Cryptographie

Jean-Marc Alliot[1]

[1]e-mail : alliot@recherche.enac.fr

Chapitre 1

Éléments mathématiques

La plupart des systèmes de cryptographie à clef publique sont basés sur des techniques mathématiques, qu'elles soient arithmétiques, algébriques ou analytiques.

L'outil indispensable à connaître est la théorie des corps quotients de $\mathbb{Z}$, que nous allons rapidement présenter.

1.1 Définitions élémentaire

Définition 1 (Groupe). *Un groupe est un couple $(G, +)$ où $+$ est une loi de composition interne sur G, associative, possédant un élément neutre, et telle que tout élément de G admet un symétrique pour cette loi. Si $+$ est commutative, le groupe est dit commutatif, ou abélien.*

S'il n'y a pas d'ambiguïté sur la loi, on parlera parfois simplement du groupe G. Le couple $(\mathbb{Z}, +)$ composé de l'ensemble des entiers relatifs et de l'addition usuelle est un groupe abélien.

Définition 2 (Sous-groupe). *Soit le groupe $(G, +)$. On dit que $(S, +)$ est un sous-groupe de G si S est une partie de G stable pour $+$ et S est un groupe pour la loi $+$ induite par G sur S.*

Les entiers pairs $2\mathbb{Z}$ munis de l'addition sont un sous groupe de $(\mathbb{Z}, +)$.

Définition 3 (Anneau). *Un anneau est un triplet $(A, +, .)$ où la loi $+$ (dite "additive") est une loi de groupe abélien sur A et la loi $.$ (dite "multiplicative") est une loi de composition interne, associative, et distributive par rapport à l'addition. Si la multiplication est commutative, l'anneau est dit commutatif, et si elle possède un élément neutre, l'anneau est dit unitaire.*

Là encore, s'il n'y a pas d'ambiguïté sur les lois, on parlera parfois simplement de l'anneau A. Le triplet $(\mathbb{Z}, +, .)$ composé de l'ensemble des entiers relatifs, de l'addition et de la multiplication usuelles est un anneau commutatif unitaire.

Définition 4 (Corps). *Un corps est un anneau unitaire $(K, +, .)$ tel que $(K - \{0\}, .)$ (où 0 est l'élément neutre de l'addition) est un groupe.*

Tout élément non nul de K est donc inversible dans K. Des exemples classiques de corps sont $(\mathbb{R}, +, .)$ (ensemble des nombres réels) et $(\mathbb{Q}, +, .)$ (ensemble des nombres rationnels).

Définition 5 (Idéal d'un anneau commutatif A). *I est un idéal de A si et seulement si I est un sous-groupe additif de A et pour tout élément x de A et tout élément y de I, $x.y \in I$.*

Les idéaux de l'anneau $\mathbb{Z}$ sont les sous-groupes $n\mathbb{Z}$ (ensemble des multiples de n) avec $n \geq 0$.

Définition 6 (Relation sur un ensemble E). *Une relation $\mathcal{R}$ sur un ensemble E est un couple (E, G) ou G est une partie du produit cartésien $E \times E$, appelée graphe de la relation. On dit que a est en relation avec b, et l'on note $a\,\mathcal{R}\,b$, si et seulement si $(a, b) \in G$.*

En pratique, une relation est plutôt définie par une propriété, que par la donnée extensive du graphe.

Définition 7 (Relation d'équivalence). *$\mathcal{R}$ est une relation d'équivalence sur l'ensemble E si et seulement si $\mathcal{R}$ est réflexive (pour tout x de E, on a $x\,\mathcal{R}\,x$), symétrique (si $x\,\mathcal{R}\,y$ alors $y\,\mathcal{R}\,x$) et transitive (si $x\,\mathcal{R}\,y$ et $y\,\mathcal{R}\,z$ alors $x\,\mathcal{R}\,z$).*

Un exemple simple de relation d'équivalence est, par exemple, la relation définie par "$x\,\mathcal{R}\,y$ si x a le même nombre de chiffres en base 10 que y".

Définition 8 (Classe d'équivalence). *Soit $\mathcal{R}$ une relation d'équivalence sur E. La classe d'équivalence d'un élément x de E est le sous-ensemble des éléments de E en relation avec x suivant $\mathcal{R}$.*

On dit que deux éléments x et y d'une même classe d'équivalence sont *équivalents* suivant $\mathcal{R}$. Notons également que l'ensemble des classes d'équivalence suivant $\mathcal{R}$ forme une partition de E[1].

Définition 9 (Ensemble quotient de E par $\mathcal{R}$). *Soit $\mathcal{R}$ une relation d'équivalence sur E. L'ensemble des classes d'équivalence de E suivant $\mathcal{R}$ est appelé ensemble quotient de E par $\mathcal{R}$, et il est noté $E/\mathcal{R}$.*

[1] Démonstration élémentaire laissée à la diligence du lecteur.

Définition 10 (Classes à gauche, classes à droite). *Soit $(G, +)$ un groupe, H un sous-groupe de G et a un élément de G. Alors les ensembles*

$$aH = \{a + h | h \in H\} \text{ et } Ha = \{h + a | h \in H\}$$

sont appelées respectivement classe à gauche et classe à droite de a suivant H.

Les éléments de aH (resp. Ha) sont les classes d'équivalence de a pour la relation d'équivalence définie par : $x\mathcal{R}y$ si et seulement si $(y - x) \in H$ (resp. $(x - y) \in H$).

Pour deux éléments a et b de G, les ensembles aH et bH sont soit confondus, soit disjoints (a et b sont soit dans la même classe d'équivalence, soit dans des classes d'équivalence différentes) et les ensembles de la forme aH, pour a variant sur tout G, forment une partition de G (toujours en raison des propriétés de la relation d'équivalence).

Théorème 1 (Théorème de Lagrange). *Soit G groupe fini et H un sous groupe de G. Alors le cardinal[2] de H divise le cardinal de G.*

Nous savons déjà que les classes d'équivalence de la relation : $x\mathcal{R}y$ si et seulement si $(y - x) \in H$, forment une partition de G. Remarquons maintenant que l'application qui à x associe $a + x$ definit une bijection de H sur aH. Donc le cardinal de aH est exactement le cardinal de H, et ce pour tout a de G. Donc chaque classe d'équivalence de $\mathcal{R}$ a exactement le même cardinal, qui est aussi celui de H. Donc le cardinal de H divise le cardinal de G.

Définition 11 (Congruence). *Une congruence $\mathcal{R}$ sur un ensemble E, muni d'une loi de composition interne $+$, est une relation d'équivalence sur E, compatible avec la loi de composition interne $+$: soit $x \mathcal{R} y$ et $z \mathcal{R} w$ alors $(x + z) \mathcal{R} (y + w)$.*

1.2 Éléments d'arithmétique

Théorème 2 (Division euclidienne). *Soit deux entiers naturels a et b avec $a > b$. Il existe un couple unique d'entiers naturel q et r (avec $0 \leq r < b$) vérifiant $a = bq + r$.*

q est appelé le quotient de la division euclidienne de a par b et r le reste. La démonstration est triviale.

Définition 12 (Diviseur). *On dit qu'un entier b divise un entier $a > b$ (et on note $a|b$) si et seulement si le reste de la division euclidienne de a par b est égal à 0. On dit aussi que a est un multiple de b.*

[2] On appelle aussi parfois le cardinal d'un groupe, l'*ordre* de ce groupe.

Définition 13 (Nombre premier). *Un nombre p est dit premier si et seulement si il n'a que deux diviseurs positifs : 1 et lui-même.*

Théorème 3 (Théorème fondamental de l'arithmétique). *Tout entier naturel n peut s'écrire de façon unique en un produit de nombre premiers, appelé décomposition en facteurs premiers de n.*

Une assertion équivalente au théorème fondamental consiste à dire que si un nombre premier p divise ab alors p divise a ou p divise b. Un nombre premier est, quant à lui, dit irréductible[3].

Définition 14 (Plus grand diviseur commun (pgcd)). *Le plus grand diviseur commun de deux entiers a et b, noté pgcd(a, b) est le plus grand entier d divisant à la fois a et b.*

Une définition équivalente du pgcd consiste à dire qu'il s'agit du seul entier divisant a et b et divisible par tous les autres entiers divisant à la fois a et b. Il est aisé de trouver le pgcd de deux nombres lorsque l'on connaît leurs décompositions en facteurs premiers : il suffit de prendre le produit des entiers premiers apparaissant dans les deux décompositions avec l'exposant minimal. Il est malheureusement rare de connaître dans le cas général la décomposition en facteurs premiers d'un nombre quelconque (la sécurité de nombreux systèmes cryptographiques comme le RSA repose précisément sur la difficulté qu'il y a à décomposer un nombre en facteurs premiers). Il existe pourtant une méthode rapide permettant de trouver le pgcd de deux nombres.

Théorème 4 (Algorithme d'Euclide). *Soit deux entiers a et b ($b < a$). On définit la suite r_n suivante :*

$$r_{n-1} = q_n r_n + r_{n+1} \text{ avec } 0 \leq r_{n+1} < r_n$$

avec $r_0 = a$ et $r_1 = b$. Alors, il existe n_0 tel que $r_{n_0+1} = 0$ et r_{n_0} est le pgcd de a et b.

Démonstration : La suite r_n est strictement décroissante et minorée par 0, puisqu'il s'agit de la définition même de la division euclidienne. Donc il existe nécessairement n_0 tel que $r_{n_0+1} = 0$. Montrons maintenant que r_{n_0} est le pgcd de a et b. Pour cela, utilisons la seconde définition du pgcd, c'est à dire qu'il s'agit du seul entier divisant a et b et divisible par tous les autres entiers divisant simultanément a et b.

[3]Ces définitions, valables pour l'arithmétique des entiers naturels ou relatifs, devient fausse pour l'arithmétique des nombres algébriques, comme par exemple les nombres de la forme $a + b\sqrt{10}$, pour lesquels l'irréductibilité n'est pas équivalente à la primalité.

Vérifions tout d'abord que r_{n_0} divise a et b. On a $r_{n_0-1} = q_{n_0} r_{n_0} + 0$. Donc r_{n_0} divise r_{n_0-1} Mais s'il divise r_{n_0-1} il divise aussi r_{n_0-2} puisque $r_{n_0-2} = q_{n_0-1} r_{n_0-1} + r_{n_0}$, etc. Par récurrence, on démontre ainsi aisément que r_{n_0} divise tous les r_n et donc divise a et b.

Réciproquement, considérons un nombre c qui divise a et b. c divise donc r_0 et r_1 par définition. Mais alors, il divise également r_2 puisque $r_0 = q_1 r_1 + r_2$, etc. Par récurrence, on démontre donc qu'il divise tous les r_n et donc qu'il divise r_{n_0}.

L'algorithme d'Euclide permet d'établir aisément le théorème suivant.

Théorème 5 (Identité de Bezout). *Soit a et b deux nombres tels que pgcd$(a, b) = d$. Il existe alors deux entiers relatifs u et v tels que $au + bv = d$.*

Démonstration : récrivons les relations ci-dessus :

$$\begin{aligned} r_{n_0} &= r_{n_0-2} - q_{n_0-1} r_{n_0-1} && (1.1)\\ \cdots &= \cdots && (1.2)\\ r_{n-1} &= r_{n-3} - q_{n-2} r_{n-2} && (1.3)\\ \cdots &= \cdots && (1.4)\\ r_3 &= r_1 - q_2 r_2 && (1.5)\\ r_2 &= r_0 - q_1 r_1 && (1.6) \end{aligned}$$

On voit donc que r_2 peut s'écrire comme une combinaison linéaire de r_0 et r_1 (c'est à dire de a et b). r_3 peut donc s'écrire comme une combinaison linéaire de a et b en remplaçant r_2 par son expression en a et b. On peut ainsi vérifier par récurrence que tous les r_n peuvent s'écrire sous la forme d'une combinaison linéaire de a et b, et ce résultat est donc également valable pour le pgcd r_{n_0}.

Définition 15 (Relation de congruence pour les entiers relatifs). *Soit a et b deux entiers relatifs. Soit p un entier naturel fixé. On dit que a et b sont congrus modulo p si et seulement si $a - b$ est un multiple de p. On note alors :*

$$a \equiv b \ [p]$$

Il est aisé de vérifier que la relation définie ci dessus est une relation d'équivalence (réflexive, symétrique et transitive).

Définition 16 (Ensemble quotient). *On note $\mathbb{Z}/p\mathbb{Z}$ l'ensemble des classes d'équivalence de la relation de congruence modulo p et $\widehat{\ }$ la fonction qui à chaque élément a de $\mathbb{Z}$ associe sa classe d'équivalence $\widehat{a}$ dans $\mathbb{Z}/p\mathbb{Z}$.*

Notons que $\mathbb{Z}/p\mathbb{Z}$ contient exactement p éléments qui sont représentés par les éléments canoniques $\widehat{0}, \widehat{1}, \cdots, \widehat{p-1}$.

Définition 17 (Arithmétique de $\mathbb{Z}/p\mathbb{Z}$). *On étend l'arithmétique de $\mathbb{Z}$ à $\mathbb{Z}/p\mathbb{Z}$ en définissant les fonctions $\widehat{+}$ et $\widehat{\times}$ de la façon suivante :*

$$\begin{aligned} \widehat{a} \,\widehat{+}\, \widehat{b} &= \widehat{a+b} \\ \widehat{a} \,\widehat{\times}\, \widehat{b} &= \widehat{a \times b} \end{aligned}$$

Pour que cette définition ait un sens, il faut vérifier que les opérations définies ci-dessus sont bien indépendantes du représentant choisi dans la classe d'équivalence. Cela est rendu évident par les formules : $(pa+b)+(pc+d) = p(a+b)+(c+d)$ et $(pa+b)(pc+d) = p(pac+cb+ad)+bd$.

Théorème 6. *$\mathbb{Z}/p\mathbb{Z}$ muni des opérations $\widehat{+}$ et $\widehat{\times}$ est un anneau. La fonction $\widehat{\ }$ est un morphisme surjectif d'anneau.*

On abandonne généralement la notation $\widehat{\ }$ pour les opérateurs et les classes d'équivalence de $\mathbb{Z}/p\mathbb{Z}$, et on les note simplement $+$, $\times$ et $0 \cdots p-1$, notation que nous adopterons dans la suite.

Exemple 1. *Posons $p = 5$. Les élément de $\mathbb{Z}/5\mathbb{Z}$ sont 0, 1, 2, 3 et 4. 0 est bien évidemment élément neutre pour l'addition et 1 élément neutre pour la multiplication. L'inverse (pour l'addition) de 2 est 3 ($2+3 = 5 \equiv 0\ [5]$), celui de 4 est 1.*

Théorème 7 (Inversibilité dans $\mathbb{Z}/p\mathbb{Z}$). *Un élément $\widehat{a}$ de $\mathbb{Z}/p\mathbb{Z}$ est inversible si et seulement si a et p sont premiers entre eux.*

Démonstration : si a et p sont premiers entre eux, alors il existe u et v tels que $au + pv = 1$. Modulo p, cette relation devient $au \equiv 1\ [p]$. u est donc l'inverse de a dans $\mathbb{Z}/p\mathbb{Z}$.

Réciproquement, si a et p ne sont pas premiers entre eux alors il existe trois nombres q, r, s avec $1 < q < p$ et $1 < s < p$ tels que $qr = a$ et $qs = p$ (q est le pgcd de a et p). On en déduit $qrs = qsr = pr = as$ qui devient modulo p : $as \equiv 0\ [p]$. Donc $\widehat{a}$ est un diviseur de zéro dans $\mathbb{Z}/p\mathbb{Z}$ et n'admet donc pas d'inverse[4].

Théorème 8 (Corps $\mathbb{Z}/p\mathbb{Z}$). *$Z/p\mathbb{Z}$ est un corps si et seulement si p est premier.*

Démonstration : si p est premier, alors tout nombre compris strictement entre 1 et p est premier avec p, donc tout nombre de $\mathbb{Z}/p\mathbb{Z}$ est inversible. Réciproquement, si p n'est pas premier, il admet au moins un diviseur compris strictement entre 1 et p, qui ne sera donc pas inversible.

[4] S'il en admettait un, que nous noterions a^{-1}, on aurait (comme $as = 0$) : $a^{-1}as = 0$, soit $s = 0$ dans $\mathbb{Z}/p\mathbb{Z}$, ce qui est contredit l'hypothèse $1 < s < p$ dans $\mathbb{Z}$.

Théorème 9 (Théorème chinois). *Soit le système de s congruences suivant :*

$$\begin{aligned} x &\equiv a_1 \ [m_1] \\ x &\equiv a_2 \ [m_2] \\ \cdots &\equiv \cdots \\ x &\equiv a_s \ [m_s] \end{aligned}$$

et $\forall i, j, \ j \neq i$, pgcd$(m_i, m_j) = 1$. Alors il existe une solution x_0 commune à toutes les congruences ci dessus et toute autre solution est congruente à x_0 modulo $M = m_1 m_2 \cdots m_s$.

Démonstration : posons $M_i = M/m_i$, alors pgcd$(M_i, m_i) = 1$. Donc d'après l'identité de Bezout, il existe N_i tel que $M_i N_i \equiv 1 \ [m_i]$. Posons $x_0 = \sum_i a_i M_i N_i$. Alors pour tout j : $x_0 \equiv a_j \ [m_j]$. Supposons maintenant que nous ayons une deuxième solution x_1 de notre système. Posons $x = x_0 - x_1$. x est congru à 0 modulo chacun des m_i, et donc également congru à 0 module M. Donc x_0 et x_1 sont congrus modulo M.

Définition 18 (Fonction indicatrice d'Euler). *Soit n un entier naturel. On appelle fonction indicatrice d'Euler, et on note $\varphi(n)$ le nombre d'entiers naturels strictement positifs premiers avec n et strictement inférieurs à n.*

On remarque que pour p premier, $\varphi(p) = p - 1$; d'autre part, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, puisque les nombres premiers avec p^α et inférieurs à p^α sont tous les nombres inférieurs à p^α moins les multiples de p (et il y en a $p^{\alpha-1}$).

Nous allons maintenant donner une formule générale permettant de calculer $\varphi(n)$ connaissant la décomposition en facteurs premiers de n. Avant cela, nous aurons besoin du lemme suivant.

Lemme 1. *La fonction φ est multiplicative pour les nombres premiers entre eux : si pgcd$(p, q) = 1$ alors $\varphi(pq) = \varphi(p)\varphi(q)$*

Démonstration : nous devons compter les nombres i compris entre 0 et $pq - 1$ qui sont premiers avec pq. Or, d'après le théorème chinois, un nombre i n'aura pas de facteur commun avec pq si et seulement si le nombre $i_1 \equiv i \ [p]$ n'a aucun facteur commun avec p et le nombre $i_2 \equiv i \ [q]$ n'a pas de facteur commun avec q. On a donc grâce au théorème chinois une bijection entre les couples (i_1, i_2) tels que i_1 est premier avec p et i_2 est premier avec q, et les nombre i tel que i est premier avec pq. Or, nous avons $\varphi(p) \times \varphi(q)$ couples de ce type, donc $\varphi(pq) = \varphi(p)\varphi(q)$

De façon générale :

Théorème 10. *Soit n un entier naturel avec $n = \prod_{1 \leq i \leq k} p_i^{e_i}$ où les (p_i, e_i) sont la décompositions en facteurs premiers de n. Alors :*

$$\varphi(n) = \prod_{1 \leq i \leq k} (p_i - 1) p_i^{e_i - 1}$$

Démonstration : φ étant multiplicative, il suffit d'utiliser la formule $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$ pour p premier.

Théorème 11. *Soit a et n deux nombres premiers entre eux et $x_1, x_2, \cdots x_k$ les nombres $(x_i)_{i=1}^{\varphi(n)}$ premiers avec n et inférieurs à n. Alors l'ensemble des $(ax_i)_{i=1}^{\varphi(n)}$ dans $\mathbb{Z}/n\mathbb{Z}$ est égal à l'ensemble des $(x_i)_{i=1}^{\varphi(n)}$.*

Démonstration : Tout d'abord remarquons que si x_i et a sont premiers avec n alors ax_i est premier avec n. Maintenant, supposons qu'il existe deux nombre i et j distincts tels que $ax_i \equiv ax_j \ [n]$. Cela implique que $a(x_i - x_j) \equiv 0 \ [n]$. Mais a étant premier avec n, il est inversible et donc on a $x_i - x_j \equiv 0 \ [n]$. Donc $x_i \equiv x_j \ [n]$, ce qui est contraire à l'hypothèse.

Théorème 12 (Généralisation d'Euler). *Soit a et n deux nombres premiers entre eux. Alors $a^{\varphi(n)} \equiv 1 \ [n]$*

L'ensemble des $(x_i)_{i=1}^{\varphi(n)}$ premiers avec n et inférieurs à n et l'ensemble des $(ax_i \mod n)_{i=1}^{\varphi(n)}$ étant les mêmes, on a

$$\prod_{i=1}^{\varphi(n)} x_i \equiv \prod_{i=1}^{\varphi(n)} ax_i \equiv a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} x_i \ [n]$$

Donc $a^{\varphi(n)} \equiv 1 \ [n]$

Ce théorème est appelé généralisation d'Euler, car il généralise le petit théorème de Fermat qui dit que si n est premier, alors pour tout $a < n$, $a^{n-1} \equiv 1 \ [n]$.

On peut également remarquer une propriété utile liée au théorème d'Euler : si l'on souhaite calculer a^r modulo n, alors on peut réduire r en s avec $s \equiv r \ [\varphi(n)]$ et $a^r \equiv a^s \ [n]$

1.3 Résidus quadratiques

Définition 19 (Résidu quadratique). *Soit $a \in \mathbb{Z}/n\mathbb{Z}$. a est appelé résidu quadratique modulo n ou carré modulo n si et seulement si il existe $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $b^2 \equiv a \ [n]$*

Théorème 13 (Racines carrés dans le corps $\mathbb{Z}/n\mathbb{Z}$). *Soit $n > 2$ premier. Alors si a est un résidu quadratique dans $\mathbb{Z}/n\mathbb{Z}$ différent de 0, a a exactement deux racines carrées.*

La démonstration est élémentaire. Soit b et c, deux racines de a quelconques et non nécessairement distinctes. Nous avons alors $b^2 \equiv c^2\ [n]$. Donc $b^2 - c^2 \equiv 0\ [n]$, ou encore $(b-c)(b+c) \equiv 0\ [n]$. n étant premier, $\mathbb{Z}/n\mathbb{Z}$ est un corps. On a donc soit $b = c$, soit $b = n - c$. a admet donc bien exactement deux racines carrées distinctes, l'une inférieure ou égale à $\frac{n-1}{2}$ et l'autre strictement supérieure.

Théorème 14 (Nombre de résidus quadratiques). *Soit $n > 2$ premier. Alors il y a exactement $\frac{n-1}{2}$ résidus quadratiques différents de 0 dans $\mathbb{Z}/n\mathbb{Z}$.*

Le résultat découle directement du théorème précédent. L'ensemble des résidus quadratiques est simplement obtenu en calculant le carré de tous les nombres de 1 à $\frac{n-1}{2}$.

Définition 20 (Symbole de Legendre). *Soit $n > 2$ premier et a un entier quelconque. On définit le symbole de Legendre $(\frac{a}{n})$ par :*

Théorème 15.

$$(\frac{a}{n}) \equiv a^{(n-1)/2}\ [n]$$

Chapitre 2

Cryptage à clef publique

2.1 Introduction

Le cryptage traditionnel repose sur l'existence d'une clef privée, commune à l'émetteur et au récepteur du message, qui doit rester secrète pour garantir la confidentialité de la transaction. Cela pose le problème du transport de cette clef (comment la faire parvenir de façon sûre à quelqu'un se trouvant à l'étranger), mais aussi du maintien de sa confidentialité sur le long terme. Dans le cryptage traditionnel, la connaissance de l'algorithme de cryptage et de ses paramètres permet de construire l'algorithme de décryptage.

Dans le cryptage à clef publique, la clef de cryptage est au contraire diffusée largement, même par des canaux absolument non sûrs. Simplement, la connaissance de l'algorithme de cryptage et sa clef ne permet pas de reconstituer l'algorithme de décryptage.

Nous allons maintenant examiner quelques exemples de cryptage à clef publique.

2.2 L'algorithme Merkle-Hellman

L'algorithme Merkle-Hellman [MH78] est historiquement le premier algorithme montrant le fonctionnement d'un système à clef publique. Il appartient à la famille des algorithmes de cryptage de type "sac à dos" (ou *knapsack* en anglais).

Le problème du sac à dos est un problème classique en théorie de la complexité. On sait qu'une instance générale du problème est NP-complète. La formulation du problème du sac à dos est simple : un randonneur possède un sac à dos pouvant contenir x kgs, et il dispose d'un ensemble I d'objets, chacun pesant un poids x_i. Il souhaite savoir s'il existe un sous ensemble de J, tel que la somme

des poids des éléments de J soit exactement x. Mathématiquement :

$$x \in \mathbb{N}, I = \{x_1, x_2, \cdots, x_i, \cdots, x_n\}, \text{ trouver } J \text{ tel que : } \sum_{i \in J} x_i = x$$

Remarquons tout d'abord que, s'il est possible de montrer que le problème du sac à dos est NP-complet dans le cas général, il existe des instances extrêmement faciles à résoudre, ce sont celles faisant intervenir les séquences super-croissantes :

Définition 21 (Séquence super-croissante). *Soit une suite u_n et la série associée $S_n = \sum_{i=1}^{n} u_n$. On dit que u_n est super-croissante si l'on a :*

$$\forall n,\ u_{n+1} > S_n$$

Notons tout de suite que les bases de numérations sont toutes des exemples de séquence super-croissante ($1 + 2 < 4$, $1 + 2 + 4 < 8$, etc).

Il est clair que le problème du sac à dos est trivial lorsque l'on utilise une séquence super-croissante. Il est tout aussi clair qu'il n'a pas toujours de solution. Ainsi, si l'on choisit la base 2 comme séquence super-croissante, tout nombre pourra se décomposer sur cette base au sens du problème du sac à dos. Il n'en va pas de même si l'on choisit la base 10 (par exemple, $13 = 8+4+1$ se décompose aisément sur la séquence $\{1, 2, 4, 8\}$, alors que le même nombre ne peut pas se décomposer sur la séquence $\{1, 10\}$).

L'idée de Merkle-Hellman est de transformer un problème du sac à dos trivial basé sur une séquence super-croissante en problème du sac dos général, qui devient alors NP-complet, donc "insoluble". Nous allons tout d'abord présenter une version simplifiée de l'algorithme Merkle-Hellman.

Algorithme 1 (Génération de la clef pour l'algorithme Merkle-Hellman). *L'algorithme se décompose de la façon suivante :*

1. *Choisir une séquence super-croissante $\{a_1, a_2, \cdots, a_n\}$ et un nombre N avec $N > a_1 + a_2 + \cdots + a_n$*
2. *Choisir un nombre $A < N$ tel que pgcd$(A, N) = 1$*
3. *Calculer les $b_i \equiv Aa_i\ [N]$*

La clef publique est $(\{b_1, b_2, \cdots, b_n\})$ et la clef privée $(N, A, \{a_1, a_2, \cdots, a_n\})$.

Il suffit maintenant pour l'émetteur de récupérer la clef publique $(\{b_1, b_2, \cdots, b_n\})$, qui peut être transmise par n'importe quel canal, même non sûr, puis d'appliquer l'algorithme de cryptage suivant :

Algorithme 2 (Cryptage par l'algorithme de Merkle-Hellman). *Soit un message binaire composée de la suite de chiffre $d_1 d_2 \cdots d_n$, avec $d_i = 0$ ou $d_i = 1$. Alors, le message crypté est :*

$$c = \sum_{i=1}^{n} d_i b_i$$

où les b_i sont la clef publique calculée par l'algorithme précédent.

Supposons maintenant qu'un individu mal intentionné tente de décrypter le message c. Il est en possession de la séquence $I = \{b_1, b_2, \cdots, b_n\}$ et du nombre c. Il lui faut donc résoudre un problème de sac à dos, puisqu'il lui faut trouver le sous ensemble J de I tel que $\sum_{j \in J} b_j = c$. Or ce problème de sac à dos n'a a priori aucune structure particulière, puisque la séquence b_i n'est pas super-croissante après l'application de la multiplication par A et du modulo N. Ce problème est donc a priori NP-complet.

En revanche, si nous sommes en possession de la clef privée, le décryptage est élémentaire :

Algorithme 3 (Décryptage par l'algorithme de Merkle-Hellman). *Soit le message cryptée c. Soit $m \equiv A^{-1} c \ [N]$. Calculons les nombres binaires d'_i tel que $m = \sum_{i=1}^{n} d'_i a_i$. Alors $d_i = d'_i$, où les d_i représentent les chiffres du message initial.*

L'algorithme de décryptage de Merkle-Hellman consiste à résoudre un problème de sac à dos, mais cette fois ci sur une instance super-croissante. On peut aisément vérifier que l'algorithme de décryptage est correct en raison de la propriété suivante :

$$m \equiv A^{-1} c \equiv A^{-1} \sum_{i=1}^{n} d_i b_i \equiv \sum_{i=1}^{n} d_i (A^{-1} b_1) \equiv \sum_{i=1}^{n} d_i a_i \ [N]$$

Nous allons maintenant développer un exemple pour bien montrer le fonctionnement de l'algorithme Merkle-Hellman. Nous allons choisir des nombres artificiellement petits, sachant bien entendu qu'il faudrait normalement choisir des nombres plus grands de plusieurs ordres de magnitude.

Exemple 2 (Application de l'algorithme de Merkle-Hellman). *Nous allons prendre $n = 8$, et comme suite : $\{a_1, a_2, \cdots, a_8\} = \{3, 7, 15, 31, 63, 151, 317, 673\}$. Nous choisissons $N = 1511$ et $A = 643$. Nous calculons alors la séquence : $\{b_1, b_2, \cdots, b_8\} = \{418, 1479, 579, 290, 1223, 389, 1357, 593\}$, et aussi $643^{-1} = 47 \, [1511]$.*

La seule information diffusée est la liste des b_i. Supposons maintenant que nous ayons à coder le message 10011010. Il suffit de calculer puis de transmettre $c = 418 + 290 + 1223 + 1357 = 3288$.

Pour décrypter le message, nous calculons $m = A^{-1}c\,[N] = 47{\times}3288\,[1511] = 414$*. Il nous suffit alors de résoudre le problème du sac à dos avec la séquence super-croissante* a_i *et* $x = 414 = 317 + 63 + 31 + 3$*, soit* 10011010*. Nous retrouvons bien le message initial.*

L'algorithme de Merkle-Hellman est aujourd'hui complètement abandonné. Même avec diverses améliorations (permutation sur les éléments de la base, algorithme itéré, etc), il n'est pas sûr et l'on a trouvé des algorithmes capables de le "casser" en un temps polynomial. Le premier exemple d'un tel algorithme est dû à Shamir en 1982 (publié seulement en 1984 [Sha84]).

Notons enfin qu'il n'existe qu'un seul système de cryptage sûr basé sur le principe du "sac à dos". Il s'agit de l'algorithme de Chor-Rivest. Son principal inconvénient est la taille des clefs (de l'ordre de 50000 bits).

2.3 L'algorithme RSA (Rivest-Shamir-Adleman)

L'algorithme RSA est actuellement le cryptosystème le plus employé. Inventé en 1977, il est basé sur l'impossibilité, tout au moins à ce jour, de factoriser rapidement de grands nombres composites.

Algorithme 4 (Génération d'une clef pour l'algorithme RSA). *La construction d'une clef pour l'algorithme RSA se fait en trois étapes :*

1. *Générer deux grands nombres premiers* p *et* q *et calculer* $n = pq$ *et* $\phi = (p-1)(q-1)$
2. *Trouver un entier* e *tel que* $1 < e < \phi$ *et pgcd*$(e, \phi) = 1$
3. *Calculer* $d = e^{-1}\,[\phi]$.

La clef publique diffusée est (n, e) *et la clef privée est* d*.*

Notons que la connaissance de n et e ne permet pas de reconstituer d. Il faudrait pour cela être capable de factoriser n, ce qui est impossible dès que l'on choisit p et q suffisamment grands.

Algorithme 5 (Cryptage par l'algorithme RSA). *Le message* m *à transmettre doit appartenir à l'intervalle* $[0, n-1]$*. On calcule alors :*

$$c \equiv m^e\,[n]$$

c *est le message crypté à transmettre.*

Algorithme 6 (Décryptage par l'algorithme RSA). *Soit* c *le message crypté. Il suffit de calculer :*

$$m \equiv c^d\,[n]$$

Démonstration : il nous faut montrer que $c^d \equiv (m^e)^d \equiv m^{ed}\,[n]$ est également congru à m modulo n. Nous savons que $d \equiv e^{-1}\,[\phi]$, donc $\exists k,\ ed = 1 + k\phi$. Donc $m^{ed} \equiv m^{1+k\phi} \equiv m(m^{\phi})^k\,[n]$. Le théorème d'Euler permet d'écrire : $m^{\phi} \equiv 1[n]$. Donc $m^{ed} \equiv m\,[n]$.

Nous allons maintenant montrer un exemple d'utilisation de l'algorithme RSA. Les paramètres sont là aussi pris artificiellement petits.

Exemple 3. *On choisit* $p = 313$ *et* $q = 547$. *Donc* $n = pq = 171211$ *et* $\phi = 170352$. *On choisit* $e = 83$ *et l'on trouve* $d = 108779$. *Supposons que nous souhaitions coder le message* $m = 123456$. *On trouve alors* $c \equiv m^e \equiv 123456^{83} \equiv 49619\,[n]$. *Pour retrouver le message initial, il suffit de calculer* $m \equiv c^d \equiv 49619^{108779} \equiv 123456\,[n]$.

Bibliographie

[MH78] R.C. Merkle and M.E. Hellman. Hiding information and signatures in trapdoor knapsacks. *IEEE transactions on information theory*, 24 :525–530, 1978.

[Sha84] R. Shamir. A polynomial time algorithm for breaking the merkle-hellman cryptosystem. *IEEE transactions on information theory*, 30 :699–704, 1984.