FMSI

Cour 1 13/02

Support de cour autorisé au partiel

Sécurité : technique pour rendre difficile d'accès de données ?

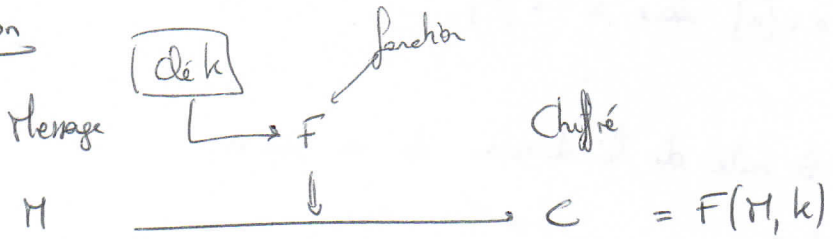
progrès technologique ⇒ personne qui fraude en l'obligeant.
vol / calomnie / ...

sécurité : jusqu'à y'a ~~de~~ 10 ans : sécurité du système d'info

→ protection de l'information elle-même (crypto)
→ technique d'architecture (serveur..)

C J F O W F O V F (= Bienvenue)

Introduction



Algorithme symétrique

M ⟶ C = F(M, k)

M' ⟵ = F⁻¹(C, k)

Signature

Asymétrique

⟶ K F

∈ F⁻¹

Connaissant ∈.

Arithmétique modulaire

n : entier ≥ 2

Def : $a, b \in \mathbb{Z}$

$a \equiv b \ [n] \iff a - b \mid n$ (divisible par n)

$n = 2$: — pair
— impair (départager)

Prop : Congruence = "relation d'équivalence"

$\forall x, y, z \ldots$

$x \equiv x \ [n]$

si $x \equiv y \ [n]$ $\quad y \equiv x \ [n]$

si $x \equiv y \ [n]$ et $y \equiv z \ [n]$ alors $x \equiv z \ [n]$

Si $a \in \mathbb{Z}$, r le reste de la division de a par n.

$0 \leq r < n$ $\quad$ ($a \% n = r$)

$\exists q : a = qn + r$

alors $a \equiv r \ [n]$

Classe de a :

$\bar{a} = \{ b \text{ tq } b \equiv a \ [n] \}$

$\bar{a} = \bar{r}$

Il y a exactement n classes d'équivalences, $\bar{0}, \bar{1}, \ldots, \overline{n-1}$

$\mathbb{Z}/n\mathbb{Z} = \{ \bar{0}, \bar{1}, \ldots, \overline{n-1} \}$

Addition dans $\mathbb{Z}/n\mathbb{Z}$

Prop : Soient $a_1, \ldots, b_n$ dans $\mathbb{Z}$ tq $a_1 \equiv a_2 \ [n]$ $\quad b_1 \equiv b_2 \ [n]$

Alors $a_1 + b_1 \equiv a_2 + b_2 \ [n]$

(2)

Soient $a_1, a_2, b_1, b_2 \in \mathbb{Z}$

On suppose $a_1 \equiv a_2 \ [n]$ $\quad b_1 \equiv b_2 \ [n]$

Il existe k et ℓ

$a_1 - a_2 = kn$

$b_1 - b_2 = \ell n$

$(a_1 + b_1) - (a_2 + b_2) = (k + \ell) n$

$a_1 + b_1 \equiv a_2 + b_2 \ [n]$

Définition : $\bar{a} + \bar{b} = \overline{a+b}$

$= (a+b) \% n$

$\mathbb{Z}/5\mathbb{Z}$ $\quad n = 5.$

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$