Cryptographie Symétrique Moderne

Partie 2

Dr. Noureddine Chikouche

noureddine.chikouche@univ-msila.dz

https://sites.google.com/view/chikouchenoureddine

Plan du cours

- Advanced Encryption Standard (AES)
- Modes d'opérations de chiffrement

AES: Advanced Encryption Standard

- C'est un chiffrement symétrique par bloc.
- Connu sous le nom de Rijndael.
- conçu par deux cryptographe belges, J. Daemen et V. Rijmen.
- En 1998, NIST (National Institue of Standards and Technology) a organisé un concours de trouver un successeur à l'algorithme DES.
- Rijndeal a participé à cette compétition et a été choisi en octobre 2000.
- Standardisé par FIPS (*Federal Information Processing Standard*) en 2001.

AES: Advanced Encryption Standard

Il possède les propriétés suivantes:

- Plusieurs longueurs de clé sont possibles: 128, 192, ou 256 bits;
- Basé sur la structure réseau de substitution/permutation. Elle ne comprend qu'une série de transformations, permutations, sélections;

AES: Advanced Encryption Standard

- Notations:
  - Mot: ensemble de32 bits ou un vecteur de 4 octets.
  - Bloc: séquence de bits binaires comprenant l'entrée (input), la sortie (output), état (State), et clé de ronde (Round Key). Les blocs sont également interprétés comme des matrices d'octets.
  - Nb: nombre des colonne de la matrice du bloc. Pour l'AES, Nb = 4 (longueur des blocs est 32*4=128 bits)
  - Nk: nombre des colonne de la matrice de la clé de chiffrement. Pour AES Nk = 4,6 ou 8.
  - Nr: nombre de tournées (rondes).

AES: Advanced Encryption Standard

- **Nombre des rondes:**

Le nombre des rondes (ou cycles) dépend la taille de la clé.

	Taille de clé (Nk)	Taille de bloc (Nb)	Nbre de ronde (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

AES: Advanced Encryption Standard

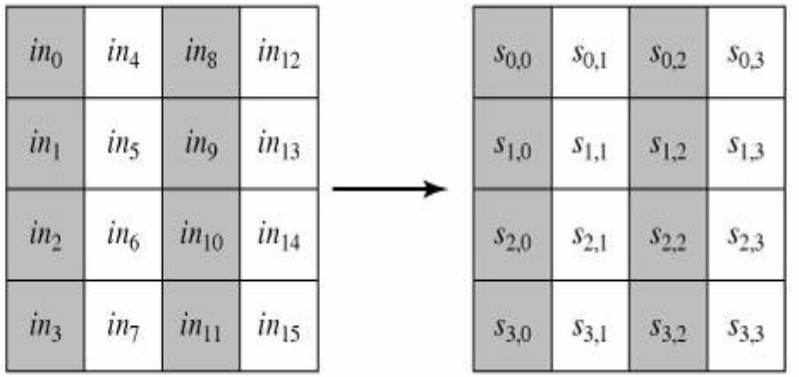
- Pour AES-128:
  - 128 représentant la taille de la clé.
  - Nb = 4; //Nombre des colonnes du block.
  - Nk = 4; //Nombre des mots dans la clé (un mot = 4 octet)
  - Nr = 10; //Nombre des tours (rondes)

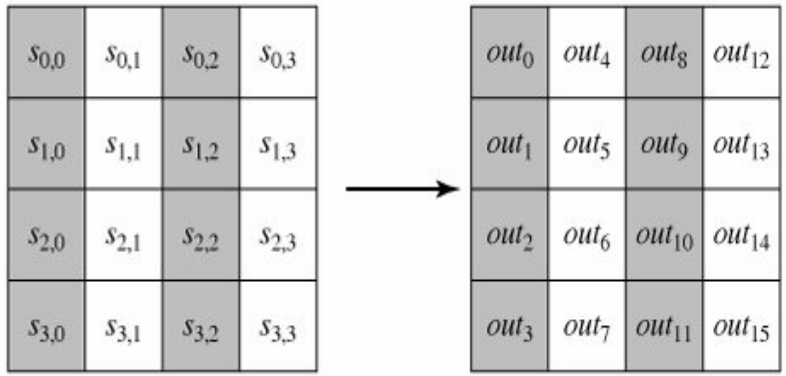
AES: Advanced Encryption Standard

- Chiffrement de bloc clair
- Extension de la clé
- Déchiffrement de bloc chiffré

Chiffrement

- Les matrices d'état (*State*) du bloc clair et le bloc chiffré ont 4 lignes et *Nb* colonnes.

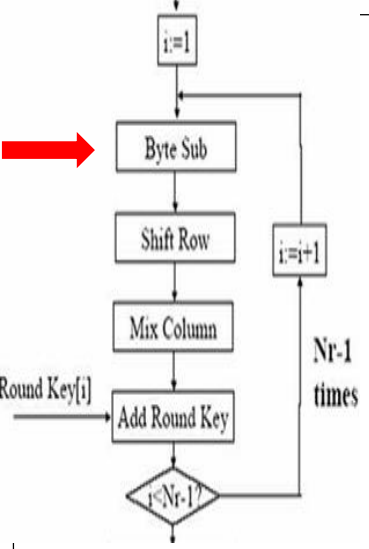




Chiffrement

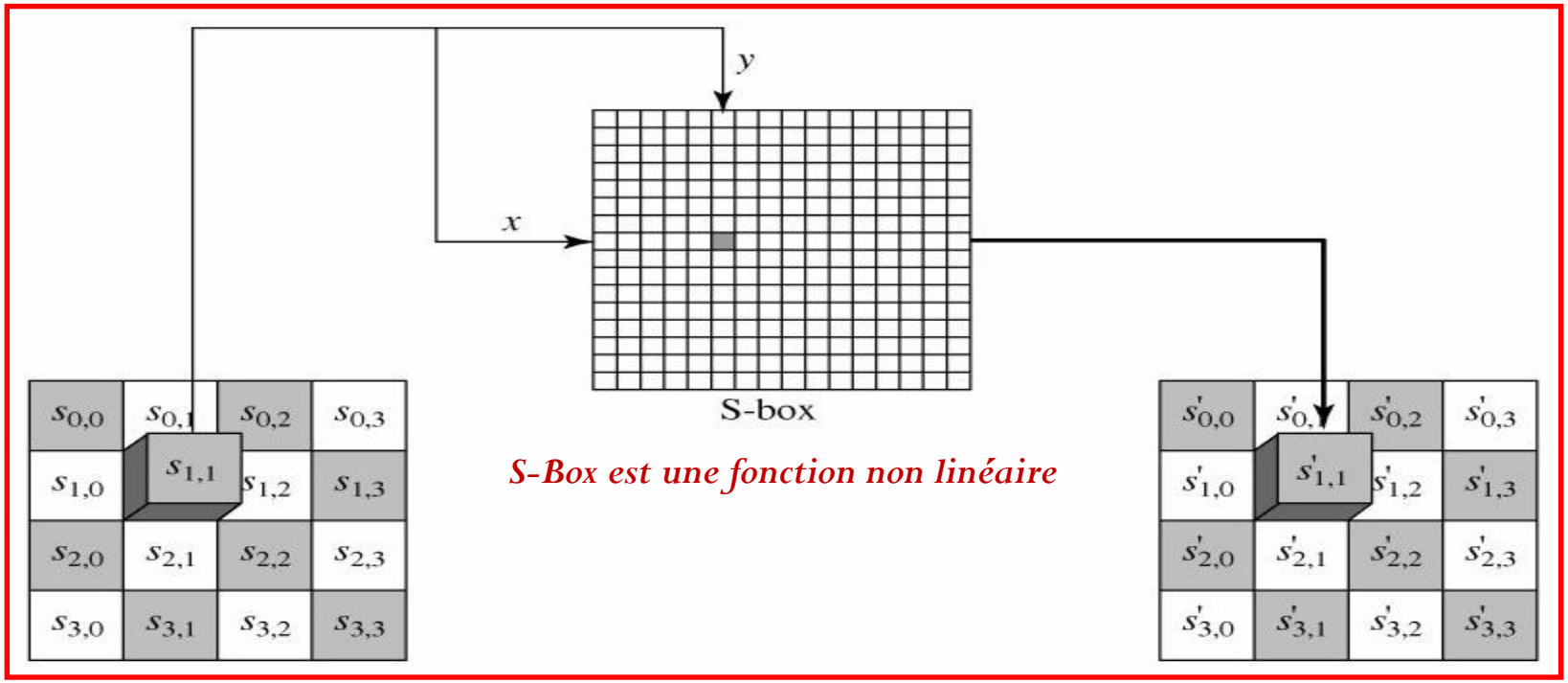
A chaque ronde, 4 transformations sont appliquées:

1) SubByte: **substitution** d'octets dans le tableau d'état
2) ShiftRow: **décalage** de rangées dans le tableau d'état
3) MixColumn: **déplacement** de colonnes dans le tableau d'état (sauf à la dernière ronde)
4) AddRoundKey: **addition** d'une "clé de ronde " qui varie à chaque ronde.



Chiffrement → SubByte

Les octets sont transformés en appliquant une *S-Box* inversible (afin de permettre un déchiffrement unique).



Chiffrement → SubByte

Exemple:

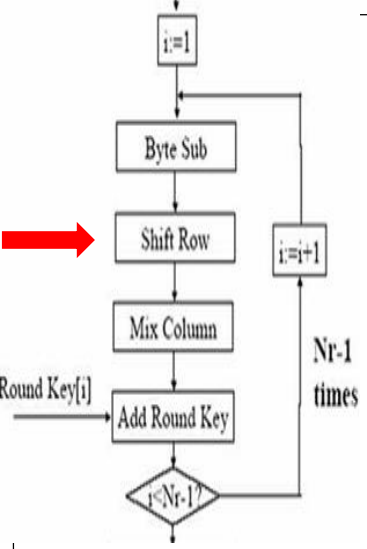
19

hex	y															
	0	1	2	3	4	5	6	7				b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5				2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0				af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc				f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a				e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

x

d4

S-BOX byte substitution table

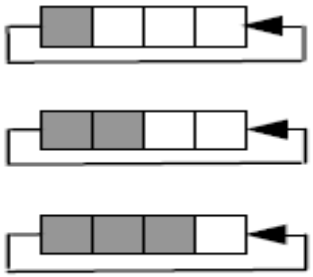


Chiffrement → ShiftRow

- La fonction ShiftRow modifie les lignes de la matrice (tableau *state*) en faisant certaines permutation circulaires.

s

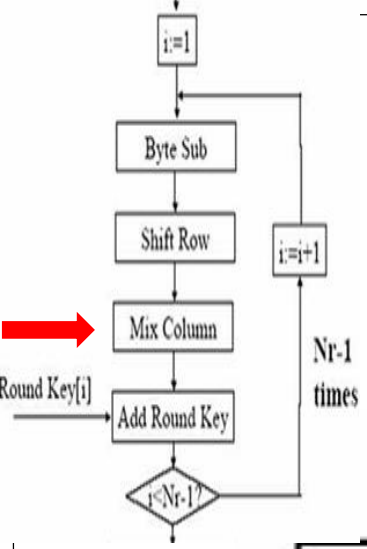
$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$



s '

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,1}$	$s_{1,2}$	$s_{1,3}$	$s_{1,0}$
$s_{2,2}$	$s_{2,3}$	$s_{2,0}$	$s_{2,1}$
$s_{3,3}$	$s_{3,0}$	$s_{3,1}$	$s_{3,2}$

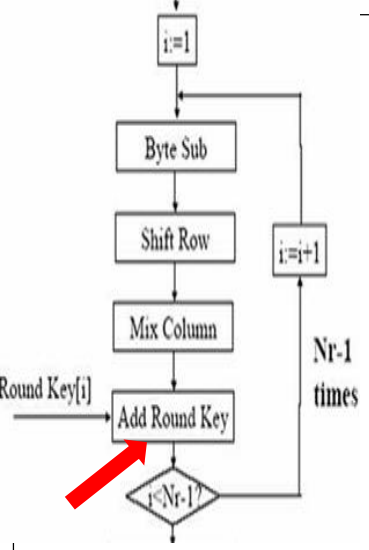
Chiffrement → MixColum



$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} \quad \end{bmatrix} = \begin{bmatrix} \quad \end{bmatrix}$$

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

$s'_{0,0}$	$s'_{0,1}$	$s'_{0,2}$	$s'_{0,3}$
$s'_{1,0}$	$s'_{1,1}$	$s'_{1,2}$	$s'_{1,3}$
$s'_{2,0}$	$s'_{2,1}$	$s'_{2,2}$	$s'_{2,3}$
$s'_{3,0}$	$s'_{3,1}$	$s'_{3,2}$	$s'_{3,3}$



Chiffrement → AddRoundKey

- C'est un simple addition modulo 2 bit par bit des clés.
- Il s'agit d'additionner des sous-clés aux sous-blocs correspondants.

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

$\oplus$

w_i	w_{i+1}	w_{i+2}	w_{i+3}

$=$

$s'_{0,0}$	$s'_{0,1}$	$s'_{0,2}$	$s'_{0,3}$
$s'_{1,0}$	$s'_{1,1}$	$s'_{1,2}$	$s'_{1,3}$
$s'_{2,0}$	$s'_{2,1}$	$s'_{2,2}$	$s'_{2,3}$
$s'_{3,0}$	$s'_{3,1}$	$s'_{3,2}$	$s'_{3,3}$

Chiffrement

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
 byte state[4,Nb]
 state = in
 AddRoundKey(state, w[0, Nb-1])
 for round = 1 step 1 to Nr-1
   SubBytes(state)
   ShiftRows(state)
   MixColumns(state)
   AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
 end for
 SubBytes(state)
 ShiftRows(state)
 AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
out = state
end
```

Extension de la clé

- AES utilise un processus (*KeyExpansion*) pour produire une clé étendue *w* à partir de clé de chiffrement de AES; qu'on notera *Key* (sa longueur *Nk*)

(b) Key and expanded key

Ex. Nk=4

Extension de la clé

La phase d'extension de la clé (*Key Expansion*) utilise notamment les éléments suivants:

- SubWord: est une fonction qui applique la boîte S-Box sur un mot.
- RotWord: est une fonction qui effectue une permutation circulaire vers gauche à une position.
- Rcon[i]: est un tableau de constantes de rondes, indépendant de *Nk*.

Extension de la clé

```
KeyExpansion(byte key[4*Nk], word w[Nb*(Nr+1)], Nk)
begin
word temp
i = 0
   while (i < Nk)  // recpoie key dans les Nk premiers mots de w
   w[i] = word(key[4*i], key[4*i+1], key[4*i+2], key[4*i+3])
   i = i+1
  end while
i = Nk
   while (i < Nb * (Nr+1)]
     temp = w[i-1]
     if (i mod Nk = 0)  // positions multiples de Nk
        temp = SubWord(RotWord(temp)) xor Rcon[i/Nk]
     else if (Nk > 6 and i mod Nk = 4)
        temp = SubWord(temp)
     end if
     w[i] = w[i-Nk] xor temp
     i = i + 1
  end while
end
```

key [16], w[44] , 4

Déchiffrement

```
InCipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
 byte state[4,Nb]
 state = in
 AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
 for round = Nr-1 step -1 downto 1
   InShiftRows(state)
   InSubBytes(state)
   AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
   InMixColumns(state)
 end for

 InShiftRows(state)
 InSubBytes(state)
 AddRoundKey(state, w[0, Nb-1])

 out = state
end
```

Avantages & Inconvénients

- **Avantages:**
  - De performance très élevée, il est 2,7 fois plus rapide que 3 DES.
  - Il comprend des opérations simples, ces sont des décalages, substitutions, déplacements et des additions,
  - Le nombre de rondes peut facilement être augmenté si c'est requis,
- **Inconvénients:**
  - Concernant le chiffrement et déchiffrement, les processus et les tables sont différents,
  - Le déchiffrement est plus difficile à implanter en carte à puce,

Cryptanalyse de AES

- Il ne possède pas de clés faibles,
- Il résiste la cryptanalyse différentielle et linéaire.
- Recherche exhaustive (force brute):
  - AES-128, nombre de clés possibles: $2^{128} = 3.4 \times 10^{38}$
  - Age de l'univers: 10^{10} années.
  - 1 année = 3.1536×10^{7} secondes.

Recommandation

- Il est approuvé et recommandé par NIST et NSA (National Security Agency).
- AES offre un niveau de cryptage acceptable ou moins jusqu'à 2030.
- Pour protéger des informations les plus sensibles «*Top Secret*», NSA recommande d'utiliser AES avec des clés de 256 bits.

Date	Niveau de Sécurité	Algorithme symétrique	Factorisation Module	Logarithme discret Clef	Logarithme discret Groupe	Courbe elliptique	Hash (A)	Hash (B)
Legacy (1)	80	2TDEA	1024	160	1024	160	SHA-1 (2)	
2019 - 2030	112	(3TDEA) (3) AES-128	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2019 - 2030 et au-delà	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1 KMAC128
2019 - 2030 et au-delà	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224 SHA3-224
2019 - 2030 et au-delà	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-256 SHA3-384 SHA3-512 KMAC256

https://www.keylength.com/fr/4/

Comparaison

	DES	3DES	AES
Date	1976	1978	**2000**
Taille de blocs	64 bits	64 bits	**128 bits**
Taille de clefs	64 bits	112 - 192 bits	**128, 192 et 256 bits**
Sécurité	Faible	Moyenne	**Haute**

Plan du cours

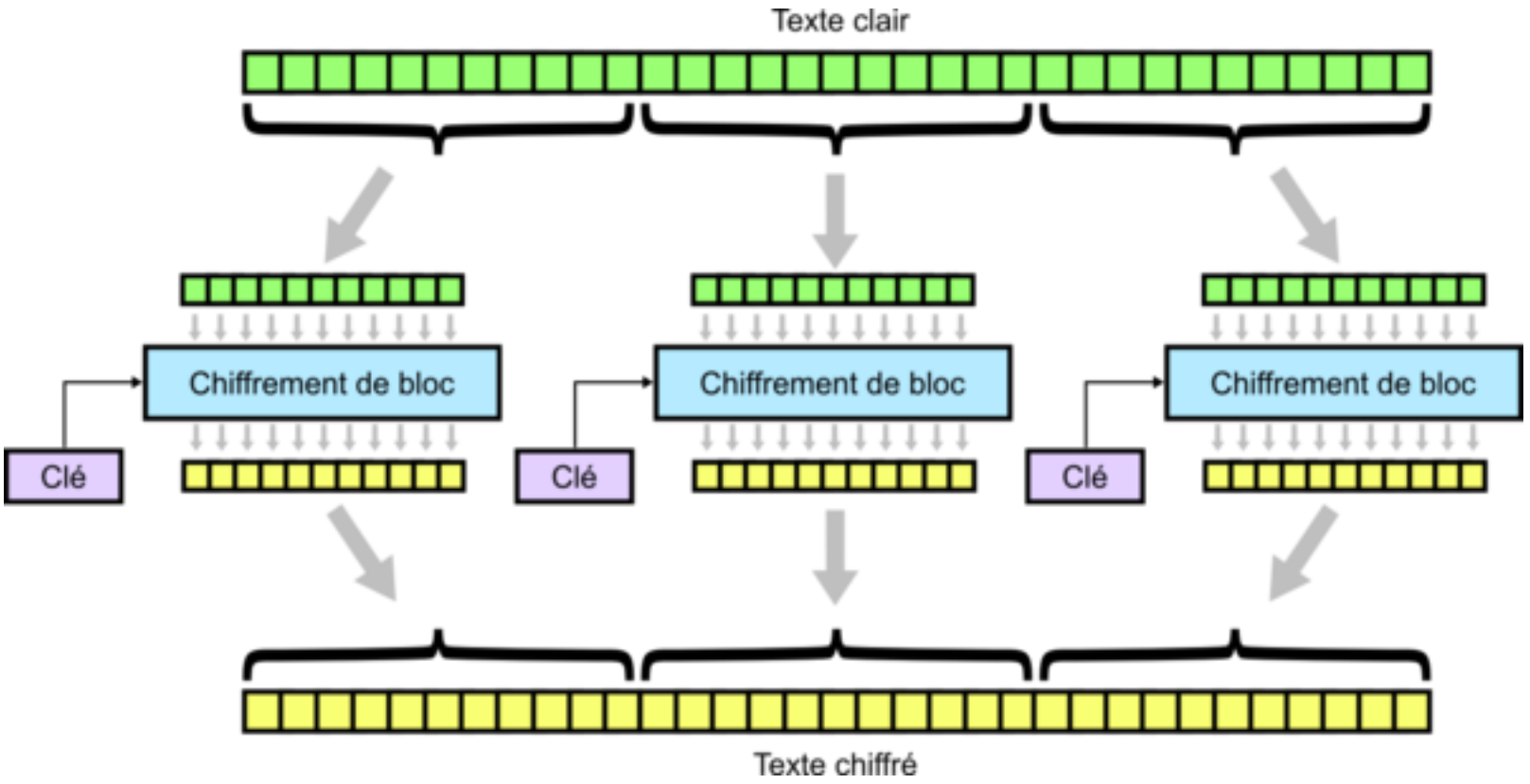
- Advanced Encryption Standard (AES)
- Modes d'opérations

Modes d'opération

- Un **mode d'opération** est la méthode de combiner les blocs de messages clairs et chiffrés au sein de la cryptographie bloc.
- Plusieurs modes existent, certains sont plus vulnérables que d'autres :
  - Electronic Codebook (ECB)
  - Cipher Block Chaining (CBC)
  - Cipher Feedback (CFB)
  - Output Feedback (OFB)
  - …

Le mode ECB
(Electronic Codebook (ECB)

- Il est le plus simple,
- Les blocs sont chiffré de manière indépendante.



Wikipedia

Les avantages et les inconvénients ECB

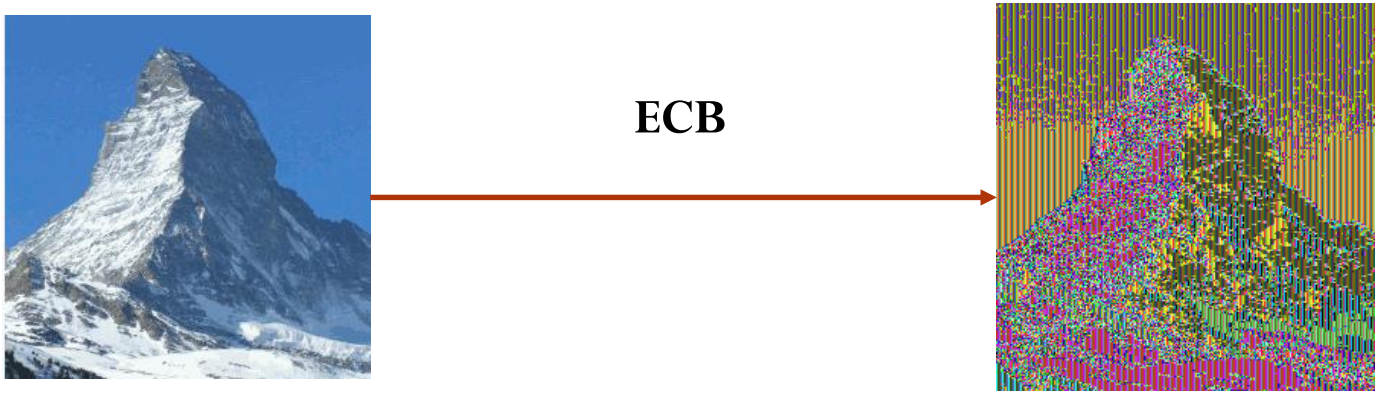
Les avantages :

- Le travail de chiffrement ou de déchiffrement peut être parallélisé.
- Il permet un accès aléatoire dans le texte chiffré.
- Une erreur de transmission d'un bit affecte uniquement le décodage du bloc courant.

Les avantages et les inconvénients ECB

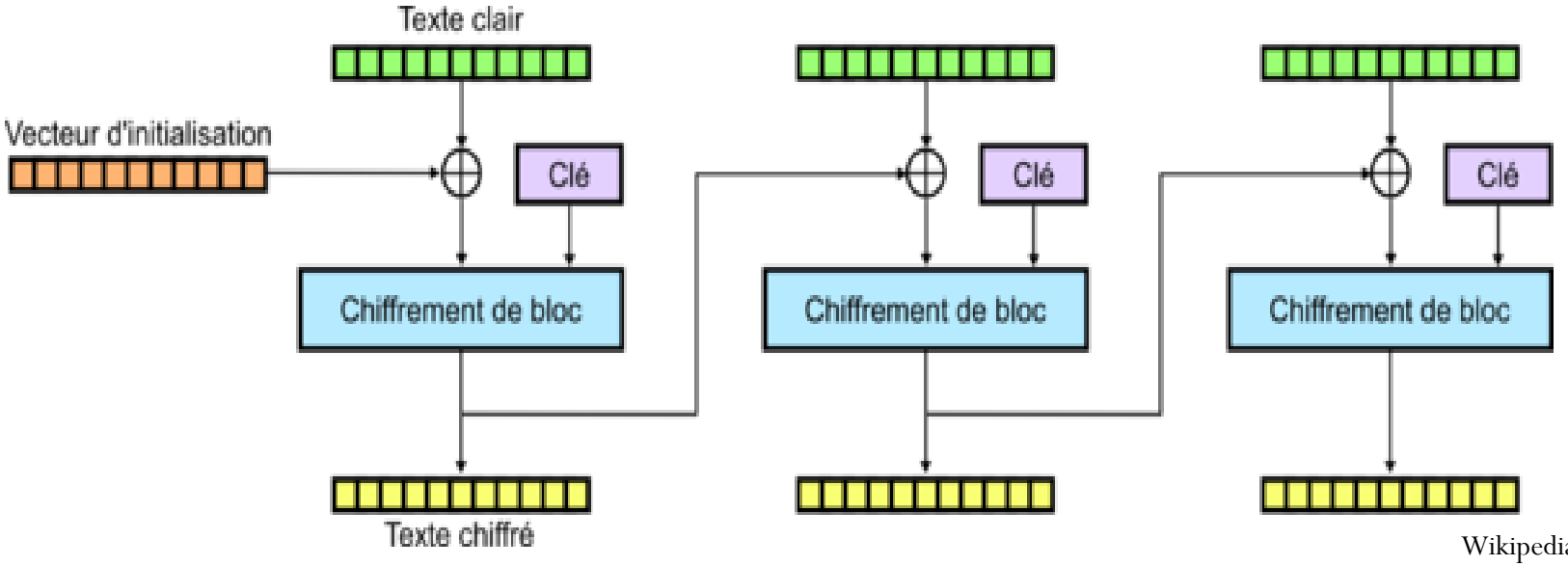
Les inconvénients :

- Si on utilise la même clé pour chiffrer deux fois un message clair, alors le résultat est identique.
- Les répétitions des fragments de messages clairs ne sont pas masquées et se retrouvent sous la forme des fragments répétés dans le message chiffré.



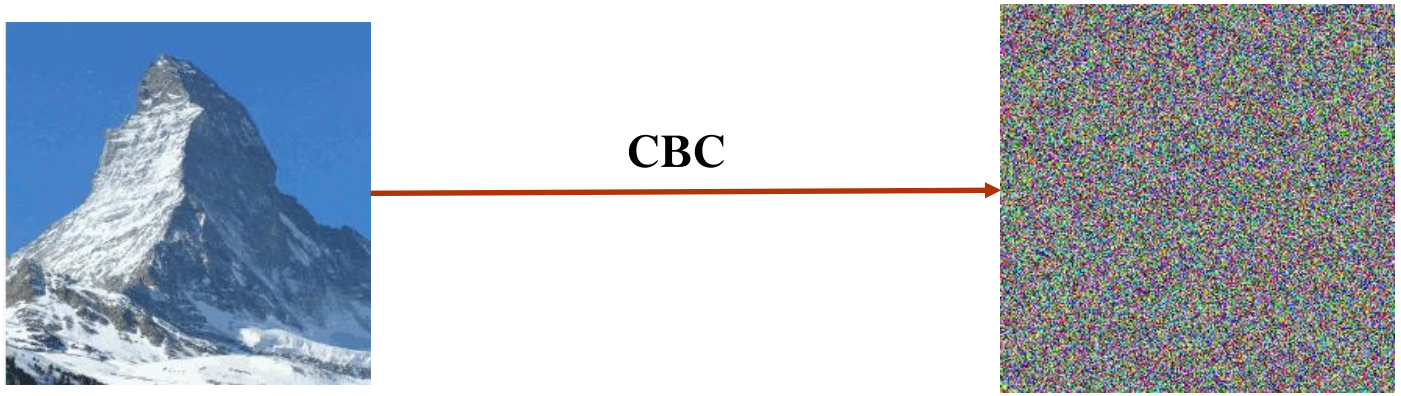
Le mode CBC
Cipher Block Chaining

- Chaque bloc de texte en clair est d'abord combiné par un **ou exclusif** avec le dernier bloc du texte chiffré.
- La sortie de ce **ou exclusif** est ensuite appliquée à la fonction de chiffrement.
- Ce mode de chiffrement dispose en plus d'un vecteur d'initialisation appelée IV qui permet d'initialiser le processus quand aucun bloc n'a encore été chiffré.



Wikipedia

Le mode CBC
Cipher Block Chaining



Limitation:

- Le mode CBC est un mode séquentiel, ne peut pas être parallélisé.

Références

- Daemen, J., & Rijmen, V. Specification for the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197, 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
- Dworkin, M. J. Recommendation for block cipher modes of operation. methods and techniques. No. NIST-SP-800-38A. National Inst of Standards and Technology Gaithersburg MD Computer security Div, 2001. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf