** Chiffrement par permutations

Soit l'alphabet $A = \{a_1, \dots, a_n\}$ et $f \in S_n$ (une permutation de n éléments).

Chiffrement : chiffrer un mot $a_{i_1} \dots a_{i_k}$ par $a_{f(i_1)} \dots a_{f(i_k)}$

Déchiffrement : pour déchiffrer le mot $b_{i_1} \dots b_{i_m}$ on applique f^{-1} aux indices $i_1, \dots, i_m$.

Dans ce cas l'espace de clés est de taille $n!$

Exemple : pour $p = 29$, $\left(\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*, \cdot\right)$ est un groupe cyclique d'ordre $p-1 = 28$, posons $A = \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^* = \{1, \dots, 28\}$ et

A	B	C	D	E	......
1	2	3	...	...	...

, considérons la bijection $x \xrightarrow{f} x^{-1}\ [29]$

chiffrer BAC par $2\,1\,3 \xrightarrow{f} 2^{-1} \cdot 1^{-1} \cdot 3^{-1} = 15 \cdot 1 \cdot 10$

car $2 \cdot 15 \equiv 1\ [29]$, $3 \cdot 10 \equiv 1\ [29]$, $1 \equiv 1\ [29]$.

*** Chiffrement de Hill

Soit $\Omega = \frac{\mathbb{Z}}{n\mathbb{Z}}$ et l'alphabet $A = \Omega^k$.

posons S une matrice inversible d'ordre k et à coefficients dans Ω, on chiffre $X = \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix}$ par $S \cdot X = Y$,

on déchiffre Y par $S^{-1} \cdot Y$.

Chapitre II

1. Anneaux

Soit A un ensemble non vide muni de deux lois internes $+, \cdot$

$$A \times A \longrightarrow A \qquad , \qquad A \times A \longrightarrow A$$
$$(x,y) \longrightarrow x+y \qquad\qquad (x,y) \longrightarrow x \cdot y$$

vérifiant les conditions suivantes:

1) $(A,+)$ est un groupe commutatif.

2) $(\cdot)$ est associative: $\forall a,b,c \in A \quad a(bc) = (ab)c$

3) $(\cdot)$ est distributive par rapport à $(+)$:

$$a(b+c) = ab + ac \quad , (b+c)a = ba + ca$$

on dit que $(A,+,\cdot)$ est un anneau.

Si de plus $(\cdot)$ est commutative, on dit que A est un anneau commutatif.

Si $(A,+,\cdot)$ admet un élément neutre 1 pour $(\cdot)$ on dit que A est un anneau unitaire.

Ex: $(\mathbb{Z},+,\cdot)$ est un anneau commutatif unitaire.

2. Corps: Si $(K,+,\cdot)$ est un anneau unitaire tel que tout élément non nul $x \neq 0$ admet un inverse pour $(\cdot)$ on dit que $(K,+,\cdot)$ est un corps.

Ex: $(\mathbb{R},+,\cdot)$ est un corps commutatif.

3. Sous anneau:

Soit A' une partie non vide d'un anneau $(A,+,\cdot)$. A' est un sous-anneau de A s'il est anneau pour les lois induits.

On montre que A' est un sous-anneau de A si

1) $x, y \in A' \Rightarrow x - y \in A'$
2) $x, y \in A' \Rightarrow x . y \in A'$

<u>ex:</u> $A' = 2\mathbb{Z}$ est un sous-anneau de $A = \mathbb{Z}$:

* $A' \neq \phi$, $0 \in 2\mathbb{Z}$

1) $x, y \in 2\mathbb{Z} \Rightarrow x - y = 2k - 2k' = 2(k - k') \in 2\mathbb{Z}$
2) $x, y \in 2\mathbb{Z} \Rightarrow x . y = (2k)(2k') = 2(2kk') \in 2\mathbb{Z}$.

Le résultat reste valable si on prend $A' = n\mathbb{Z}$, $n \in \mathbb{N}$.

4. <u>anneau intègre</u> :

un anneau $(A, +, .)$ est dit intègre si :

$x, y \in A$, $x . y = 0 \Rightarrow x = 0 \lor y = 0$

Si A n'est pas intègre $\exists x \neq 0, y \neq 0$ tel que $x . y = 0$

x, y sont appelés diviseurs de 0.

<u>ex:</u> a) $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}$ sont des anneaux intègres :

$$x . y = 0 \Rightarrow x = 0 \lor y = 0$$

b) $M_2(\mathbb{R})$ l'anneau des matrices d'ordre 2 et à coefficient dans $\mathbb{R}$ est non intègre :

Pour $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in M_2(\mathbb{R})$ on a :

$A, B \neq 0$ et $A . B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$.

5. <u>caractéristique d'un anneau</u>

Soit $(A, +, .)$ un anneau unitaire, la caractéristique de A est le plus petit entier $n \neq 0$ tel que $n . 1 = 0$.

Si n n'existe pas on dit que A est de caractéristique nulle.

Ex: a) $Cara(\mathbb{Z}) = 0$; $n.1 = 0 \Rightarrow n = 0$.

. b) $\frac{\mathbb{Z}}{6\mathbb{Z}}$ muni des deux lois $(+), \cdot$: $\bar{a}+\bar{b} = \overline{a+b}$, $\bar{a}.\bar{b} = \overline{ab}$

est un anneau commutatif unitaire non intègre :

$$\bar{2} \neq \bar{0} \ , \bar{3} \neq \bar{0} \ \text{ et } \ \bar{2}.\bar{3} = \bar{6} = \bar{0}$$

$Cara(\frac{\mathbb{Z}}{6\mathbb{Z}}) = 6$ car $6.\bar{1} = \bar{6} = \bar{0}$, $12.\bar{1} = \bar{0}$, $18.\bar{1} = \bar{0}$, ...

6 est le plus entier $n \neq 0$ vérifiant $n.\bar{1} = \bar{0}$.

6. idéal :

Soit I une partie nonvide d'un anneau commutatif A,

I est dit idéal si

1) $x, y \in I \Rightarrow x - y \in I$

2) $x \in A, y \in I \Rightarrow xy \in I$

Ex: $I = 3\mathbb{Z}$ est un idéal de l'anneau$(\mathbb{Z}, +, \cdot)$.

1) et 2) sont vérifiés.

Le résultat reste valable si on prend $I = n\mathbb{Z}, n \in \mathbb{N}$.

7. Anneau quotient :

Soit I un idéal d'un anneau $(A, +, \cdot)$, on définit une relation R dans A par :

$$x R y \Leftrightarrow x - y \in I$$

* R est reflexive :

$$x R x \Leftrightarrow x - x = 0 \in I \quad (\text{vérifié}).$$

* R est symétrique :

$x R y \Rightarrow x - y \in I$

$\Rightarrow -(x-y) = y - x \in I$ (d'aprés 1) de l'idéal).

$\Rightarrow y R x$

* R est transitive :

$x R y$ et $y R z$ $\Rightarrow x - y \in I, y - z \in I$

$\Rightarrow (x-y)+(y-z) = x - z \in I$ (car I est idéal)

$\Rightarrow x R z$

Donc R est une relation d'équivalence dans A.

La classe de x est $\bar{x} = \{y \in A \,/\, y R x\}$.

$yRx \Rightarrow y - x = a \in I$

$\Rightarrow y = x + a$ et $\bar{x} = x + I$.

On note par $\frac{A}{I}$ l'ensemble des classes : $\bar{x} = x + I$

on vérifie que $(\frac{A}{I}, +, .)$ est un anneau pour les lois $(+)$ et $(.)$

définies par $\bar{x} + \bar{y} = \overline{x+y}$, $\bar{x} . \bar{y} = \overline{xy}$

$\frac{A}{I}$ est dit anneau quotient, $\bar{0}$ est l'élément neutre pour $(+)$,

$-\bar{x} = \overline{(-x)}$ est le symétrique de $\bar{x}$.

Si A est unitaire, 1 son élément neutre alors

$\bar{1}$ est l'élément neutre pour $(.)$ dans $\frac{A}{I}$.

Ex : pour $I = 5\mathbb{Z}$ on obtient un anneau à cinq éléments

$\frac{A}{I} = \frac{\mathbb{Z}}{5\mathbb{Z}} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$.

Dans $\frac{\mathbb{Z}}{5\mathbb{Z}}$ tout élément non nul est inversible :

x	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
x^{-1}	$\bar{1}$	$\bar{3}$	$\bar{2}$	$\bar{4}$

, d'où $\frac{\mathbb{Z}}{5\mathbb{Z}}$ est un corps.

Dans la suite on va montrer que si p est premier

$\frac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps.

8. homomorphisme d'anneaux :

Soit f une application d'un anneau $(A_1, +, .)$ dans un anneau $(A_2, +, .)$ si :

1) $\forall a, b \in A_1$: $f(a+b) = f(a) + f(b)$

2) $\forall a, b \in A_1$: $f(ab) = f(a) . f(b)$

Si les 2 anneaux sont unitaires on ajoute une troisième condition : $f(1_{A_1}) = 1_{A_2}$

Si f est bijective on dit que f est un isomorphisme d'anneaux, dans ce cas les deux anneaux A_1 et A_2 ont les mêmes propriétés.

Pour tout homomorphisme d'anneaux f on définit $\ker f$ et $\mathrm{Im} f$ par :

$$\ker f = \{ x \in A_1 / f(x) = 0 \} \subset A_1$$

$$\mathrm{Im} f = \{ y \in A_2 / y = f(x), x \in A_1 \} \subset A_2$$

On montre que $\ker f$ est un idéal de A_1 et

$$\frac{A_1}{\ker f} \simeq \mathrm{Im} f \quad (\text{isomorphisme d'anneaux}).$$

9. Opérations sur les idéaux :

9.1 Somme de deux idéaux, Produit de deux idéaux

Soient $I + J = \{ z = x + y, \; x \in I, y \in J \}$ la somme de deux idéaux I, J et

$$I \cdot J = \{ z = x_1 y_1 + \cdots + x_n y_n \; / \; x_i \in I \text{ et } y_i \in J \}$$ le produit de deux idéaux I et J.

On montre que $I + J$, $I \cdot J$ sont des idéaux de A.
$I \cap J$ est aussi idéal de A.

__Ex :__ Soit $A = \mathbb{Z}$, $I = 6\mathbb{Z}$, $J = 9\mathbb{Z}$ alors

$$I + J = 6\mathbb{Z} + 9\mathbb{Z} = 3\mathbb{Z}$$

$$I \cap J = 18\mathbb{Z}, \quad I J = 54\mathbb{Z}$$

Si $I_1 = 3\mathbb{Z}$ et $J_1 = 4\mathbb{Z}$ on a $I_1 + J_1 = 3\mathbb{Z} + 4\mathbb{Z} = \mathbb{Z}$

et $I_1 \cdot J_1 = (3\mathbb{Z})(4\mathbb{Z}) = 12\mathbb{Z}$, $I_1 \cap J_1 = 12\mathbb{Z}$.

D'une façon générale on peut montrer que :

$m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ avec $d = PGCD(m,n)$.

$m\mathbb{Z} \cap n\mathbb{Z} = m\mathbb{Z}$ avec $m = PPCM(m,n)$

$m\mathbb{Z} \cdot n\mathbb{Z} = mn\mathbb{Z}$

9.2 Idéaux étrangers :

Soient I et J deux idéaux de A.

I et J sont dits étrangers si $I + J = A$.

Ex : $5\mathbb{Z}$ et $7\mathbb{Z}$ sont étrangers car $5\mathbb{Z} + 7\mathbb{Z} = \mathbb{Z}$.

10. Produit direct de deux anneaux

Soient A_1 et A_2 deux anneaux. Dans le produit cartésien $A_1 \times A_2$ on définit deux lois $(+)$ et $(\cdot)$ par :

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$
$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2, y_1 y_2)$$

$(A_1 \times A_2, +, \cdot)$ est un anneau appelé l'anneau produit.

Ex : $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$

est un anneau unitaire à 6 éléments.

11. Théorème chinois

Soient I et J deux idéaux étrangers d'un anneau commutatif unitaire A alors :

1. $IJ = I \cap J$
2. $\frac{A}{IJ} \simeq \frac{A}{I} \times \frac{A}{J}$ (isomorphisme d'anneaux).

Corollaire:

Si $\Delta(m,n)=1$ alors $\frac{\mathbb{Z}}{mn\mathbb{Z}} \simeq \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$

Preuve : on pose $A=\mathbb{Z}$, $I=n\mathbb{Z}$, $J=m\mathbb{Z}$.

D'après le théorème précédent : $IJ = I\cap J = nm\mathbb{Z}$ et

$$\frac{A}{IJ} = \frac{\mathbb{Z}}{nm\mathbb{Z}} \simeq \frac{A}{I}\times\frac{A}{J} = \frac{\mathbb{Z}}{n\mathbb{Z}}\times\frac{\mathbb{Z}}{m\mathbb{Z}}.$$

Pour expliciter cet isomorphisme il faut utiliser l'application

$f : A=\mathbb{Z} \longrightarrow \frac{A}{I}\times\frac{A}{J} = \frac{\mathbb{Z}}{n\mathbb{Z}}\times\frac{\mathbb{Z}}{m\mathbb{Z}}$ définie par

$f(x) = (\bar{x}, \bar{\bar{x}})$ avec $\bar{x}$ est la classe de x mod n et $\bar{\bar{x}}$ est la classe de x mod m

et vérifier que $\ker f = nm\mathbb{Z}$ et appliquer l'isomorphisme

$\frac{A}{\ker f} \simeq \operatorname{Im} f$.

La surjection f affirme que pour tout $(\bar{a}, \bar{\bar{b}}) \in \frac{\mathbb{Z}}{n\mathbb{Z}}\times\frac{\mathbb{Z}}{m\mathbb{Z}}$

il existe $x\in\mathbb{Z}$ tel que $\begin{cases} \bar{x} = \bar{a} \\ \bar{\bar{x}} = \bar{\bar{b}} \end{cases}$ autrement dit le système

$\begin{cases} x \equiv a \, [n] \\ x \equiv b \, [m] \end{cases}$ admet une solution si $\Delta(m,n)=1$.

Système de congruence :

Soit le système $\begin{cases} x \equiv u_1 \, [m_1] \\ \vdots \\ x \equiv u_n \, [m_n] \end{cases}$ avec $\Delta(m_i, m_j)=1$, $i\neq j$

Notons x_0 une solution particulière de ce système.

Alors la solution générale est $x = x_0 + \prod_{i=1}^{n} m_i \cdot k$, $k\in\mathbb{Z}$.

Si $n=2$ x_0 peut être calculée à l'aide de la relation de Bezout.

Dans le cas général on applique l'algorithme de Lagrange pour le calcul de x_0 :

1. on pose $M = \prod_{i=1}^{n} m_i$
2. $M_i = \frac{M}{m_i}$, $i = 1, \dots, n$
3. on calcule $N_i = M_i^{-1} \, [m_i]$
4. on obtient la solution particulière $x_0 = \sum_{i=1}^{n} u_i N_i M_i \; [M]$

ex : Résoudre dans $\mathbb{Z}$ le système :

$$\begin{cases} x \equiv 2 \, [3] \\ x \equiv 3 \, [5] \\ x \equiv 1 \, [7] \end{cases}$$

1) on a $M = 3 \times 5 \times 7 = 105$

2) $M_1 = \frac{105}{3} = 35$, $M_2 = \frac{105}{5} = 21$, $M_3 = \frac{105}{7} = 15$

3) $N_1 \equiv M_1^{-1} [3] \equiv 35^{-1} [3] \equiv 2^{-1} [3] = 2$

$N_2 = M_2^{-1} [5] \equiv 21^{-1} [5] = 1$

$N_3 = M_3^{-1} [7] \equiv 15^{-1} [7] = 1$

4) $x_0 = u_1 N_1 M_1 + u_2 N_2 M_2 + u_3 N_3 M_3 = 2.2.35 + 3.1.21 + 1.1.15 \; [105$

$= 8$

d'où la solution générale est :

$x = 8 + 105k$, $k \in \mathbb{Z}$.