Arithmétique modulaire et applications à la cryptographie

Etant donné un entier $n \geq 2$, l'arithmétique modulo n consiste à faire des ***calculs sur les restes*** dans la division euclidienne des entiers par n.

Exemples :

(1) Je me couche à 21 h et je dors pendant 10 h. Quelle heure est-il alors ? ***Réponse*** : 7 h, puisque $21+10=31\equiv 7 \pmod{24}$.

(2) Aujourd'hui on est mardi (2^{e} jour de la semaine). Quel jour sera-t-on dans 30 jours ? ***Réponse*** : Jeudi, puisque : $2+30=32\equiv 4 \pmod{7}$.

(3) La mesure d'un angle est définie à 360° près. Cela veut dire que la différence entre deux mesures quelconques d'un angle est un multiple entier de 360°. Par exemple : $-750^\circ \equiv -30^\circ \pmod{360^\circ}$.

Définition. Soient a, b et n des entiers, avec $n \neq 0$. On dit que a est congru à b modulo n et on note $a \equiv b \pmod{n}$, si $n \mid (a-b)$, c.-à-d. s'il existe un entier x tel que $a-b=nx$.

Proposition 1. La relation de congruence modulo n est une ***relation d'équivalence***, c.-à-d. elle est ***réflexive***, ***symétrique*** et ***transitive***.

Proposition 2.

a) Il existe un et un seul entier r dans $\{0,1,2,...,n-1\}$ tel que $a \equiv r \pmod{n}$. Cet entier r est le reste dans la division euclidienne de a par n.

b) $a \equiv b \pmod{n}$ si et seulement si a et b ont le même reste dans la division euclidienne par n.

Proposition 3. Soient a, a', b, b' et k des entiers. Alors :

$$a \equiv a' \pmod{n} \text{ et } b \equiv b' \pmod{n} \quad \Rightarrow \quad a+b \equiv a'+b' \pmod{n}$$

$$a \equiv a' \pmod{n} \text{ et } b \equiv b' \pmod{n} \quad \Rightarrow \quad a-b \equiv a'-b' \pmod{n}$$

$$a \equiv a' \pmod{n} \text{ et } b \equiv b' \pmod{n} \quad \Rightarrow \quad a \cdot b \equiv a' \cdot b' \pmod{n}$$

$$a \equiv a' \pmod{n} \quad \Rightarrow \quad a^k \equiv a'^k \pmod{n}$$

Démonstrations : Exercices !

Applications :

(1) ***Etudier la parité d'un nombre*** revient à calculer son reste dans la division euclidienne par 2. Si ce reste est 0, alors le nombre est pair, si le reste est 1, alors le nombre est impair. En d'autres termes, on fait de l'arithmétique modulo 2. Par exemple : le produit de deux nombres impairs est impair puisque :

$$a \equiv 1 \pmod{2} \text{ et } b \equiv 1 \pmod{2} \quad \Rightarrow \quad a \cdot b \equiv 1 \pmod{2}$$

(2) ***Trouver le dernier chiffre*** d'entier revient à calculer son reste dans la division euclidienne par 10. Déterminons par exemple le dernier chiffre de 7^{20}.

$$7 \equiv -3 \pmod{10}, \text{ donc } 7^2 \equiv 9 \equiv -1 \pmod{10}$$

Par conséquent : $7^{20} \equiv \left(7^2\right)^{10} \equiv \left(-1\right)^{10} \equiv 1 \pmod{10}$, c.-à-d. le dernier chiffre de 7^{20} est 1.

(3) ***Construction de critères de divisibilité.*** Rappelons par exemple qu'un nombre est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9. Démontrons ce résultat pour un nombre à 4 chiffres $\overline{abcd} = 1000a + 100b + 10c + d$. On a :

$$10 \equiv 1 \pmod{9}, \; 100 \equiv 1 \pmod{9} \text{ et } 1000 \equiv 1 \pmod{9}.$$

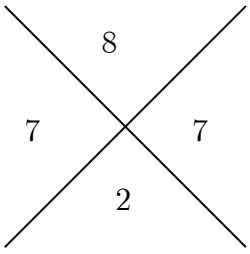
Par conséquent :

$$1000a + 100b + 10c + d \equiv a + b + c + d \pmod{9}$$

D'après la proposition 2, ces deux nombres ont le même reste dans la division euclidienne par 9. En particulier, l'un est divisible par 9 si et seulement si l'autre est divisible par 9.

(4) La ***preuve par 9*** que l'on apprenait autrefois à l'école primaire est un test permettant de détecter une erreur dans un calcul mental. Par exemple, supposons qu'un élève souhaite vérifier que : $458 \cdot 47 = 21'526$. Dans le schéma en croix de la preuve, il place alors :

- en haut et en bas respectivement, les restes de 458 et de 47 par 9, soit 8 et 2 ;
- à gauche, le reste du résultat 21'526 par 9, soit 7 ;
- à droite finalement, le reste de $8 \cdot 2 = 16$ par 9, donc 7.



Si les nombres à droite et à gauche dans la croix diffèrent, l'élève sait que le résultat est faux, sinon il ne peut pas conclure. (Expliquer pourquoi … !).

L'algorithme d'Euclide permet de trouver rapidement le pgcd de deux entiers a et b. Son fonctionnement est explicité dans la proposition suivante :

Proposition 4 (Algorithme d'Euclide). Soient a et b deux entiers tels que $a > b \geq 0$.

- Si $b = 0$ alors $\text{pgcd}\big(a,b\big) = \text{pgcd}\big(a,0\big) = a$.
- Si $b \neq 0$ alors $\text{pgcd}\big(a,b\big) = \text{pgcd}\big(b,r\big)$, où r est le reste de la division euclidienne de a par b.

L'algorithme d'Euclide consiste à réitérer la 2e formule jusqu'à ce que l'on tombe sur un reste nul. Dans ce cas, on applique la 1re formule.

Démonstration. La 1re formule est évidente. Prouvons la 2e. Soit $a = bq + r$, $0 \leq r < b$ la division euclidienne de a par b. Soit d un diviseur commun de a et de b. Alors $d \mid r$, puisque $r = a - bq$. Donc d est un diviseur commun de b et de r. Réciproquement, si d est un diviseur commun de b et de r, c'est évidemment aussi un diviseur de a, donc un diviseur commun de a et de b. Ainsi les diviseurs communs de a et de b sont exactement les diviseurs communs de b et de r. En particulier, $\text{pgcd}\big(a,b\big) = \text{pgcd}\big(b,r\big)$.

Il reste à voir que l'on tombe toujours sur un reste nul si l'on itère la 2e formule. Or ceci est évident puisque la suite des restes est une suite d'entiers positifs strictement décroissante (puisque $0 \leq r < b$), elle finit donc par s'annuler.

□

Exemple. $\text{pgcd}\big(96,81\big) = ?$

$96 = 81 \cdot 1 + 15$ donc $\text{pgcd}\big(96,81\big) = \text{pgcd}\big(81,15\big)$

$81 = 15 \cdot 5 + 6$ donc $\text{pgcd}\big(81,15\big) = \text{pgcd}\big(15,6\big)$

$15 = 6 \cdot 2 + 3$ donc $\text{pgcd}\big(15,6\big) = \text{pgcd}\big(6,3\big)$

$6 = 3 \cdot 2 + 0$ donc $\text{pgcd}\big(6,3\big) = \text{pgcd}\big(3,0\big) = 3$

Ainsi : $\text{pgcd}\big(96,81\big) = 3$.

Un corollaire très important de l'algorithme d'Euclide est la fameuse :

Identité de Bezout. Soient a et b sont des entiers non nuls et d leur pgcd. Il existe deux entiers u et v tels que : $au + bv = d$.

Démonstration. Supposons a et b strictement positifs. Reprenons l'algorithme d'Euclide pour la détermination du pgcd :

$$a = bq_1 + r_1,\ 0 \leq r_1 < b$$

$$b = r_1 q_2 + r_2,\ 0 \le r_2 < r_1$$
$$r_1 = r_2 q_3 + r_3,\ 0 \le r_3 < r_2$$
$$\dots$$
$$r_{n-2} = r_{n-1} q_n + r_n,\ 0 \le r_n < r_{n-1}$$
$$r_{n-1} = r_n q_{n+1} + 0$$

On peut montrer par récurrence que tous les restes $r_1, r_2, r_3, \dots$ s'écrivent sous la forme $r_i = au_i + bv_i$. Cela est vrai pour r_1 et pour r_2 :

$$r_1 = a \cdot 1 - b \cdot q_1$$
$$r_2 = b - r_1 q_2 = b - \big(a - bq_1\big) q_2 = -aq_2 + b\big(1 + q_1 q_2\big).$$

En utilisant la relation $r_3 = r_1 - r_2 q_3$, on prouve facilement l'assertion pour r_3. Et ainsi de suite, jusqu'à r_n. Mais r_n est le dernier reste non nul, donc $r_n = \text{pgcd}\big(a, b\big)$ s'écrit bien sous la forme $au + bv$. On montre facilement que l'identité s'étend au cas d'entiers négatifs en remplaçant au besoin a par $-a$ ou b par $-b$.

□

Remarque. Cette preuve est très importante car elle établit non seulement l'existence des entiers u et v tels que $d = au + bv$, mais elle montre de plus comment les construire :

Exemple. Chercher deux entiers u et v tels que $96u + 81v = 3$.
On part de l'avant-dernière ligne dans l'algorithme d'Euclide (cf. page 3), puis on remonte successivement jusqu'à la 1re :

$$\begin{aligned} 3 &= 15 - 6 \cdot 2 \\ &= 15 - \big(81 - 5 \cdot 15\big) \cdot 2 \\ &= -2 \cdot 81 + 11 \cdot 15 \\ &= -2 \cdot 81 + 11 \cdot \big(96 - 81\big) \\ &= -13 \cdot 81 + 11 \cdot 96 \end{aligned}$$

Donc : $11 \cdot 96 - 13 \cdot 81 = 3$.

Voici une extension de l'identité de Bezout dans un cas particulier :

Théorème de Bezout. Soient a et b sont des entiers non nuls. a et b sont premiers entre eux ***si et seulement si*** il existe deux entiers u et v tels que : $au + bv = 1$.

Démonstration. L'implication directe est un cas particulier de l'identité de Bezout. Réciproquement, si $au + bv = 1$ et si d est un diviseur positif commun de a et de b, c'est aussi un diviseur de 1, c'est-à-dire d = 1. Donc a et b sont premiers entre eux.

□

Les deux résultats qui suivent sont élémentaires et intuitifs, mais se démontrent bien à l'aide de l'identité de Bezout :

Lemme de Gauss. Soit $a,b,c \in \mathbb{N}$. Si $c \mid ab$ et $\text{pgcd}\big(c,b\big)=1$ alors $c \mid a$.

Démonstration. Comme $\text{pgcd}\big(c,b\big)=1$, il existe deux entiers x et y tels que $cx+by=1$. En multipliant cette égalité par a, il vient : $acx+aby=a$. Or, $c \mid ab$ et $c \mid ac$, donc $c \mid acx+aby$. En d'autres termes : $c \mid a$.

□

Nous donnons sans démonstration un cas particulier du lemme de Gauss :

Lemme d'Euclide. Si p est un nombre premier et $p \mid ab$ alors $p \mid a$ ou $p \mid b$.

Le théorème suivant est crucial en arithmétique modulaire.

Théorème et définition. Soit $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. L'équation $ax \equiv 1 \ \big(\text{mod}\, n\big)$ admet une solution entière x si et seulement si $\text{pgcd}\big(a,n\big)=1$. Dans ce cas la solution x est unique modulo n et x est appelé ***inverse de*** a ***modulo*** n.

Démonstration. $ax \equiv 1 \ \big(\text{mod}\, n\big) \Leftrightarrow ax-1=ny \Leftrightarrow ax-ny=1$, avec $y \in \mathbb{Z}$. Cette dernière égalité, d'après le théorème de Bezout, ne peut avoir lieu que si a et n sont premiers entre eux. Dans ce cas, si x' est une 2^{e} solution de l'équation, c.-à-d. $ax' \equiv 1 \ \big(\text{mod}\, n\big)$ alors $ax-ax'=a\big(x-x'\big) \equiv 0 \ \big(\text{mod}\, n\big)$. En d'autres termes : $n \mid a\big(x-x'\big)$. Comme $\text{pgcd}\big(a,n\big)=1$, on a d'après le lemme de Gauss : $n \mid x-x'$, c.-à-d. $x-x' \equiv 0 \ \big(\text{mod}\, n\big)$.

□

Définition. On appelle fonction ***indicatrice d'Euler*** la fonction $\varphi : \mathbb{N}^* \to \mathbb{N}^*$, qui à n associe le nombre d'entiers positifs inférieurs à n et premiers avec n.

L'intérêt de cette fonction provient du théorème précédent : $\varphi\big(n\big)$ est aussi le nombre d'entiers dans $\big\{1,2,...,n-1\big\}$ qui sont inversibles modulo n. Par exemple, $\varphi\big(8\big)=4$ car 1, 3, 5 et 7 sont les entiers positifs <8 et premiers avec 8, donc inversibles modulo 8. (Cherchez leurs inverses modulo 8 !) La fonction φ intervient très souvent en théorie des nombres et possède de nombreuses propriétés très intéressantes. Elle est nommée en l'honneur du mathématicien suisse Leonhard Euler (1707 - 1783) qui fut le premier à l'étudier. Nous énoncerons seulement deux propriétés de la fonction φ :

Propriétés de la fonction φ :

a) Si p est un nombre premier, alors $\varphi\big(p\big)=p-1$ et plus généralement : $\varphi\big(p^k\big)=p^{k-1}\big(p-1\big),\ k\in\mathbb{N}$

b) φ est une ***fonction multiplicative*** : Si m et n sont deux entiers premiers entre eux, alors $\varphi\big(mn\big)=\varphi\big(m\big)\varphi\big(n\big)$

Démonstration. Le point a) est facile : parmi les entiers $1,2,...,p^k$, seuls les multiples de p ne sont pas premiers avec p^k. Il y en a exactement p^{k-1} : $1\cdot p$, $2\cdot p$, ..., $p^{k-1}\cdot p$. Donc $\varphi\big(p^k\big)=p^k-p^{k-1}=p^{k-1}\big(p-1\big)$. Nous admettons le point b) qui est un peu plus difficile à prouver.

Remarque : Les propriétés énoncées permettent de calculer $\varphi\big(n\big)$ pour un entier quelconque n. En effet, en partant de la factorisation première $n=p_1^{\,k_1}\cdot p_2^{\,k_2}\cdot\ldots\cdot p_m^{\,k_m}$ on aura successivement :

$$\begin{aligned}
\varphi\big(n\big)&=\varphi\Big(p_1^{\,k_1}\Big)\cdot\varphi\Big(p_2^{\,k_2}\Big)\cdot\ldots\cdot\varphi\Big(p_m^{\,k_m}\Big)\\
&=p_1^{\,k_1-1}\big(p_1-1\big)\cdot p_2^{\,k_2-1}\big(p_2-1\big)\cdot\ldots\cdot p_m^{\,k_m-1}\big(p_m-1\big)\\
&=p_1^{\,k_1}\cdot p_2^{\,k_2}\cdot\ldots\cdot p_m^{\,k_m}\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_m}\right)\\
&=n\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_m}\right)\\
&=n\prod_{\substack{p_i\ \text{premier}\\ \text{et } p_i\mid n}}\left(1-\frac{1}{p_i}\right)
\end{aligned}$$

Petit théorème de Fermat. Si p est un nombre premier, alors pour tout entier a ***non divisible par*** p, on a : $a^{p-1}\equiv 1\ \big(\mathrm{mod}\ \ p\big)$. [1]

Démonstration. Considérons la suite des multiples de a : a, $2a$, $3a$, ..., $\big(p-1\big)a$. Comme a n'est pas divisible par p, aucun de ces multiples n'est divisible par p (lemme d'Euclide). Ces multiples, divisés par p, donnent donc un ***reste non nul.*** Ces restes sont de ***plus tous distincts*** puisque, si $1\le k,l\le p-1$, on a :

$ka\equiv la\ \big(\mathrm{mod}\ \ p\big)$
$\Rightarrow\big(k-l\big)a\equiv 0\ \big(\mathrm{mod}\ \ p\big)$
$\Rightarrow k-l\equiv 0$ ou $a\equiv 0\ \big(\mathrm{mod}\ \ p\big)$ (lemme d'Euclide !)

[1] On peut énoncer de manière équivalente : pour tout entier a : $a^p\equiv a\ \big(\mathrm{mod}\ \ p\big)$

$\Rightarrow k-l \equiv 0 \pmod{p}$
$\Rightarrow k \equiv l \pmod{p}$
$\Rightarrow k = l$ puisque $1 \leq k,l \leq p-1$

En résumé : Les nombres a, $2a$, $3a$, …, $(p-1)a$, divisés par p, donnent des ***restes non nuls*** et ***distincts***. Ces restes sont donc, à l'ordre près, les nombres de la suite $1,2,\ldots,p-1$. Par conséquent :

$$\begin{aligned}
&a \cdot 2a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p} \\
&\Leftrightarrow a^{p-1}(p-1)! \equiv (p-1)! \pmod{p} \\
&\Leftrightarrow (a^{p-1}-1)(p-1)! \equiv 0 \pmod{p} \\
&\Leftrightarrow a^{p-1}-1 \equiv 0 \pmod{p} \quad \text{(lemme d'Euclide !)} \\
&\Leftrightarrow a^{p-1} \equiv 1 \pmod{p}
\end{aligned}$$

□

Le théorème suivant est une généralisation du petit théorème de Fermat :

Théorème d'Euler (ou de Fermat-Euler). Si a et n sont premiers entre eux, alors : $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Démonstration : Elle est très analogue à celle du petit théorème de Fermat. Au lieu de prendre tous les multiples a, $2a$, $3a$, …, $(n-1)a$, on prend seulement ceux de la forme ka, où k est premier avec n. Il y en a $\varphi(n)$. Ces multiples, divisés par n donnent encore des restes non nuls et distincts (d'après le lemme de Gauss). De plus, ces restes constituent de nouveau, à l'ordre près, les entiers $k \in \{1,2,\ldots,n-1\}$ qui sont premiers avec n (à démontrer). Par conséquent, en multipliant tous les multiples de a considérés, on obtient l'égalité :

$$a^{\varphi(n)} \cdot \prod_{\substack{1 \leq k \leq n \\ \text{pgcd}(k,n)=1}} k \equiv \prod_{\substack{1 \leq k \leq n \\ \text{pgcd}(k,n)=1}} k \pmod{n}$$

On en déduit le théorème d'Euler sans difficulté, en « simplifiant » par $\prod_{\substack{1 \leq k \leq n \\ \text{pgcd}(k,n)=1}} k$.

□

Corollaire. Soient $a,a' \in \mathbb{Z}$ deux entiers premiers avec n et $k,k' \in \mathbb{N}$.

$$a \equiv a' \pmod{n} \text{ et } k \equiv k' \pmod{\varphi(n)} \quad \Rightarrow \quad a^k \equiv a'^{k'} \pmod{n}$$

La démonstration est laissée au lecteur en exercice !

Exercices.

(1) Démontrer les propositions 1, 2 et 3.

(2) Etablir les tables d'addition et de multiplications modulo 2, modulo 3, ..., modulo 8. Ecrire un programme en Delphi permettant d'afficher ces tables.

(3) Montrer que $2^{36} + 5^{18}$ est divisible par 41.

(4) Calculer le reste dans la division euclidienne

a) de $1'035'125^{5642}$ par 11 ;

b) de 5^{2010} par 13 ;

(5) Calculer $55'555^{55'555}$ modulo 7.

(6) a) Montrer qu'un entier n est divisible par 7 si et seulement si le nombre obtenu en retranchant le double de son chiffre des unités au nombre formé des autres chiffres est divisible par 7.

b) Montrer qu'un entier n est divisible par 7 si et seulement si la somme alternée de ses chiffres est divisible par 11.

c) Montrer qu'un entier n est divisible par 13 si et seulement si le nombre obtenu en additionnant le quadruple de son chiffre des unités au nombre formé des autres chiffres est divisible par 13.

(7) Soit n_1, n_2, ... , n_k des entiers deux à deux premiers entre eux. Le ***théorème des restes chinois*** affirme alors que le système de congruences :

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \dots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

admet une solution unique modulo $n_1 \cdot n_2 \cdot \ldots \cdot n_k$, quels que soient les entiers a_1, a_2, ..., a_k donnés. Le but de l'exercice n'est pas de démontrer le théorème en général, mais de comprendre comment il fonctionne sur des exemples :

a) Quel est le reste de la division de x par 15 sachant que $x \equiv 2 \pmod 3$ et $x \equiv 4 \pmod 5$?

b) Dans l'armée de Han Xing il y a entre 1000 et 1100 soldats. Combien cette armée comporte-t-elle de soldats si, rangés par 3 colonnes, il reste 2 soldats, rangés par 5 colonnes, il reste 3 soldats et, rangés par 7 colonnes, il reste 2 soldats ?

c) Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les partager également, et de donner le reste au

cuisinier chinois. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et six d'entre eux sont tués. Un nouveau partage donnerait au cuisinier 4 pièces. Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ?

(8) Appliquer « à la main » l'algorithme d'Euclide pour déterminer le pgcd des nombres a et b :

a) $a = 528$ et $b = 312$

b) $a = 4'725$ et $b = 3'792$

c) $a = 26$ et $b = 19$

(9) a) Déteminer deux entiers x et y tels que $15x + 77y = 1$.

b) Quelles sont tous les couples d'entiers solutions de cette équation ?

c) Trouver une solution en entiers de l'équation $15x + 77y = 2$, puis toutes les solutions de cette équation.

(10) Montrer que, pour tout entier n, les entiers $2n+1$ et $9n+4$ sont premiers entre eux.

(11) Soient a, b et c sont des entiers non nuls. Montrer que l'équation $ax + by = c$ admet des solutions entières si et seulement si c est un multiple de $d = \text{pgcd}\big(a, b\big)$.

(12) Déterminer les valeurs de n, entier naturel pour que la fraction suivante soit irréductible :

a) $\dfrac{3n-2}{n+7}$ b) $\dfrac{n^2+6}{n+1}$

(13) Déterminer l'inverse de 12 modulo 47, de 13 modulo 24, et de 12 modulo 18.

(14) a) Montrer que 35 est inversible modulo 129.

b) Calculer l'inverse de 35 modulo 129 à l'aide de l'algorithme d'Euclide.

(15) Déterminer tous les entiers naturels n et p pour lesquels $15^n - 21^p$ est divisible par 12.

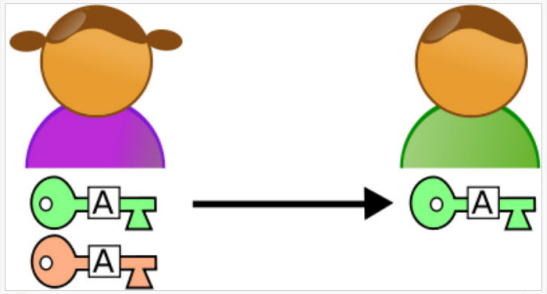
(16) Montrer en utilisant le petit théorème de Fermat que, pour tout entier naturel n, $n^5 - n$ est divisible par 30.

(17) Montrer que si $n \in \mathbb{N}$ et $p \in \mathbb{N}^*$, alors n^{p+4} et n^p ont le même chiffre des unités.

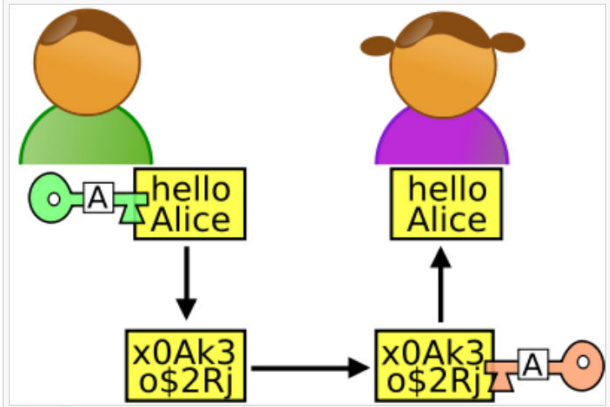
Application à la cryptographie : méthode de codage RSA

L'algorithme de chiffrement « ***à clé publique*** » RSA a été développé en 1978 par Ron Rivest, Adi Shamir et Len Adleman. Cet algorithme est fondé sur l'utilisation d'une ***paire*** de clés :

- une ***clé publique*** pour ***chiffrer***, accessible à n'importe quelle personne souhaitant chiffrer des informations et
- une ***clé privée*** pour ***déchiffrer***, réservée au receveur des messages chiffrés, qui est en même temps le créateur de la paire de clés.



1re étape : Alice génère deux clés. La clé publique (verte) qu'elle envoie à Bob et la clé privée (rouge) qu'elle conserve précieusement sans la divulguer à quiconque.



2e et 3e étapes : Bob chiffre le message avec la clé publique d'Alice et envoie le texte chiffré. Alice déchiffre le message grâce à sa clé privée.

Le receveur, nommé par convention ***Alice*** prend en charge la création de la paire de clés, envoie sa clé publique aux autres personnes ***Bob***, ***Carole***... qui peuvent alors chiffrer les données confidentielles à l'aide de celle-ci puis envoyer les données chiffrées à Alice. Cette dernière peut alors déchiffrer les données confidentielles à l'aide de sa clé privée (cf. schéma ci-dessus).

a) Création des clés

1re étape : Alice choisit deux nombres premiers distincts très grands p et q et calcule $n = pq$. n est appelé ***module de chiffrement***.

2e étape : Alice calcule $\varphi(n) = (p-1)(q-1)$ et choisit un nombre assez grand e, premier avec $\varphi(n)$. e est appelé ***exposant de chiffrement***.

$$\boxed{\textbf{\textit{Le couple } } (n, e) \textbf{\textit{ est la clé publique.}}}$$

3e étape : Comme e est premier avec $\varphi\big(n\big)$, e est inversible modulo $\varphi\big(n\big)$, c.-à-d. il existe un entier d tel que $ed \equiv 1 \ \Big(\mathrm{mod}\, \varphi\big(n\big)\Big)$. d est appelé ***exposant de déchiffrement***.

Le couple $\big(n, d\big)$ ***est la clé privée.***

b) Chiffrement des messages

Soit M un entier inférieur à n représentant le message original. Bob calcule $C \equiv M^e \ \big(\mathrm{mod}\, n\big)$. C représente le message chiffré que Bob envoie à Alice.

c) Déchiffrement des messages

Alice calcule le reste de la division de C^d par n et obtient ainsi le message original M de Bob. En effet, comme $ed \equiv 1 \ \Big(\mathrm{mod}\, \varphi\big(n\big)\Big)$, il existe un entier k tel que $ed = 1 + k \cdot \varphi\big(n\big)$. Donc :

$$C^d = M^{ed} = M^{1+k\cdot\varphi(n)} = M \cdot \Big(M^{\varphi(n)}\Big)^k.$$

Or, d'après le petit théorème de Fermat :

$$M^{\varphi(n)} \equiv 1 \ \big(\mathrm{mod}\, n\big).$$

Par conséquent :

$$C^d \equiv M \cdot 1^k \equiv M \ \big(\mathrm{mod}\, n\big).$$

d) Sécurité

On constate que pour chiffrer un message, il suffit de connaître e et n. En revanche, pour déchiffrer, il faut connaître d et n. Or, pour déterminer d, on a besoin de $\varphi\big(n\big) = \big(p-1\big)\big(q-1\big)$. Calculer l'entier très grand $\varphi\big(n\big)$ sans connaître p et q est un problème de factorisation duquel les ordinateurs ne viennent pas à bout en un temps raisonnable. Par sûreté, il est couramment recommandé que la taille des clés RSA soit au moins de 2048 bits.

(Source : Wikipédia)