

# PROTECTION DES DONNÉES VISUELLES : LE CHIFFREMENT MULTIMÉDIA

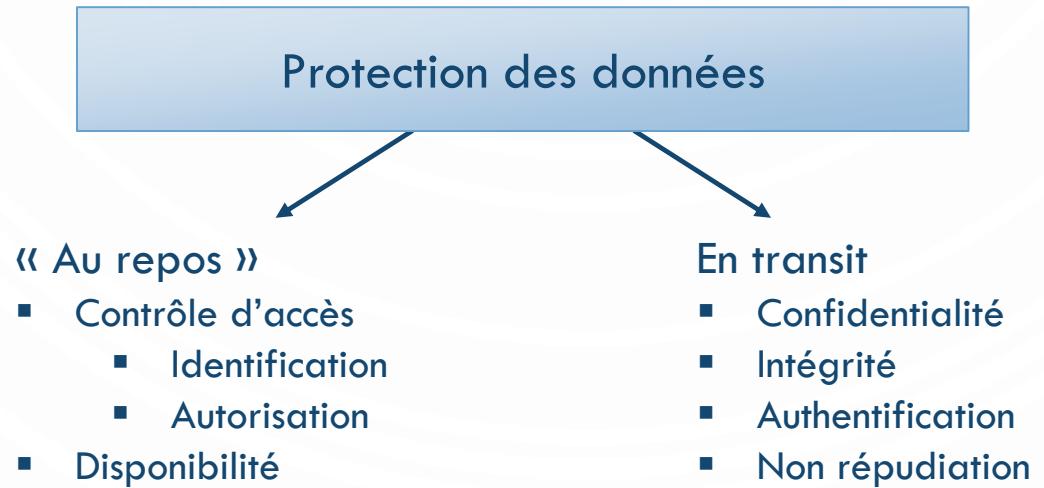
HMIN322 – CODAGE ET COMPRESSION (OCTOBRE 2019)

PAULINE PUTEAUX



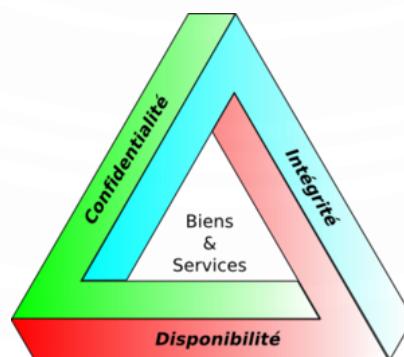
# BESOIN IMPORTANT EN SÉCURITÉ

- Essor du « cloud computing »
- De nombreuses menaces potentielles...



# PRINCIPES DE SÉCURITÉ

- **Confidentialité** : L'information n'est accessible qu'à ceux dont l'accès est autorisé
- **Authentification** : Chaque personne est bien celui qu'elle prétend être (légitimité)
- **Intégrité** : Le message envoyé n'a pas été altéré de manière volontaire ou involontaire
- **Non-répudiation** : Aucune des deux parties ne pourra assurer ne pas être l'auteur du message
- **Disponibilité** : L'accès à un service ou à des ressources est garanti



# PROTECTION DES DONNÉES VISUELLES

- D'après CISCO, les données visuelles = **80% du trafic Internet mondial** en 2019 (contre 67% en 2014).
  - Nécessité de proposer des méthodes efficaces pour protéger ces données visuelles !

# PROTECTION DES DONNÉES VISUELLES

- D'après CISCO, les données visuelles = **80% du trafic Internet mondial** en 2019 (contre 67% en 2014).
  - Nécessité de proposer des méthodes efficaces pour protéger ces données visuelles !
- De nombreux axes :
  - Tatouage
  - Stéganographie (insertion de données cachées)
  - Multimédia forensics (déttection de manipulations, identification de capteurs)
  - Biométrie
  - **Cryptographie**



Attention à ne pas confondre stéganographie et cryptographie !

# TATOUAGE



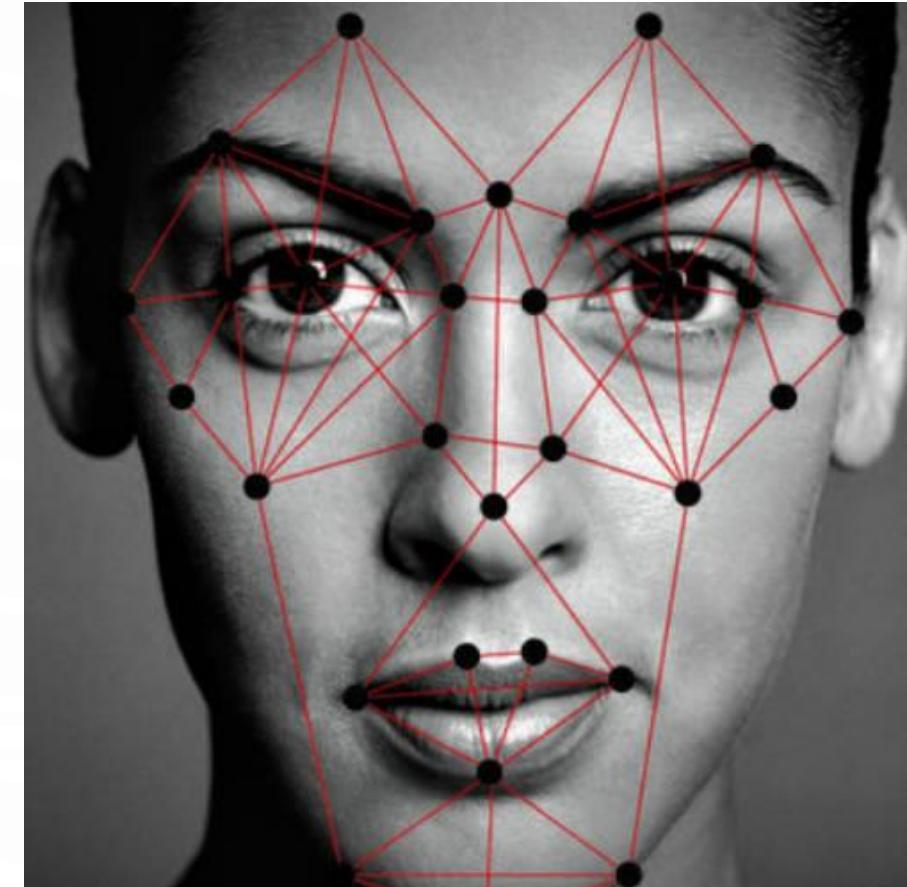
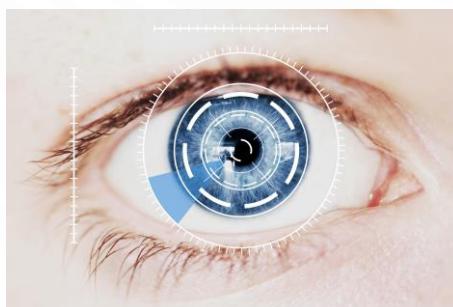
# STÉGANOGRAPHIE



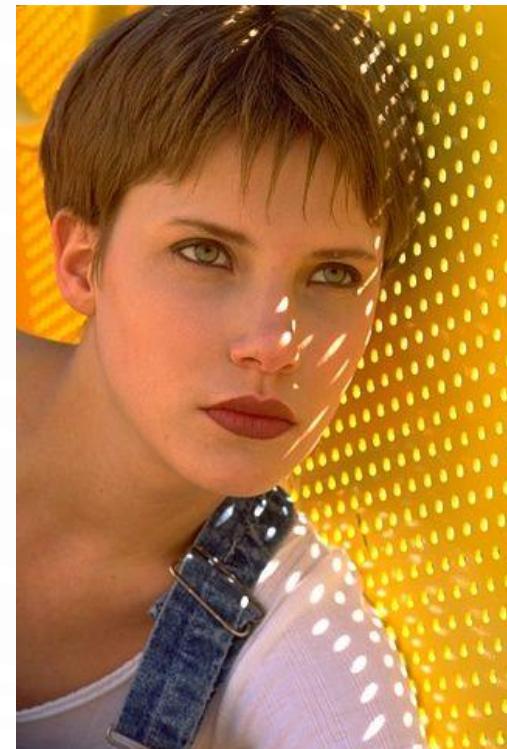
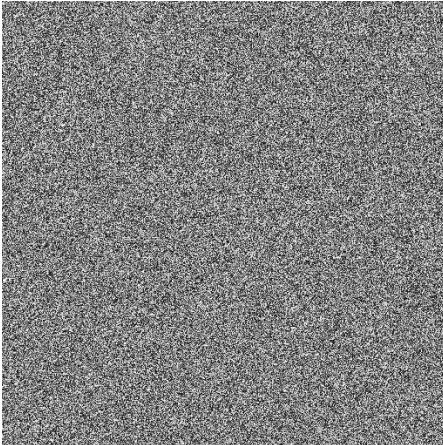
# FORENSICS



# BIOMÉTRIE



# CRYPTOGRAPHIE



# PLAN DU COURS

- Introduction à la cryptographie
  - Enjeux de sécurité
  - Rappels de mathématiques, terminologie et outils
- Méthodes de chiffrement classiques
  - Bref historique
  - Cryptographie moderne
- Conclusion
  - Ouverture : Analyse et traitement des images dans le domaine chiffré

# RAPPELS DE MATHÉMATIQUES

- **Anneau  $\mathbb{Z}/n\mathbb{Z}$**  : Anneau correspondant au calcul modulaire sur les restes des entiers dans la division par  $n$ .
- **Congruence** : Soit  $n \geq 2$  un entier fixé, on dit que  $a$  est congru à  $b$  modulo  $n$ , si  $n$  divise  $b - a$ .  
On note alors :  $a \equiv b \pmod{n}$ .
- **Propriétés algébriques** :
  - Si  $a_1 \equiv b_1 \pmod{n}$  et  $a_2 \equiv b_2 \pmod{n}$ , alors  $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$  et  $a_1 a_2 \equiv b_1 b_2 \pmod{n}$ .
  - Si  $a \equiv b \pmod{n}$ , alors  $ac \equiv bc \pmod{n}$  pour tout entier  $c$  et  $a^q \equiv b^q \pmod{n}$  pour tout entier  $q > 0$ .

# RAPPELS DE MATHÉMATIQUES

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Table d'addition dans  $\mathbb{Z}/6\mathbb{Z}$

x	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Table de multiplication dans  $\mathbb{Z}/6\mathbb{Z}$

Q : Calculez les tables d'addition et de multiplication dans  $\mathbb{Z}/7\mathbb{Z}$ .

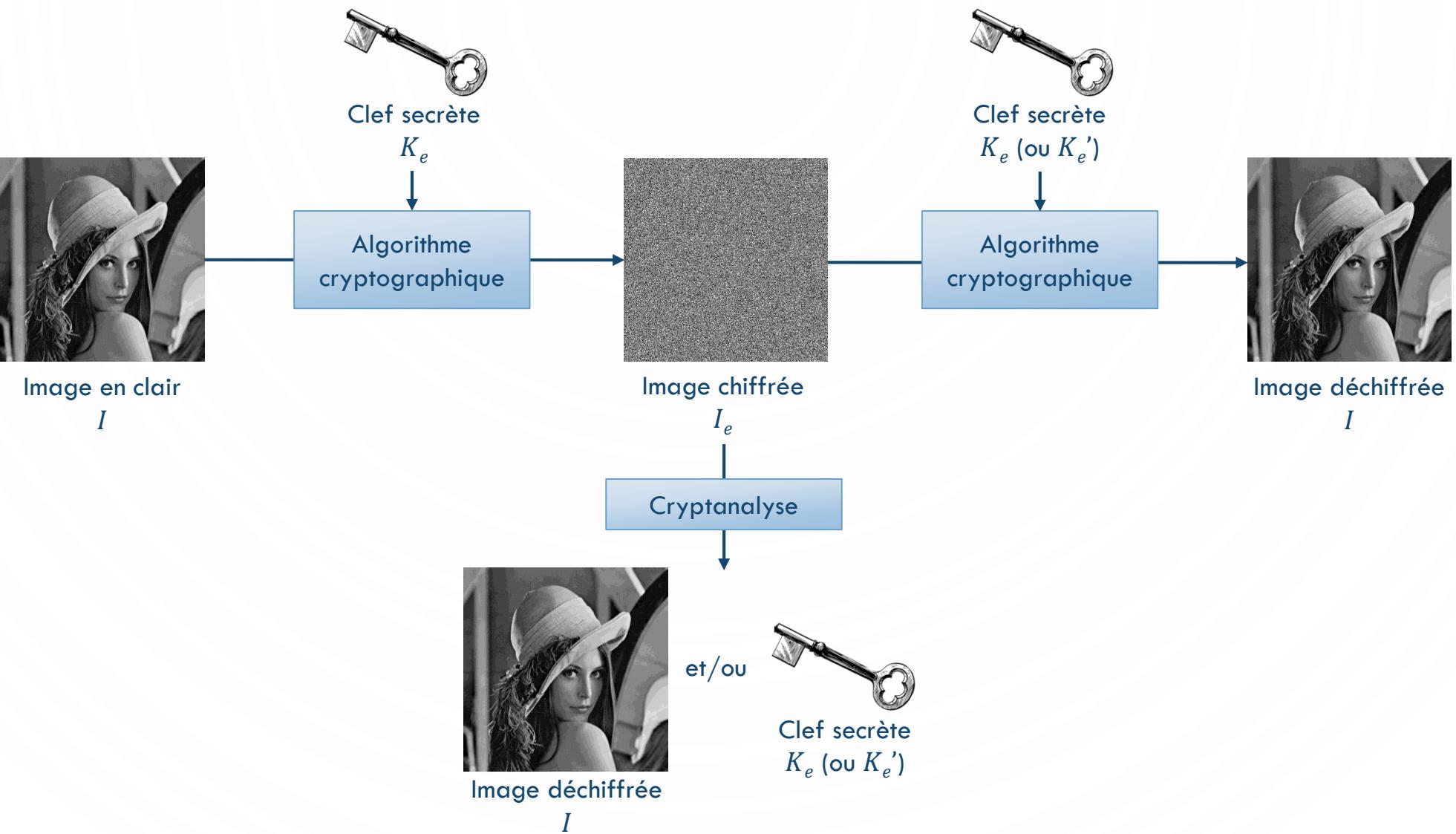
# TERMINOLOGIE

- **Cryptologie** : Science mathématique comportant deux branches : la **cryptographie** et la **cryptanalyse**.
- **Cryptographie** : Etude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle.
- **Chiffrement** : Transformation **à l'aide d'une clef** d'un **message en clair** en **message chiffré** (ou cryptogramme) pour le rendre incompréhensible.
- **Déchiffrement** : Action qui permet de reconstruire le **message en clair** à partir du **message chiffré**.
- **Cryptanalyse** : Etude des procédés cryptographiques dans le but de trouver des faiblesses, et en particulier, réussir à déchiffrer un **message chiffré sans connaître la clef de chiffrement** et/ou retrouver la **clef de chiffrement**



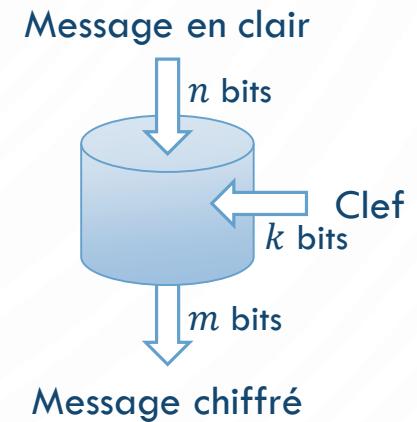
On ne parlera pas de « **cryptage** » ou de message « **(dé)crypté** » !  
On évitera aussi d'utiliser le mot « **coder** » pour dire « **chiffrer** »...

# TERMINOLOGIE



# CRYPTOSYSTÈME

- Les opérations de **chiffrement/déchiffrement** sont basées sur deux éléments fondamentaux :
    - Un **algorithme cryptographique** qui est une fonction mathématique réalisant ces deux opérations
    - Une **clef secrète**
  - Ces éléments sont appliqués au message à transformer
  - Un **cryptosystème** est défini comme l'ensemble :
    - Des **clefs** possibles (espace de clefs)
    - Des messages **clairs** possibles
    - Des messages **chiffrés** possibles
- } associés à un algorithme donné



# PRINCIPE DE KERCKHOFFS

- Aucun secret ne doit résider dans l'algorithme cryptographique utilisé : **tout réside dans la clef !**
  - « La sécurité ne doit pas dépendre de tout ce qui ne peut pas être facilement changé. »
  - Pour un algorithme : **secret  $\neq$  robustesse**
- Sans la clef, il doit être impossible de retrouver le message clair à partir du chiffré.
- Si on connaît la clef, on doit pouvoir déchiffrer le chiffré sans problème.



Auguste Kerckhoffs, *La cryptographie militaire*, Journal des sciences militaires, vol. IX, pp. 5–38, jan. 1883, pp. 161–191, févr. 1883.

# ALGORITHME PUBLIÉ VS SECRET

## ALGORITHME PUBLIÉ

- Possible d'évaluer la sécurité de manière fiable
- Empêche les backdoors cachées par les concepteurs
- Grand nombre d'utilisateurs = Prix réduit + performance élevée
- Pas besoin de protection contre le reverse engineering
- Implémentations logicielles
- Standardisation locale et internationale

## ALGORITHME SECRET

- La cryptanalyse doit inclure la récupération de l'algorithme
- Petit nombre d'utilisateurs = Plus petite motivation à essayer de casser l'algorithme
- Indisponible pour un autre pays

# NOTATIONS

## EN GÉNÉRAL

- $M$  : message en clair
- $C$  : message chiffré
- $K$  : clef secrète
- $E(\cdot)$  : fonction de chiffrement
- $D(\cdot)$  : fonction de déchiffrement
- On doit avoir :  $M = D(E(M))$

## POUR DES IMAGES

- $I$  : image en clair
- $I_e$  : image chiffrée
- $K_e$  : clef secrète
- $E(\cdot)$  : fonction de chiffrement
- $D(\cdot)$  : fonction de déchiffrement
- On doit avoir :  $I = D(E(I))$

# ENTROPIE

- **Entropie d'ordre zéro :** Si  $X$  est une variable aléatoire discrète, l'entropie de  $X$  est définie par :

$$H(X) = - \sum_x P(X = x) \log(P(X = x))$$

- **Entropie conditionnelle :** Incertitude qui reste sur  $X$  quand on connaît déjà  $Y$  :

$$H(X|Y) = - \sum_{x,y} P(X = x, Y = y) \log(P(X = x|Y = y)) \text{ avec } P(X = x, Y = y) = P(X = x|Y = y)P(y)$$

- **Entropie jointe :**  $H(X, Y) = H(Y) + H(X|Y)$

- Lien entre les entropies :  $H(X, Y) \leq H(X) + H(Y)$
- Si  $X$  et  $Y$  sont indépendantes :  $H(X, Y) = H(X) + H(Y)$



Claude E. Shannon, *A mathematical theory of communication*, Bell System Technical Journal, vol. 27, p. 379-423 and 623-656, 1948.

# ENTROPIE ET CRYPTOGRAPHIE

- L'incertitude liée à un système est  $H(M)$  : besoin de  $H(M)$  bits d'information pour retrouver le message
- Pour qu'un système cryptographique soit sûr, il faut et il suffit que :

$$H(M|C) = H(M)$$

**Q : Démontrez-le.**

# ENTROPIE ET CRYPTOGRAPHIE

- L'incertitude liée à un système est  $H(M)$  : besoin de  $H(M)$  bits d'information pour retrouver le message
- Pour qu'un système cryptographique soit sûr, il faut et il suffit que :

$$H(M|C) = H(M)$$

**Q : Démontrez-le.**

**R : On rappelle qu'un système est sûr si la connaissance de  $C$  (sans la clef) n'apporte aucune information sur  $M$ .**

$$H(M|C) = H(M) \Leftrightarrow H(M|C) + H(C) = H(M) + H(C)$$

$$\Leftrightarrow H(M, C) = H(M) + H(C)$$

**$\Leftrightarrow M$  et  $C$  sont indépendants**

$$\Leftrightarrow P(M|C) = P(M)$$

# PLAN DU COURS

- Introduction à la cryptographie
  - Enjeux de sécurité
  - Rappels de mathématiques, terminologie et outils
- Méthodes de chiffrement classiques
  - Bref historique
  - Cryptographie moderne
- Conclusion
  - Ouverture : Analyse et traitement des images dans le domaine chiffré

# BREF HISTORIQUE

- Depuis l'antiquité : Comment envoyer des messages sans que personne ne puisse les intercepter ?



**Tablette d'argile**

Irak – XVI<sup>e</sup> siècle av. J.-C.

Premier document chiffré connu  
Suppression des consonnes  
Modification de l'orthographe



**Scytale (ou bâton de Plutarque)**

Sparte – 404 av. J.-C.

Plus ancien dispositif de cryptographie militaire  
Chiffrement par **transposition/permuation**  
**Q : En quoi consiste la clef ?**

# BREF HISTORIQUE

- **Chiffrement de César** : Permutation circulaire des lettres de l'alphabet

- 1<sup>er</sup> siècle av. J.-C.
- Chiffrement par **substitution monoalphabétique**
- La longueur du décalage constitue la clef de chiffrement
- Généralement la clef est égale à 3 :

$$C[i] = E(M[i]) = M[i] + 3 \pmod{26}$$

$$M[i] = D(C[i]) = C[i] - 3 \pmod{26}$$



**Q : Quelle est la taille de l'espace des clefs ?**

**Q : Déchiffrez le message XQHPHWKRGHSDVYUDLPHQWVHFXULVHH.**

# BREF HISTORIQUE

## ▪ Chiffrement de Vigenère

- XVI<sup>e</sup> siècle
- Chiffrement par **substitution polyalphabétique**
- Une même lettre, suivant sa position, peut être remplacée par des lettres différentes.
- Clef = un mot ou une phrase (à répéter)

$$C[i] = E(M[i]) = (M[i] + K[i]) \pmod{26}$$

$$M[i] = D(C[i]) = (C[i] - K[i]) \pmod{26}$$



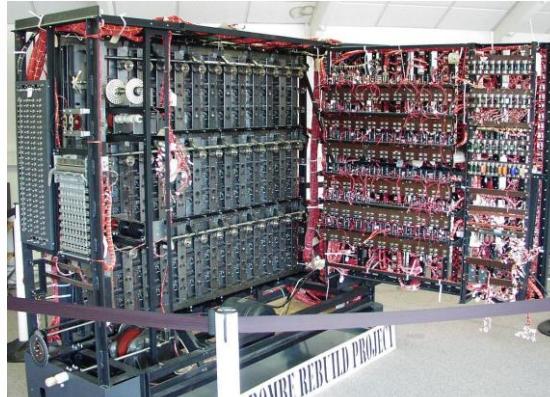
Q : Si on choisit d'utiliser un mot de  $k$  lettres comme clef, quelle est la taille de l'espace des clefs ?

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

# BREF HISTORIQUE

## ▪ Machine ENIGMA

- XX<sup>e</sup> siècle – Utilisée pendant la Seconde Guerre Mondiale
- Lettre pressée → circuit fermé → ampoule éclairée pour lettre codée
- Tour des rotors → changement de substitution
- Chiffrement réversible
- Clef : position initiale des rotors (changée chaque jour)
- Espace des clefs très grand (de l'ordre de  $10^{20}$ )
- Cryptanalyse par Alan Turing

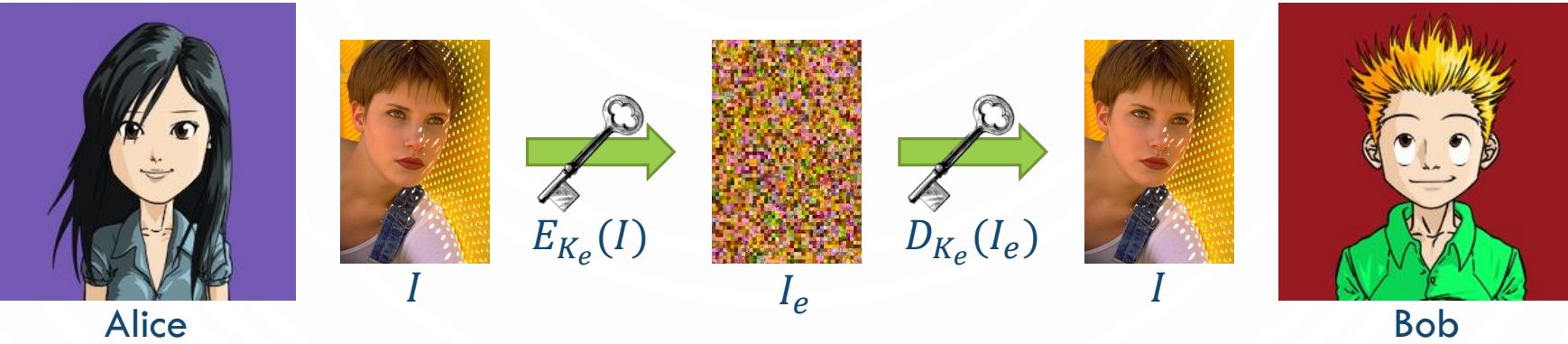


# PLAN DU COURS

- **Introduction à la cryptographie**
  - Enjeux de sécurité
  - Rappels de mathématiques, terminologie et outils
- **Méthodes de chiffrement classiques**
  - Bref historique
  - Cryptographie moderne
- **Conclusion**
  - Ouverture : Analyse et traitement des images dans le domaine chiffré

# CRYPTOGRAPHIE SYMÉTRIQUE

- La **cryptographie symétrique**, également dite **à clef secrète** permet à la fois de chiffrer et de déchiffrer des messages à l'aide d'une même clef secrète



- Deux catégories de méthodes :
  - Chiffrement **par flot** : traitement des données de longueur quelconque, sans besoin de les découper
  - Chiffrement **par bloc** : découpage des données à chiffrer en blocs de taille généralement fixe

# CRYPTOGRAPHIE SYMÉTRIQUE

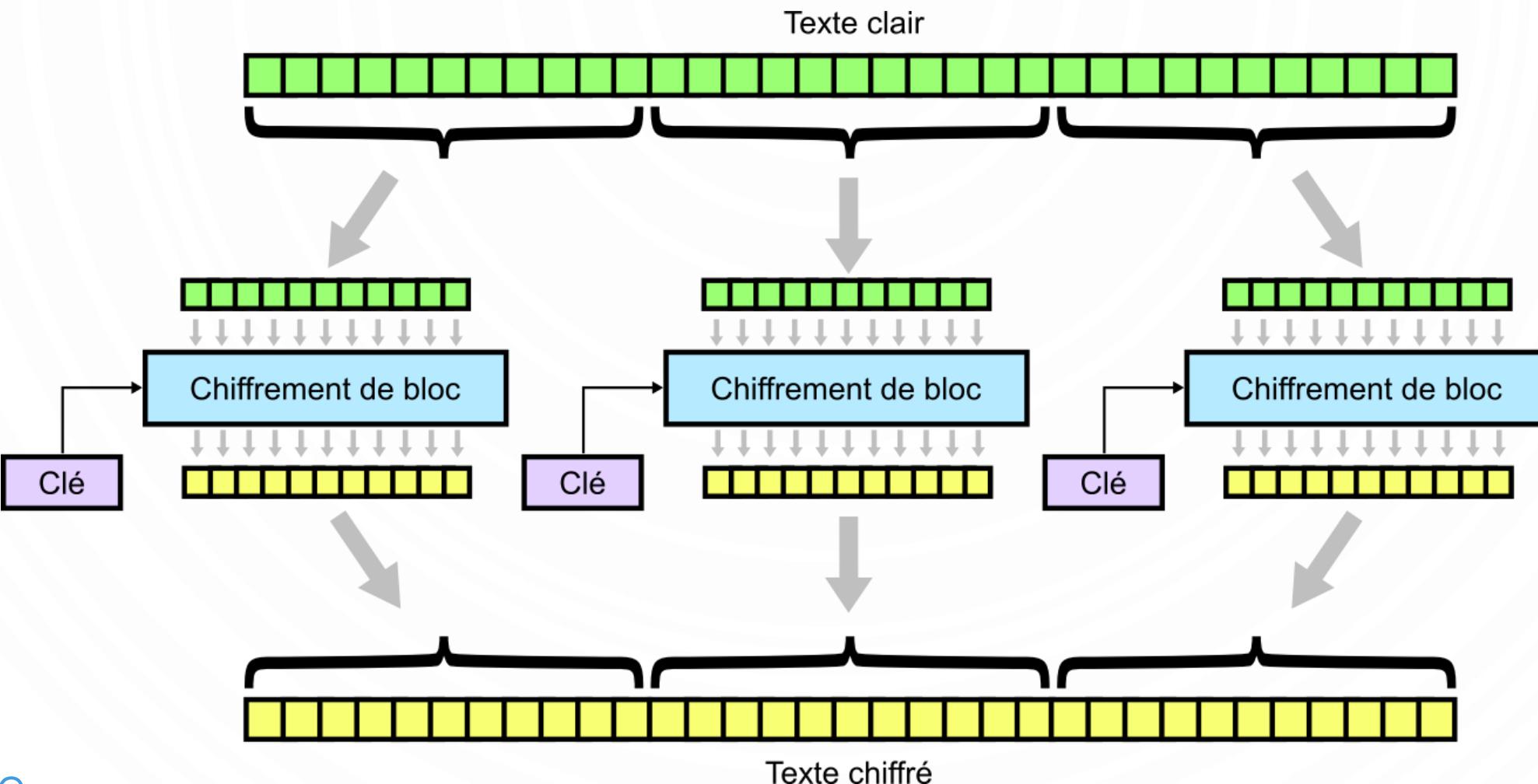
## ■ Caractéristiques

- Principe : Algorithmes basés sur des opérations de **transposition/permuation** et de **substitution** des bits du texte clair, en fonction de la clef
- Taille des clefs : (standard) 128 bits minimum
- Performances : Très rapide
- Distribution des clefs :
  - Très critique
  - Doit s'effectuer de manière sécurisée

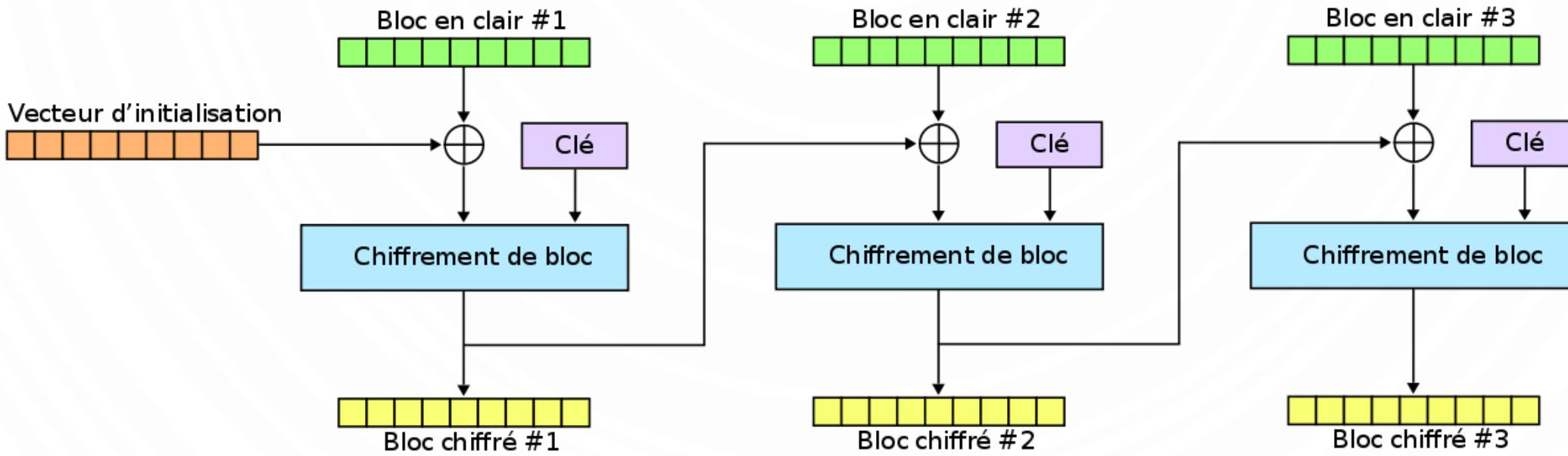
# MODES DE CHIFFREMENT

- Généralement défini pour le chiffrement par bloc (peut-être étendu au chiffrement de pixels)
- 5 modes de chiffrement principaux :
  - ECB (« Electronic CodeBook » - Dictionnaire de codes)
  - CBC (« Cipher Block Chaining » - Enchaînement de blocs)
  - CFB (« Cipher FeedBack » - Chiffrement à rétroaction)
  - OFB (« Output FeedBack » - Chiffrement à rétroaction de sortie)
  - CTR (« CounTeR » - Chiffrement basé sur un compteur)

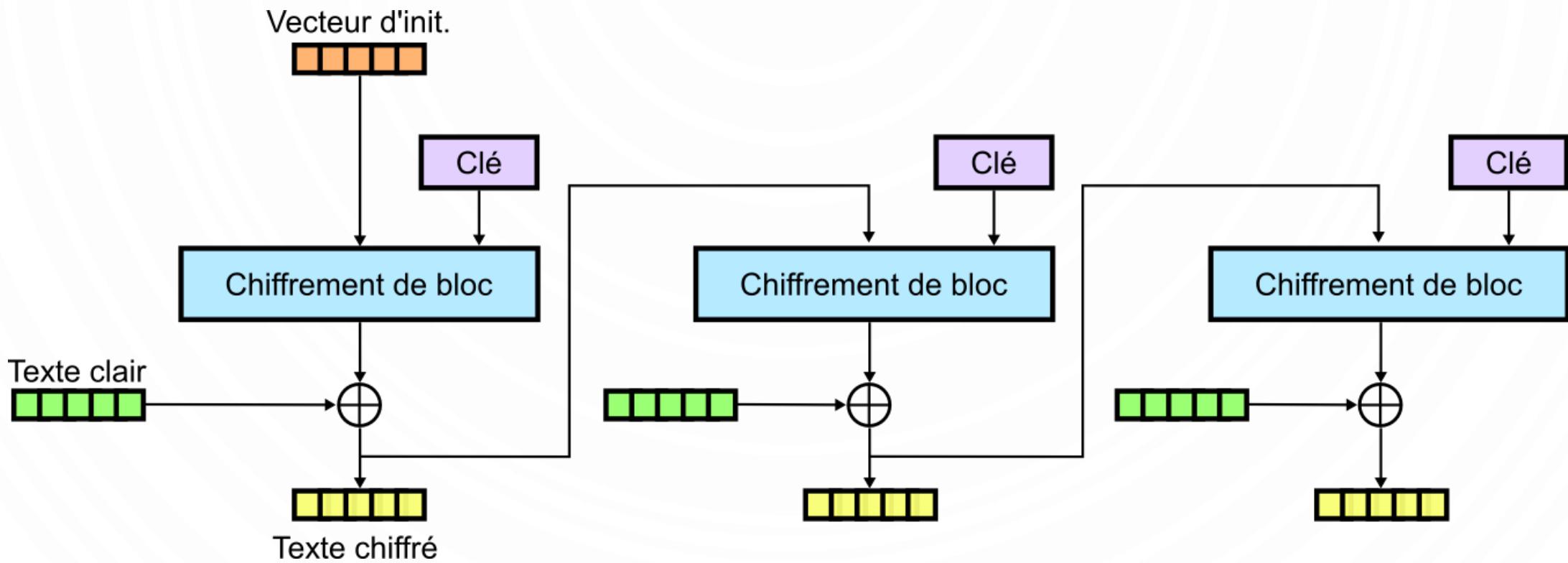
# ECB (« ELECTRONIC CODEBOOK »)



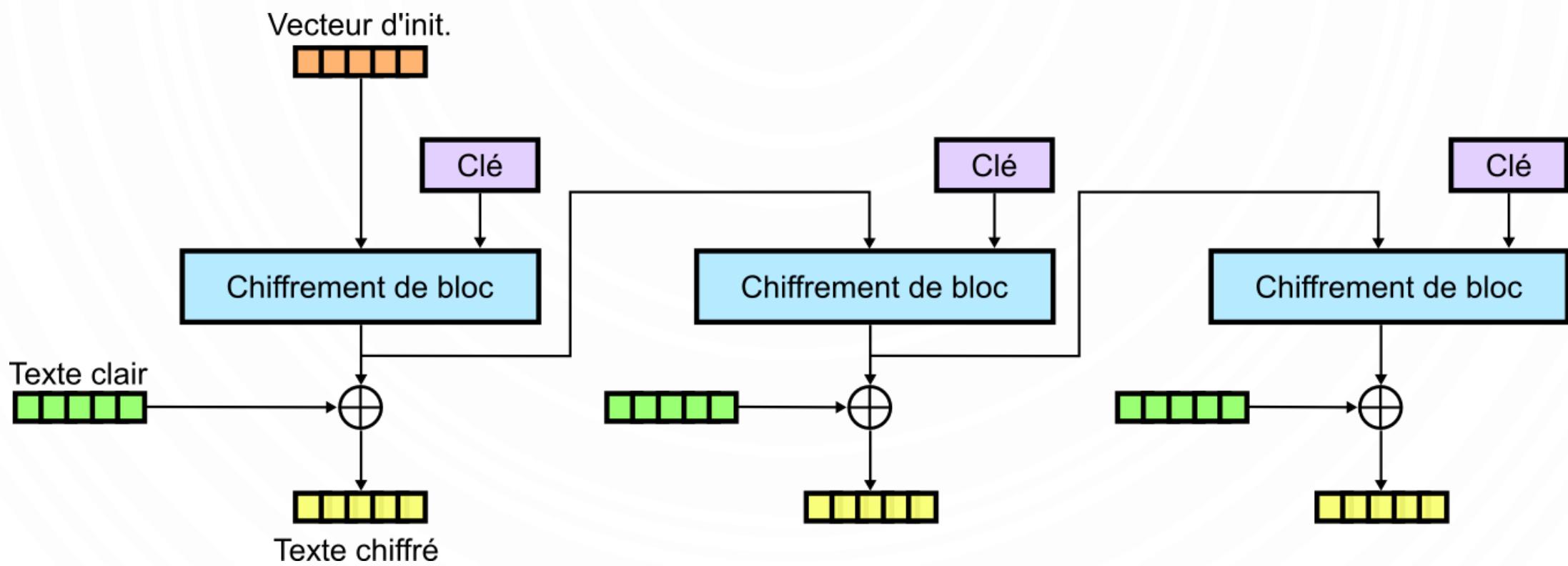
# CBC (« CIPHER BLOCK CHAINING »)



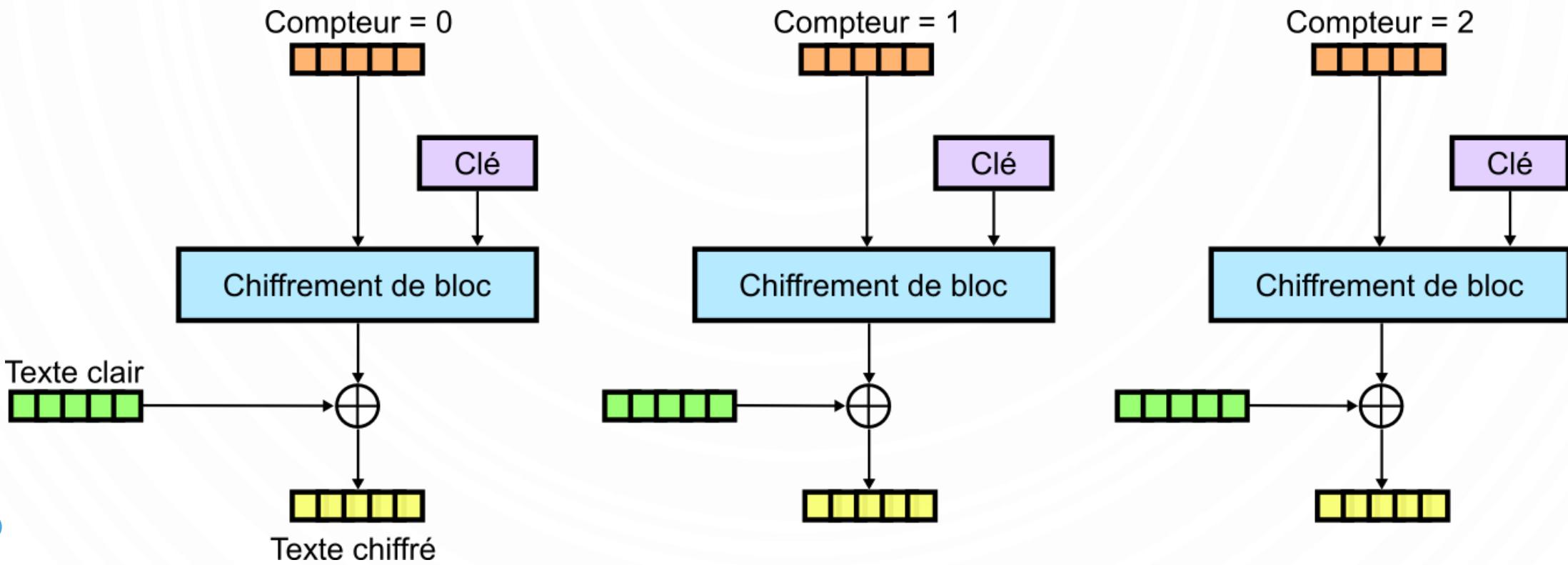
# CFB (« CIPHER FEEDBACK »)



# OFB (« OUTPUT FEEDBACK »)



# CTR (« COUNTER »)



# CHIFFREMENT PAR MÉLANGE

- Génération d'une **séquence pseudo-aléatoire** à l'aide d'un **PRNG**
- Clef utilisée comme graine d'initialisation du PRNG
- Utilisation de la séquence pseudo-aléatoire pour **permuter** les pixels (ou les bits) de l'image en clair



$$\sigma = \begin{pmatrix} p(0,0) & p(0,1) & p(0,2) & p(1,0) & p(1,1) & p(1,2) & p(2,0) & p(2,1) & p(2,2) \\ p(2,0) & p(1,2) & p(0,1) & p(2,2) & p(0,2) & p(0,0) & p(1,1) & p(1,0) & p(2,1) \end{pmatrix}$$

Q : Quel est le nombre de permutations possibles ?

# CHIFFREMENT XOR

- Génération d'une **séquence pseudo-aléatoire** à l'aide d'un **PRNG**
- Clef utilisée comme graine d'initialisation du PRNG
- Utilisation de la séquence pseudo-aléatoire pour modifier la valeur des pixels de l'image en clair : ou-exclusif entre l'image en clair et la séquence (**substitution**)

Clair	0	1	1	1	0	0	1	1
Séquence	1	0	1	0	0	1	0	1
Chiffré	1	1	0	1	0	1	1	0

**Q : Vérifiez que l'opération est symétrique.**

# CHIFFREMENT PAR XOR

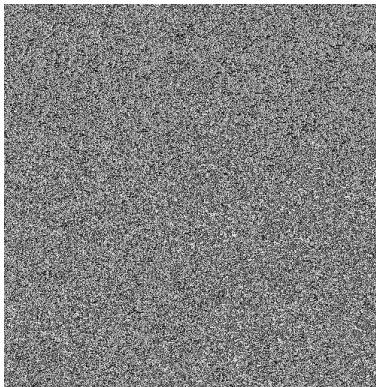
- Utiliser deux fois la même clef ?



$I_1$



$E_{K_e}(I_1)$



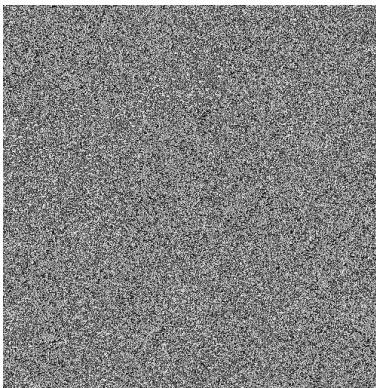
$I_{1e}$



$I_2$



$E_{K_e}(I_2)$



$I_{2e}$

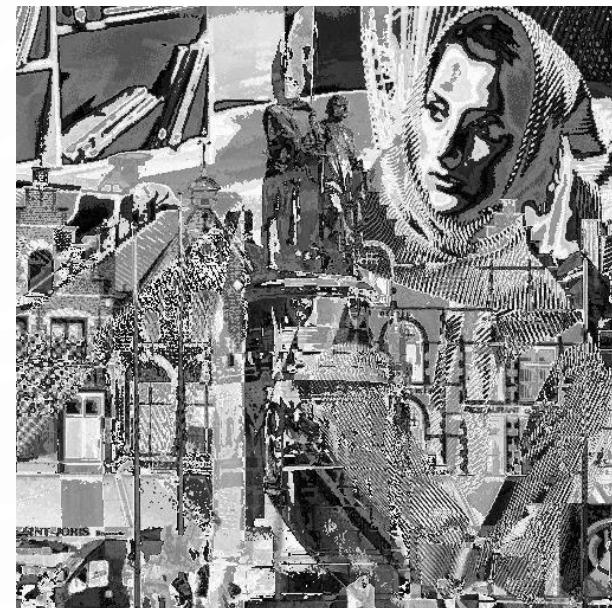


# CHIFFREMENT PAR XOR

- Utiliser deux fois la même clef ?



Négatif



Q : Comment expliquez-vous cette faiblesse ?

# CHIFFREMENT PARFAIT

- Chiffre de Vernam (1926) ou « masque jetable »
- Trois impératifs pour la clef :
  - Aussi longue que le message à chiffrer
  - Parfaitement aléatoire
  - Utilisée pour chiffrer **un seul message**, puis **détruite**
- Modèle théorique car très difficile à mettre en place...

**Q : Quelle est la probabilité d'apparition d'un niveau de gris dans l'image chiffré ?**

**Q : Quelle est la valeur de l'entropie mesurée dans l'image chiffrée ?**