Modern Symmetric Cryptography

Part 2

Pr. Noureddine Chikouche
noureddine.chikouche@univ-msila.dz
https://sites.google.com/view/chikouchenoureddine

Course plan

- Advanced Encryption Standard (AES)
- Encryption operation modes

AES: Advanced Encryption Standard

- This is a symmetric block cipher.
- Known as Rijndael.
- Designed by two Belgian cryptographers, J. Daemenet V. Rijmen.
- In 1998, NIST (National Institute of Standards and Technology) organized a competition to find a successor to the DES algorithm.
- Rijndeala participated in this competition and was chosen in October 2000.
- Standardised by FIPS (*Federal Information Processing Standard*) in 2001.

AES: Advanced Encryption Standard

It has the following properties:

- Several key lengths are possible: 128, 192, or 256 bits ;
- Based on the substitution/permutation network structure. It only includes a series of transformations, permutations, selections;

AES: Advanced Encryption Standard

- Notions:
  - Word: 32-bit set or 4-byte vector.
  - Block: sequence of binary bits including input, output, state, and round key. Blocks are also interpreted as byte matrices.
  - Nb: number of columns in the block matrix. For AES, Nb = 4 (block length is 32*4=128 bits)
  - Nk : number of columns in the encryption key matrix. For AES Nk= 4,6 or 8 .
  - Nr: number of rounds.

AES: Advanced Encryption Standard

- **Number of rounds:**

The number of rounds (or cycles) depends on the size of the key.

	Key size (Nk)	Block size (Nb)	Round Nber (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

AES: Advanced Encryption Standard

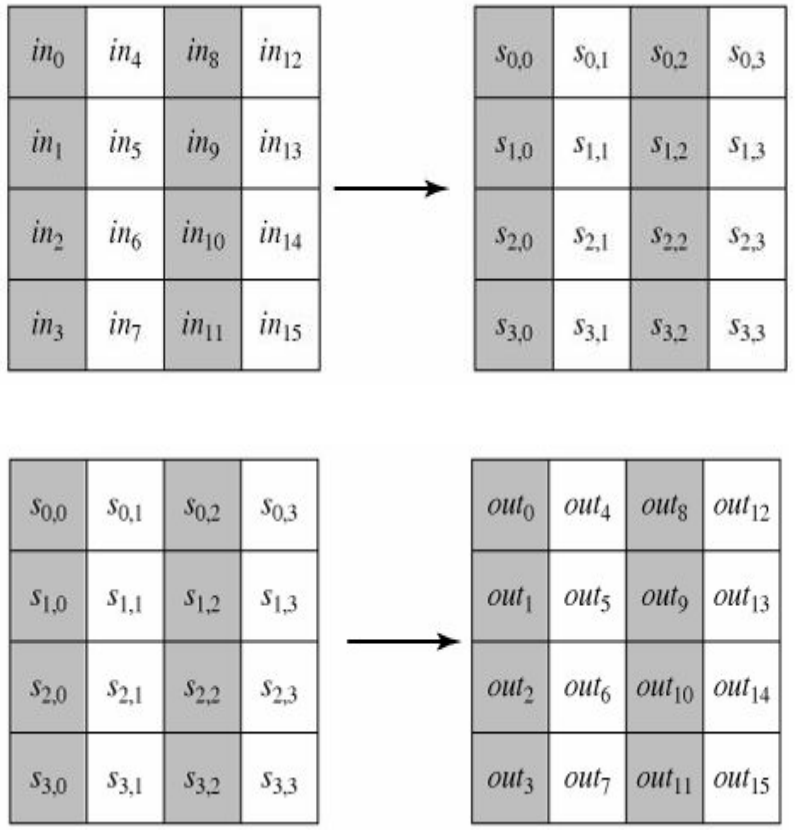
- For AES-128:
  - 128 representing the size of the key.
  - Nb = 4; //Number of columns in the block.
  - Nk = 4; //Number of words in the key (one word = 4 byte)
  - Nr = 10; //Number of rounds

AES: Advanced Encryption Standard

- Clear block encryption
- Key extension
- Decryption of encrypted block

Encryption

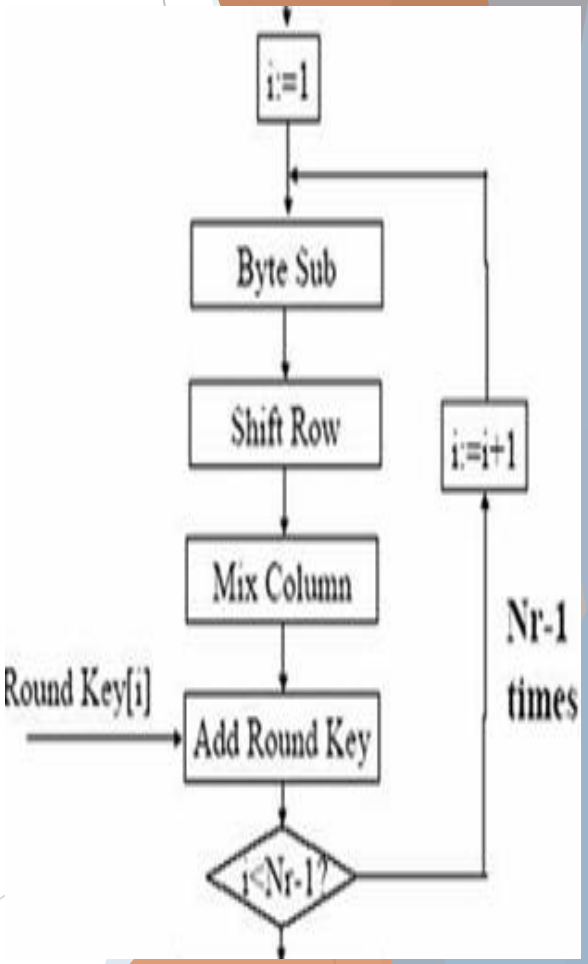
- The state matrices *of* the clear block and the encrypted block have 4 lines and *Nb* columns.

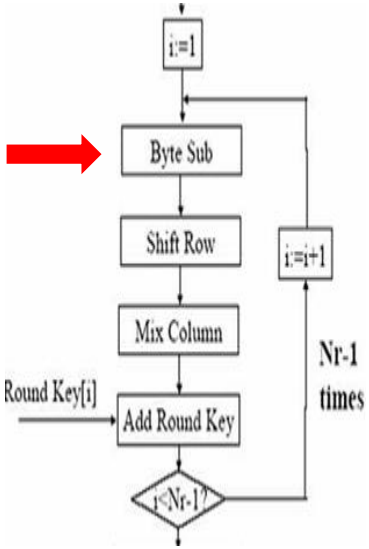


Encryption

In each round, 4 transformations are applied:

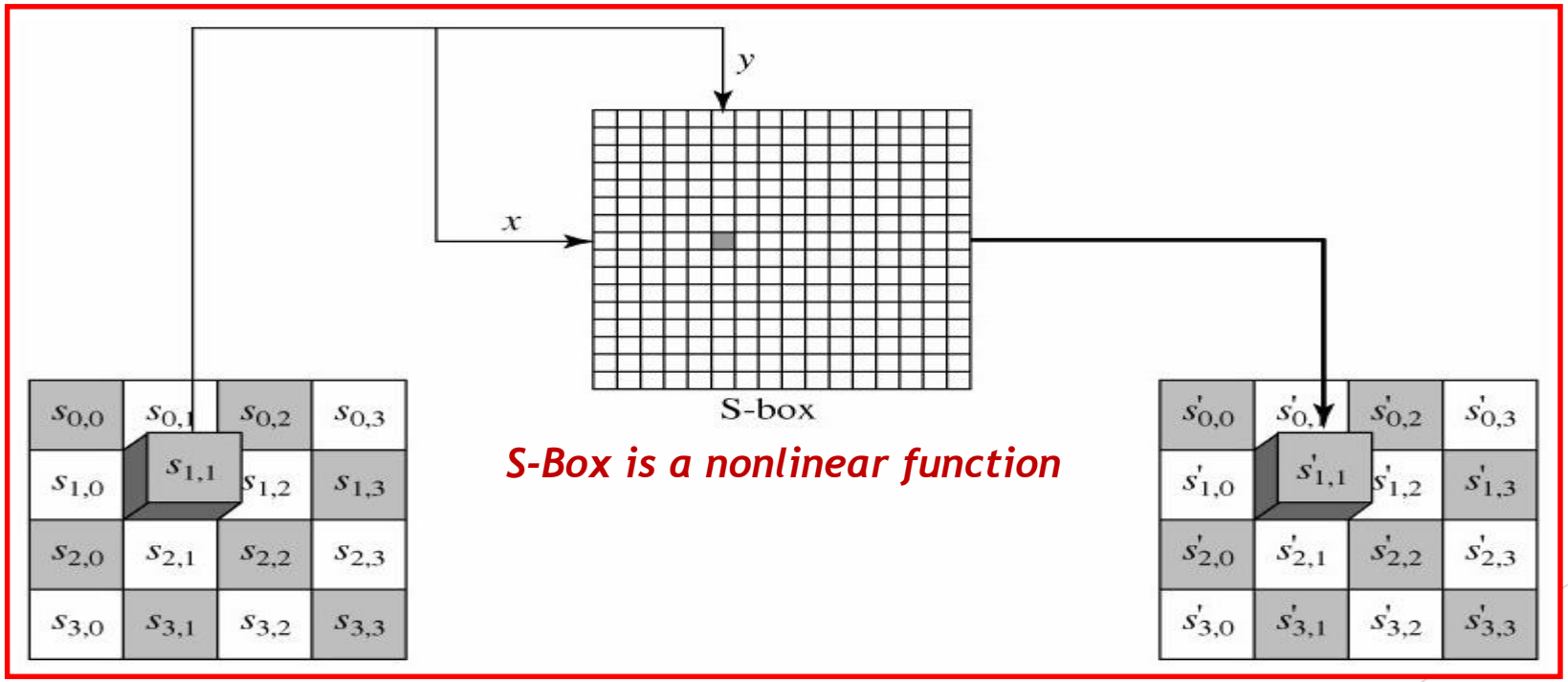
1) SubByte : **substitution** of bytes in the state table
2) ShiftRow : **offset** rows in the state table
3) MixColumn : **move** columns in the state table (except in the last round)
4) AddRoundKey : **in addition** to a "round key" that varies with each round.





Encryption → SubByte

Bytes are transformed by applying an *inversible S-Box (in order to allow a unique decryption).*



Encryption → SubByte

Example:

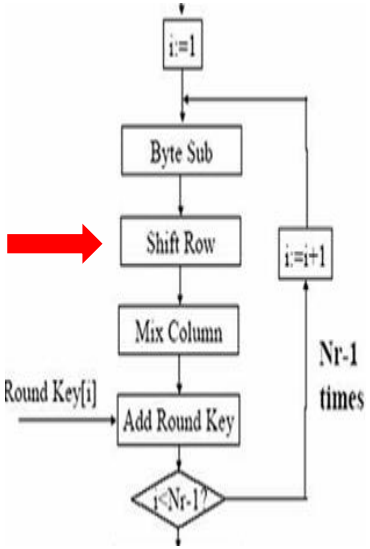
19

hex	y															
	0	1	2	3	4	5	6	7	8	9	a	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

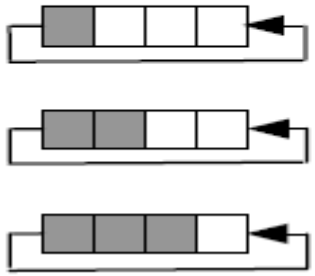


Encryption → ShiftRow

- The ShiftRow function modifies the rows of the matrix (array *state*) by making certain circular permutations.

s

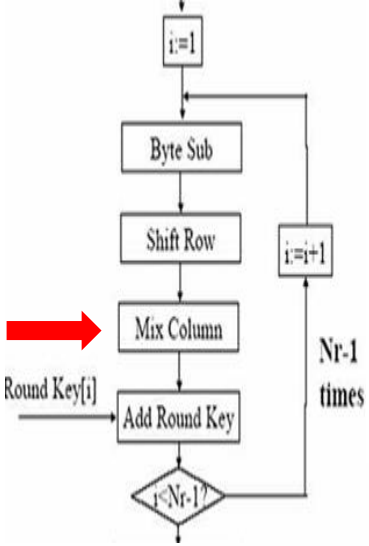
$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

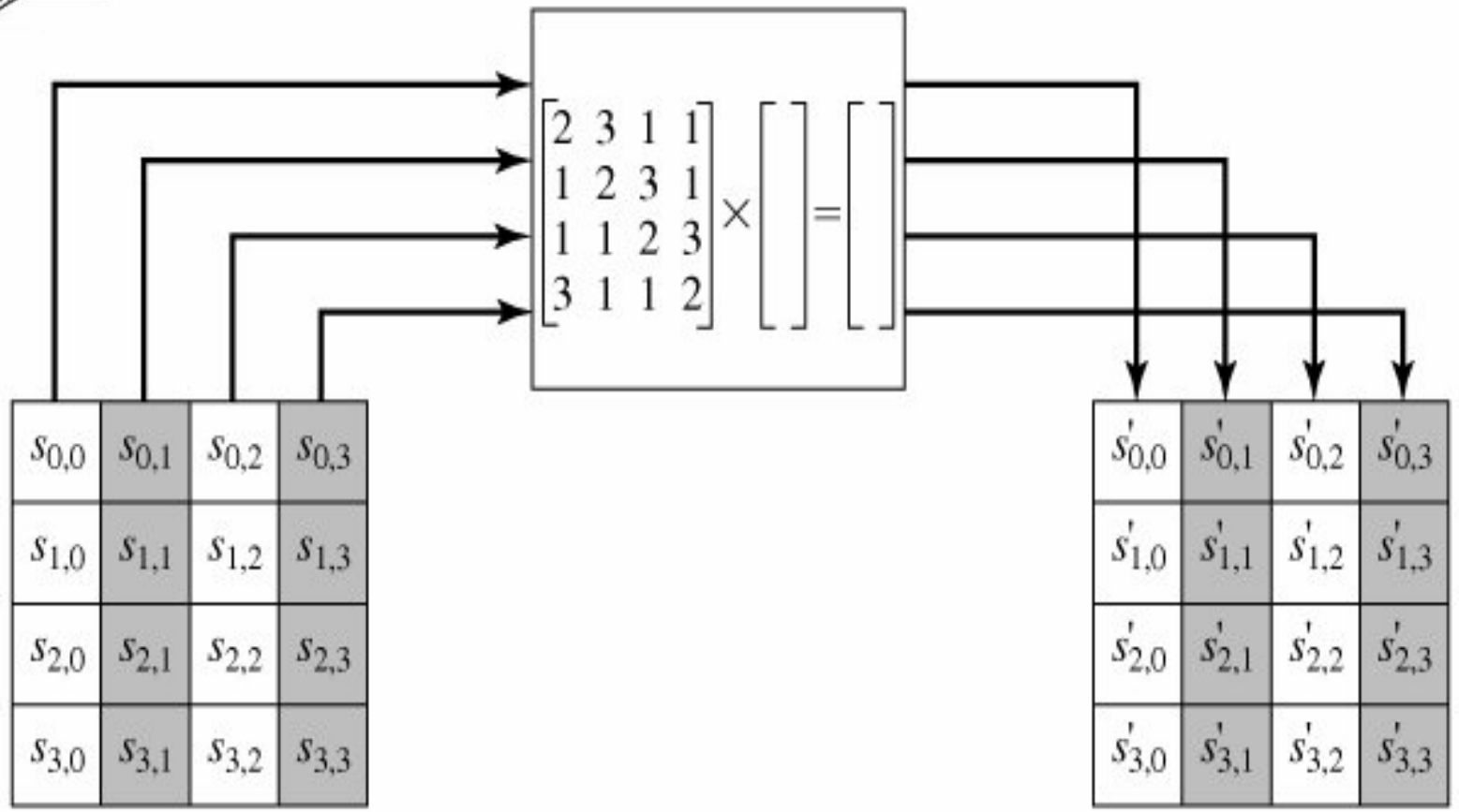


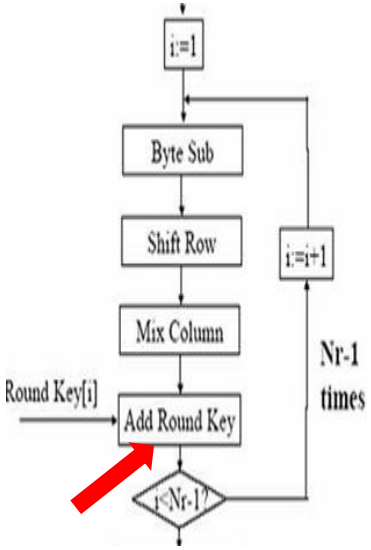
s'

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

Encryption → MixColum







Encryption → AddRoundKey

- It is a simple addition modulo 2 bit by bit of the keys.
- It is a matter of adding corresponding sub-blocks.

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

$\oplus$

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

$=$

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

Pseudo-Code of Encryption

```
1.  Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
2.  begin
3.   byte state[4,Nb]
4.   state = in
5.   AddRoundKey(state, w[0, Nb-1])
6.   for round = 1 step 1 to Nr-1
7.     SubBytes(state)
8.     ShiftRows(state)
9.     MixColumns(state)
10.    AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
11.  end for
12.  SubBytes(state)
13.  ShiftRows(state)
14.  AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
15. out = state
16. end
```

Key extension

- AES uses a process (*KeyExpansion*) to produce an extended key *w* from AES encryption key; that we will note *Key* (its length *Nk*).

(b) Key and expanded key

Ex. Nk=4

Key extension

The key expansion *phase* uses the following elements in particular:

- SubWord: is a function that applies the S-Box to a word.
- RotWord : is a function that performs a circular permutation to the left at a position.
- Rcon[i]: is an array of round constants, independent of Nk.

Pseudo-code of the key extension

```
1.  KeyExpansion(byte key[4*Nk], word w[Nb*(Nr+1)], Nk)
2.  begin                    key [16],  w[44] ,          4
3.  word temp
4.  i = 0
5.  while    ( i >  Nk) // recpoie key inthe Nkfirst words of w
6.       w[i] = word(key[4*i], key[4*i+1], key[4*i+2], key[4*i+3]))
7.        i = i+1
8.  end while
9.  i = Nk
10. while (i < Nb * (Nr+1)]
11.   temp = w[i-1]
12.   if (i mod Nk = 0)   // positions multiples de Nk
13.       temp = SubWord(RotWord(temp)) xor Rcon[i/Nk]
14.   else if (Nk > 6 and i mod Nk = 4)
15.       temp = SubWord(temp)
16.   end if
16. w[i] = w[i-Nk] xor temp
17.    i   = i+ 1
18. end while
19. end
```

Demonstration

AES

Pseudo-code of Decryption

```
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
```

Advantages & Disadvantages

- **Benefits:**
  - Very high performance, it is 2.7 times faster than 3 DES.
  - It includes simple operations, these are shifts, substitutions, displacements and additions,
  - The number of rounds can easily be increased if required,
- **Disadvantages:**
  - Regarding encryption and decryption, the processes and tables are different,
  - Decryption is more difficult to implement in a smart card.

AES Cryptanalysis

- He does not have weak keys,
- It resists differential and linear cryptoanalysis.
- Exhaustive research (brute force):
  - AES-128, number of possible keys: $2128 = 3.4 \times 1038$
  - Universe age: 1010 years.
  - 1 year = 3.1536 x 107 seconds.

Recommendation

- It is approved and recommended by NIST and NSA (National Security Agency).
- AES offers an acceptable level of encryption or less until 2030.
- To protect the most sensitive «Top Secret» *information*, NSA recommends using AES with 256-bit keys.

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/

Comparison

	DES	3DES	AES
Date	1976	1978	2000
Block Size (bit)	64	64	128
Key Size (bit)	64	112 - 192	128, 192 and 256
Security	Weak	Average	High

Course plan

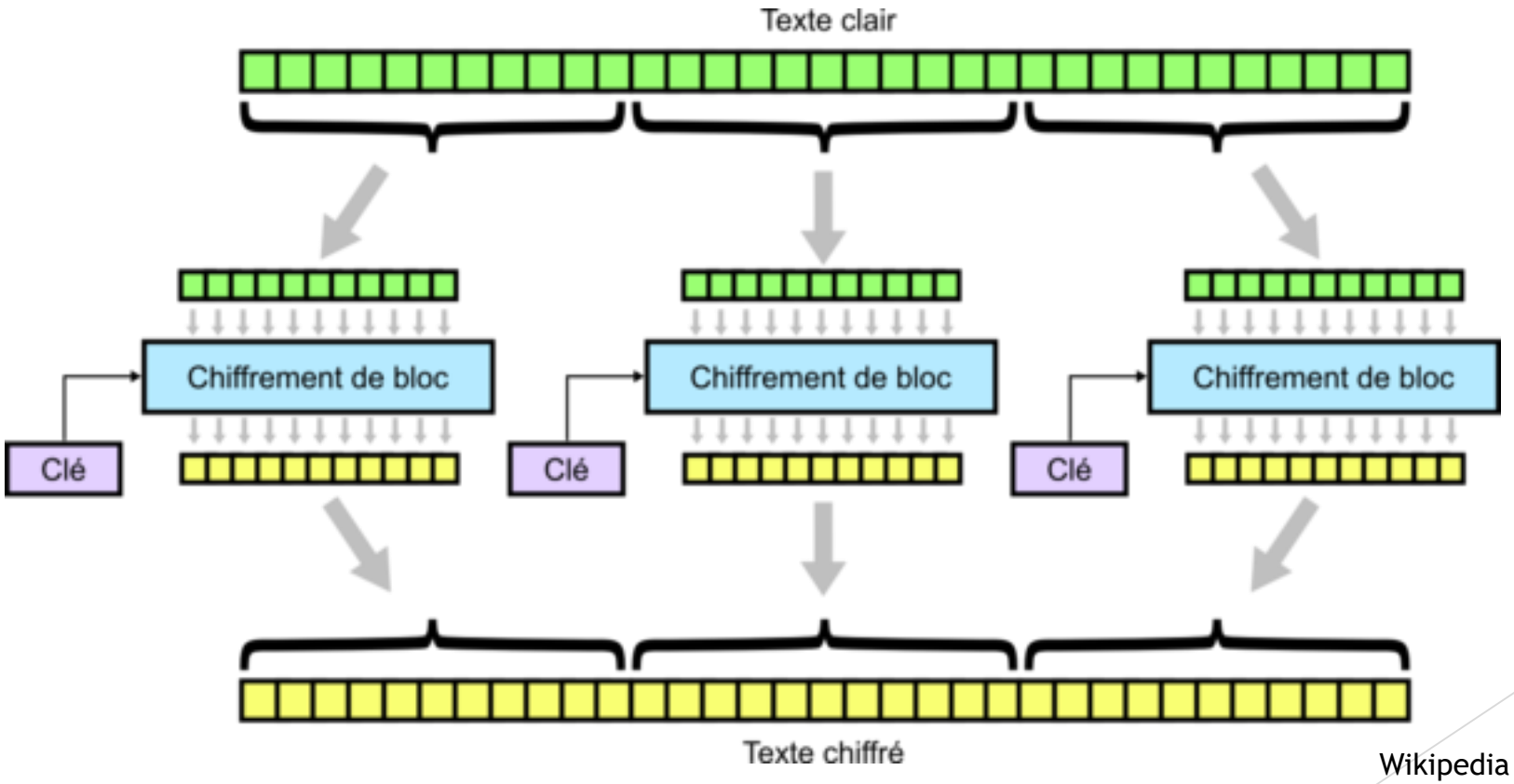
- Advanced Encryption Standard (AES)
- Modes of operation

Modes of operation

- A **mode of** operation is the method of combining clear and encrypted message blocks within block cryptography.
- Several modes exist, some are more vulnerable than others:
  - Electronic Codebook (ECB)
  - Cipher Block Chaining (CBC)
  - Cipher Feedback (CFB)
  - Output Feedback (OFB)
  - …

Le mode ECB
(Electronic Codebook (ECB)

- He is the simplest,
- The blocks are independently encrypted.



Wikipedia

The advantages and disadvantages of ECB

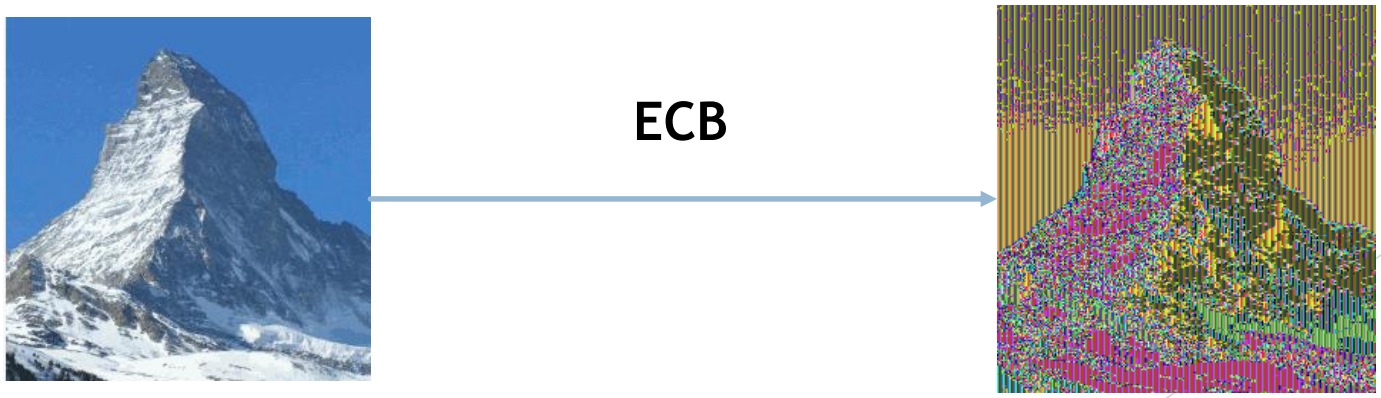
The advantages:

- The encryption or decryption process can be parallelized.
- It allows random access in encrypted text.
- A one-bit transmission error affects only the decoding of the current block.

The advantages and disadvantages of ECB

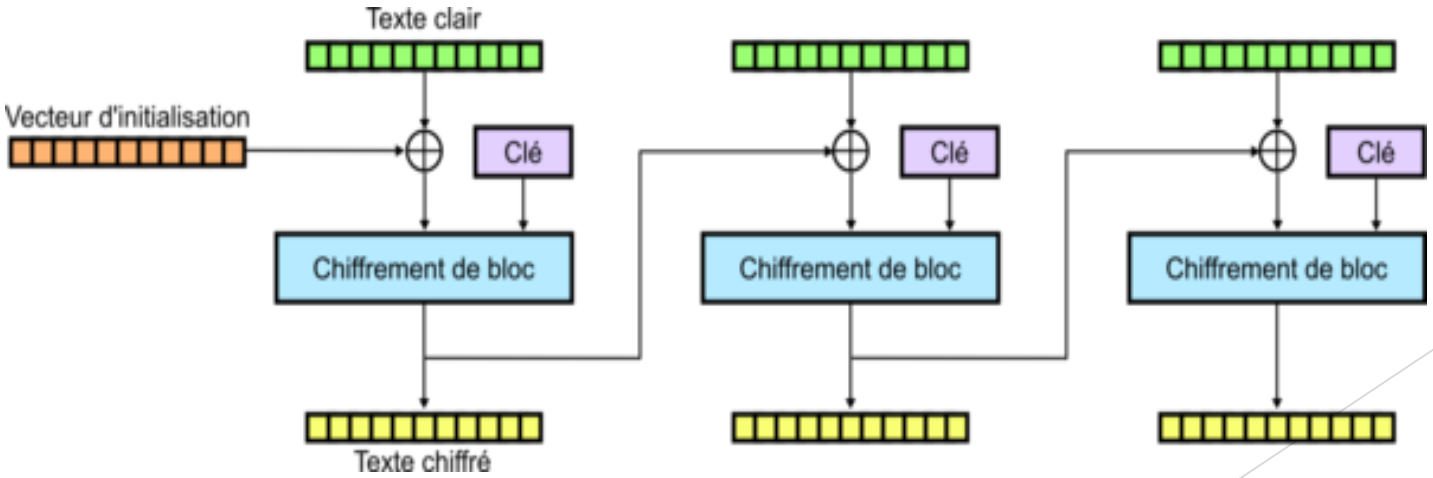
The disadvantages:

- If we use the same key to encrypt a clear message twice, then the result is identical.
- The repetitions of fragments of clear messages are not masked and are found in the form of repeated fragments in the encrypted message.



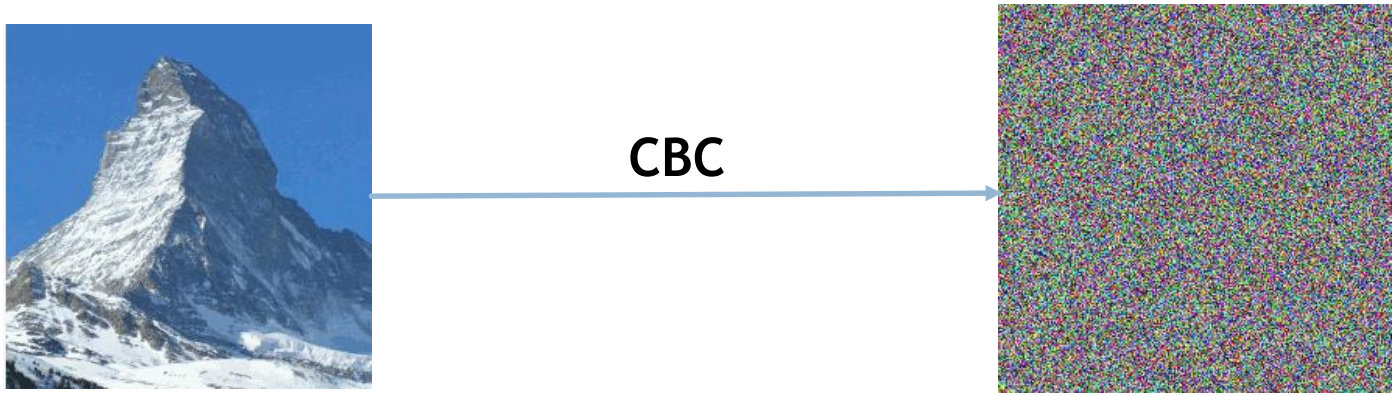
The Cipher Block Chaining mode

- Each block of plain text is first combined by one or **exclusif with** the last block of ciphered text.
- The output of this **or exclusif is applied to the encryption function.**
- This encryption mode also has an initialization vector called IV which allows the process to be initialized when no block has yet been encrypted.



Wikipedia

The Cipher Block Chaining mode



Limitation:

- CBC mode is a sequential mode, cannot be parallelized.

References

- 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

Quiz

1. In the encryption operation with the AES algorithm, the following transformations are used:
    1. SubBytes
    2. PC1
    3. ShiftRows
    4. InvSubBytes
- Which of these concepts are modes of operation?
    1. ECB
    2. AES
    3. OF
    4. CBC