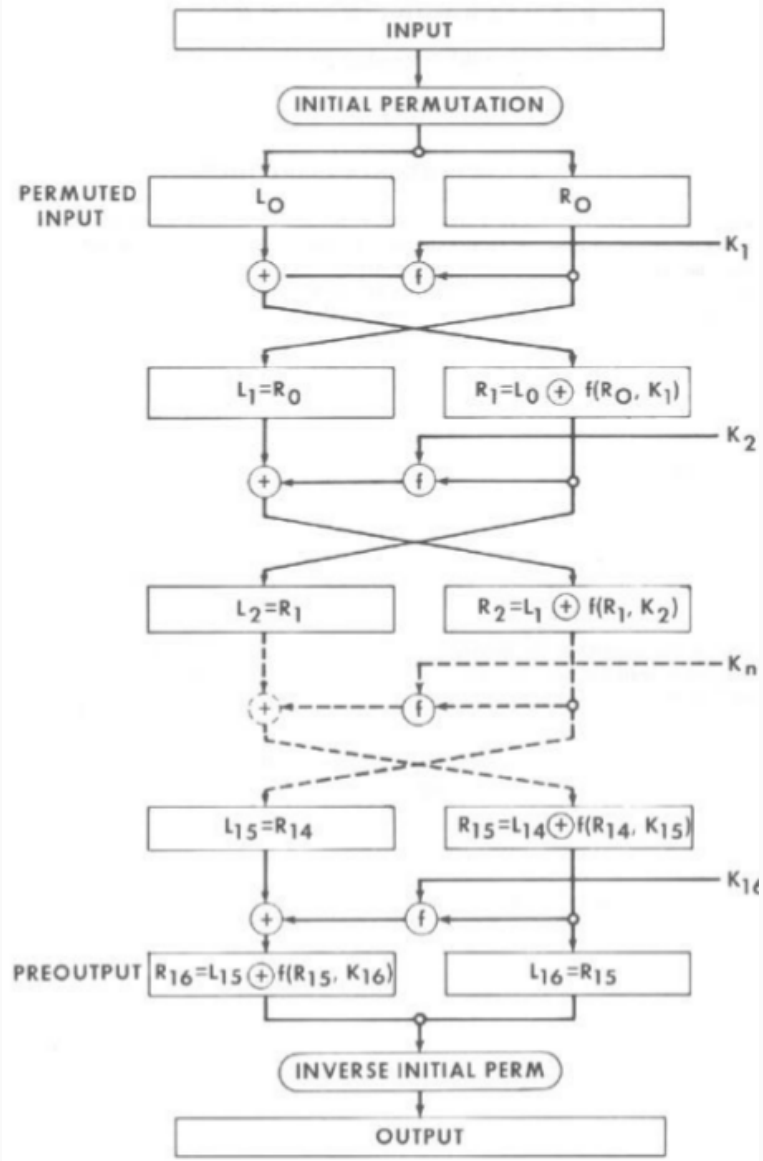
'data encryption standard' - 1975

'data encryption standard'

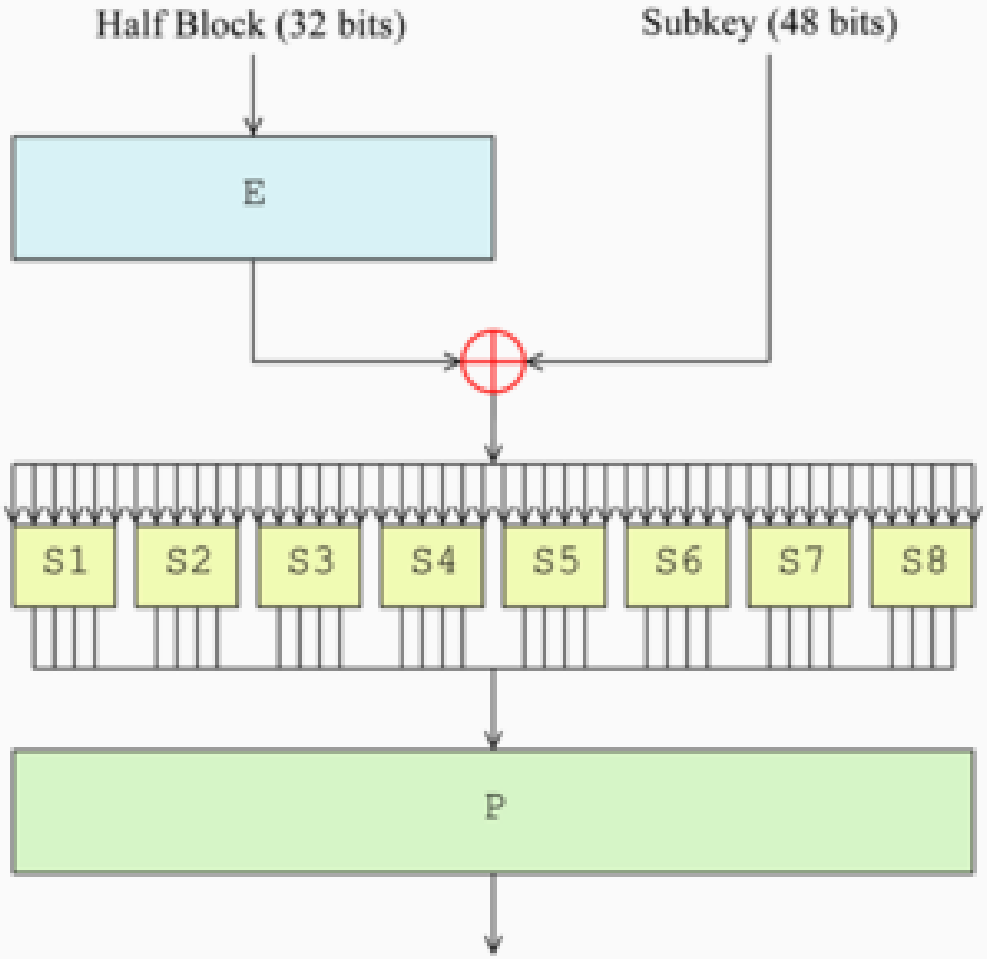
- NIST. *Data Encryption Standard*. 1977

illustrations: -must see-

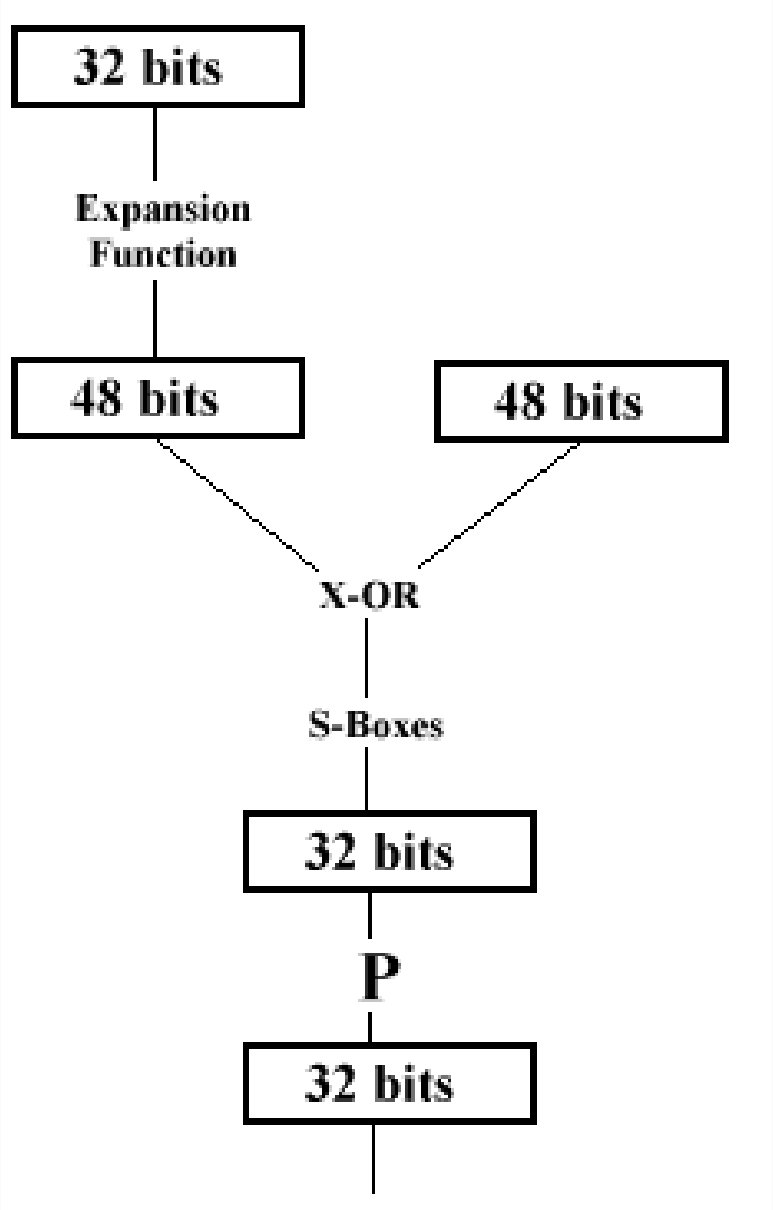
`https://fr.wikipedia.org/wiki/Constantes_du_DES`


INPUT
INITIAL PERMUTATION
PERMUTED INPUT
L_0
R_0
K_1
f
$L_1=R_0$
$R_1=L_0 \oplus f(R_0, K_1)$
K_2
$L_2=R_1$
$R_2=L_1 \oplus f(R_1, K_2)$
K_n
$L_{15}=R_{14}$
$R_{15}=L_{14} \oplus f(R_{14}, K_{15})$
K_{16}
PREOUTPUT
$R_{16}=L_{15} \oplus f(R_{15}, K_{16})$
$L_{16}=R_{15}$
INVERSE INITIAL PERM
OUTPUT

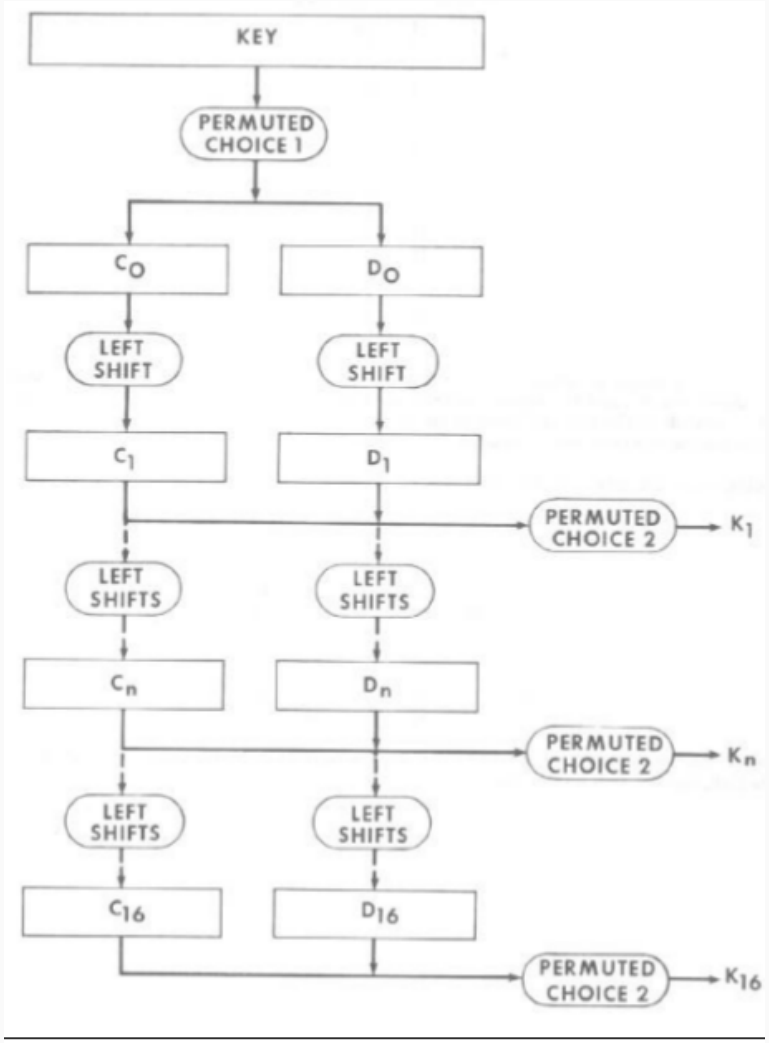
la function f



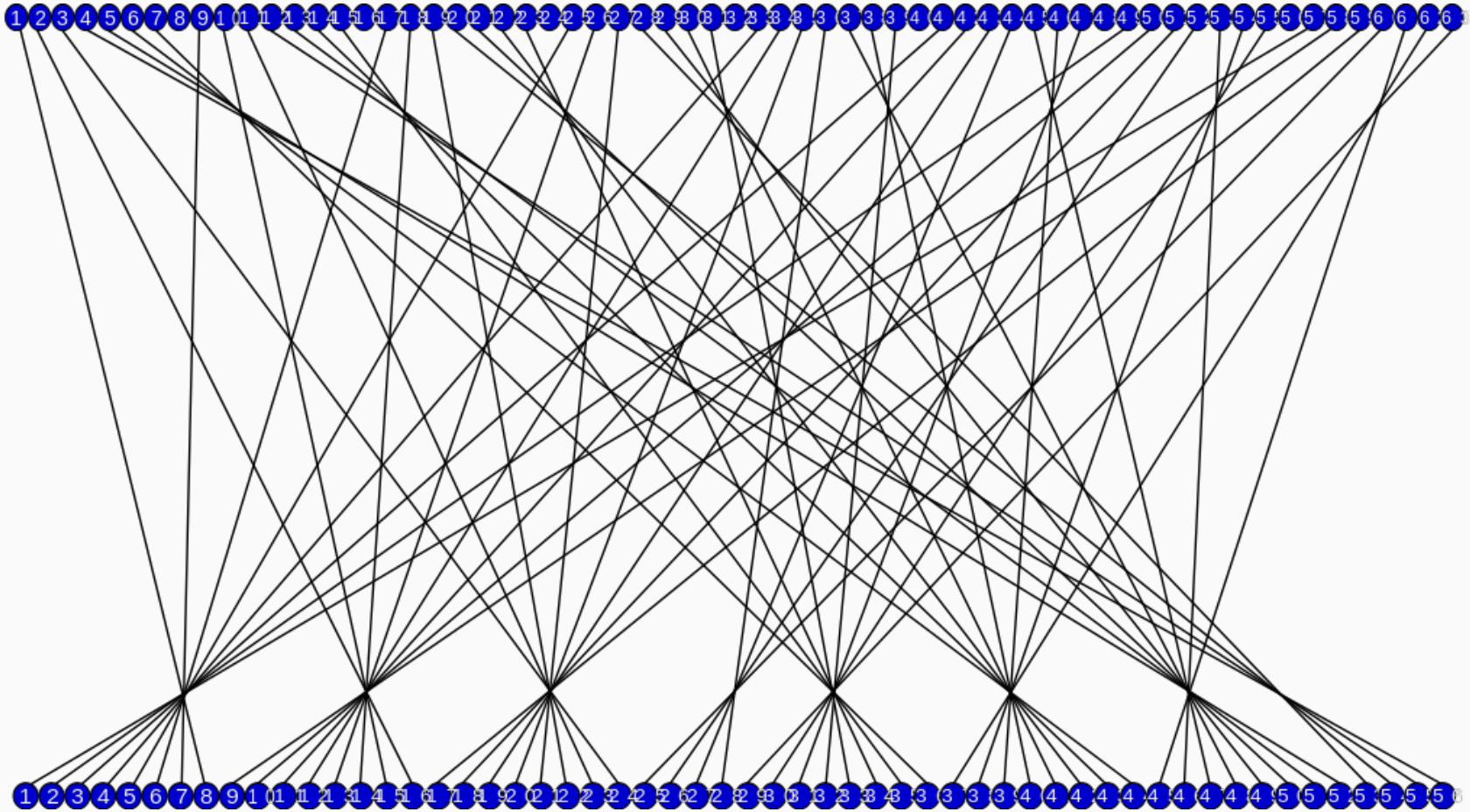
taille des donnes - function f



derivation de cle



derivation de cle - function pc1



Voyez vous un probleme ?

source: *Constantes du DES — Wikipédia*

controverse a propos du des

- suprenament efficace et robuste
- Optimisation des sbox (cryptanalyse differentielle 95')
- Key size = 64 bits

brute force du des

gagnant du concour DES Challenge II

brute force du des

gagnant du concour DES Challenge II

- 1998 - 'EFF DES cracker' - 250.000$
- 64 microchips par carte
- 29 cartes par serveur
- 6 serveurs
- Key size = 64 bits
- 90 Milliards de clef DES par seconde

total brute force : 9 jours

brute force du des

- 2006 - copacabana
- FPGA
- 10.000$

total brute force : qq jours

brute force du des

total brute force : moin d'un jours ...

des et aes - fonctionnement

http://people.eku.edu/styere/Encrypt/JS-DES.html

http://people.eku.edu/styere/Encrypt/JS-AES.html

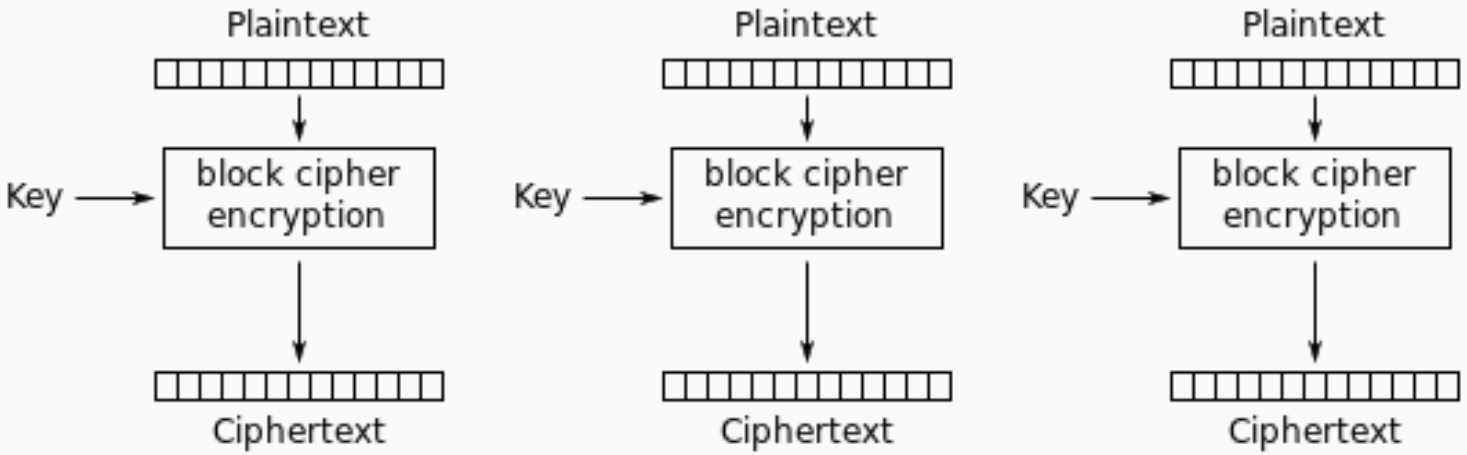
modes d'opérations

chiffrement par bloc: vocabulaire pourris

/!\Warning /!\

Malgré son nom un chiffrement par bloc n'est pas une méthode de chiffrement, c'en est seulement un brique élémentaire.
Pour créer une méthode chiffrement a partir d'un chiffrement par bloc il faut lui adjoindre un mode d'opération.

ecb mode 'electronique code book'

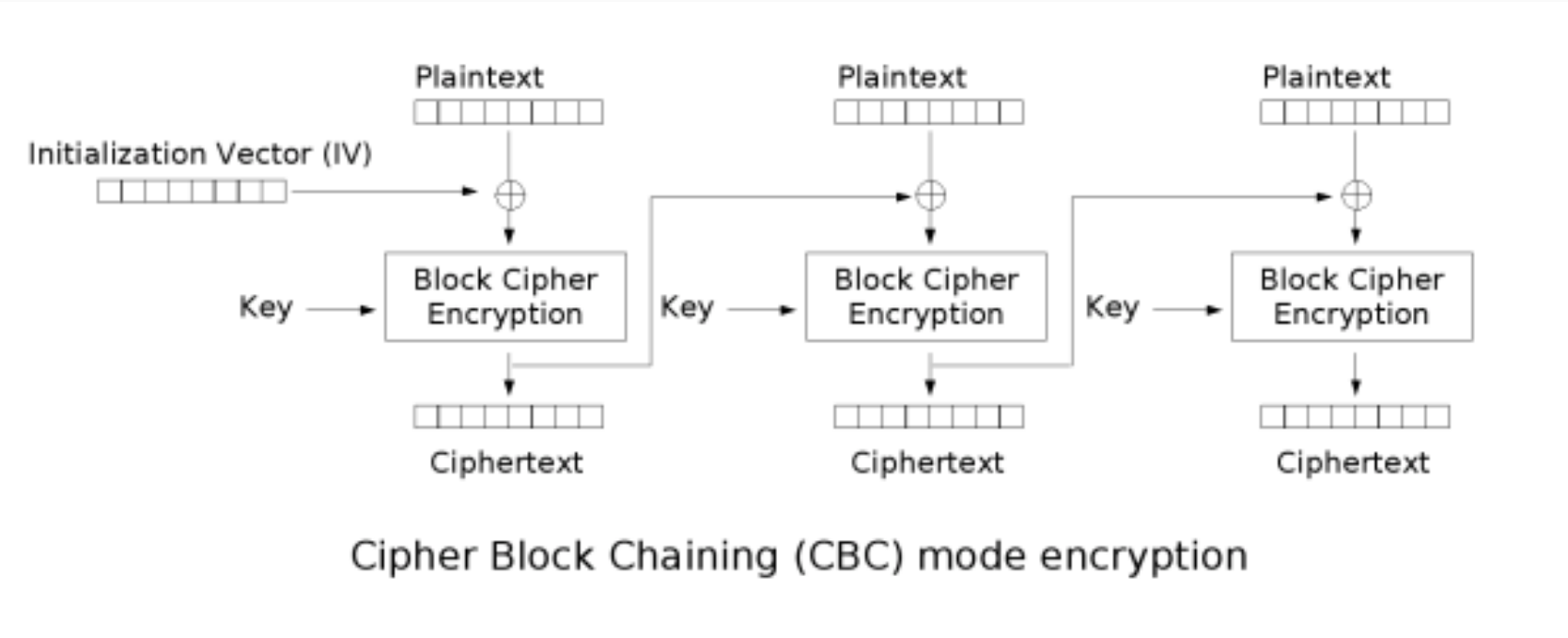


Electronic Codebook (ECB) mode encryption

ecb mode 'electronique code book'

- les motifs du clair ne sont pas masques
- le chiffre est manipulable
+ parallélisable
+ pas de propagation d'erreur
+ 'random read access'

cbc mode 'cipher block chaining'

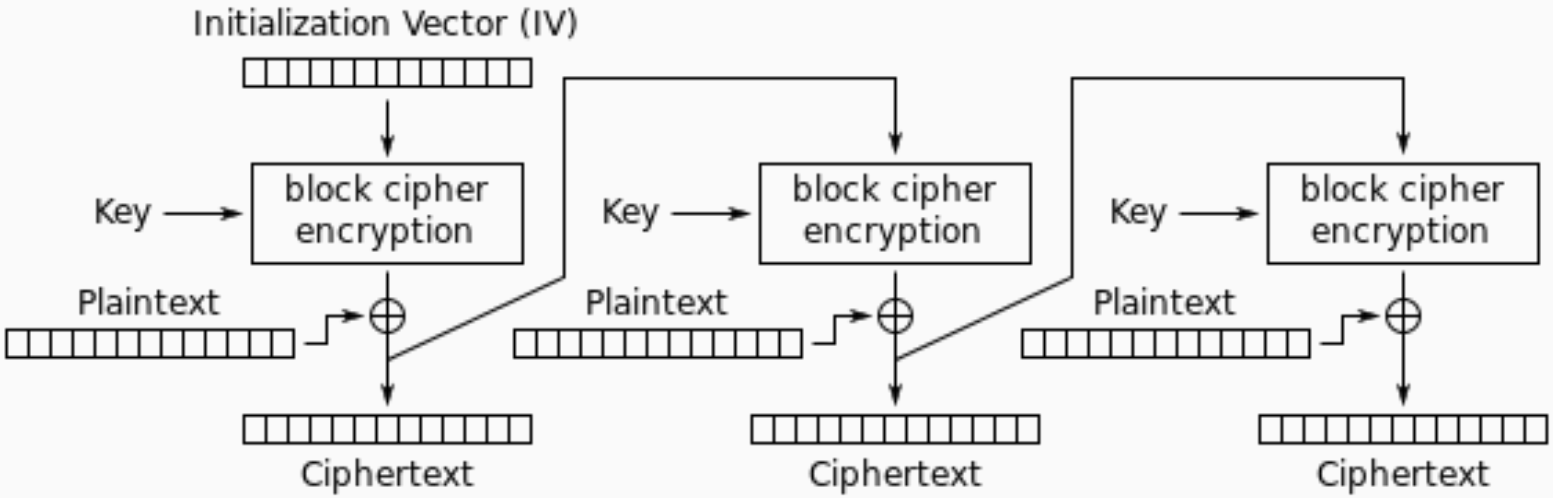


Cipher Block Chaining (CBC) mode encryption

cbc mode 'cipher block chaining'

+ les motifs du clair sont masques
+ le chiffre est difficilement manipulable
- non parallélisable
- propagation d'erreur
- si l'IV est null, le premier bloc est constant
+ 'random read access'

cfb mode 'cipher feedback mode'



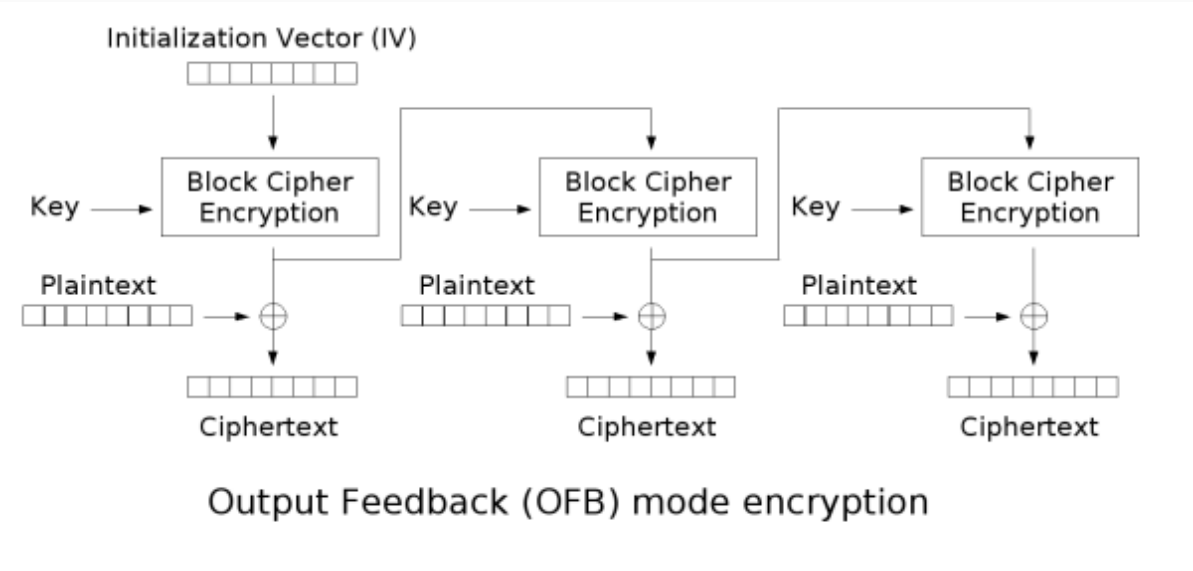
Cipher Feedback (CFB) mode encryption

cfb mode 'cipher feedback mode'

+ les motifs du clair sont masques
+ le chiffre est difficilement manipulable
- non parallélisable
- propagation d'erreur
+ l'IV passe par un chiffrement
+ 'random read access'

- chiffrement a flot (auto-synchrone)

ofb mode 'output feedback mode'



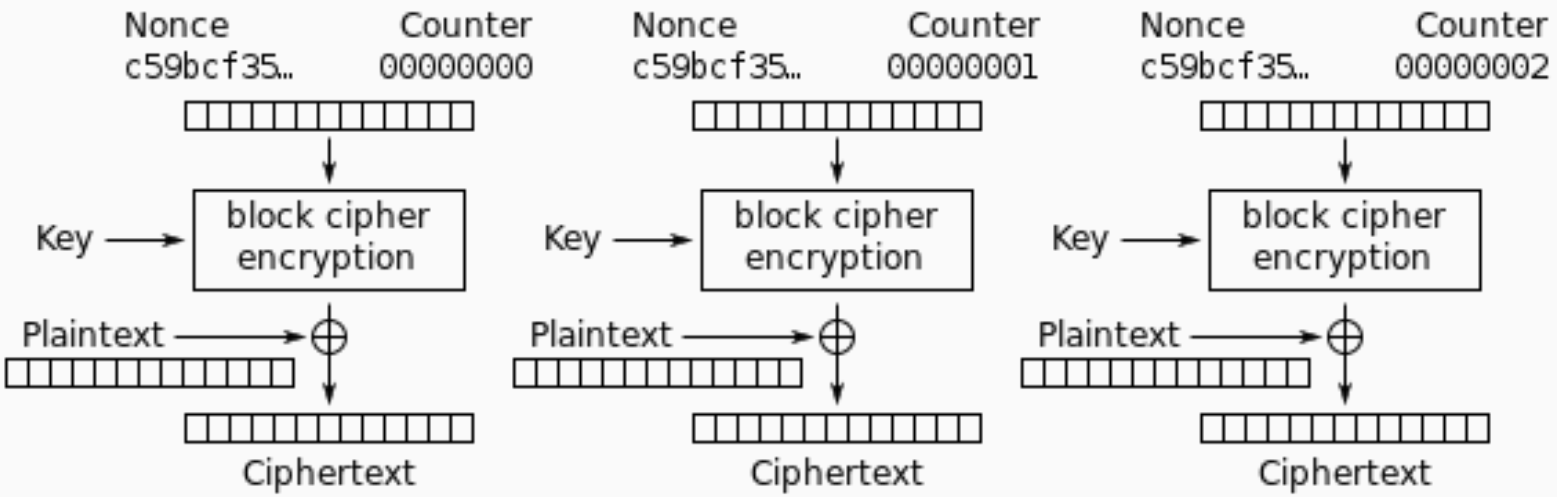
Output Feedback (OFB) mode encryption

ofb mode 'output feedback mode'

+ les motifs du clair sont masques
+ le chiffre est difficilement manipulable
- pas parallélisable, a moitie si pré-connaissance de l'IV
- propagation d'erreur
+ l'IV passe par un chiffrement
- pas de 'random read access'

- chiffrement a flot (synchrone)

ctr mode 'counter mode'



Counter (CTR) mode encryption

ctr mode 'counter mode'

  + les motifs du clair sont masques
  + le chiffre est difficilement manipulable
  + parallélisable
  + pas de propagation d'erreur
  + l'IV passe par un chiffrement
  + 'random read access'
- chiffrement a flot (synchrone)

mode de chiffrement

Le mode d'utilisation d'un chiffrement symétrique a bloc affecte:

- La vitesse de chiffrement/déchiffrement
- La malléabilité du chiffré
- Le déterminisme du chiffre
- Le visibilité de la structure du clair
- La capacité de récupérer partie d'un chiffre corrompue

questions a trancher

questions et développements

- Découvrir l'AES, GHOST etc
- Découvrir les attaques modernes
- Quel mode de chiffrement, -info additionnelles requises-
- le problème de l'intégrité
- le problème de l'authenticité