Sécurité informatique
- Notes d'introduction sur la théorie de Galois -

Febuary 2021

Corps de Galois

Groupe*: Un groupe est un ensemble d'éléments G muni d'une opération $*$ qui combine les éléments de G t.q. les 4 propriétés suivantes sont satisfaites:*

1. *le groupe est fermé sous l'opération* $*$: $\forall a, b \in G, \quad a * b \in G$
2. $*$ *doit être associative:* $a * (b * c) = (a * b) * c$
3. *présence d'un élément identité e t.q. :* $\forall a \in G, \quad a * e = a$
4. $\forall a \in G, \exists a^{-1} \in G$ *t.q.* $a * a^{-1} = e$

Note: si $*$ est commutative, le groupe est appelé Abélien.

Exemple 1:

$\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ avec l'addition modulo m.
C'est un groupe!

Exemple 2:

$\mathbb{Z}_3 = \{0, 1, 2\}$ avec la multiplication modulo 3.
Ce n'est pas un groupe, puisque 0 ne peut pas avoir d'inverse.
Pour un certain m, tout les éléments qui ne sont pas copremiers avec m n'auront pas d'inverse. (Copremier: $PGCD(x, m) = 1$.)

Coprs *(Field): Un ensemble d'éléments F t.q. les propriétés suivantes sont satisfaites:*

1. *Tous les éléments forment un groupe avec l'opération d'addition (e = 0.)*
2. *Tous les éléments (sauf 0) forment un groupe avec l'opération de multiplication (e = 1.)*
3. *La distributivité est respectée quand on combine les 2 opérations:*

$$\forall a, b, c, d \in F, \quad a(b + c) = (ab) + (ac)$$

Exemple: $\mathbb{R}$

Coprs fini (Corps de Galois): Un coprs ayant un nombre fini d'éléments.

Théorème: Soit $GF(p) = \{0, 1, \ldots, p-1\}$ un corps de Galois ou p est prmier et l'arithmétique est calculée modulo p. Tout élément non-nul de $GF(p)$ possède un inverse.

Pour AES, on veut faire un extension $GF(p) \to GF(2^8)$ qui a 256 éléments. On devra se munir:

1. une nouvelle notation pour les éléments du corps de Galois
2. des nouvelles règles arithmétiques

$$A \in GF(2^8): \quad A(x) = a_7x^7 + \cdots + a_1x + a_0 \qquad a_i \in GF(2) = \{0, 1\}$$
$$A = (a_7a_6a_5 \ldots a_1a_0)$$

Addition et soustraction:

$$C(x) = A(x) + B(x) \implies \sum_{i=0}^{m-1} c_ix^i \quad , \quad c_i = a_i + b_i \mod 2$$
$$C(x) = A(x) - B(x) \implies \sum_{i=0}^{m-1} c_ix^i \quad , \quad c_i = a_i - b_i \mod 2$$

Dans modulo 2, l'addition et la soustraction sont en fait la même opération. En fait, c'est exactement le "ou exclusif" (XOR, $\bigoplus$).

Multiplication: $C(x) = A(x) \cdot B(x) \mod P(x)$

$$P(x) = \sum_{i=0}^{m} p_ix^i \quad , \quad p_i \in GF(2) \quad , \quad P(x) \text{ irréductible}$$

Pour AES $P(x) = x^8 + x^4 + x^3 + x + 1$. C'est dans la spécification.

Exemple:

Soient $A(x) = x^3 + x^2 + 1$, $B(x) = x^2 + x$, $P(x) = x^4 + x + 1$:

$$\begin{aligned} C^{'}(x) &= A(x)B(x) = (x^3 + x^2 + 1)(x^2 + x) \\ &= x^5 + x^4 + x^4 + x^3 + x^2 + x \\ &= x^5 + 2 \cdot x^4 + x^3 + x^2 + x \\ &= x^5 + x^3 + x^2 + x \end{aligned}$$

Divion par $P(x)$:

$$\begin{array}{rl|l} - & x^5 + x^3 + x^2 + x & x^4 + x + 1 \\ \cline{3-3} & x^5 \qquad\; + x^2 + x & x \\ \cline{1-2} & x^3 & \end{array}$$

Donc, modulo $P(x)$, on a $C(x) = x^3$

Inverse:

$$A^{-1}(x) \cdot A(x) \equiv 1 \mod P(x)$$