Chap. II : Outils mathématiques pour la cryptographie à clef secrète

Laurent Poinsot

25 septembre 2009

Plan

Plan

Plan

Plan

Plan

Plan

Choix de la clef secrète

Lorsqu'Alice et Bob utilisent un système de chiffrement à clef secrète pour communiquer de façon confidentielle, ils doivent impérativement s'accorder sur le choix de la clef utilisée.
Ils vont utiliser cette clef secrète commune pour chiffrer et déchiffrer leurs messages.
Il est primordial que cette clef - comme son nom l'indique - ne soit connue que par les interlocuteurs légitimes : Alice et Bob, et eux seulement : la confidentialité repose sur ce secret partagé par Alice et Bob.
Pour effectuer le choix de cette clef secrète, Alice et Bob ne disposent que de deux possibilités :

1. Soit ils se rencontrent physiquement ;
2. Soit ils communiquent *via* un canal **privé sécurisé**.

Remarque 1

Mais si on dispose d'un canal de communication privé sécurisé, alors pourquoi ne pas l'utiliser directement pour toutes les communications entre Alice et Bob ?
En général, un tel réseau est très coûteux en temps de traitement et en infrastructure. C'est pourquoi on utilise de tels canaux seulement pour communiquer la clef secrète. Puis on utilise un canal public pour l'envoi des messages chiffrés car le traitement est alors beaucoup plus rapide et on emploie les infrastructures de communication existantes (Internet, téléphone, *etc.*).

Remarque 2

La façon de choisir la clef secrète n'est pas décrite dans les protocoles que l'on va étudier. Autrement dit, à partir de maintenant on suppose qu'Alice et Bob se sont mis d'accord d'une manière ou d'une autre quant au choix de la clef secrète. Ce problème ne nous concerne pas !

Bijection (1)

La cryptographie moderne met essentiellement en œuvre des objets mathématiques : fonctions, substitutions, transpositions, matrices, *etc.* Nous nous y intéressons dans cette section.
La cryptographie **a besoin** des bijections afin de réaliser le déchiffrement. Une bijection entre deux ensembles finis X et Y est une fonction $f : X \to Y$ telle quels que soient $x_1, x_2 \in X$, si $x_1 \neq x_2$, alors $f(x_1) \neq f(x_2)$. De façon équivalente, $f : X \to Y$ est une bijection, si, et seulement si, quel que soit $y \in Y$, il existe un $x \in X$ tel que $f(x) = y$.

Bijection (2)

En termes moins formels, $f : X \to Y$ est une bijection, si, et seulement si, on peut mettre en correspondance chaque élément de Y avec un et un seul élément de X. L'idée étant que l'on peut **renommer** chaque élément de X en un élément de Y.
Par exemple, soient $X = \{a, b, c\}$ et $Y = \{1, 2, 3\}$. On définit l'application $f : X \to Y$ par $f(a) = 1$, $f(b) = 3$, $f(c) = 2$. Alors f est une bijection. Soit $g : X \to Y$ telle que $g(a) = 1$, $g(b) = g(c) = 2$. Alors g n'est pas une bijection (pourquoi ?). Une conséquence de la définition des fonctions bijectives : soient deux ensembles finis X, Y quelconques, il ne peut y avoir une bijection $f : X \to Y$ que si X et Y ont exactement le même nombre d'éléments. Par exemple, entre $X = \{a, b, c, d\}$ et $Y = \{1, 2, 3\}$, il n'existe aucune bijection.

Bijection (3)

L'intérêt cryptographique des bijections repose sur leur propriété d'**inversibilité**. Si $f : X \to Y$ est une bijection, alors il existe une fonction $g : Y \to X$ (qui est elle-même également une bijection) telle que quel que soit $x \in X$, $g(f(x)) = x$ et quel que soit $y \in Y$, $f(g(y)) = y$. On dit que g est la **fonction inverse** (ou **réciproque**) de f, et on la note parfois f^{-1}.
Exemple : reprenons $X = \{a, b, c\}$, $Y = \{1, 2, 3\}$ et $f : X \to Y$ définie par $f(a) = 1$, $f(b) = 3$ et $f(c) = 2$. Quelle est la fonction inverse de f ? C'est la fonction $g : Y \to X$ définie par $g(1) = a$, $g(2) = c$ et $g(3) = b$.

Bijection (4)

Pourquoi la propriété d'inversibilité des bijections est-elle intéressante d'un point de vue cryptographique ?
Pour que le déchiffrement soit possible. En effet, soit un message clair M qu'Alice chiffre avec la fonction E et la clef secrète K, de sorte que l'on obtienne le message chiffré $C := E_K(M)$. Lorsque Bob reçoit C, il va devoir le déchiffrer afin de comprendre le message d'Alice. Pour ce faire, il utilise la fonction de déchiffrement D et la clef secrète K : en effet, on sait que l'on a $D_K(C) = D_K(E_K(M)) = M$. En d'autres termes, la fonction E_K qui transforme un message clair en un message chiffré est une bijection et sa fonction inverse n'est autre que D_K.

Substitution (1)

Une substitution est une bijection qui consiste à remplacer chaque lettre d'un message par une autre lettre. Attention : partout où une lettre donnée apparaît, elle est toujours remplacée par la **même** lettre. Ainsi, si dans le texte original, "a" devient "u", alors dès qu'on verra un "a", on le remplacera par un "u".
Par exemple,

$$\begin{array}{lcccccccccccccc} M = & m & e & s & s & a & g & e & & s & e & c & r & e & t \\ C = & b & x & v & v & g & o & x & & v & x & u & l & x & e \end{array}$$

m est remplacée par *b*, *e* par *x*, *s* par *v*, *a* par *g*, *g* par *o*, *c* par *u*, *r* par *l* et *t* par *e*.

Substitution (2)

La ”substitution” ainsi définie est-elle une bijection de l'alphabet usuel dans lui-même ? On ne peut pas le certifier car il faudrait que l'on sache par quelle lettre est remplacée **chaque lettre** de l'alphabet et pas seulement les lettres a,c,e,g,m,r,s,t comme dans notre exemple.
Une substitution qui par exemple transformerait à un endroit d'un texte une lettre ”a” par un ”u” puis à un autre endroit du texte, une autre lettre ”a” cette fois-çi par un ”n” n'est pas une bijection !
Une substitution qui par exemple transforme deux lettres distinctes en une même lettre, par ex., ”a” $\longrightarrow$ ”u” et ”b” $\longrightarrow$ ”u”, n'est pas une bijection !

Substitution (3)

Dans les substitutions on peut transformer des lettres en d'autres symboles et non nécessairement d'autres lettres du **même alphabet**.
Par exemple, on définit une substitution de l'alphabet $\{a, b, c, d\}$ dans l'alphabet $\{1, 2, 3, 4\}$ par "a" $\longrightarrow$ "3", "b" $\longrightarrow$ "1", "c" $\longrightarrow$ "4" et "d" $\longrightarrow$ "2".
Avec cette substitution, le texte "abbcdadd" est transformé en "31142322".

Substitution (4)

Une substitution ne change pas l'**ordre** des lettres dans un message mais seulement les lettres elle-mêmes figurant dans le message. En d'autres termes, à partir d'un message, on remplace chaque lettre par un autre symbole mais en conservant l'ordre d'apparition des lettres. Par exemple, si une lettre "e" apparaît en positions 3, 8, 25 d'un message "$\ldots \underbrace{e}_{3} \ldots \underbrace{e}_{8} \ldots \underbrace{e}_{25} \ldots$", alors on la remplace, disons, par le symbole "@" exactement aux positions 3, 8 et 25 de telle sorte que l'on obtienne : "$\ldots \underbrace{@}_{3} \ldots \underbrace{@}_{8} \ldots \underbrace{@}_{25} \ldots$". Pour changer l'ordre, on utilise les **transpositions**.

Transposition (1)

Dans une transposition, on ne modifie pas l'écriture des lettres mais leur ordre dans un message. Par exemple,

$$\begin{array}{lcccccccccccccc} M = & m & e & s & s & a & g & e & & s & e & c & r & e & t \\ C = & e & m & e & a & s & g & s & & e & c & s & r & t & e \end{array}$$

Regardons plus en détails cet exemple.

Transposition (2)

m e s s a g e s e c r e t

Transposition (2)

m e s s a g e s e c r e t
e

Transposition (2)

m e s s a g e s e c r e t

e m

Transposition (2)

m e s s a g e s e c r e t
e m s

Transposition (2)

m e s s a g e s e c r e t

e m s s

Transposition (2)

m e s s a g e s e c r e t

e m a s s

Transposition (2)

m e s s a g e s e c r e t

e m a s g s

Transposition (2)

m e s s a g e s e c r e t

e m e a s g s

Transposition (2)

m	*e*	*s*	*s*	*a*	*g*	*e*		*s*	*e*	*c*	*r*	*e*	*t*
e	*m*	*e*	*a*	*s*	*g*	*s*				*s*			

Transposition (2)

m	*e*	*s*	*s*	*a*	*g*	*e*		*s*	*e*	*c*	*r*	*e*	*t*
e	*m*	*e*	*a*	*s*	*g*	*s*				*s*			*e*

Transposition (2)

m	*e*	*s*	*s*	*a*	*g*	*e*		*s*	*e*	*c*	*r*	*e*	*t*
e	*m*	*e*	*a*	*s*	*g*	*s*			*c*	*s*			*e*

Transposition (2)

m	*e*	*s*	*s*	*a*	*g*	*e*		*s*	*e*	*c*	*r*	*e*	*t*
e	*m*	*e*	*a*	*s*	*g*	*s*			*c*	*s*	*r*		*e*

Transposition (2)

m	*e*	*s*	*s*	*a*	*g*	*e*		*s*	*e*	*c*	*r*	*e*	*t*
e	*m*	*e*	*a*	*s*	*g*	*s*		*e*	*c*	*s*	*r*		*e*

Transposition (2)

m	*e*	*s*	*s*	*a*	*g*	*e*		*s*	*e*	*c*	*r*	*e*	*t*
e	*m*	*e*	*a*	*s*	*g*	*s*		*e*	*c*	*s*	*r*	*t*	*e*

Transposition (3)

Une transposition opère de façon identique quel que soit le message. Cela signifie que la transposition ne dépend que de l'ordre des lettres dans un message et non des lettre elles-mêmes. Si on reprend l'exemple précédent, on peut représenter de façon graphique la transposition :

1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	1	7	5	3	6	4	8	13	11	9	12	14	10

Arithmétique modulaire (1)

De nombreux cryptosystèmes sont (au moins en partie) basés sur l'**arithmétique modulaire**.

Définition

Si a, b et n sont des entiers, et si $n > 0$, on écrit

$$a = b \pmod{n} \tag{1}$$

si, et seulement si, n divise $b - a$. La phrase "$a = b \pmod{n}$" se prononce "a est congru à b modulo n". L'entier n est parfois appelé le **modulus**.

Arithmétique modulaire (2)

Supposons que l'on effectue une division euclidienne de a et de b par n. On obtient des quotients et des restes, ceux-ci étant compris entre 0 et $n-1$. Précisément, on a $a = q_1 n + r_1$ et $b = q_2 n + r_2$ avec $0 \leq r_1 \leq n-1$ et $0 \leq r_2 \leq n-1$. Ainsi il est facile de voir que $a = b \pmod{n}$ si, et seulement si, $r_1 = r_2$, c'est-à-dire que a et b ont le même reste dans la division entière par n. On note également "$a \pmod{n}$" le reste de la division euclidienne de a par n. Si on remplace a par $a \pmod{n}$, on dit que l'on *réduit a modulo n*.

Arithmétique modulaire (3)

On est maintenant en mesure de définir l'arithmétique modulo n. $\mathbb{Z}_n$ symbolise l'ensemble $\{0, \ldots, n-1\}$. On définit sur $\mathbb{Z}_n$ deux opérations notées $+$ et $\times$. L'addition et la multiplication dans $\mathbb{Z}_n$ fonctionnent exactement comme l'addition et la multiplication usuelles, excepté le fait que tous les résultats sont réduits modulo n.
Supposons par exemple que l'on veuille calculer 11×13 dans $\mathbb{Z}_{16}$. En tant qu'entiers ordinaires, on a $11 \times 13 = 143$. Pour réduire 143 modulo 16, on réalise une division euclidienne : $143 = 8 \times 16 + 15$, donc $143 \pmod{16} = 15$, et par conséquent, $11 \times 13 = 15$ dans $\mathbb{Z}_{16}$.

Arithmétique modulaire (4)

Addition modulo n : Pour a et b des entiers quelconques, l'addition modulo n de a et b est $(a+b) \pmod{n}$ soit le reste modulo n de $a+b$. Concrétement pour calculer cette somme, on commence par calculer $a+b$ de façon usuelle, puis on réduit le résultat modulo n. Le résultat de cette addition appartient à l'ensemble $\mathbb{Z}_n$. En particulier l'addition modulo n définis une opération **interne** de $\mathbb{Z}_n$ autrement dit, $+$ envoie un couple d'éléments a, b de $\mathbb{Z}_n$ dans $\mathbb{Z}_n$.
Exemples :

1. $3+7 \pmod{2} = 0$;
2. $3+7 \pmod{5} = 0$;
3. $3+7 \pmod{6} = 4$;
4. $3+7 \pmod{11} = 10$.

Arithmétique modulaire (5)

Soustraction modulo n : Pour a et b des entiers tels que $a \geq b$, la soustraction modulo n de a et b est $(a - b) \pmod{n}$ soit le reste modulo n de $a - b$. Concrétement pour effectuer cette soustraction, on commence par calculer $a - b$ de façon usuelle, puis on réduit le résultat modulo n.

Exemples :

1. $7 - 3 \pmod{2} = 0$;
2. $7 - 2 \pmod{3} = 2$.

Arithmétique modulaire (6)

Opposé modulo n : Soit $a \in \mathbb{Z}_n$, alors $n - a$ satisfait la propriété $a + (n - a) = 0 = (n - a) + a$ (additions modulo n). $n - a$ est l'**opposé modulo** n **de** a, qui est noté $-a$. Remarquons que si $a = 0$, alors $n - a = n = 0 \pmod{n}$.
Exemples :

1. $-3 \pmod 5 = 2$. On a donc $3 + 2 = 0 \pmod 5$;
2. $-4 \pmod 8 = 4$. On a donc $4 + 4 = 0 \pmod 8$.

Arithmétique modulaire (7)

Multiplication modulo n : Pour a et b des entiers quelconques, la multiplication modulo n de a par b est $(a \times b) \pmod{n}$ soit le reste modulo n de $a \times b$.
Concrètement pour calculer ce produit, on commence par calculer $a \times b$ de façon usuelle, puis on réduit le résultat modulo n. La multiplication modulo n est également une opération interne à $\mathbb{Z}_n$.
Exemples :

1. $3 \times 2 \pmod{2} = 0$;
2. $3 \times 2 \pmod{5} = 1$;
3. $3 \times 2 \pmod{6} = 0$;
4. $3 \times 2 \pmod{4} = 2$.

Arithmétique modulaire (8)

L'addition et la multiplication dans $\mathbb{Z}_n$ satisfont la plupart des règles familières en arithmétique que l'on rappelle ci-dessous. Soient $a, b, c \in \mathbb{Z}_n$.

1. L'addition est commutative : $a + b = b + a$;
2. L'addition est associative : $(a + b) + c = a + (b + c)$;
3. 0 est neutre pour $+$: $a + 0 = a = 0 + a$;
4. L'opposé $-a$ de a est $-a := n - a$: $a + (n - a) = (n - a) + a = 0$. En particulier l'opposé de 0 est 0 ;
5. La multiplication est commutative : $ab = ba$;
6. La multiplication est associative : $a(bc) = (ab)c$;
7. 1 est neutre pour la multiplication : $a1 = a = 1a$;
8. La multiplication est distributive sur l'addition : $(a + b)c = ac + bc$ et $a(b + c) = ab + ac$.

Groupes pour la cryptographie

Les propriétés (2), (3) et (4) précisent que $\mathbb{Z}_n$ possède une structure algébrique de **groupe**. De façon général un groupe G est un ensemble non vide muni d'une loi de composition interne

$$\begin{array}{rccc} * : & G \times G & \to & G \\ & (g_1, g_2) & \mapsto & g_1 * g_2 \end{array} \tag{2}$$

tels que

1. $*$ est associative : $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$;
2. Il existe un unique élément $e \in G$ tel que $e * g = g * e = g$ pour tout $g \in G$. e est appelé **élément neutre de** G ;
3. Quel que soit $g \in G$, il existe un unique élément $g' \in G$ tel que $g * g' = g' * g = e$. g' est appelé l'**opposé de** g et noté $-g$ ou l'**inverse de** g et noté g^{-1}.

Pourquoi est-ce intéressant d'utiliser des groupes en cryptographie ?

Le plus important dans un groupe est l'existence d'un inverse (ou opposé) de chaque élément. Cela implique que les "translations" sont des bijections. Une translation par un élément g_0 de G est l'application

$$\begin{array}{rccc} G_{g_0} : & G & \longrightarrow & G \\ & g & \longmapsto & g_0 * g \, . \end{array} \tag{3}$$

Puisque g_0 admet un inverse g_0^{-1}, G_{g_0} est une fonction inversible et sa fonction inverse n'est autre que la translation $G_{g_0^{-1}}$ par g_0^{-1}. En effet, $G_{g_0}(G_{g_0^{-1}}(g)) = G_{g_0}(g_0^{-1} * g)$ $= g_0 * (g_0^{-1} * g) = (g_0 * g_0^{-1}) * g = e * g = g$. Les groupes fournissent donc des fonctions qui peuvent être utilisées dans des algorithmes de chiffrement car elles sont inversibles et permettent donc de réaliser le déchiffrement.