

ch 2 : Chiffrement symétrique

I) Modélisation

II) DES

III) AES (Advanced Encryption Standard)

① Historique

DES → clé 56 bits → insuffisant actuellement
taille des blocs : 64 bits

Remarque : le Triple-DES résout le pb de la taille de clé (pour le Triple-DES, la clé fait 112 bits et il n'y a pas le pb de l'attaque meet-in-the-middle)
mais le temps de calcul est 3 fois celui du DES...

1998 : le NIST (National Institute for Standards and Technology)
successeur du NBS

lance un concours international pour un algo de chiffrement par blocs AES
- avec des blocs de 128 bits
- une clé de 128, 192 ou 256 bits
- "plus rapide" que le Triple-DES

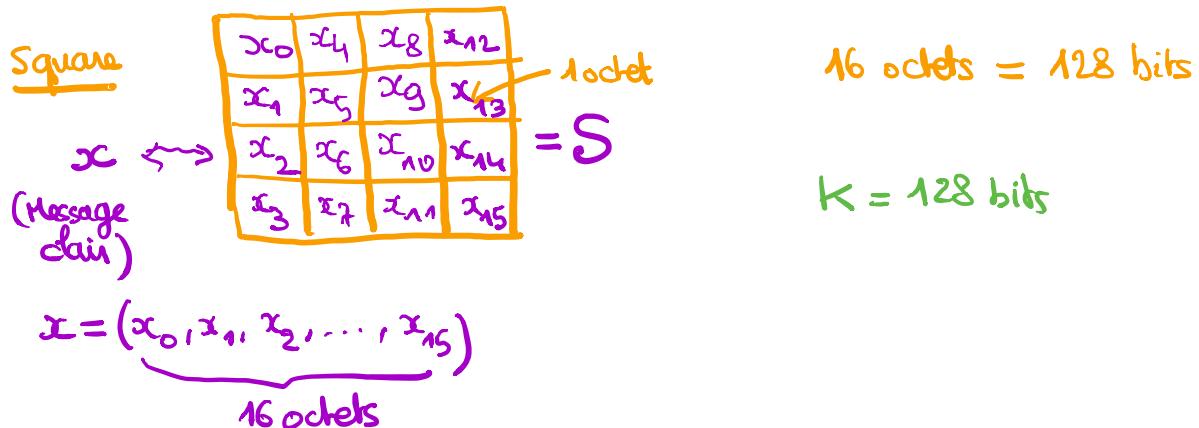
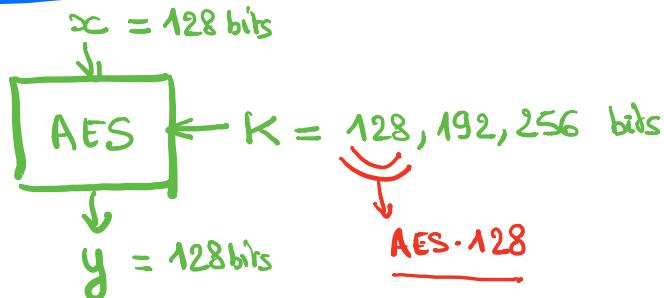
phase 1 : \approx 50 candidats

phase 2 : 15 candidats

phase 3 : 5 finalistes → élé 2001 : vainqueur

RIJNDAEL → AES : standardisé en décembre 2001
 Vincent RIJTMEN Joan DAEMEN (Belges)

② Description de l'AES

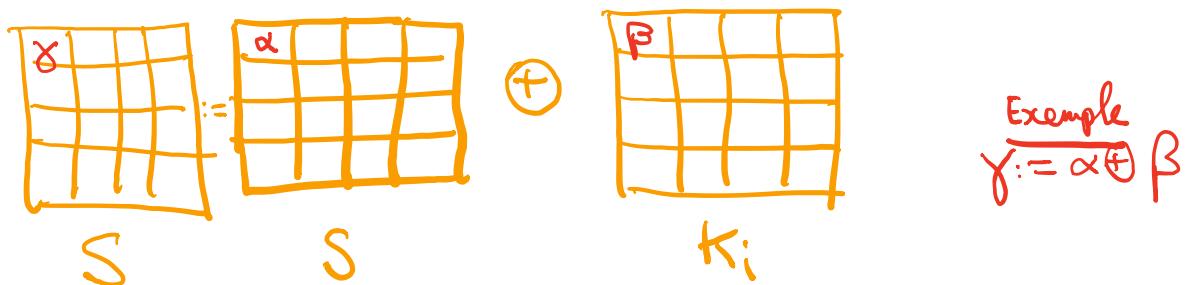


Description de $\text{AES}_K(x)$

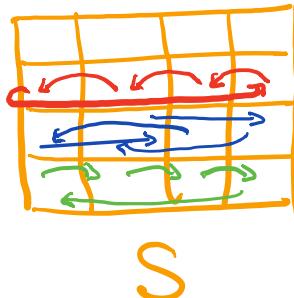
- $K \rightsquigarrow \underbrace{K_0, K_1, \dots, K_{10}}_{11 \text{ sous-clés, de 128 bits chacune, éclatées aussi sous forme de tableau } 4 \times 4}$
- $x \rightsquigarrow S$
- $S := \underbrace{S}_{K_0} \oplus \underbrace{K_0}_{K_i \rightsquigarrow \begin{matrix} & & & \\ & & & \\ & & & \\ & & & \end{matrix} (16 \text{ octets} = 128 \text{ bits})}$
- Pour i de 1 à 10
 - | $S := \text{ByteSub}(S)$
 - | $S := \text{ShiftRows}(S)$
 - | Si ($i \leq 9$) alors $S := \text{MixColumn}(S)$
 - | $S := S \oplus K_i$

L'état final de S contient le message chiffré y

a) $S := S \oplus K_i$



b) $S := ShiftRows(S)$

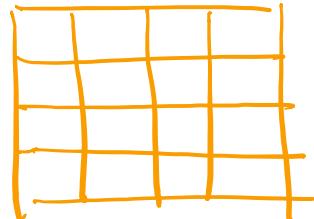


Décalage (circular) de :

- 0 cran vers la gauche
- 1 cran _____
- 2 cran _____
- 3 cran _____

c) $S := ByteSub(S)$

Chaque octet (= 1 case) va être modifié par cette opération



Qu'est-ce qu'un octet ?
plusieurs représentations possibles
[octet]

$$\{x, 0 \leq x \leq 255\} \leftrightarrow (b_7, b_6, b_5, \dots, b_0) \quad [8 \text{ bits}]$$

Ex: $x = 137 \leftrightarrow (1, 0, 0, 0, 1, 0, 0, 1) \leftrightarrow x^7 + x^3 + 1$

[polynôme]

1 bit
1 bit

$$\begin{aligned} 137 + 214 \\ = 351 \end{aligned}$$

128

8

1

Addition : XOR

$$\begin{array}{c}
 \text{ex : } a = 137 \quad \longleftrightarrow (1, 0, 0, 0, 1, 0, 0, 1) \quad \longleftrightarrow X^7 + X^3 + 1 \\
 \text{b} = 214 \quad \longleftrightarrow (1, 1, 0, 1, 0, 1, 1, 0) \quad \longleftrightarrow X^7 + X^6 + X^4 + X^2 + X \\
 \hline
 a \oplus b = 95 \quad \longleftrightarrow (0, 1, 0, 1, 1, 1, 1, 1) \quad \longleftrightarrow \frac{(1+1)X^7 + X^6 + X^4 + X^3}{=0} \\
 \text{(ou } 5F \text{ en hexadécimal)}
 \end{array}$$

8 bits Polynôme

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

128 64 32 16 8 4 2

1 bit = {0/1}
 $\in \mathbb{Z}/2\mathbb{Z}$

Multiplication :

octet polynôme qui représente l'octet

$$\begin{aligned}
 a &\leftrightarrow A(X) \leftarrow d^\circ A \leq 7 \\
 b &\leftrightarrow B(X) \leftarrow d^\circ B \leq 7
 \end{aligned}$$

$$a+b \leftrightarrow A(X)+B(X) \quad (\text{car } + \text{ est mod } 2)$$

$$a \times b \leftrightarrow \underbrace{A(X)B(X)}_{d^\circ \leq 14} \mod I(X) \quad d^\circ I = 8$$

$d^\circ \leq 7$

ex : $a = 137 \leftrightarrow A(X) = X^7 + X^3 + 1$
 $b = 214 \leftrightarrow B(X) = X^7 + X^6 + X^4 + X^2 + X$

$$\begin{aligned}
 A(X)B(X) &= (X^7 + X^3 + 1)(X^7 + X^6 + X^4 + X^2 + X) \\
 &= X^{14} + X^{13} + X^{11} + X^9 + X^8 \\
 &\quad + X^{10} + X^9 + X^7 + X^5 + X^4 \\
 &\quad + X^7 + X^6 + X^4 + X^2 + X
 \end{aligned}$$

$$= X^{14} + X^{13} + X^{11} + X^{10} + X^8 + X^6 + X^5 + X^2 + X$$

On calcule ensuite $A(X)B(X) \bmod I(X)$

où $I(X) = X^8 + X^4 + X^3 + X + 1$

$$\begin{array}{r}
 X^{14} + X^{13} + X^{11} + X^{10} + X^8 + X^6 + X^5 + X^2 + X \\
 - (X^{14} + X^{10} + X^8 + X^7 + X^6) \\
 \hline
 X^{13} + X^{11} + X^9 + X^8 + X^7 + X^5 + X^2 + X \\
 - (X^{13} + X^9 + X^8 + X^6 + X^5) \\
 \hline
 X^{11} + X^7 + X^6 + X^2 + X \\
 - (X^{11} + X^7 + X^6 + X^5 + X^3) \\
 \hline
 X^4 + X^3 + X^2 + X
 \end{array}$$

= reste de la division euclidienne

$$A(X)B(X) \bmod I(X) = X^4 + X^3 + X^2 + X$$

multiplication
d'octets

$$137 \times 214 = 30$$

$$\underbrace{30}_{\text{décimal}} = (0, 0, 0, 1, 1, 1, 1, 0)$$

↓	↓	↓	↓	↓	↓	↓	↓
16	8	4	2				

$E = \{\text{octets}\}$ est muni de deux opérations (la de composition interne)
(l'addition et la multiplication)

Théorème: $(E, +, \times)$ est un corps commutatif

Démonstration : • $(E, +)$ est un groupe commutatif

$(E, +)$ est
un groupe

- $E \neq \emptyset$
- Il existe un élément neutre :
 $\forall x \in E, x + 0 = 0 + x = x$
 où 0 est l'élément nul $= (0, 0, 0, 0, 0, 0, 0, 0)$
- Tout $x \in E$ a un élément symétrique y :
 $x + y = y + x = 0$ (opposé de x)
 (mais en particulier : $y = -x$
ex : $137 + 137 = 0$)

commutatif : $\forall x, y \in E, x + y = y + x$

• $(E \setminus \{0\}, \times)$ est un groupe

$(E \setminus \{0\}, \times)$
est un groupe
(commutatif)

- $E \setminus \{0\} \neq \emptyset$
- Élément neutre
 $\forall x \in E \setminus \{0\}, \textcircled{x} \times 1 = 1 \times x = \textcircled{x}$
 où 1 est l'élément $\begin{cases} \text{de valeur } 1 \\ (0, 0, 0, 0, 0, 0, 0, 1) \end{cases}$
 le polynôme 1
- Élément symétrique (inverse de x)
 pour tout $x \in E \setminus \{0\}$, il existe $y \in E \setminus \{0\}$
 tel que $x \times y = y \times x = 1$

$$x \leftrightarrow A(x)$$

on cherche $y \leftrightarrow B(x)$ tel que $x \times y = 1$

C'est à dire $A(X)B(X) = 1 \pmod{I(X)}$

Comment obtenir $B(X)$?

$$I(X) = \underbrace{x^8 + x^4 + x^3 + x + 1}_{() \times ()} \text{ est un polynôme irréductible}$$

$$\implies \text{pgcd}(A(X), I(X)) = 1$$

$d \leq 7$ $d \geq 8$

Th. de Bézout

Il existe des polynômes $U(X)$ et $V(X)$

tels que

$$U(X)A(X) + V(X)I(X) = 1$$

$$\begin{aligned} \text{avec } & \left\{ \begin{array}{l} d^{\circ} U < d^{\circ} I = 8 \\ d^{\circ} V < d^{\circ} A \end{array} \right. \end{aligned}$$

$U(X)$ représente bien un octet

et

$$A(X)U(X) = 1 \pmod{I(X)}$$

↓
inverse de $A(X) \pmod{I(X)}$

• Distributivité : $\forall x, y, z \in E$

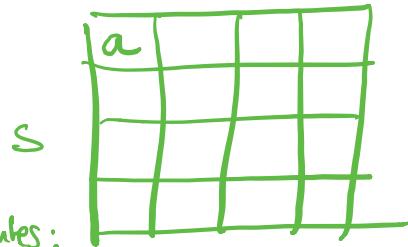
$$x \times (y + z) = (x \times y) + (x \times z)$$

$$(x + y) \times z = (x \times z) + (y \times z)$$

(Cela provient du fait que, sur les polynômes, la multiplication est distributive par rapport à l'addition)

$S := \text{ByteSub}(S)$

pour chaque octet a de S
on effectue les opérations suivantes:



- $b := \text{INV}(a) = \begin{cases} \text{inverse de } a \\ \text{pour la multiplication} & \text{si } a \neq 0 \\ 0 & \text{si } a = 0 \end{cases}$

- on écrit $b = (b_7, b_6, \dots, b_0)$
et on calcule

$$\text{ByteSub}(a) := \left(\begin{array}{c} \text{matrice } 8 \times 8 \\ \text{fixée} \end{array} \right) \oplus \left(\begin{array}{c} b_7 \\ b_6 \\ b_5 \\ b_4 \\ b_3 \\ b_2 \\ b_1 \\ b_0 \\ \text{vecteur colonne fixé} \end{array} \right)$$