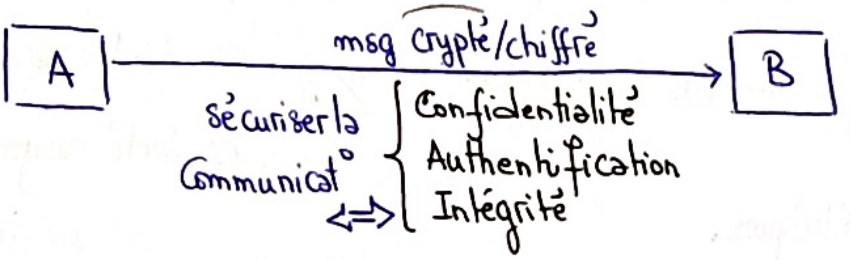
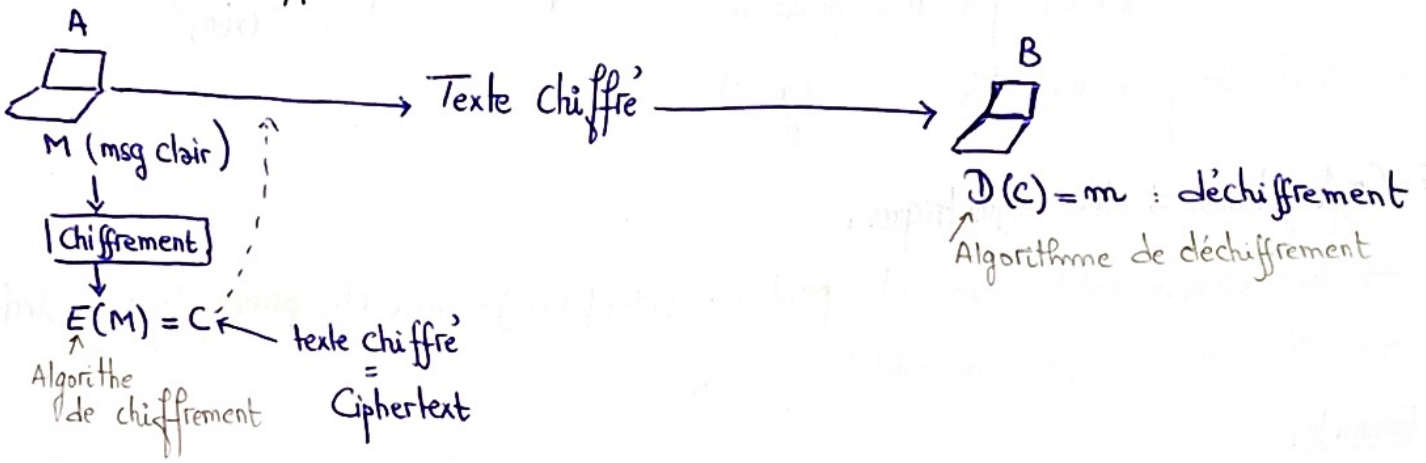
Chapitre 1. Définitions et Concepts de Base

› **Cryptographie ?** Science mathématique permettant d'effectuer des opérations sur un texte intelligible afin d'assurer une ou plusieurs propriétés de la sécurité informatique.



› Places du chiffrement : 3 niveaux possibles → liaison, Réseau, De bout en bout

Modèle de chiffrement :



Quelques exemples de chiffrement.

① Chiff. de **Cesar** : (vulnérable)

↳ se repose sur une clé k qui est le nbre de décalage

Ex. : A --(+3)--> D

② Chiff. de **Vigenère** :

↳ la clé est une chaîne

Ex. : m = 'RARE'
+
k = 'AREB' → on décale selon la position d'apparition des lettres du mot k
=
c = 'SSWG'

nbre de clés k possibles : $26 \cdot 26 \cdot 26 \cdot 26 = 26^4 \rightsquigarrow 26^m$ (m : nbre de lettres)

(de 4 lettres)

Principe de Kerckhoff ↓ Algorithme connu (public) + clé secrète

Vs

Principe de Shannon ↓ un chiffrement doit apporter de la confusion et la diffusion

> **Cryptosystème ?** c'est l'ensemble des clés possibles des textes clairs et chiffrés possibles associés à un algorithme donné.

On distingue 2 grandes **familles** de cryptosystèmes. → CS à **clés symétriques** / → CS à **clés asymétriques**

diapo 16 ↓ HR. du secret parfait

✱ Cryptosystèmes à clés symétriques.

→ clés identiques : clé de chiff = clé de déchiff

→ clé secrète

- 2 types → chiff. par substitution / → chiff par transposition → ⚠ { Block Cipher (DES, AES) / Steam Cipher (RC4) (XOR) }

Algorithmes.

- Nbre de clés pour n entités (à savoir) : $\frac{n(n-1)}{2}$

✱ Cryptosystèmes à clés asymétriques.

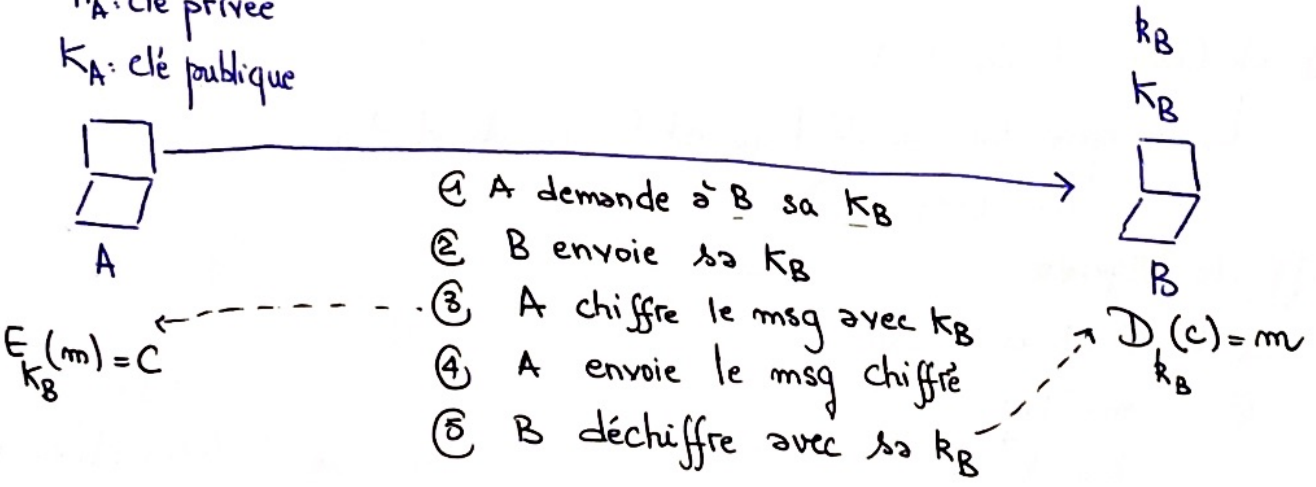
→ Pour chaque entité, une clé **publique** (diffusée), une clé **privée** (gardée secrète)

→ Nbre de clé pour n entités : $2n$

Exemple :

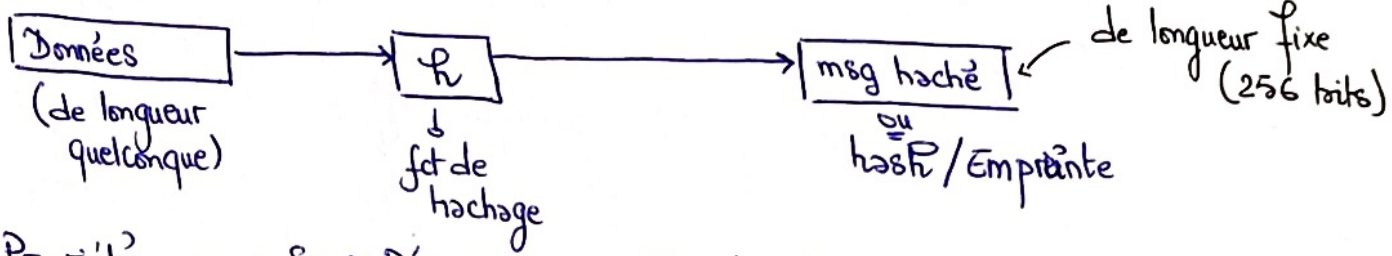
k_A : clé privée

K_A : clé publique



Algorithmes de Hachage.

* fonction de Hachage : c'est une fct qui n'a pas de réciproque



Propriétés
- Sans Réciproque ⟷ Unidirectionelle
- Résistance aux collisions : Pr x_1 et x_2 → $h(x_1) \neq h(x_2)$
- hash à longueur fixe.

Protocoles Cyptographiques.

Un Protocole est un ensemble de règles qui définit de quelle manière les participants à la communication doivent communiquer.

Chapitre 2. Chiffrement Symétrique

- chif. classiques
- Algo DES
- Algo AES
- Modes de chif.

Problèmes :

- il faut un échange au préalable de la clé.
- Dans un réseau à N entités, il faut distribuer $\frac{N(N-1)}{2}$ clés.

① Les Méthodes de chiffrement Classiques :

- **Par substitution Mono-alphabétique :**

→ la subs simple ⟺ subs mono alphabétique :

Pour chaque lettre de l'alphabet de base, on se donne une autre lettre utilisée dans le texte chiffré.

Ex : chiff de César (décalage).

- **Techniques d'attaques statistiques :**

→ on réalise une analyse statistique des textes chiffrés.

Et on détermine la fréq d'apparition des symboles

\+ Comparaison à celle dans les langues.

- **Substitution poly-alphabétique :**

Ex : chiff de Vigenère → c'est une amélioration de César

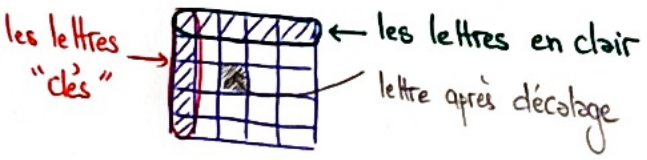
(Meya3malch mafs el pas de décalage)

Exemple : Texte clair : V I G E N E R E !

clé : B A C H E L I E R

Décalage :	1	0	2	7	4	11	8	4
chiffré :	W	I	I	L	R	P	Z	I

L'outil indispensable → "la table de Vigenère" (slides).



Autres Substitutions :

- Sub. homophoniques
- Sub. polygrammes → Au moyen d'une table (Système de Playfair)
  → Au moyen d'une transformation mathématique (Système de Hill)

Système de Playfair :

Matrice 5x5

Exemple : ① on découpe le texte clair en 2 lettres

Texte clair : CH IF FR E DE PL AY FA IR X

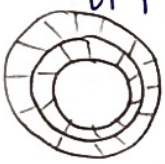
↑ on ajoute le X car le nombre de lettre est impair.

B	Y	D	G	Z
J	S	F	U	P
L	A	R	K	X
C	O	I	V	E
Q	N	M	H	T

→ Texte chiffré : VQ MR RI IZ TX AR DS RO KL

- Chiff de Sub à longueur de clé égale à celle du texte ⇔ clés jetables :
  → Pour éviter les attaques statistiques.
  ⇒ Solution :
  - A chaque fois, on génère une clé qui est une suite binaire parfaitement aléatoire.
  - Pour chiffrer le msg : msg ⊕ clé → msg chiffré
    ↑ ou exclusif (=1 si on a 0 et 1)

- Chiff par transposition :
  ↳ à base matricielle. (voir slide 19)



Exemple (Page 21)

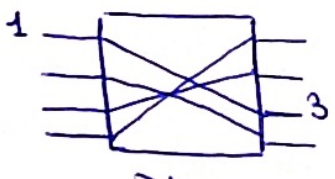
② L'Algorithme Data Encryption Standard (DES)

DES → produit de transpositions et substitutions nombreuses et compliquées pour une clé relativement courte.

→ Transposition à l'aide des P-Box (Permutation)
→ Substitution à l'aide des S-Box

Boîte de transposition : « P-Box »

Exemple de 4 bits :

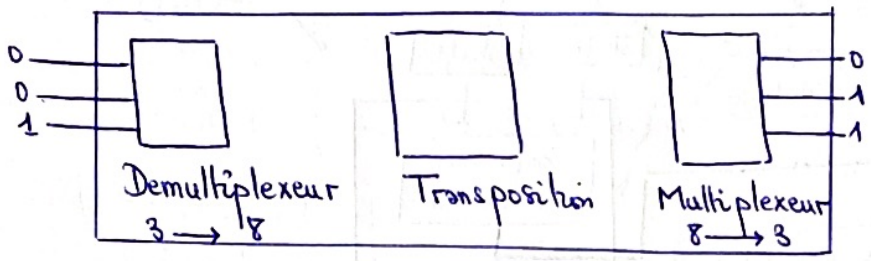


P-box

⇒ le bit 1 remplace le 3

Boite de substitution : « S-box »

Exemple :



Principe du DES :

1. Taille de bloc : 64 bits (8 octets)
2. clé de 64 bits à laquelle on enlève les 8 bits de parité ≃ 56 bits
3. Permutation initiale des blocs.
4. Découpage des blocs en 2 parties → Gauche / Droite
5. 16 itérations de permutation + substitution
6. Recollement des parties G et D puis permutation initiale inverse.

DES est basé sur 2 concepts. → Product ciphers / Feistel ciphers

Feistel Ciphers :

Texte clair de longueur 2t-bit (L_0, R_0)

↓ → processus de r-tours ; où $r >= 1$

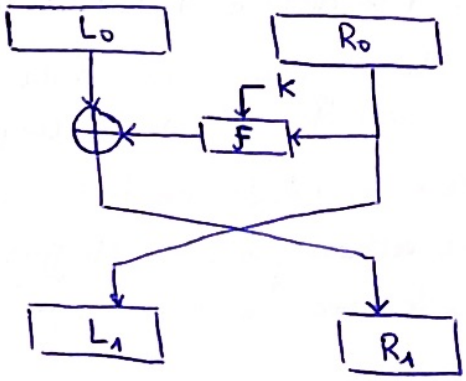
Texte chiffré (L_r, R_r)

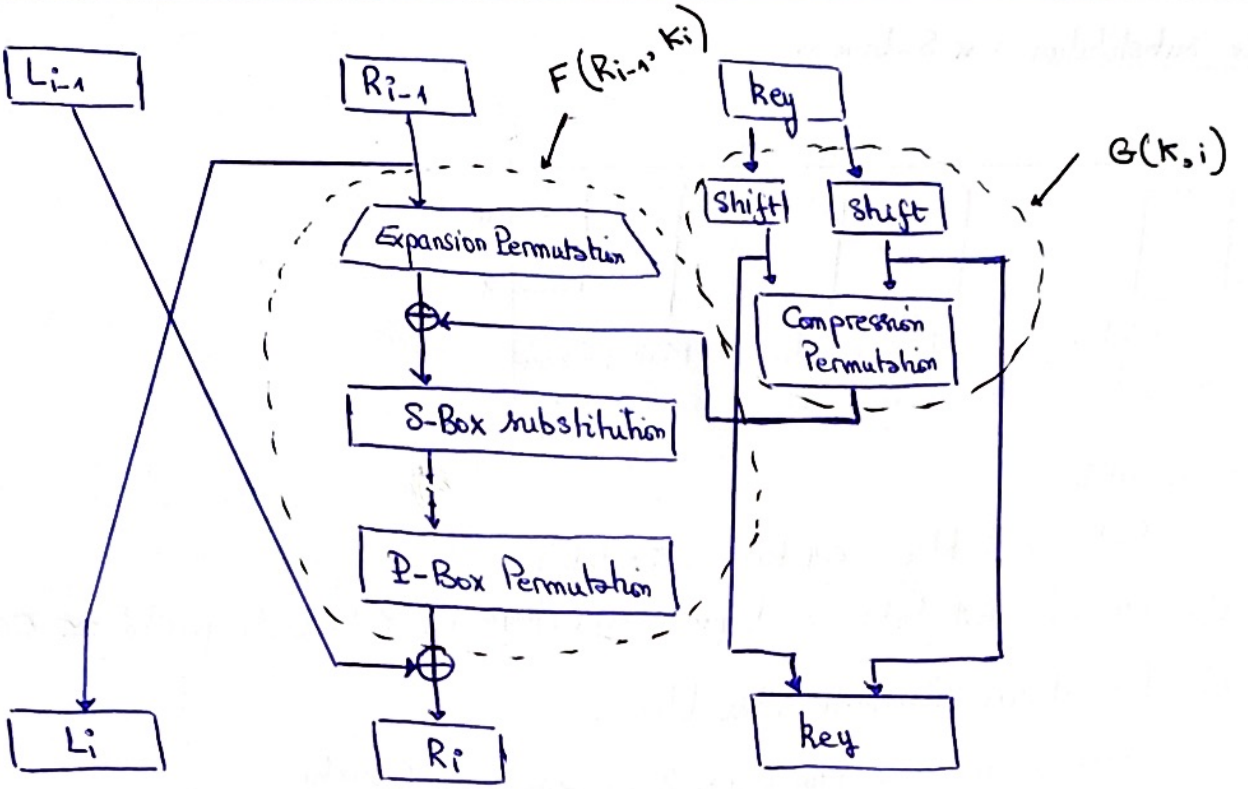
Pour $1 \leq i \leq r$:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(\widetilde{R_{i-1}, K_i})$$

K_i ← clé dérivée à partir de la clé de chiff K.





Les caractéristiques du DES.

- Tous les bits de C dépendent de tous les bits de M ⇒ effet d'avalanche
- faiblesses : → les S-box peuvent contenir des failles
  → la taille de la clé
  ⇓
  Solution : Utiliser le DES 3 fois en série, avec 2 ou 3 clés #.

Le 3DES.

→ Permet ↗ la sécurité du DES mais demande plus de ressources.

On a plusieurs types.

- DES-EEE3 : 3 chiff DES avec 3 clés #
- DES-EDE3 : 1 clé # pour chaque operation du DES (chiff, Déc, chiff)
- DES-EEE2 et DES-EDE2 : seulement la clé de chiff est #.

Attaques sur DES.

→ Cryptoanalyse différentielle. (on dispose de la boîte noire) 2^{47} textes clairs
→ Cryptoanalyse linéaire : Plus efficace mais moins pratique (Pas de boîte noire) 2^{43} couples.
→ Compromis temps-mémoire : on calcule une table immense qui contient toutes les versions possibles chiffrés de ce msg. lorsque l'on intercepte avec un msg chiffré, on peut déduire la clé utilisée

⑧ L'Algorithme Advanced Encryption Standard : AES (slide 53)

Algorithme de Rijndael : (symétrique)

- Taille de blocs = 128 bits
- Taille clé : 128 bits, 192 ou 256 bits

Structure de l'Algorithme :

↳ c'est un algo itératif, peut être découpé en 3 blocs :

① **Initial Round** = Add Round Key

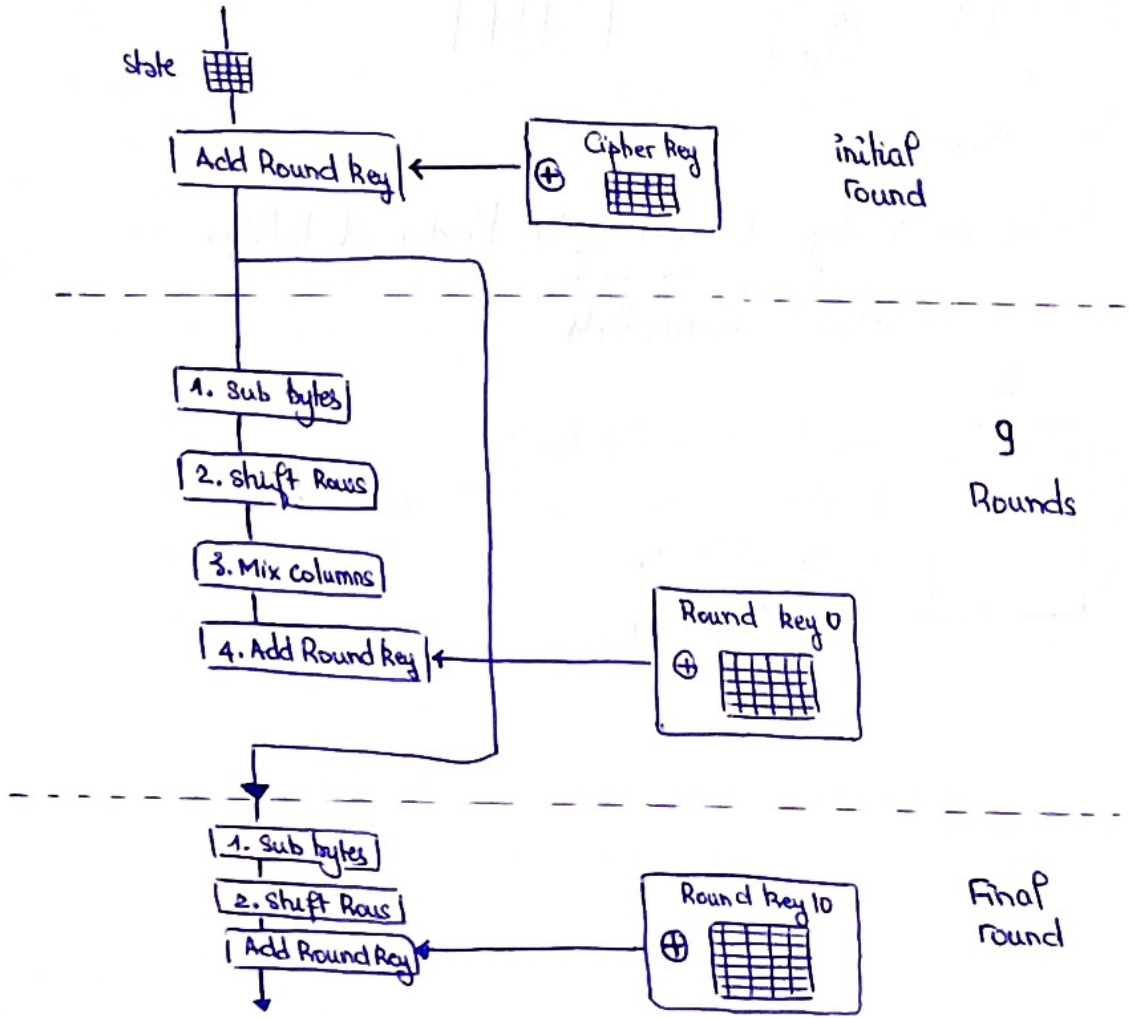
② **N Rounds** avec : { N=9 si clé = 128 bits ; N=11 si clé = 192 bits ; N=13 si clé = 256 bits

↓

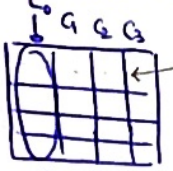
chaque itération, on a 4 opérations : { Sub bytes ; Shift Rows ; Mix Columns ; Add Round key

③ **Final Round** → Elle est identique à ② sauf pas de "Mix columns"

Exemple Pour clé = 128 bits ⟺ N=9 :



State ← Matrice de octets de taille 4×4



↳ Contient les 4 premiers octets

↑ (taille en octet du mot) = 32 bits

(4×4)×8 ← (khaler 3la 3ana 128 bits au total)

Nk → number of 32-bits words comprising the Cipher key.

Nk = 4, 6 ou 8.

1 octet = 8 bits = 2 chiffres hexa

Explication du AES :

I.R : Round 0

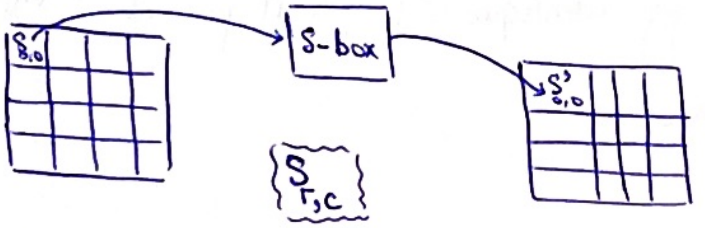
→ State (plain text) ⊕ (XOR) Cipher Key

⇓

Output = Matrice d'entrée de l'étape suivante

2ème étape : Rounds 1-9

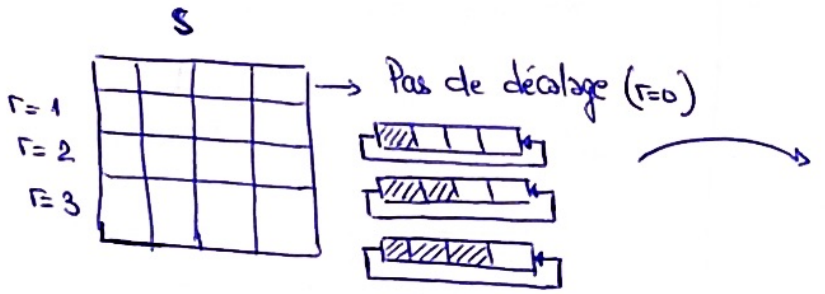
① Sub-bytes



② shift-Rows

↓ c'est un décalage des octets selon l'indice de la ligne

$$S'_{r,c} = S_{r,(c+r) \bmod 4}$$



③ Mix - columns :

↳ c'est une transformation linéaire : un produit matriciel utilisant les 4 octets d'une colonne.

Ex :

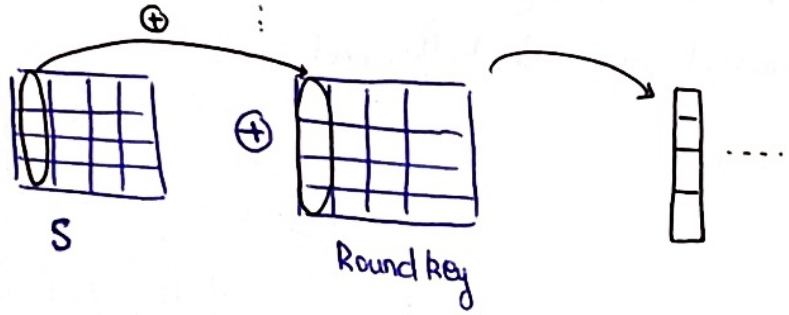
$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix}$$

④ Transformation Add Round key :

Prérequis : $X \oplus X = 0$

$0 \oplus a = a$

$X \oplus a \oplus X = a$



④ Les modes de chiffrement :

- Un mode d'opération est la manière de traiter les blocs en texte clairs et chiffrés au sein d'un algo de chiffrement par bloc

Electronic codebook Mode - ECB

Si on a $\begin{cases} X_1, X_2, \dots, X_n \text{ blocs de textes clairs} \\ k \text{ clé} \end{cases}$

Alors. $C_1, C_2, C_3 \dots C_n = E_k(X_1) \cdot E_k(X_2) \dots E_k(X_n)$

Caractéristique :

→ Limitation de la propagation d'erreur

→ la sécurité repose entièrement sur le secret de la clé

⇓

Solution. Enchaînement des blocs.

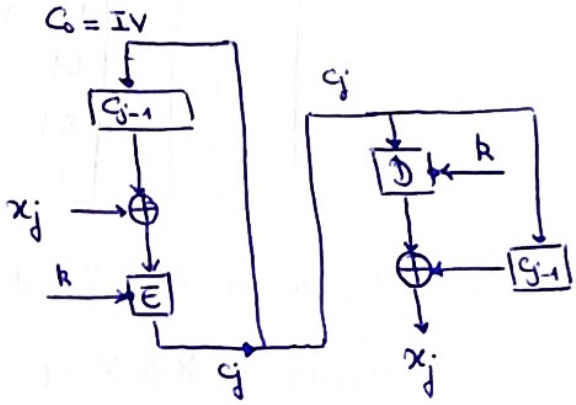
Vecteur d'initialization ? → bloc de bits utilisé pour initialiser un état de chif.
↳ doit être connu par le destinataire

Cipher Block Chaining Mode - CBC

$$C_j \leftarrow E_k\left(X_j \oplus C_{j-1}\right)$$

↓

déchiffrement : $X_j \leftarrow D_k(C_j) \oplus C_{j-1}$



Seul Inconvenient : Propagation d'erreur ?

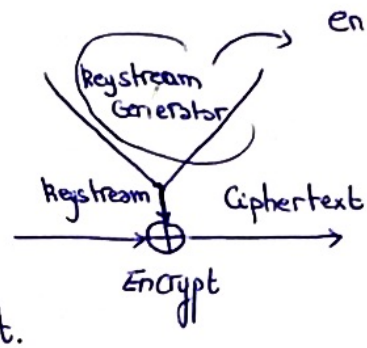
→ une erreur en X_j modifie tous les C_j qui suivent Mais ne se retrouve qu'en X_j après déchiff.

→ la perte ou ajout d'un bit C_i affecte tous les blocs qui suivent après déchiffrement.

Cipher-Feedback Mode - CFB

Chiffrement par flux (Stream Cipher)

$C_i \leftarrow m_i \oplus k_i$



- une erreur dans C_i n'affecte qu'un 1 bit de M_i.
- la perte ou l'ajout d'un bit de C_i affecte tous les bits suivants de M après déchiffrement.