الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Minstère de l'Enseignement Supérieur et de la Recherche Scientifique

CENTRE UNIVERSITAIRE DE MILA
INSTITUT DES SCIENCES ET DE LA TECHNOLOGIE

Réf. ***/11***

Mémoire de fin d'étude
Présenté pour l'obtention du diplôme de

Licence Académique

Domaine : **Mathématiques et Informatique**
Filière : **Mathématiques**
Spécialité : **Mathématiques Fondamentales**

Thème

Arithmétique Elémentaire et Cryptographie (Exemple du RSA)

Présenté par :
Zerizer Hayat
Chebbat Ilhem

Dirigé par :
Bouguebina Mounir

Année universitaire 2010-2011

Remerciements

Louange à dieu tout puissant de nous avoir aidé, éclairer le chemin pour achever notre travail et nos études.

Nos remerciements à très chers parents, frères, sœurs, collègues et amis respectifs qui nous ont encouragés, soutenu durant tout notre parcours.

Un remerciement particulier à notre

Encadreur Mr Bouguebina Mounir

Pour sa présence, son aide et surtout

Pour ses précieux conseils qui nous

Ont assistés pour l'accomplissement de notre projet.

Nous tenons à exprimer nos sincères remerciement à tout le personnel de l'institut de sciences et de la technologie surtout les enseignants qui nous ont enseigné durant toutes nos années d'étude.

Enfin nous remercions toutes les personnes qui ont contribué de prés ou de loin à l'achèvement de ce travail.

*** Dédicace ***

Je remercie dieu qui a toujours été à mes côtes.

Je dédie ce travail à mes parent que dieu les gardes pour moi : mon père qui et

mon idole et exemple de la vie, ma mère qui m'a tout donné pour réussir.

A mes chers frères.

A mes belles Sœurs.

A l'enseignant Mr Bouguebina Mounir.

A mes amis et mes collègues d'étude.

A toutes mes tantes et tous mes oncles, a mes cousines et mes cousins.

A tous ceux qui me connaissent.

Arithmétique Elémentaire et Cryptographie: Exemple du RSA

Zerizer Hayet et Chebbat Ilham

18 mai 2011

Table des matières

Introduction :

Le codage, le cryptage ne date pas d'aujourd'hui, il avait et a encore son utilité dans les guerres et les conflits mondiaux. Ce qui est nouveau c'est la banalisation et l'utilisation courante et dans tous les domaines du code secret (les cartes bancaires, ccp, etc). Les cryptographes utilisent deux systèmes de cryptage : Le système standard à clé secrète DES et le système RSA, ces deux systèmes utilisent la cryptographie qui n'est qu'une application de notre ancienne arithmétique celle des théorèmes d'Euclide, de Bézout ou de Fermat. Donc l'arithmétique joue un rôle primordial dans les méthodes modernes de chiffrement et de cryptonalyse. Dans notre analyse nous allons traiter trois chapitre successifs : l'arithmétique élémentaire, la cryptographie et le système RSA.

Dans le premier chapitre, nous rappelons quelques notions d'arithmétique telle que les nombres premier, les congruences, le petit théorème de fermat ou encore la fonction ϕ d'Euler.

Dans le deuxième chapitre, nous parlons de la cryptographie qui est une science du secret et du chiffrement des messages et qui apparait aujourd'hui comme une applicatoin de l'arithmétique. la cryptographie a deux types : La cryptographie à clé symetrique et la cryptographie à clé publique.

Dans le dernière chapitre, nous précisions notre analyse sur la cryptographie á clé publique. Pour cela nous étudions l'exemple du RSA qui est l'une des méthodes de cryptage à clé publique.

Chapitre 1

Arithmétique Elémentaire

L'Arithmétique (ou théorie des nombres) a longtemps été considérée comme une science noble et pure, loin des préoccupations (surtout militaires) et mesquineries humaines. Mais l'avènement de l'informatique aprés la deuxième guerre mondiale et surtout de la cryptographie à clé publique à la fin des années 70 a complètement changé la donne. De nos jours il est trés courant d'envoyer des messages cryptés à travers les réseaux informatiques mais bien peu de gens savent que des notions d'arithmétique comme les nombres premiers, les congruences, le petit théorème de Fermat ou encore la fontion ϕ d'Euler sont à la base des techniques qui permettent cela. Dans ce chapitre nous allons introduire ces notions en donnant quelques exemples élémentaires. Nous verrons dans les chapitres suivants comment ils vont être utilisés en cryptographie.

1.1 Divisibilité dans $\mathbb{Z}$

L'ensemble des entiers relatifs est :

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

Il contient comme sous-ensemble l'ensemble des entiers naturels :

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}.$$

Définition 1 *: Soient a, b deux éléments de $\mathbb{Z}$. On dit que a est divisible par b ou encore que a est un multiple de b ou encore que b divise a s'il existe un élément $c \in \mathbb{Z}$ tel que :*

$$a = bc.$$

On notera $b \mid a$. Remarquer que si $a \neq 0$ et si b divise a, alors $b \neq 0$ et c est unique. c est appelé le quotient de a par b. Remarquer aussi que cette définition peut s'appliquer aux éléments de $\mathbb{N}$ seuls c'est-à-dire qu'on peut aussi parler de la divisibilité dans $\mathbb{N}$.
Exemple : 6 divise 18 ; -4 divise 24 ; 5 ne divise pas 27.
On peut énoncer un certain nombre de propriétés élémentaires qui découlent directement de la définition :
Propriétés :
1) $a \mid a$.
2) $c \mid b$ et $b \mid a$ implique $c \mid a$.
3) $a \mid b$ et $b \mid a$ implique $\mid a \mid = \mid b \mid$.
4) $ac \mid ab$ et $a \neq 0$ implique $c \mid b$.
5) $1 \mid a$ et $a \mid 0$ $\forall a$. De plus $0 \mid a$ implique $a = 0$.
6) $b \mid a$ et $a \neq 0$ implique $0 < \mid b \mid \leq \mid a \mid$.

Le premier resultat non trivial concernant la divisibilité est la division euclidienne dans $\mathbb{Z}$:

Théorème 1 *: Soient a un entier et b un entier non nul. Il existe un unique entier q et un unique entier r tels que :*

$$a = qb + r,$$

avec

$$0 \leq r < \mid b \mid .$$

Preuve : La démonstration va consister tout d'abord à établir l'existence de q et r en donnant un algorithme produisant ces nombres. C'est l'algorithme décrit par Euclide lui-même. Il procède par soustractions successives. On suppose dans un premier temps que $a \geq 0$ et $b > 0$. Pour effectuer la division euclidienne de a par b, on soustrait b à a et on recommence tant que cela est possible. On construit ainsi une suite arithmétique strictement décroissante (a_n) de raison $-b$:

$$a_0 = a,$$

$$a_{n+1} = a_n - b = a - (n+1).b$$

Il existe donc un plus petit entier m tel que $a_m < b$ vérifiant $a - m.b < b \leq a - (m-1).b$ et donc $0 \leq a - m.b < b$. Le quotient q cherché est donc m et le reste est $r = a - m.b$.

Faire la division euclidienne de a par b consiste à déterminer q et r appelés respectivement le quotient et le reste de la division. Lorsque b divise a, on a $r = 0$. Etudions maintenant le cas où a et b ne sont pas nécessairement positifs en se ramenant à l'étude précédente :

- $a \geq 0$ et $b < 0$. On fait la division euclidienne de a par $-b$, ce qui donne $a = q(-b) + r$ ou encore $a = (-q)b + r$. Le quotient est $-q$ et le reste est r.
- $a < 0$ et $b > 0$. On fait la division euclidienne de $-a$ par b, ce qui donne $-a = qb + r$ ou encore $a = -qb - r = -(q+1)b + b - r$. Le quotient est $-(q+1)$ et le reste est $b - r$.
- $a < 0$ et $b < 0$. On fait la division euclidienne de $-a$ par $-b$, ce qui donne $-a = q(-b) + r$ ou encore $a = qb - r = (q+1)b - b - r$. Le quotient est $q + 1$ et le reste est $-b - r$.

Reste à montrer l'unicité. Supposons qu'il y ait une deuxième écriture $a = qb^{'} + r^{'}$ avec $0 \leq r^{'} <\mid b \mid$. On a donc $\mid r - r^{'} \mid <\mid b \mid$ et nécessairement $q = q^{'}$ et $r = r^{'}$.

Faire la division euclidienne de a par b consiste à déterminer q et r appelés respectivement le quotient et le reste de la division. Lorsque b divise a, on a $r = 0$.

Nous allons étudier les diviseurs d'un ou plusieurs entiers. Comme les diviseurs de a sont les mêmes que ceux de $-a$ et que si d est un diviseur de a, il en est de même de $-d$, on peut restreindre dans un premier temps l'étude à $\mathbb{N}$. Elle s'étendra naturellement à $\mathbb{Z}$.

Définition 2 *: Soient a, b deux nombres entiers. Le plus grand commun diviseur de a et b est le plus grand entier non nul qui les divise tous les deux. On le note $pgcd(a, b)$.*

On a donc :

$$pgcd(a, b) = max\{d : d \mid a \wedge d \mid b\}.$$

Par convention $pgcd(0, 0) = 0$.

Exemple :

1) $pgcd(6, 9) = 3$.
2) $pgcd(2, 5) = 1$.
3) $pgcd(0, a) = pgcd(a, 0) = a$.
4) $pgcd(1, 10) = 1$.

On dispose d'un moyen assez simple pour determiner le plus grand commun diviseur de deux entiers. C'est l'**algorithme d'Euclide** dont l'idée est

la suivante : Soient a et b deux entiers dont l'un est strictement positif. Faisons la division euclidienne de a par b :

$$a = qb + r,$$

avec $0 \leq r < b$. On voit que les diviseurs de a et b sont les diviseurs de b et r. On peut alors repeter le procédé, en faisant la division euclidienne de b par r et ainsi de suite jusqu'à obtenir un reste nul ce qui se produira necessairement car les restes des divisions décroissent strictement et sont tous ≥ 0. Appelons d le dernier reste non nul. Les diviseurs de a et b sont alors les diviseurs de d et 0 c'est-à-dire de d. Ainsi d est un diviseur commun de a et b et tout autre diviseur commun de a et b divise d. Ce qui veut dire que d est le plus grand commun diviseur de a et b.
Exemple : On prend $a = 325$ et $b = 145$. Les divisions euclidiennes successives donnent :

$$325 = 2.145 + 35$$

$$145 = 4.35 + 5$$

$$35 = 7.5 + 0$$

Donc $pgcd(325, 145) = 5$.

Voici quelques propriétés élémentaires du $pgcd$:
Propriétés
1) $pgcd(a, b) = pgcd(b, a)$.
2) $pgcd(a, pgcd(b, c)) = pgcd(pgcd(a, b), c)$.
3) $pgcd(ca, cb) = c.pgcd(a, b)$.
4) Soit $pgcd(a, b) = d$. Alors on a $pgcd(\frac{a}{d}, \frac{b}{d}) = 1$

Définition 3 *: Les nombres entiers a, b sont dits* ***premiers entre eux*** *si* $pgcd(a, b) = 1$.

Reprenons l'exemple précédent du calcul du pgcd de $a = 325$ et $b = 145$. En arrangeant un peu les calculs on arrive aux égalités suivantes :

$$325 = 2.145 + 35$$

$$35 = 325 - 2.145$$

$$145 = 4.35 + 5$$

$$5 = 145 - 4.35 = 9.145 - 4.325$$

$$35 = 7.5 + 0$$

Les calculs s'arretent ici car le reste est nul.On a donc obtenu $pgcd(325, 145) = 5$ comme combinaison linéaire de 325 et 145 :

$$5 = 9.145 - 4.325.$$

La proposition suivante montre que ceci est un fait général :

Proposition 1 *(**algorithme d'Euclide étendu**) : Si $pgcd(a, b) = d$, alors il existe deux entiers u et v tels que $u.a + b.v = d$*

Preuve : L'algorithme d'Euclide étendu est similaire à l'algorithme d'Euclide normal mais avec deux suites supplémentaires u_i et v_i. On pose $r_0 = a$ et $r_1 = b$ et pour $i \geq 0$, $r_i = q_i.r_{i+1} + r_{i+2}$, puis on définit $u_0 = 1$, $v_0 = 0$, $u_1 = 0$, $v_1 = 1$ et pour $i \geq 2$, $u_i = u_{i-2} - q_{i-2}.u_{i-1}$ et $v_i = v_{i-2} - q_{i-2}.v_{i-1}$. La suite des restes r_i étant décroissante, il existe un k tel que $r_k = 0$. On a alors :

$$pgcd(a, b) = r_{k-1} = u_{k-1}.a + v_{k-1}.b$$

En effet on peut montrer par recurrence sur i qu'on a toujours $r_i = u_i.a + v_i.b$. Ceci est vrai pour $r_0 = a = 1.a + 0.b$ et pour $r_1 = b = 0.a + 1.b$. Si $r_{i-2} = u_{i-2}.a + v_{i-2}.b$ et $r_{i-1} = u_{i-1}.a + v_{i-1}.b$, on a alors $u_i.a + v_i.b = (u_{i-2} - q_{i-2}.u_{i-1}).a + (v_{i-2} - q_{i-2}.v_{i-1}).b = r_{i-2} - q_{i-2}.r_{i-1} = r_i$.

On peut utiliser cette proposition pour caractériser les nombres premiers entre eux : c'est le célèbre théorème de Bezout.

Théorème 2 *(**Théorème de Bezout**) : Deux nombres entiers a et b sont premiers entre eux si et seulement s'il existe deux entiers u et v tels que $u.a + b.v = 1$.*

Preuve : D'aprés la proposition précédente, si $pgcd(a, b) = 1$, il existe u, v tels que $u.a + v.b = 1$. Inversement supposons qu'il existe u, v tels que $u.a + v.b = 1$. Alors tout diviseur de a et b doit diviser 1 qui est donc leur plus grand commun diviseur. Les nombres entiers a et b sont donc premiers entre eux.

L'algorithme d'Euclide étendu va nous permettre de montrer le théorème fondamental de l'arithmétique en utilisant le resultat suivant :

Proposition 2 *(**lemme de Gauss**) : Si c divise ab et si c est premier avec b, alors il divise a.*

Preuve : Si c est premier avec b, on peut trouver u, v tels que $u.c + v.b = 1$. On aura alors $auc + avb = a$. Mais auc est divisible par$c$ ainsi que $avb = abv$. Donc a est divisible par c.

Définition 4 *: Soient a et b deux nombres entiers. Le plus petit commun multiple de a et b est le plus petit entier ≥ 0 qui soit multiple de a et b. On le note $ppcm(a, b)$.*

Exemple :
1) $ppcm(2, 4) = 4$.
2) $ppcm(3, 5) = 15$.
3) $ppcm(6, 0) = 0$.

On dispose d'une formule qui permet de calculer le plus petit commun multiple en utilisant le plus grand commmun diviseur :

Proposition 3 *: On a $ppcm(a, b).pgcd(a, b) = a.b$.*

Preuve : Soient a et b deux nombres entiers. Si l'un d'eux est nul, alors tous leurs multiples communs sont nuls. Sinon, posons $d = pgcd(a, b)$. On a alors $a = k_1 d$ et $b = k_2 d$ avec $pgcd(k_1, k_2) = 1$. Si m est un multiple commun de a et b, on doit avoir

$$m = \alpha k_1 d = \beta k_2 d$$

et donc

$$\alpha k_1 = \beta k_2.$$

Ainsi k_1 divise βk_2 et étant premier avec k_2, il doit diviser β. On obtient donc

$$m = u k_1 k_2 d$$

pour un certain $u > 0$. Ainsi tout multiple de a et b est de la forme uk_1k_2d et tout nombre de cette forme est clairement un multiple de a et b. Le plus petit commun multiple s'obtient pour la plus petite valeur de u qui est $u = 1$. Donc :

$$ppmc(a, b) = \frac{ab}{d} = \frac{ab}{pgcd(a, b)}.$$

En particulier si a et b sont premiers entre eux, on a $ppmc(a, b) = ab$.

Définition 5 *: Un nombre entier $p > 1$ est dit premier si les seuls diviseurs de p sont 1 et p lui-même. Autrement dit :*

$$a \mid p \Longrightarrow a = 1 \vee a = p.$$

Par exemple $2, 5, 2003$ sont des nombres premiers. Mais $4, 666, 2001$ ne le sonts pas. On dit que ce sont des nombres composés.
Remarque : Si un nombre premier p divise un produit ab, il doit diviser l'un des facteurs a ou b. En effet supposons que p ne divise pas a. Il est alors premier avec a et d'aprés le lemme de Gauss, il divise b.

Si un nombre entier n'est pas premier on peut montrer qu'il est toujours produit de nombres premiers :

Théorème 3 *(**théorème fondamental de l'arithmétique**) : Tout nombre entier positif s'écrit comme un produit de nombres premiers et ce de manière unique à l'ordre des facteurs prés.*

Preuve : Soit n un entier positif. Pour montrer la première partie du théorème utilisons une récurrence sur n. Si n est premier, on a fini. Sinon on a $n = ab$ avec $a, b < n$. Par hypothèse de récurrence a et b sont produits de nombres premiers et donc n aussi. Passons à l'unicité. Supposons qu'on ait deux factorisations :

$$n = p_1.p_2 \dots p_m$$

et

$$n = q_1.q_2 \dots q_l,$$

avec les p_i et les q_i des nombres premiers. Comme p_1 divise $n = q_1.(q_2 \dots q_l)$, on doit avoir $p_1 = q_1$ ou $p_1 \mid q_2 \dots q_m$. Par induction on a $p_1 = q_i$ pour un certain i. En simplifiant par p_1 et q_i et en répetant l'argument précédent pour les nombres premiers qui restent, on arrive au resultat.
Exemple : On a :

$$666 = 2.3^2.37.$$

$$2001 = 3.23.29.$$

$$12 = 22.3.$$

On peut montrer qu'il y a une infinité de nombres premiers. En effet supposons que non et soient $p_1 = 2, p_2 = 3, \dots, p_n$ tous les nombres premiers et posons :

$$N = 2.3.5 \dots p_n + 1.$$

Alors N est un entier qui n'est divisible par aucun nombre premier, ce qui contredit le théorème fondamental de l'arithmétique.
Remarque : Soit n un entier. Pour tout nombre premier p, posons $\alpha_p = 0$

si p n'est pas présent dans la décomposition de n en facteurs premiers, et, sinon, donnons à α_p la valeur de l'exposant de p dans cette décomposition de n en facteurs premiers. Avec ces notations on peut écrire :

$$n = \prod_p p^{\alpha_p}.$$

Ce produit qui semble porter sur une infinité de nombres premiers est en fait fini puisque seuls un nombre fini de facteurs sont différents de 1. De plus on peut utiliser cette décomposition pour calculer le plus grand commun diviseur et le plus petit commun multiple.

1.2 Congruences

Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}$. On dit que a est congru à b modulo n si n divise $a - b$. Autrement dit il existe $k \in \mathbb{Z}$ tel que :

$$a - b = nk.$$

On note $a \equiv b \pmod{n}$. On vérifie facilement que la relation de congruence est une relation d'équivalence sur $\mathbb{Z}$ (elle est reflexive, symétrique et transitive). La classe d'équivalence de a sera notée $\overline{a}$:

$$\overline{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\}.$$

L'ensemble quotient est :

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{a}, a \in \mathbb{Z}\}.$$

On l'appelle l'ensemble des congruences modulo n.
Exemple : Pour $n = 3$, on obtient :

$$\overline{0} = \{\ldots, -3, 0, 3, \ldots\},$$

$$\overline{1} = \{\ldots, -2, 1, 4, \ldots\},$$

$$\overline{2} = \{\ldots, -1, 2, 5, \ldots\},$$

et

$$\frac{\mathbb{Z}}{3\mathbb{Z}} = \{\overline{0}, \overline{1}, \overline{2}\}.$$

De manière générale l'ensemble des congruences modulo n contient exactement n éléments :

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}.$$

Si $a \equiv a^{'} \pmod{n}$ et $b \equiv b^{'} \pmod{n}$, on a (vérification facile) :

$$a + b \equiv a^{'} + b^{'} \pmod{n},$$

et

$$ab \equiv a^{'}b^{'} \pmod{n}.$$

Ceci nous permet de définir une addition et une multiplication sur l'ensemble des congruences et ainsi faire de l'arithmétique modulo n :

Définition 6 *: On peut additionner et multiplier des congruences en posant :*

$$\overline{a} + \overline{b} = \overline{a+b}$$

et

$$\overline{a}.\overline{b} = \overline{a.b}.$$

Ces deux opérations font de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ un anneau commutatif unitaire : l'addition en fait un groupe abélien (l'élément neutre de l'addition est $\overline{0}$ et le symétrique de $\overline{a}$ est $\overline{-a}$) et la multiplication est associative, commutative et distributive par rapport à l'addition et d'élément neutre $\overline{1}$.
Exemple : L'addition et la multiplication modulo 2 représentent les opérations booléennes bien connues de la disjonction exclusive (le ou exclsif ou XOR) et de la conjonction (le et logique) :

$$\frac{\mathbb{Z}}{2\mathbb{Z}} = \{0, 1\},$$

avec l'addition et la multiplication données par :

$$0 + 1 = 1 + 0 = 1,$$

$$0 + 0 = 1 + 1 = 0$$

et

$$0.1 = 1.0 = 0.0 = 0,$$

$$1.1 = 1.$$

(Avec les notations $\overline{0} = 0$ et $\overline{1} = 1$).
Remarque : Dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$ on peut simplifier par les éléments m qui sont premiers avec n. Plus exactement si $am \equiv bm \pmod{n}$ et si $pgcd(m, n) = 1$ alors $a \equiv b \pmod{n}$. En effet si n divise $am - bm$, alors il doit diviser $a - b$ s'il est premier avec m.

Définition 7 *: Un ensemble complet R de résidus modulo n est le choix d'un représentant de chaque classe de congruences modulo n.*

En général le choix le plus simple est :

$$R = \{0, 1, 2, \ldots, n-1\}$$

mais d'autres choix sont possibles. Par exemple pour $n = 3$ on peut prendre

$$R = \{0, 1, -1\}.$$

Proposition 4 *: Si R est un ensemble complet de résidus modulo n, il en est de même de $mR = \{mx, x \in R\}$ pour tout entier m premier avec n.*

Preuve : Il suffit de montrer que les éléments de mR sont tous distincts. En effet on aura alors $\#mR = \#R = n$ et donc mR est un ensemble complet de résidus. Supposons que $mx \equiv mx' \pmod{n}$ pour $x \neq x'$ dans R. Comme m est premier avec n, on peut simplifier par m et donc $x \equiv x' \pmod{n}$. Contradiction.

En utilisant ces ensembles R, on va montrer que l'equation $ax \equiv b \pmod{n}$ a toujours une solution en x si a est premier avec n.

Proposition 5 *: Si $pgcd(a, n) = 1$ alors l'équation linéaire $ax \equiv b \pmod{n}$ admet une solution.*

Preuve : Soit R un ensemble complet de résidus modulo n. Alors aR est aussi un ensemble complet de résidus. Cela veut dire qu'il existe un x dans R tel que $ax \equiv b \pmod{n}$.
Exemple : Soit l'équation $2x \equiv 3 \pmod{5}$. Comme 2 est premier avec 5, cette équation doit avoir une solution. Soit $R = \{0, 1, 2, 3, 4\}$ un ensemble complet de résidus modulo 5. On a :

$$2R = \{2.0, 2.1, 2.2, 2.3, 2.4\} = \{0, 2, 4, 6, 8\}$$

donc

$$2.4 = 8 \equiv 3 \pmod 5$$

et la solution cherchée est $x = 4$.

Ce résultat peut être généralisé à un système de congruences modulo plusieurs entiers premiers entre eux. On va démontrer ici le cas particulier correspondant à deux entiers m et n.

Proposition 6 ***(théorème des restes chinois)*** *: Soient $a, b \in \mathbb{Z}$ et soient $m, n \in \mathbb{N}$ deux nombres entiers premiers entre eux. Alors il existe $x \in \mathbb{Z}$ tel que :*

$$x \equiv a \pmod m$$

$$x \equiv b \pmod n$$

Autrement dit le système des deux congruences a une solution.

Preuve : L'équation $ym \equiv b - a \pmod n$ a une solution y puisque m est premier avec n. Posons $x = a + ym$. On a alors :

$$x \equiv a + (b - a) \equiv b \pmod n,$$

et

$$x = a + ym \equiv a \pmod b.$$

Exemple : Soit à résoudre le système :

$$x \equiv 2 \pmod 3$$

$$x \equiv 3 \pmod 5.$$

On a donc ici $a = 2, b = 3, m = 3$ et $n = 5$. On doit d'abord trouver une solution à l'équation $3y \equiv 3-2 = 1 \pmod 5$. $y = 2$ fait l'affaire. La solution cherchée est donc $x = a + ym = 2 + 2.3 = 8$.

1.3 Fonction indicatrice d'Euler

Soit n un nombre entier plus grand que 1 et soit E_n le sous-ensemble de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ formé des éléments inversibles pour la multiplication. E_n, muni de la multiplication est un groupe par sa définition même.

Proposition 7 *: Les éléments de E_n sont les classes des m tels que $0 < m \leq n-1$ et m premier avec n.*

Preuve : Désignons chaque classe par son unique représentant m tel que $0 < m \leq n-1$. Alors m est inversible dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$ si et seulement si il existe un entier u tel que $mu \equiv 1 \pmod{n}$, ce qu'on peut réecrire en disant qu'il existe des entiers u, v avec $mu+nv = 1$. Donc, d'aprés le théorème de Bezout, m est inversible si et seulement si m est premier avec n.

Définition 8 *: La fonction indicatrice d'Euler est la fonction ϕ définie pour tout $n \in \mathbb{N}^*$ par :*

$$\phi(n) = \#E_n.$$

C'est donc une fonction qui comptabilise le nombre d'éléments de E_n. Il résulte immédiatement de la proposition précédente que :

$$\phi(n) = \{m \in \mathbb{N} \mid m \leq n \wedge pgcd(m,n) = 1\}$$

Exemple
1) $\phi(1) = \#\{1\} = 1$.
2) $\phi(3) = \#\{1,2\} = 2$.
3) $\phi(8) = \#\{1,3,5,7\} = 4$.
En général si p est un nombre premier on a :

$$\phi(p) = \#\{1,2,\ldots,p-1\} = p-1.$$

On va utiliser le théorème fondamental de l'arithmétique pour calculer $\phi(n)$ à partir de la décomposition de n en facteurs premiers. Pour cela calculons d'abord ϕ pour les entiers n de la forme $n = p^\alpha$ pour p un nombre premier et α un entier plus grand que 1.

Proposition 8 *: Si p est un nombre premier et α un entier > 1, alors on a $\phi(p^\alpha) = (p-1)p^{\alpha-1}$.*

Preuve : Il nous faut chercher le nombre d'entiers x tels que $1 \leq x \leq p^\alpha - 1$ qui sont premiers avec p^α c'est-à dire avec p. Les entiers non premiers avec p dans cet intervalle sont exactement les multiples de p : $p, 2p, \ldots, p^{\alpha-1}p$ et qui sont au nombre de $p^{\alpha-1}$. Il rest donc $p^\alpha - p^{\alpha-1} = (p-1)p^{\alpha-1}$ éléments qui sont tous dans E_{p^α}.

Proposition 9 *: La fonction ϕ d'Euler est multiplicative : si m et n sont premiers entre eux, on a :*

$$\phi(mn) = \phi(m).\phi(n).$$

Preuve : Soit l'application :

$$f : E_{mn} \longrightarrow E_m \times E_n$$

donnée par :

$$f(t) = (t_m, t_n)$$

pour $t \in E_{mn}$ et t_m, t_n sont respectivement les classes de t modulo m et n. Il faut montrer que f est une bijection. Si $f(t) = f(t^{'})$, alors m divise $t - t^{'}$ et n divise $t - t^{'}$ et donc nm divise aussi $t - t^{'}$ puisque m et n sont premiers entre eux. Ceci montre que $t = t^{'}$ et que f est injective. Passons à la surjectivité. Soient $a \in E_m$ et $b \in E_n$. On a donc $pgcd(a, m) = 1$ et $pgcd(b, n) = 1$. Comme m et n sont premiers entre eux le système de congruences :

$$x \equiv a \pmod{m}$$

$$x \equiv b \pmod{n}$$

a une solution t qui vérifie $pgcd(t, mn) = 1$. Donc $t \in E_{mn}$ et f(t)=(a,b), ce qui montre que f est surjective. f étant bijective, les ensembles E_{mn} et $E_m \times E_n$ ont même nombre d'éléments ce qui par définition donne :

$$\phi(mn) = \phi(m).\phi(n).$$

Exemple : Comme $35 = 5.7$, on a :

$$\phi(35) = \phi(5).\phi(7) = 4.6 = 24.$$

On peut maintenant calculer $\phi(n)$ pour tout entier n :

Théorème 4 *: Si un nombre entier $n > 1$ a pour décomposition en nombres premiers*

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$

alors on a

$$\phi(n) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_k}).$$

Preuve : En utilisant la multiplicativité de ϕ et le calcul de $\phi(p^\alpha)$, on obtient

$$\phi(p_1^{\alpha_1} \dots p_k^{\alpha_k}) = (p_1 - 1)p_1^{\alpha_1 - 1} \dots (p_k - 1)p_k^{\alpha_k - 1}.$$

En mettant $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ en facteur dans cette quantité on obtient le résultat.

La fonction ϕ d'Euler calcule l'ordre du groupe E_n des éléments inversibles de l'anneau $\frac{\mathbb{Z}}{n\mathbb{Z}}$ pour la multiplication. Ces éléments inversibles sont les classes des entiers qui sont premiers avec n. Donc si $a \in E_n$, l'ordre r de a (c'est-à-dire du sous-groupe engendré par a) doit diviser $\phi(n)$ (d'aprés le théorème de Lagrange). Comme $a^r \equiv 1 \pmod{n}$, on doit aussi avoir

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Comme conséquence on obtient le **petit théorème de Fermat** :

Proposition 10 *: Si p est un nombre premier, on a :*

$$a^{p-1} \equiv 1 \pmod{p}$$

pour tout $a \in \mathbb{Z}$ non congru à 0 modulo p.

Preuve : Il suffit de remarquer que $\phi(p) = p - 1$.

Chapitre 2

Cryptographie

De nos jours la necessité de protéger l'information ou de la garder confidentielle n'est plus à prouver. La circulation des données numériques à travers les réseaux informatiques doit être securisée. Bon nombre de mécanismes sont utilisés pour atteindre cet objectif de protection. La cryptographie est l'un de ces mécanismes. On dit souvent que la cryptographie est la science du secret et du chiffrement. Elle a longtemps eté considérée comme un art (pratiqué le plus souvent par les militaires et les diplomates depuis les égyptiens jusqu'à la deuxième guerre mondiale) avant qu'elle ne subisse une mathématisation forcée par le developpement rapide de l'informatique et des nouvelles technologies. La cryptographie protége les données en les changeant de telles sortes qu'elles soient illisibles pour les personnes non autorisées ou celles pour lesquelles elles ne sont pas destinées. Cette alteration volontaire des données s'effectue par l'utilisation d'algorithmes mathématiques de cryptage et de décryptage qui utilisent des paires de clés secrètes : Celui qui n'a pas la clé de décryptage ne peut pas déchiffrer un message crypté avec la clé de cryptage et n'a donc pas accés à l'information. Une grande partie de ces algorithmes font partie de ce qu'on appelle la cryptographie à clé symétrique : les clés de cryptage et de décryptage s'obtiennent l'une à partir de l'autre et sont le plus souvent les mêmes. Elles doivent aussi être gardées secrètes. L'un des developpement majeurs de la cryptographie est l'avènement de la cryptographie à clé publique en 1976 quand Diffie et Hellmann publient leur article : *New Directions in Cryptography* qui présentait l'idée de clé publique et une méthode ingénieuse d'échange de clés. Dans ce type de cryptographie, la clé de cryptage est publique et connue de tout le monde mais la clé de décryptage doit rester secrète. En 1978 Rivest, Shamir et Adleman découvrent le pre-

mier schéma de cryptographie à clé publique pour le chiffrement des données (et aussi leur signature numérique). Ce shéma est maintenant appelé RSA suivant les initiales de ses inventeurs. Une étude détaillée du RSA fera l'objet du chapitre suivant. Dans le présent chapitre nous présentons les concepts de base de tout systéme cryptographique et donnons les définitions des schémas à clé symétrique et à clé publique. Les concepts d'échange de clés et de signature numérique nous serviront à montrer l'utilité de la cryptographie à clé publique.

2.1 Fonctions à sens unique

Une fonction f d'un ensemble X vers un ensemble Y est un moyen qui associe à chaque élément de X au plus un élément de Y. Si $x \in X$, $f(x)$ est son image dans Y par la fonction f. Les images de f constituent un sous-ensemble de Y qu'on note $Im(f)$. Les éléments $x \in X$ qui ont une image par f constituent un sous-ensemble de X qu'on appelle le domaine de définition de f et qu'on note $Dom(f)$.
Exemple : Soit $X = \{1, 2; 3, \ldots, 10\}$ et soit f la fonction qui à tout $x \in X$ associe le reste r_x de la division de x^2 par 11. On a

$$f(1) = 1; f(2) = 4; f(3) = 9; f(4) = 5; f(5) = 3$$

$$f(6) = 3; f(7) = 5; f(8) = 9; f(9) = 4; f(10) = 1.$$

Si on pose $Y = \{1, 3, 4, 5, 9\}$, alors f est une fonction de X vers Y d'image $Im(f) = Y$ et de domaine de définition $Dom(f) = X$.
En général on ne peut pas définir une fonction aussi simplement que dans l'exemple précédent. Si $X = \{1, 2, 3, \ldots, 10^{50}\}$ et si $f(x)$ est le reste r_x de la division de x^2 par $10^{50} + 1$, on ne peut pas calculer explicitement toutes les valeurs de f qui, néanmoins, est une fonction bien définie.

Une fonction est injective si deux éléments différents ont des images différentes. Elle est surjective si tout élément de Y est l'image d'un élément de X. Elle est bijective si elle est à la fois injective et surjective. Autrement dit tout élément de X correspond á un élément et un seul de Y. C'est pour cela qu'on parle aussi de correspondance entre X et Y. En particulier si X et Y sont finis ils doivent avoir le même nombre d'éléments. L'interêt des bijections est qu'on peut les inverser : si $f : X \longrightarrow Y$ est une bijection, son inverse est la fonction $g = f^{-1} : Y \longrightarrow X$ donnée par

$$f^{-1}(y) = x \Longleftrightarrow f(x) = y.$$

Exemple : Soient $X = \{a, b, c, d, e\}$ et $Y = \{1, 2, 3, 4, 5\}$. Soit f la fonction de X vers Y définie par

$$f(a) = 4; f(b) = 2; f(c) = 5; f(d) = 1; f(e) = 3.$$

Cette fonction est bijective et son inverse est la fonction f^{-1} de Y vers X donnée par

$$f^{-1}(1) = d; f^{-1}(2) = b; f^{-1}(3) = e; f^{-1}(4) = a; f^{-1}(5) = c.$$

Remarquer que si f est une bijection, il en est de même de f^{-1}. En cryptographie les bijections sont utilisées pour crypter les messages et leurs inverses pour les deécrypter.

Des bijections particulièrement importantes en cryptographie sont les permutations et les involutions.

Définition 9 *: Soit S un ensemble fini. Une permutation de S est une bijection $f : S \longrightarrow S$.*

Le plus souvent on considère l'ensemble fini $S = \{1, 2, \ldots, n\}$ et les permutations sont écrites sous forme d'un tableau à deux lignes : la première représente les éléments de S et sur la seconde on écrit leurs images.
Exemple : Soit $S = \{1, 2, 3, 4, 5\}$ et soit la permutation f donnée par

$$f(1) = 3; f(2) = 5; f(3) = 4; f(4) = 2; f(5) = 1.$$

Le tableau correspondant est

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$$

Comme f est une bijection ella a une permutation inverse f^{-1} de tableau

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 3 & 2 \end{pmatrix}$$

Définition 10 *: Soit S un ensemble fini et soit f une permutation de S. f est une involution si f est sa propre inverse :*

$$f = f^{-1}.$$

De manière équivalente f est une involution si $f \circ f = Id_S$ ou encore $f(f(x)) = x$ pour tout $x \in S$.
Exemple : Une transposition t_{ij} de $S = \{1, 2, 3, \ldots, n\}$ est une permutation qui transforme i en j et j en i mais qui n'affecte pas les autres éléments. Une transposition est une involution.

Définition 11 *: Une fonction f d'un ensemble X vers un ensemble Y est dite à sens unique si $f(x)$ est facile à calculer pour tout $x \in X$ et pour presque tous les éléments $y \in Im(f)$, il est difficile de trouver $x \in X$ tel que $f(x) = y$.*

Autrement dit une fonction à sens unique est facile à calculer dans un sens mais difficile à calculer dans l'autre sens et on comprend facilement l'interêt de telles fonctions pour la cryptographie.
Exemple
1) Soit $X = \{1, 2, 3, \ldots, 16\}$ et soit f la fonction $f(x) = r_x$ avec r_x le reste de la division de 3^x par 17. Il est facile de calculer les valeurs de f. Par exemple $f(2) = 9$ et $f(11) = 7$. Mais pour presque tous les éléments de l'image de f il est difficile de trouver un élément de X dont ils sont l'image. Pour presque tous mais pas tous. Par exemple pour 3 il est facile de trouver $x = 1$.
2) Soient $p = 48611$ et $q = 53993$ deux nombres premiers et soit $n = pq = 2624653723$ leur produit. Posons $X = \{1, 2, 3, \ldots, n-1\}$ et définissons f sur X par $f(x) = r_x$ avec r_x le reste de la division de x^3 par n. On peut calculer les valeurs de f facilement. Par exemple $f(2489991) = 1981394214$. Mais la procédure inverse est trés difficile.

Définition 12 *: Une fonction à sens unique avec trappe est une fonction à sens unique $f : X \longrightarrow Y$ munie d'une information supplémentaire (la trappe) qui permet pour tout $y \in Im(f)$ de déterminer x tel que $f(x) = y$.*

le dernier exemple est un exemple d'une fonction à sens unique avec trappe. Le problème du calcul d'une racine cubique modulo n est trés difficile si on ne connait pas les facteurs premiers p et q de n mais devient faisable (dans le sens ou il existe un algorithme pour calculer ces racines) dés qu'on connait cette factorisation. Dans ce cas la trappe est la connaissance de p et q tels que $n = pq$.

2.2 Concepts de Base

On présente ici les concepts de base de tout système cryptographique. Au départ on a toujours un alphabet de définition A qui est un ensemble fini dont les éléments sont des lettres qu'on va utiliser pour écrire les mots d'un message. L'exemple le plus courant est l'alphabet binaire $A = \{0, 1\}$. Viennent ensuite un ensemble M de messages en clair qui sont des suites finies de symboles ou de lettres de l'alphabet de définition et un ensemble C de messages cryptés qui sont aussi des suites de lettres de l'alphabet de définition (qui peut différer de l'alphabet de définition de M). Pour crypter et décrypter les messages il faut en plus qu'on dispose d'un ensemble K dont les éléments sont appelés des clés. Chaque clé $e \in K$ détermine uniquement une bijection de M vers C qu'on note E_e et qu'on appelle la fonction de cryptage. Appliquer E_e au message m c'est crypter le message m :

$$E_e(m) \in C.$$

On doit aussi disposer pour chaque clé $d \in K$ d'une bijection D_d de C vers M qu'on appelle la fonction de décryptage. Appliquer D_d au message crypté c c'est le décrypter :

$$D_d(c) \in M.$$

Définition 13 *: Un schéma de cryptage consiste en le choix d'un ensemble* $\{E_e, e \in K\}$ *de fonctions de cryptage et d'un ensemble correspondant* $\{D, d \in K\}$ *de fonctions de décryptage de telle sorte que pour toute clé* $e \in K$*, il existe une unique clé* $d \in K$ *avec* $D_d = E_e^{-1}$.

Les clés e et d forment une paire (e, d) qu'on appelle la paire de cryptage-décryptage. Remarquer qu'on peut avoir $e = d$.

Un schéma de cryptage est utilisé de la manière suivante. Supposons que deux individus, Kaddour et Messaouda, veulent échanger des messages en toute confidentialité. Ils commencent par choisir et se communiquer une paire de clés (e, d). Si Kaddour veut envoyer le message $m \in M$ à Messaouda, il lui applique la transformation E_e pour obtenir le message crypté $E_e(m) = c$ qu'il transmet. Quand Messaouda recoit c, elle lui applique la transformation inverse D_d pour récuperer le message d'origine $m = D_d(c)$.
Exemple : Soient $M = \{m_1, m_2, m_3\}$ et $C = \{c_1, c_2, c_3\}$. Les bijections de M vers C sont au nombre de $3! = 6$. On peut donc prendre comme ensemble de clés $K = \{1, 2, 3, 4, 5, 6\}$. Par exemple E_1 est la transformation telle que

$$E_1(m_1) = c_3$$

$$E_1(m_2) = c_1$$
$$E_1(m_3) = c_2.$$

d'inverse disons D_4

$$D_4(c_1) = m_2$$
$$D_4(c_2) = m_3$$
$$D_4(c_3) = m_1.$$

Si Kaddour et Messaouda choisissent la paire de clés $(1, 4)$, alors pour envoyer le message m_1, Kaddour calcule $E_1(m_1) = c_3$ et le transmet à Messaouda qui calcule à son tour $D_4(c_3) = m_1$ pour décrypter le message.

Kaddour et Messaouda sont des entités. Une entité est quelqu'un (ou quelque chose) qui envoie, recoit ou manipule une information. Dans notre cas Kaddour est un envoyeur et Messaouda est un receveur. Un adversaire est une troisième entité qui n'est ni l'envoyeur ni le receveur mais qui essaie de s'interposer entre les deux pour subtiliser (voler) l'information. L'adversaire peut être passif (il ne fait que lire l'information) ou actif (il altère ou change l'information). Les entités communiquent via un canal de communication.
Remarque : En général les ensembles M, C, K sont connus de tout le monde (ainsi que les fonctions de cryptage E_e et de décryptage D_d). La sécurité d'un schéma de cryptage est basée uniquement sur la paire de clé (e, d) qui doit donc être gardée secrète. Si un adversaire peut récuperer le message en clair m à partir du message crypté c en un temps raisonnable sans connaitre la paire de clés de cryptage-décryptage on dit que le schéma est cassable (ou qu'il n'est pas sûr). L'adversaire peut par exemple essayer toutes les paires de clés possibles. C'est ce qu'on appelle une recherche exhaustive sur l'ensemble des clés K qui doit donc être trés large pour ne pas permettre ce genre d'attaques.

Définition 14 *: La cryptographie est l'étude de techniques mathématiques basées sur des schémas de cryptage pour le traitement de l'information dans le domaine de la confidentialité, de l'intégrité des données et de leur authentification. La cryptanalyse est l'étude des techniques mathématiques qui permettent de casser (attaquer) un système cryptographique. La cryptologie est l'étude de la cryptographie et de la cryptanalyse.*

On divise les techniques cryptographiques en deux grandes familles : la cryptographie à clé symétrique et la cryptographie à clé publique. Dans la pratique elles sont utilisées conjointement l'une pour génerer des clés et l'autre pour le chiffrement proprement dit.

2.3 Cryptographie à clé symétrique

Définition 15 *: Un schéma de cryptage est dit à clé symétrique si pour toute paire de clés (e, d) il est possible de déterminer d à partir de e et inversement.*

Dans la plupart des cas on a même $e = d$ d'où le terme symétrique pour décrire ce genre de cryptographie : la clé de décryptage est déduisible de la clé de cryptage.
Exemple : Soit $A = \{a, b, \ldots, x, y, z\}$. L'ensemble des messages en clair M et l'ensemble des messages cryptés C sont formés de tous les mots de longueur finie sur l'alphabet A. L'ensemble des clés K est l'ensemble des permutations de A. Pour crypter un message m, on choisit une clé (une permutation de A) e et on l'applique à chaque lettre de m. Pour clé de décryptage on choisit la clé $d = e^{-1}$ et pour décrypter on applique donc la permutation inverse e^{-1} à chaque lettre du message crypté. Le schéma est bien symétrique puisque la clé de décryptage s'obtient immédiatement à partir de la clé de cryptage. Si par exemple la permutation e consiste en la transformation qui remplace chaque lettre par la lettre justa à sa droite alors le message

$$m = kaddourestunbonetudiant$$

devient

$$c = lbeepvsftuvocpofuvejbou.$$

La sécurité d'un schéma de cryptage à clé symétrique repose entièrement sur la connaissance de l'une des deux clés e, d (puisqu'on peut récuperer facilement l'une à partir de l'autre). Se pose donc le problème de la distribution de ces clés. En particulier l'espace des clés K doit être assez large pour éviter toute recherche exhaustive. Le seul schéma dont on peut prouver théoriquement qu'il est sûr (ou incassable) est le chiffremnt de Vernam : l'alphabet A est l'alphabet binaire $A = \{0, 1\}$. Pour tout message écrit en binaire $m = m_1 m_2 \ldots m_t$ (avec $m_i = 0$ ou 1) le cryptage consiste en le choix d'une clé (qui est un autre mot écrit en binaire de même longueur) $k = k_1 k_2 \ldots k_t$ qu'on XOR avec m : le message crypté est $c = c_1 c_2 \ldots c_t$ avec

$$c_i = m_i \oplus k_i$$

pour $1 \leq i \leq t$. L'opération $\oplus$ est définie sur les binaires par

$$0 \oplus 0 = 0$$

$$0 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$
$$1 \oplus 1 = 0.$$

La clé k est choisie au hasard et n'est utilisée qu'une seule fois (one-time pad). Pour décrypter on XOR à nouveau avec k :

$$c_i \oplus k_i = m_i \oplus k_i \oplus k_i = m_i.$$

Le désavantage avec le chiffrement de Vernam est que la clé doit être de même longueur que le message en clair ce qui le rend peu praticable et de plus le problème de l'échange de la clé persiste.

2.4 Cryptographie à clé publique

Un schéma de cryptage sera dit à clé publique si, dans la paire de cryptage-décryptage (e, d), il est impossible de déterminer d à partir de e. Une autre manière d'exprimer cela est de dire que la transformation de cryptage correspondant à la clé e est une fonction à sens unique avec d comme trappe : il est impossible, connaissant un message crypté c de trouver le message en clair m tel que $E_e(m) = c$ sans connaitre d et donc la transformation de décryptage D_d. La clé e est publique et est connue de tout le monde et c'est pour cela qu'on parle de cryptographie à clé publique. La clé d quand à elle doit rester secrète puisque c'est elle qui constitue la trappe du chiffrement.

En général ce schéma est utilisé de la maniière suivante : Kaddour choisit une paire de clés (e, d). Il rend publique la clé e (qui est ainsi connue de tous et en particulier de Messaouda) mais garde secrète la clé d qui n'est donc connue que par lui même. Si Messaouda veut envoyer un message m à Kaddour, elle commence par le crypter en utilisant la clé e pour obtenir le message chiffré

$$c = E_e(m)$$

qu'elle envoie à Kaddour. Celui-ci en recevant c lui applique la transformation de décryptage D_d (correspondant à sa clé secrète d) pour retrouver le message en clair

$$m = D_d(c).$$

Ceci nous amène à la définition suivante :

Définition 16 *: Un schéma de cryptage est dit à clé publique si, dans la paire de clés (e, d), l'une des clés, e, est rendue publique alors que l'autre, d, reste privée avec la condition qu'il soit impossible de retrouver d à partir de e.*

L'un des grands avantages de la cryptographie à clé publique est justement le fait que seule la clé privée d doit être gardée secrète bien qu'on doive quand même s'assurer de l'authenticité de la clé publique e (Messaouda pourrait trés bien utiliser une clé $e^{'}$ émise par un adversaire tout en croyant qu'elle provient de Kaddour ce qui est une grande atteinte à la sécurité). Dans bon nombre de situations la cryptographie à clé publique est utilisée pour générer et s'échanger une paire de clés pour un système de cryptage à clé symétrique (dont les techniques de chiffrement sont beaucoup plus rapides).
Exemple : Kaddour construit un schéma à clé publique et envoie sa clé publique à Messaouda. Celle-ci génére une paire de clés pour un schéma à clé symétrique, la crypte en utilisant la cé publique de Kaddour et la lui envoie. Kaddour décrypte la paire de clés en utilisant sa clé privée et tous les deux commencent à communiquer en utilisant cette paire de clés pour crypter et décrypter leurs messages.

Le système RSA qu'on va voir dans le chapitre suivant utilise la cryptographie à clé publique pour générer les clés et pour le chiffrement lui-même. Mais avant d'en arriver là, voyons sur l'exemple de la signature numérique, l'utilité des techniques à clé publique.

La signature numérique est un outil cryptographique trés important pour l'authentification et la non répudiation de l'information (Si une entité signe un message, elle ne peut plus le nier par la suite). Pour que l'entité K puisse signer des messages dans un ensemble M il faut disposer d'un ensemble S dont les éléments seront appelés des signatures et d'une application de signature

$$S_K : M \longrightarrow S$$

$S_K(m)$ est donc la signature de l'entité K sur le message m. Cette fonction de signature S_K doit être gardée secrète par K. Il faut aussi disposer d'une fonction de vérification

$$V_K : M \times S \longrightarrow \{0, 1\}$$

qui sert aux autres entités à vérifier les signatures de K. Si $V_K(m, s) = 1$ la signature s correspond bien au message m et si $V_K(m, s) = 0$ la signature du

message m n'est pas authentique. V_K doit être publique (connue de tout le monde).

Définition 17 *: Un schéma de signature numérique est la spécification des deux fonctions S_A et V_A.*

La procédure de signature et de vérification se déroule de la manière suivante : Le signataire K (pour Kaddour) signe le message m en calculant $s = S_K(m)$ puis envoie la paire (m, s). s est la signature du message m. Si l'entité M (pour Messaouda) veut s'assurer que la signature s du message m a bien eté crée par Kaddour, elle commence par obtenir la fonction de vérification V_K puis calcule $v = V_K(m, s)$. Si $v = 1$, Messaouda accepte la signature et la rejette si $v = 0$.
Remarque : Les fonctions de signature et de vérification sont le plus souvent des algorithmes publiquement accessibles caractérisé chacun par une clé. La clé de signature doit donc être gardée secrète et la clé de vérification doit être rendue publique. De plus la fonction de vérification doit être une fonction à sens unique : étant donné un message m, il est impossible pour toute autre entité autre que Kaddour de trouver une signature s telle que $V_K(m, s) = 1$.

Soit un schéma de cryptage à clé publique dans lequel $M = C$ (les ensembles des messages en clair et des messages cryptés sont identiques). Pour toute paire de clés (e, d) on a donc les égalités suivantes concernant les fonctions de cryptage E_e et de décryptage D_d :

$$D_d(E_e(m)) = m$$

et

$$E_e(D_d(m)) = m$$

pour tout $m \in M$. (Remarquer que ceci est possible car $M = C$).
On peut utiliser ce schéma pour signer les messages de M comme suit : On prend

$$S = M = C$$

et on définit la fonction de signature S_K par

$$S_K(m) = D_d(m)$$

et la fonction de vérification V_K par

$$V_K(m, s) = 1$$

si $E_e(s) = m$ et

$$V_K(m, s) = 0$$

sinon. Ici e est la clé publique de Kaddour et d est sa clé privée (ou secrète).

Chapitre 3

Exemple du RSA

Le RSA, pour Rivest, Shamir et Adleman ses inventeurs en 1978, est un algorithme pour cryptographie à clé publique. C'est le premier algorithme connu utilisé en même temps pour chiffrer les messages et pour les signer. C'est aussi l'un des grands succés de la cryptographie à clé publique. Même actuellement il est largement utilisé dans les protocoles de commerce electronique. Sa sécurité est basée sur la difficulté de factoriser de grands nombres entiers et est jugée suffisante pourvu qu'on utilise des clés assez longues. Dans ce chapitre nous allons décrire de manière simple le chiffrement RSA (nous ne parlerons pas de la signature RSA). Nous détaillerons son fonctionnement en utilisant les notions apprises dans les chapitres 1 et 2 et nous passerons en revue à la fin quelques methodes d'attaque du système RSA pour tester sa sécurité. Comme on le verra toutes ces attaques utilisent à la base le problème de la factorisation.

3.1 Fonctionnement du RSA

L'algorithme de chiffrement RSA est basé sur la notion de fonction à sens unique et utilise le problème mathématique trés difficile de la factorisation des grands entiers. Il est constitué de trois étapes : La génération de clé, le chiffrement et le déchiffrement. Nous allons décrire successivement ces étapes (en supposant que Messaouda veut envoyer un message à Kaddour en utilisant la clé publique de celui-ci).

3.1.1 Génération de la clé

Kaddour commence par fabriquer sa paire de clé : l'une publique qu'il va publier sur le net et l'autre privée qu'il va garder pour lui. Pour cela il choisit deux nombres premiers p et q trés grands (100 chiffres chacun ou plus) et calcule leur produit

$$n = p.q$$

En utilisant les propriétés de la fonction ϕ d'Euler il obtient facilement

$$\phi(n) = \phi(p).\phi(q) = (p-1).(q-1).$$

Kaddour pique au hasard un entier $1 < e < \phi(n)$ premier avec $\phi(n)$. Il utilise ensuite la proposition 5 pour trouver un entier d tel que

$$ed \equiv 1 \pmod{\phi(n)}.$$

La clé publique de Kaddour est le couple (n, e). Sa clé privée est l'entier d.

3.1.2 Chiffrement

Kaddour communique (d'une manière ou d'une autre par exemple par internet) sa clé publique (n, e) à Messaouda et garde secrète sa clé privée d. Pour envoyer le message m à Kaddour, Messaouda commence par transformer m en un entier u avec $0 < u < n$ (voir plus bas sur un moyen de faire cela). Elle définit ensuite une fonction de cryptage

$$E : \frac{\mathbb{Z}}{n\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{n\mathbb{Z}}$$

par

$$E(x) = x^e.$$

et envoie $E(u)$ à Kaddour.

Si $x = \overline{a}$ avec $a \in \{0, 1, \ldots, n-1\}$ alors la fonction E est l'exponentiation modulo n :

$$E(x) = E(\overline{a}) = a^e \pmod{n}.$$

On dispose d'un algorithme assez rapide (exponentiation binaire) pour calculer $a^e \pmod{n}$. En effet si on écrit e en binaire

$$e = \sum_{i=1}^{r} \epsilon_i 2^i$$

avec $\epsilon_i \in \{0,1\}$ alors

$$a^e = \prod_{\epsilon_i=1} a^{2i} \pmod{n}.$$

Exemple : Pour calculer $4^{13} \pmod{497}$ on écrit 13 en binaire

$$13 = 1.2^3 + 1.2^2 + 0.2^1 + 1.2^0 = 1101_2$$

et donc

$$4^{13} = 4^{2^3}.4^{2^2}.4 \equiv 429.256.4 \equiv 445 \pmod{497}.$$

Pour que cette procédure soit correcte il faut montrer que notre fonction de cryptage E est en fait une bijection. Ainsi on utilisera la fonction inverse E^{-1} pour décrypter.

Proposition 11 *: Soit n un nombre entier qui n'a aucun carré comme diviseur. Soient e, d des nombres entiers tels que $p-1 \mid ed-1$ pour tout nombre premier $p \mid n$. Alors on a*

$$a^{ed} \equiv a \pmod{n}$$

pour tout $a \in \mathbb{Z}$.

Preuve : $a^{ed} \equiv a \pmod{n}$ équivaut à $n \mid a^{ed} - a$ ce qui équivaut aussi à $p \mid a^{ed} - a$ pour tout diviseur premier p de n (aucun carré ne divise n). Il suffit donc de montrer la proposition pour $n = p$ un nombre premier. Si $pgcd(a,p) \neq 0$ alors p divise a. Donc $a \equiv 0 \pmod{p}$ et $a^{ed} \equiv 0 \equiv a \pmod{p}$. Si $pgcd(a,p) = 1$ alors par le petit théorème de Fermat on a $a^{p-1} \equiv 1 \pmod{p}$ et donc aussi $a^{ed-1} \equiv 1 \pmod{p}$ puisque $p-1 \mid ed-1$. Multipliant à gauche et à droite par a on obtient $a^{ed} \equiv a \pmod{p}$.

Comme $n = p.q$ n'a aucun carré comme diviseur on peut appliquer cette proposition à notre situation. Les diviseurs premiers de n sont p et q et comme $ed \equiv 1 \pmod{(p-1)(q-1)}$ on a

$$p-1 \mid ed-1$$

et

$$q-1 \mid ed-1.$$

Donc

$$(a^e)^d \equiv a \pmod{n}$$

pour tout $a \in \mathbb{Z}$. Autrement dit si on définit la fonction

$$E^{-1} : \frac{\mathbb{Z}}{n\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{n\mathbb{Z}}$$

par

$$E^{-1}(x) = x^d$$

on a

$$E^{-1}(E(x)) = x$$

et

$$E(E^{-1}(x)) = x$$

pour toute classe x modulo n. Ceci montre que E est bijective d'inverse E^{-1}.

3.1.3 Déchiffrement

En recevant $E(u)$ Kaddour récupère u (et donc le message m) en appliquant la transformation inverse E^{-1} à $E(u)$:

$$E^{-1}(E(u)) = u.$$

Ainsi la fonction E se comporte comme une fonction à sens unique avec trappe. La fonction E est facile à calculer pour quiconque dispose de la clé publique (n, e) mais son inverse E^{-1} est pratiquement impossible à trouver si on ne connait pas l'entier d. Or pour connaitre d il faut connaitre $\phi(n)$ et donc la factorisation $n = p.q$ de n. La trappe ici est donc la factorisation de n.

3.1.4 Exemple

Kaddour choisit $p = 61$ et $q = 53$ puis calcule $n = 61.53 = 3233$ et

$$\phi(3233) = (61 - 1).(53 - 1) = 3120.$$

Il choisit ensuite de manière aléatoire un élement

$$e \in \frac{\mathbb{Z}}{3233\mathbb{Z}}.$$

Supposons que ce soit $e = 17$. Pour trouver d il doit résoudre l'equation

$$17x \equiv 1 \pmod{3120}.$$

En utilisant l'algorithme d'Euclide étendu il trouve

$$d = 2753.$$

La clé publique de Kaddour est donc $(n, e) = (3233, 17)$ et sa clé privée est $d = 2753$. La fonction de cryptage

$$E : \frac{\mathbb{Z}}{3233\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{3233\mathbb{Z}}$$

est donnée par

$$E(x) = x^{17}$$

et son inverse E^{-1} est donc

$$E^{-1}(x) = x^{2753}.$$

Par exemple si $x = 65$ on a

$$E(65) = 65^{17} \pmod{3233} = 2790$$

et

$$E^{-1}(2790) = 2790^{2753} \pmod{3233} = 65.$$

Remarque : Dans la pratique les nombres premiers p et q doivent être trés larges pour éviter une possible factorisation de n qui pourrait révéler la clé privée d. Notre exemple n'a été donné qu'à titre illustratif.

3.2 Message=Nombre

Un message est formé de mots et chaque mot est une suite finie de lettres de l'alphabet latin $A = \{a, b, c, \ldots, x, y, z\}$. A cet alphabet on rajoute le blanc (ou espace) qu'on peut représenter par un #. Pour convertir un message en nombre il suffit donc d'associer à chaque lettre (plus le blanc) un entier compris entre 0 et 26. Par exemple on fait correspondre le # à 0, la lettre a à 1, la lettre b à 2,... et la lettre z à 26. Chaque message correspond donc à un nombre écrit en base 27.
Exemple : Soit le message $m = boufouh$. En base 27 cela devient

$$boufouh = 2.27^0 + 15.27^1 + 21.27^2 + 6.27^3 + 15.27^4 + 21.27^5 + 8.27^6$$

et en décimal cela donne

$$bou f ouh = 3408796388.$$

Le message $bou f ouh$ devient donc le nombre 3408796388. Le processus inverse qui consiste à diviser successivement par 27 permet de retrouver le message à partir du nombre :

$$3408796388 = 126251718.27 + 2$$

ce qui donne $b = 2$ puis

$$126251718 = 4675989.27 + 15$$

ce qui donne $o = 15$ et ainsi de suite.
Rappelons qu'un entier r écrit en base b est une notation de la forme $(d_{k-1}d_{k-2}\ldots d_1d_0)$ avec d_i compris entre 0 et $b-1$ et

$$r = d_{k-1}b^{k-1} + d_{k-2}b^{k-2} + \ldots + d_1b + d_0.$$

Si $d_{k-1} \neq 0$ on dit que l'entier r est de longueur k en base b. Tout entier entre b^{k-1} et b^k est de longueur k en base b. Ainsi un message m comportant k lettres (y compris le blanc) s'exprime par un entier de longueur k en base 27. En particulier on a

$$27^{k-1} \leq m < 27^k.$$

L'algorithme RSA utilise l'arithmétique modulo n avec n la première composante du couple (n, e) constituant la clé publique de Kaddour. Le message m une fois converti en nombre doit être $< n$:

$$m \in \frac{\mathbb{Z}}{n\mathbb{Z}} = \{0, 1, 2, \ldots, n-1\}.$$

Le message m doit donc comporter k lettres avec

$$27^k < n$$

ou encore

$$k < log(n)/log(27) = log_{27}(n).$$

Si le message m comporte plus de k lettres on le divise en blocs de k lettres et on traite chaque bloc séparément.

3.3 Sécurité du RSA

Une attaque du RSA consiste pour un adversaire à récuperer le message en clair m envoyé par Messaouda à partir du message crypté c connaissant uniquement la clé publique de Kaddour (n, e). Pour cela il faut trouver la clé secrète d. C'est ce qu'on appelle le problème RSA. La proposition suivante montre que ce problème est équivalent au problème de la factorisation de n en nombres premiers.

Proposition 12 *: Le problème RSA (trouver d à partir de (n, e)) est équivalent au problème de la factorisation de n.*

Preuve : Si on connait la factorisation $n = pq$ de n on peut facilement calculer $\phi(n) = (p-1)(q-1)$ et donc d (si on connait $\phi(n)$ on peut aussi trouver la factorisation de n. En effet $\phi(n) = (p-1)(q-1) = pq-(p+q)+1$ et on connait $pq = n$ et $p + q = n + 1 - \phi(n)$. p et q sont donc solutions de l'équation du second degré

$$x^2 - (p + q)x + pq.$$

dont la résolution est facile). Inversement supposons qu'on connaisse d. On peut alors factoriser n de la manière suivante : on sait que

$$ed \equiv 1 \pmod{\phi}$$

et il existe donc un entier k tel que

$$ed - 1 = k\phi$$

et donc

$$a^{ed} \equiv a \pmod{n}$$

pour tout a. Ecrivons $ed-1 = 2^s t$ avec t un entier impair. Il existe un $i \in [1, s]$ tel que $a^{2^{i-1}t}$ ne soit pas congru à ± 1 modulo n et $a^{2^i t} \equiv 1 \pmod{n}$ pour la moitié des a. Pour de tels entiers a et i le plus grand commun diviseur de $a^{2^{i-1}t} - 1$ et n est un diviseur non trivial de n. Il suffit donc de répéter le processus en choisissant un a au hasard et essayer de trouver un i qui satisfait les conditions précédentes.

Un imperatif majeur pour la sécurité du système RSA est donc de choisir des nombres premiers p et q assez grands pour rendre difficile la factorisation

de $n = pq$. Assez grands mais aussi pas trop proches l'un de l'autre. En effet si p et q ne sont pas assez éloignés l'un de l'autre on paut utiliser la methode suivante due à Fermat pour factoriser n. Supposons $p > q$. On peut écrire

$$n = pq = (\frac{p+q}{2})^2 - (\frac{p-q}{2})^2.$$

Comme p et q sont proches alors

$$s = \frac{p-q}{2}$$

est petit et

$$t = \frac{p+q}{2}$$

est à peine plus grand que $\sqrt{n}$. De plus $t^2 - n = s^2$ est un carré parfait. Soit m le plus petit entier supérieur ou égal à $\sqrt{n}$. On essaye donc pour t les valeurs proches de m

$$t = m, t = m + 1, \ldots$$

jusqu'à ce que $t^2 - n$ soit un carré parfait s^2. On a alors $p = t + s$ et $q = t - s$.

Bibliographie

[1] W.Stein, Elementary Number Theory : Primes, Congruences and Secrets, Springer, 2009.

[2] N.Koblitz, A course in Number Theory and Cryptography, Springer, 1994.

[3] A.Menezes, P.Van Oorschot, S.Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[4] B.Schneier, Applied Cryptography, John Wiley and Sons, Inc, 1996.