Arithmétique et cryptographie

Vincent Genilloud
Gymnase de Morges

Année 2006-2007

Table des matières

Introduction

L'homme a toujours ressenti le besoin de dissimuler des informations, bien avant même l'apparition des ordinateurs. Depuis sa création, le réseau Internet a tellement évolué qu'il est devenu un outil essentiel de communication. Cependant, cette communication met de plus en plus en jeu des problèmes d'économie des entreprises présentes sur le Web. Les transactions faites à travers le réseau peuvent être interceptées, d'autant plus que les lois ont du mal à se mettre en place sur Internet ; il faut donc garantir la sécurité de ces informations, c'est la cryptographie qui s'en charge. Le mot **cryptographie** (du grec kruptos, caché) est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans action spécifique. La cryptographie est essentiellement basée sur l'**arithmétique** (du grec arithmêtikê, science des nombres) : il s'agit dans le cas d'un texte de transformer les lettres qui composent le message en une succession de chiffres (sous forme de bits dans le cas de l'informatique car le fonctionnement des ordinateurs est basé sur le binaire), puis ensuite de faire des calculs sur ces chiffres pour :

- d'une part les modifier de telle façon à les rendre incompréhensibles. Le résultat de cette modification (le message chiffré) est appelé cryptogramme (en anglais ciphertext) par opposition au message initial, appelé message en clair (en anglais plaintext) ;
- faire en sorte que le destinataire saura les déchiffrer. Dans ce cours, nous allons principalement étudier le système de cryptographie **RSA** vieux de moins de 30 ans et encore d'actualité !

Dans ce cours, nous allons principalement étudier le système de cryptographie RSA vieux de moins de 30 ans et encore d'actualité !

1 L'anneau des entiers

Désignons par $\mathbb{Z}$ l'ensemble des nombres entiers (positifs, nuls et négatifs) :

$$\mathbb{Z} = \{\ldots; -3; -2; -1; 0; 1; 2; 3; \ldots\}.$$

On munit $\mathbb{Z}$ de l'addition usuelle (notée $+$) et de la multiplication usuelle (notée $\cdot$).
L'addition possède les propriétés suivantes :

A1 L'addition est **commutative** :

$$x + y = y + x \text{ pour tous } x, y \in \mathbb{Z}.$$

A2 L'addition est **associative** :

$$(x + y) + z = x + (y + z) \text{ pour tous } x, y, z \in \mathbb{Z}.$$

A3 Le nombre **0** est l'**élément neutre** de l'addition :

$$x + 0 = x \text{ pour tous } x \in \mathbb{Z}.$$

A4 Chaque nombre $x \in \mathbb{Z}$ possède un **opposé**, l'entier $-x$:

$$x + (-x) = 0 \text{ pour tous } x \in \mathbb{Z}.$$

La multiplication possède les propriétés suivantes :

M1 La multiplication est **commutative** :

$$xy = yx \text{ pour tous } x, y \in \mathbb{Z}.$$

M2 La multiplication est **associative** :

$$(xy)z = x(yz) \text{ pour tous } x, y, z \in \mathbb{Z}.$$

M3 Le nombre **1** est l'**élément neutre** pour la multiplication :

$$x \cdot 1 = x \text{ pour tous } x \in \mathbb{Z}.$$

Voici encore une propriété liant l'addition et la multiplication :

D La multiplication est **distributive** par rapport à l'addition :

$$x(y + z) = xy + xz \text{ pour tous } x, y, z \in \mathbb{Z}.$$

Définition

On résume les propriétés A1, A2, A3, A4, M1, M2, M3, D en disant que l'ensemble $\mathbb{Z}$ muni de l'addition (usuelle) et de la multiplication (usuelle) est un **anneau commutatif**.

Remarque

On dit que l'anneau est commutatif pour rappeler que la multiplication est commutative. (Par exemple, l'ensemble des matrices 2×2 à coefficients réels, muni de l'addition et de la multiplication usuelles, est un anneau, mais non commutatif, car la multiplication matricielle n'est pas commutative.)

Exercice 1

Trouver les opposés des nombres 5, -193 et 0.

Exercice 2

Désignons par $\mathbb{N}$ l'ensemble des entiers positifs ou nul, par $\mathbb{Q}$ l'ensemble des nombres rationnels, c'est-à-dire des nombres pouvant s'écrire sous la forme $\frac{a}{b}$ où a et b sont deux éléments de $\mathbb{Z}$ avec b non nul, et par $\mathbb{R}$ l'ensemble de tous les nombres réels. (Cet ensemble contient par exemple les nombres $\sqrt{2}$ et π qui ne sont pas rationnels.)

Les ensembles $\mathbb{N}$, $\mathbb{Q}$ et $\mathbb{R}$ munis de l'addition et de la multiplication usuelles sont-ils des anneaux commutatifs ? Si oui, quels sont les éléments neutres ?

Exercice 3

Un élément $x \in \mathbb{Z}$ est dit **inversible** s'il existe $y \in \mathbb{Z}$ tel que $xy = 1$.

1. Quels sont les éléments de $\mathbb{Z}$ qui sont inversibles ?
2. Vérifier que tous les éléments non nuls de $\mathbb{Q}$ et de $\mathbb{R}$ sont inversibles.

Remarque

Vu les exercices 2 et 3, les ensembles $\mathbb{Q}$ et $\mathbb{R}$ munis de l'addition et de la multiplication usuelles sont des anneaux commutatifs pour lesquels chaque élément non nul est inversible. On résume cela en disant que $\mathbb{Q}$ et $\mathbb{R}$ sont **des corps (commutatifs)**.

2 Algorithme d'Euclide et théorème de Bézout

Le théorème suivant, appelé **théorème de la division euclidienne**, est bien connu :

Théorème

Soit $a, b \in \mathbb{Z}$ avec $b > 0$. Il existe $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ vérifiant

$$a = bq + r \quad \text{avec } 0 \leqslant r < b.$$

De plus, étant donné a et b, les nombres q et r sont uniques.

Définition

Le nombre q est le **quotient** de la division de a par b, le nombre r est le **reste** de cette division.

Preuve

Exercice 4

Dans chacun des cas suivants, trouver le quotient et le reste de la division de a par b.

1. $a = 1253$ et $b = 17$
2. $a = -19653$ et $b = 87$
3. $a = 17865$ et $b = 973872$

Définition

Si $n \in \mathbb{Z}$, on dit que n est **divisible par** un entier d s'il existe un entier q tel que

$$n = dq.$$

On dit que d **divise** n et on note $d \mid n$.

Remarque

Dire que a est divisible par b, avec $b \neq 0$, équivaut à dire que le reste de la division de a par b est nul.

Exercice 5

1. Est-ce que 1332 est divisible par 9 ?
2. Est-ce que -12345 est divisible par 8 ?
3. Est-ce que 29 est divisible par 0 ?

Exercice 6

Soit a, b, d trois entiers. On suppose que $d \mid a$ et que $d \mid b$. Montrer que d divise toute **combinaison linéaire** de a et b, c'est-à-dire que $d \mid \alpha a + \beta b$ pour tous $\alpha, \beta \in \mathbb{Z}$.

Définition

Un **nombre premier** (on dit aussi simplement **un premier**) est un entier supérieur à 1 qui a exactement 2 diviseurs, à savoir 1 et lui-même.

Exercice 7

Le **crible d'Ératosthène** est un algorithme permettant de déterminer tous les nombres premiers plus petits qu'un entier positif n donné.

Pour ceci, on écrit la liste de tous les nombres de 2 jusqu'à n.
On souligne 2 et on élimine tous les multiples de 2.
Puis on fait de même avec 3.
On choisit alors le plus petit nombre non souligné, ici 5, et on élimine tous ses multiples.
On réitère le procédé jusqu'à la partie entière de la racine carrée de n.
Les nombres non éliminés sont les premiers jusqu'à n.

1. Justifier cet algorithme.

2. À l'aide de la grille de nombres ci-dessous et du crible d'Ératosthène, trouver tous les nombres premiers inférieurs à 100.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Exercice 8

Les nombres suivants sont-ils premiers ?

1. 11211
2. $2^{32582657} - 1$

Exercice 9

Montrer qu'il existe une infinité de nombres premiers.
(*Indication* : comme Euclide, on pourra raisonner par l'absurde : supposer qu'il n'existe que n nombres premiers distincts $p_1, \ldots, p_n$ et considérer l'entier $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.)

Remarque

Le résultat de l'exercice précédent est important, puisque le système RSA (voir le paragraphe 4) nécessite de « grands » nombres premiers.

Exercice 10

En décomposant a et b en un produit de nombres premiers, déterminer dans chacun des cas suivants le plus grand diviseur commun de a et b.

1. $a = 64$ et $b = 24$
2. $a = 210$ et $b = 825$
3. $a = 2156$ et $b = 4719$

On peut facilement se convaincre (voir l'exercice précédent) que le calcul d'un plus grand diviseur commun à l'aide de décompositions en nombres premiers est fastidieux. Lorsque les nombres a et b sont « grands », cette tâche peut même devenir interminable pour un ordinateur si ce dernier procède comme nous l'avons fait à l'exercice précédent.

Le théorème suivant, appelé **algorithme d'Euclide**, permet de calculer le plus grand diviseur commun de deux nombres en effectuant une suite de divisions euclidiennes ; il n'est pas nécessaire de connaître la décomposition en facteurs premiers des deux nombres en question.

Rappel sur le PGCD

Soit a et b deux entiers tous deux non nuls. Le **plus grand diviseur commun** de a et b est l'entier positif noté $\mathrm{PGCD}(a;b)$ vérifiant :

1. $\mathrm{PGCD}(a;b)$ divise a et b.
2. Si $d \in \mathbb{Z}$ divise a et b, alors d divise $\mathrm{PGCD}(a;b)$.

Algorithme d'Euclide

Soit $a, b \in \mathbb{N}^*$ avec $b < a$. L'algorithme consiste en la suite de divisions euclidiennes suivante :

$$\begin{aligned} a &= b \cdot q_0 + r_0 \\ b &= r_0 \cdot q_1 + r_1 \\ r_0 &= r_1 \cdot q_2 + r_2 \\ &\vdots \\ r_{m-2} &= r_{m-1} \cdot q_m + r_m \\ r_{m-1} &= r_m \cdot q_{m+1} + r_{m+1} \end{aligned}$$

où $0 \leqslant r_i < r_{i-1}$ (pour $i = 1, \ldots, m+1$).

L'algorithme se termine lorsque le dernier reste est nul : $r_{m+1} = 0$. Le plus grand diviseur commun de a et b est l'avant-dernier reste r_m.

Justification

Remarque

On peut montrer (théorème de Lamé, 1845) que le nombre D de divisions nécessaires à la terminaison de l'algorithme d'Euclide appliqué à a et b, avec $b < a$, vérifie :

$$D \leqslant \log_{\varphi}(a)$$

où $\varphi = \frac{1+\sqrt{5}}{2}$ (le nombre d'or).

Exercice 11

À l'aide de l'algorithme d'Euclide, trouver le plus grand diviseur commun de a et b dans chacun des cas suivants :

1. $a = 4131$ et $b = 1989$
2. $a = 8142$ et $b = 4127$
3. $a = 76538$ et $b = 14564$

Exercice 12

Comme pour les nombres entiers, vous avez vu en première année un algorithme de division pour les polynômes. Un algorithme analogue à celui d'Euclide pour les nombres entiers existe pour les polynômes.

1. Reformuler l'algorithme d'Euclide pour les nombres entiers dans le cas des polynômes.
2. En utilisant la première partie de cet exercice, trouver le (ou un) plus grand diviseur commun des polynômes f et g dans chacun des cas suivants :
   (a) $f(x) = 2x^2 - 5x + 4$
   $g(x) = x + 3$
   (b) $f(x) = 2x^4 + 3x^3 + 2x^2 + x - 3$
   $g(x) = 2x^3 + 5x^2 + 5x + 3$

Le résultat qui suit, appelé **théorème de Bézout**, jouera un rôle important dans les paragraphes suivants.

Théorème

Soit $a, b \in \mathbb{Z}$ non tous deux nuls. Il existe $\alpha, \beta \in \mathbb{Z}$ tels que

$$\alpha a + \beta b = \mathrm{PGCD}(a; b) \quad \text{(égalité de Bézout)}$$

La justification qui va suivre se base sur l'algorithme d'Euclide et est constructive : elle va permettre de trouver des entiers α et β vérifiant l'égalité ci-dessus.

Justification

Exercice 13

Dans chacun des cas suivants, écrire une égalité de Bézout.

1. $a = 35$ et $b = 14$
2. $a = 141$ et $b = 26$
3. $a = -102$ et $b = 276$
4. $a = 1234$ et $b = 521$

Exercice 14

Soit a et b deux entiers tels qu'il existe deux entiers α et β vérifiant l'égalité :

$$\alpha a + \beta b = 1.$$

Montrer que $\mathrm{PGCD}(a; b) = 1$.

Exercice 15

Soit a, b et c trois entiers tels qu'il existe α et β vérifiant l'égalité :

$$\alpha a + \beta b = c.$$

A-t-on $c = \mathrm{PGCD}(a; b)$?

3 Les entiers modulo n

Définition

Soit $n \in \mathbb{N}^*$. On dit que deux entiers a et b sont **congrus modulo n** si $a - b$ est un multiple de n. On écrit :

$$a \equiv b \mod n.$$

On dit aussi que a est congru à b modulo n. Autrement dit, par définition, $a \equiv b \mod n$ signifie que $a - b = kn$ pour un entier k.

Exercice 16

1. Montrer que $a \equiv a \mod n$ pour tout $a \in \mathbb{Z}$. (On dit que la congruence est une relation *réflexive*.)
2. Montrer que $a \equiv b \mod n$ entraîne $b \equiv a \mod n$. (On dit que la congruence est une relation *symétrique*.)
3. Montrer que si $a \equiv b \mod n$ et si $b \equiv c \mod n$, alors $a \equiv c \mod n$. (On dit que la congruence est une relation *transitive*.)

Exercice 17

1. Trouver tous les nombres a vérifiant $4 \equiv a \mod 11$.
2. Trouver tous les nombres a vérifiant $a \equiv -12 \mod 25$.
3. Trouver tous les nombres a et b vérifiant $a \equiv b \mod 1$.

Exercice 18

Soit a et b deux entiers. Montrer que a et b sont congrus modulo n si et seulement si le reste de la division de a par n est égal au reste de la division de b par n.

Notation

Soit $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. On note $(a)_n$ l'ensemble de tous les entiers congrus à a modulo n. On a donc

$$(a)_n = \{b \in \mathbb{Z} \mid a - b \text{ est un multiple de } n\}.$$

Exercice 19

Déterminer $(5)_7$, $(-6)_3$ et $(-9)_7$.

Exercice 20

Peut-on écrire les ensembles suivants sous la forme $(a)_n$? Si oui, y a-t-il plusieurs possibilités ?

1. $\{\ldots ; -5; -1; 3; 7; \ldots\}$
2. $\{-5; 0; 5; 10; 15; \ldots\}$
3. L'ensemble des multiples de 11 (positifs et négatifs)
4. $\{s \in \mathbb{Z} \mid s - 1 \text{ est divisible par } 6\}$
5. $\{\ldots ; -5; -3; -1; 0; 1; 3; 5; \ldots\}$

Théorème et définition

Soit $n \in \mathbb{N}^*$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble $\{(a)_n \mid a \in \mathbb{Z}\}$. Cet ensemble possède n éléments. On a (par exemple) $\mathbb{Z}/n\mathbb{Z} = \{(0)_n; (1)_n; (2)_n; \ldots ; (n-1)_n\}$.

Preuve

Exercice 21

L'égalité $(a)_n = (b)_n$ entraîne-t-elle $a = b$?

Exercice 22

Soit $n \in \mathbb{N}^*$, $a, a', b, b' \in \mathbb{Z}$. Supposons $a \equiv a' \mod n$ et $b \equiv b' \mod n$.

1. Montrer que $a + b \equiv a' + b' \mod n$.
2. Montrer que $ab \equiv a'b' \mod n$.

Théorème et définitions

Soit $n \in \mathbb{N}^*$. Pour tous $a, b \in \mathbb{Z}$ on peut définir :

$$(a)_n + (b)_n = (a + b)_n \quad \text{et} \quad (a)_n \cdot (b)_n = (ab)_n.$$

(On écrira aussi $(a)_n(b)_n$ au lieu de $(a)_n \cdot (b)_n$.)

L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de l'addition $(+)$ et de la multiplication $(\cdot)$ définies ci-dessus est un **anneau commutatif** à n éléments. L'élément neutre pour l'addition est $(0)_n$, l'élément neutre pour la multiplication est $(1)_n$ et $(-a)_n$ est l'opposé de $(a)_n$.

Cet anneau s'appelle l'**anneau des entiers modulo n**.

Preuve

Elle fait l'objet de l'exercice 27.

Exercice 23

On choisit $n = 2$. Pour alléger l'écriture, on notera $\overline{a}$ l'ensemble $(a)_2$. Établir les tables d'addition et de multiplication de $\mathbb{Z}/2\mathbb{Z}$. (Dans les tables, on utilisera seulement les symboles $\overline{0}$ et $\overline{1}$.)

Exercice 24

Répondre à la même question qu'à l'exercice précédent lorsque $n = 3, 4, 5, 6$.

Exercice 25

Définir la soustraction dans $\mathbb{Z}/n\mathbb{Z}$.

Exercice 26

On considère l'anneau $\mathbb{Z}/28\mathbb{Z}$. Effectuer les calculs suivants. On donnera les réponses sous la forme $(x)_{28}$ avec $0 \leqslant x \leqslant 27$.

1. $(12)_{28} + (25)_{28}$
2. $(14)_{28} - (17)_{28}$
3. $(3)_{28} \cdot (22)_{28}$
4. $(143)_{28} - (-12)_{28}$
5. $(2)_{28}^{6}$
6. $(5)_{28}^{432} \cdot (11)_{28}^{432}$

Exercice 27

Prouver le théorème précédent.

Définition

Un élément x de $\mathbb{Z}/n\mathbb{Z}$ est **inversible** s'il existe $y \in \mathbb{Z}/n\mathbb{Z}$ tel que $xy = (1)_n$. L'élément y s'appelle l'**inverse** de x et se note x^{-1}.

Exercice 28

Trouver les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ pour $n = 2, 3, 4, 5, 6, 7$.

Exercice 29

Soit $n \in \mathbb{N}^*$ et x, y deux éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. Montrer que xy est aussi inversible et déterminer $(xy)^{-1}$.

Définition

Deux entiers a et b sont premiers entre eux (on dit aussi que a est premier avec b ou que b est premier avec a) si $\mathrm{PGCD}(a; b) = 1$.

Théorème

Soit $n \in \mathbb{N}^*$. L'élément $(a)_n$ est inversible (dans $\mathbb{Z}/n\mathbb{Z}$) si et seulement si a est premier avec n. On dit que a est inversible modulo n si et seulement si a est premier avec n.

Preuve

Elle fait l'objet de l'exercice suivant.

Exercice 30

Prouver le théorème précédent.
Indication : utiliser le théorème de Bézout.

Corollaire

L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps (commutatif) si et seulement si n est un nombre premier.

Preuve

Elle fait l'objet de l'exercice 32.

Exercice 31

Les anneaux $\mathbb{Z}/55\mathbb{Z}$, $\mathbb{Z}/97\mathbb{Z}$ et $\mathbb{Z}/185697\mathbb{Z}$ sont-ils des corps ?

Exercice 32

Prouver le corollaire précédent.

Exercice 33

1. Soit n un nombre premier et $x, y \in \mathbb{Z}/n\mathbb{Z}$. On suppose que $xy = (0)_n$. Montrer que $x = (0)_n$ ou $y = (0)_n$.
2. Le résultat de la première partie de cet exercice est-il vrai pour les anneaux $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}/6\mathbb{Z}$?

Exercice 34

Soit a et b deux nombres premiers entre eux. Les affirmations suivantes sont-elles vraies ? Justifier.

1. Les nombres $a + b$ et $a - b$ sont premiers entre eux.
2. Les nombres $2a + b$ et $3a + 2b$ sont premiers entre eux.

Exercice 35

Pour quels entiers x le nombre $x^2 + 3x$ est-il divisible par 7 ?

Exercice 36

Résoudre les équations suivantes :

1. $4x + 5 = 0$ dans $\mathbb{R}$
2. $4x + 5 = 0$ dans $\mathbb{Z}/17\mathbb{Z}$
3. $4x + 5 = 0$ dans $\mathbb{Z}/8\mathbb{Z}$
4. $x(x + 3) = 0$ dans $\mathbb{Z}/13\mathbb{Z}$
5. $x(x + 3) = 0$ dans $\mathbb{Z}/10\mathbb{Z}$
6. $x^2 - 18x + 14 = 0$ dans $\mathbb{Z}/37\mathbb{Z}$
7. $x(x + 1) = 0$ dans $\mathbb{Z}/2\mathbb{Z}$
8. $x(x + 1) = 0$ dans $\mathbb{Z}/100\mathbb{Z}$

Exercice 37

Résoudre dans $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ le système suivant :

$$\begin{cases} 3x + 43y = 2 \\ -129x + 2y = 4 \end{cases}$$

Exercice 38

Trouver un nombre n tel que $\mathbb{Z}/n\mathbb{Z}$ possède 16 éléments inversibles.

Exercice 39

Munissons $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ de l'addition et de la multiplication suivantes :

$$\begin{aligned} (a; b) + (c; d) &= (a + c; b + d) \\ (a; b) \cdot (c; d) &= (ac + bd; ad + bc + bd) \end{aligned}$$

Montrer que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ muni de cette addition et de cette multiplication est un corps (commutatif) à quatre éléments.

4 Introduction à la cryptographie. Système RSA

4.1 Cryptographie à clé secrète

La cryptographie traditionnelle traite de la transmission confidentielle de données. C'est l'étude des méthodes permettant de transmettre des messages sous forme déguisée, de telle sorte que seuls les destinataires autorisés soient capables de les lire. Le message à envoyer est appelé message ou texte **en clair** et, sous sa forme déguisée, message **chiffré** (même s'il n'est pas représenté sous forme de chiffres), ou **cryptogramme**. Une **fonction cryptographique**, ou de **chiffrement**, est donc la donnée d'une transformation, en général bijective (une fonction est dite bijective si chaque élément de l'ensemble d'arrivée possède exactement une préimage),

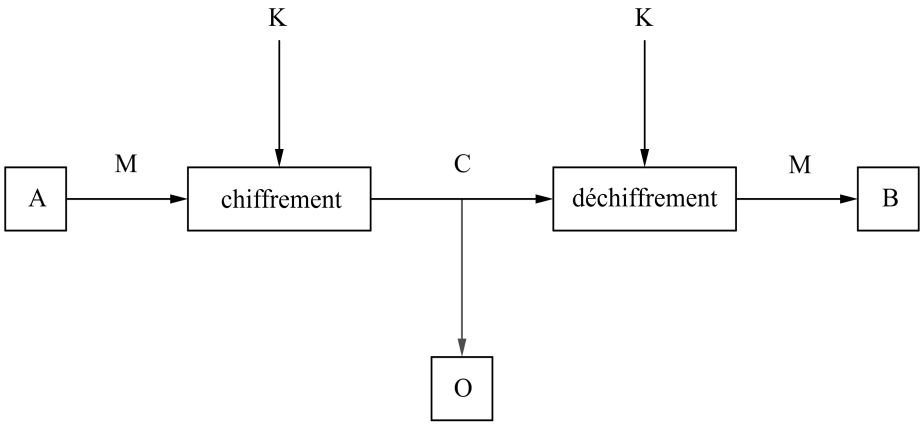
$$f : \mathcal{M} \longrightarrow \mathcal{C}$$

où $\mathcal{M}$ représente l'ensemble des messages en clair, et $\mathcal{C}$ l'ensemble des messages chiffrés. La transformation f^{-1} (fonction réciproque de la fonction bijective f) est la transformation de **déchiffrement**.

L'histoire a montré que chaque fois qu'une fonction cryptographique f est destinée à être utilisée un nombre important de fois, il devient de plus en plus difficile de la maintenir complètement secrète. Il est donc souhaitable de pouvoir changer régulièrement de fonction f. À cette fin, on définit un **système cryptographique**, ou de **chiffrement**, ou encore un **chiffre** (en anglais cipher) comme étant une famille finie

$$\mathcal{F} = (f_{\mathrm{K}})_{\mathrm{K}\in\mathcal{K}}$$

des fonctions cryptographiques, chacune étant déterminée par un paramètre K, appelé clé.



Modèle d'une communication confidentielle entre A et B
en présence de l'observateur O

La figure de la page précédente illustre le contexte type. Deux entités, expéditeur et destinataire que l'on appelle Alice et Bob, c'est la coutume, communiquent en présence d'un observateur ou **cryptanalyste** Oscar. Le but du cryptanalyste est de **décrypter** le cryptogramme transmis C, c'est-à-dire d'en déduire le message émis M. Idéalement, il souhaitera trouver la clé K et la transformation associée f_{K}.

Si le système cryptographique $\mathcal{F}$ est utilisé sur une grande échelle, il est déraisonnable de le considérer comme complètement secret. Pour cette raison, on supposera qu'Oscar connaît entièrement le système de chiffrement $\mathcal{F}$; il ne sait pas, par contre, laquelle des transformations f_K est utilisée. En d'autres termes, il lui manque juste la clé secrète K : c'est le principe de Kerckhoffs (1835-1903). Si le système est suffisamment bien conçu, le secret de la seule clé K suffit à assurer la confidentialité d'un message.

Voici maintenant, sous forme d'exercices, deux exemples historiques.

Exercice 40

Chiffrement par décalage, ou de Jules César

Le message chiffré se déduit du message en clair par un décalage circulaire des lettres de l'alphabet. On peut considérer que l'ensemble $\mathcal{M}$ des messages en clair ainsi que l'ensemble des messages chiffrés $\mathcal{C}$ est l'alphabet latin. L'ensemble des clés est $\mathcal{K} = \{0; 1; \ldots; 25\}$.

1. Si on utilise un décalage de 5 lettres de l'alphabet, déterminer le message chiffré du texte en clair :

   LES MATHÉMATIQUES SONT BELLES

2. Voici un message chiffré :

   SVUNALTWZ QL TL ZBPZ JVBJOL KL IVUUL OLBYL

   Trouver le message de Kerckhoffs est-il respecté ?

3. Que penser d'un tel système cryptographique ?

Suétone (69-122, ère chrétienne) rapporte que Jules César utilisait systématiquement la clé K = 3 dans sa correspondance avec ses proches.

Exercice 41

Chiffrement par substitution

L'ensemble des messages en clair et l'ensemble des messages chiffrés sont les mêmes que précédemment, mais on augmente l'ensemble des clés. Plutôt que de se restreindre aux décalages circulaires, on autorise toute permutation de l'alphabet : chaque bijection de $\{A; B; \ldots; Y; Z\}$ vers $\{A; B; \ldots; Y; Z\}$ est une clé.

1. Combien y a-t-il de clés ?
2. Considérons le texte en clair

   LE CIEL EST NUAGEUX

   et la clé définie par la bijection f de $\{1; 2; \ldots; 25; 26\}$ vers $\{1; 2; \ldots; 25; 26\}$ définie par $f(x) = 27 - x$. (Au nombre 1 correspond la lettre A, au nombre 2 correspond la lettre B,..., au nombre 26 correspond la lettre Z.)

   Déterminer le message chiffré.

Notons dès maintenant que dans ces systèmes la connaissance de la clé K est censée rendre facile le calcul, tant la fonction de chiffrement f que la fonction de déchiffrement f^{-1}. C'est une caractéristique des systèmes cryptographiques traditionnels ou à **clé secrète** : on parle encore de **chiffrement symétrique**. La situation sera très différente en cryptographie à clé publique (voir plus loin le système RSA).

Les systèmes ci-dessus sont bien peu résistants. Le chiffrement par décalage utilise un ensemble de clés trop petit : le cryptanalyste n'a qu'à essayer successivement toutes les clés possibles pour retrouver le message en clair à partir du message chiffré. Le chiffrement par substitution d'un texte écrit dans une langue naturelle ne résiste pas à une analyse des fréquences. Par exemple, en français la lettre la plus fréquente est « E » : le cryptanalyste qui sait qu'il a affaire à un texte français sait donc que le symbole le plus fréquent du texte chiffré représente « E ».

Retenons que pour rendre la tâche du cryptanalyste difficile, il est important de concevoir des systèmes tels que le texte chiffré ait un aspect aléatoire, même si le message en clair correspondant ne l'est pas. Comme cette remarque nécessite des idées précises sur la signification du terme « aléatoire », on a dû attendre le XX$^{\text{e}}$ siècle pour sa mise en application.

L'exercice suivant, qui utilise l'anneau des entiers modulo n, nous donne un système cryptographique beaucoup plus efficace que les deux précédents.

Exercice 42

Le système de Vernam ou « one-time pad »

Le système de Vernam (1926) fonctionne de la manière suivante. Les messages, tant en clair que chiffrés, s'écrivent sur un même alphabet Σ que l'on représentera par $\mathbb{Z}/m\mathbb{Z}$ où m est le nombre d'éléments de Σ. Un message de n symboles $M = (x_1; \ldots; x_n)$ se chiffre par la transformation f_{K} :

$$\begin{array}{rccc} f_{\text{K}} & : & \mathcal{M} = (\mathbb{Z}/m\mathbb{Z})^n & \longrightarrow & \mathcal{C} = (\mathbb{Z}/m\mathbb{Z})^n \\ & & (x_1; \ldots; x_n) & \longmapsto & (y_1; \ldots; y_n) \end{array}$$

où

$$y_i = x_i + k_i.$$

Le n-uple $\text{K} = (k_1; \ldots; k_n)$ constitue la clé de transformation et est choisi aléatoirement dans $(\mathbb{Z}/mZ)^n$.

Choisissons $m = 10$, $\text{M} = (3; 5; 1; 4; 7)$ (on a écrit 3 au lieu de $(3)_{10}$, 5 au lieu de $(5)_{10}$, etc.) et $\text{K} = (3; 8; 4; 0; 9)$.

Déterminer le message chiffré.

Dire que la clé est choisie aléatoirement, cela signifie en particulier que si un nouveau message est envoyé, un nouveau n-uple K est utilisé comme clé, et que pour chaque message, émetteur et récepteur partagent autant de symboles de clé que de symboles qu'ils souhaitent se transmettre : un n-uple clé K n'est jamais sciemment réutilisé, d'où l'appellation « one-time ».

Le système de Vernam peut être considéré comme l'aboutissement de la cryptographie traditionnelle. En effet, Shannon, dans une première approche véritablement scientifique

de la cryptographie (1949), montre que le « one-time pad » garantit une confidentialité « parfaite »(perfect secrecy) en un sens qu'il définit en termes de sa toute nouvelle théorie de l'information.

Si les quantités d'information à échanger sont importantes, le « one-time pad » devient très lourd à mettre en œuvre puisqu'il faut engendrer des clés aléatoires très longues et les mettre simultanément à disposition de l'émetteur et du destinataire. Il reste parfois utilisé, cependant, si l'exigence de confidentialité est très importante. Par exemple, la ligne téléphonique directe Kremlin-Maison Blanche a longtemps été protégée par un « one-time pad ».

4.2 Cryptographie moderne et système RSA

4.2.1 L'idée de fonction à sens unique

La notion de fonction dite « à sens unique » ou « difficilement inversible » (one-way function), appartient par nature à l'ère informatique. Lorsqu'on prit conscience, à partir du milieu des années 1970, de tout son potentiel cryptographique, ce fut une révolution. Le concept est informellement le suivant : une fonction f

$$\begin{aligned} \mathcal{E} &\longrightarrow \mathcal{F} \\ x &\longmapsto f(x) \end{aligned}$$

est dite à sens unique si :

1. Il est possible de calculer simplement $f(x)$ à partir de n'importe quel x.
2. Pour la plupart des $y \in f(\mathcal{E})$, il n'est pas possible de trouver un x tel que $f(x) = y$, à moins d'exécuter un nombre prohibitif d'opérations, ou d'avoir une chance sur laquelle il est déraisonnable de compter.

4.2.2 L'idée de clé publique

L'idée est de rompre la symétrie du chiffrement et du déchiffrement. Dans un système traditionnel, la connaissance de la fonction de chiffrement f implique la connaissance de la fonction de déchiffrement f^{-1}. Si l'on peut donner au destinataire un algorithme secret qui calcule f^{-1}, alors il n'y a plus besoin de garder secrète la fonction de chiffrement f. On a alors réalisé un système dit « à clé publique » ou « asymétrique » : seul le destinataire possède le secret permettant de déchiffrer. C'est le gros avantage d'une telle stratégie : plus besoin de se préoccuper d'un partage secret, toujours délicat.

Le premier système à clé publique solide à avoir été inventé, et le plus utilisé actuellement, est le système RSA (Rivest, Shamir, Adleman) créé en 1977 ! Mais avant de le définir, il nous faut encore quelques résultats mathématiques.

Définition

Soit $n \in \mathbb{N}^*$. La **fonction indicatrice d'Euler**, notée φ « phi » est définie par :

$$\varphi(n) \text{ est le nombre d'éléments de l'ensemble}$$
$$\{m \in \mathbb{N} \mid 1 \leqslant m \leqslant n, \text{ PGCD}(m; n) = 1\}.$$

Exercice 43

Calculer $\varphi(n)$ pour $n = 1, 2, 3, 4, 5, 6, 7, 10, 13, 16, 19$.

Notation

Soit $n \in \mathbb{N}^*$. On note $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Exercice 44

Soit $n \in \mathbb{N} \setminus \{0; 1\}$. Montrer que les deux affirmations suivantes sont équivalentes :

i) $(\mathbb{Z}/n\mathbb{Z})^* = \mathbb{Z}/n\mathbb{Z} \setminus \{(0)_n\}$

ii) L'entier n est premier.

Exercice 45

Déterminer $(\mathbb{Z}/n\mathbb{Z})^*$ pour $n = 2, 5, 6, 7, 16$.

Reformulons le théorème de la page 15 :

Théorème

Soit $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. On a

$$(a)_n \in (\mathbb{Z}/n\mathbb{Z})^* \iff \text{PGCD}(a; n) = 1.$$

Corollaire

Le nombre d'éléments de $(\mathbb{Z}/n\mathbb{Z})^*$ est égal à $\varphi(n)$.

Preuve

C'est immédiat.

Exercice 46

Soit p un nombre premier. Montrer que $\varphi(p) = p - 1$.

Exercice 47

Soit p et q deux nombres premiers distincts. Montrer que $\varphi(pq) = \varphi(p)\varphi(q)$.

Exercice 48

Calculer $\varphi(73)$ et $\varphi(407)$.

Voici maintenant l'énoncé du **théorème de Fermat-Euler**, dernière pièce du puzzle qui va nous permettre de justifier le système RSA.

Théorème

Soit $n \in \mathbb{N}^*$. Si a est un nombre premier avec n, c'est-à-dire si $\text{PGCD}(a; n) = 1$, alors

$$a^{\varphi(n)} \equiv 1 \mod n.$$

La preuve de ce théorème sera établie plus loin.

Exercice 49

Soit $n = 6$ et $a = 5$.

1. Vérifier que a et n sont premiers entre eux.
2. Vérifier le théorème précédent dans ce cas particulier.

Exercice 50

Répondre aux mêmes questions qu'à l'exercice précédent lorsque $n = 51$ et $a = 8$.

Exercice 51

Prouver le **lemme d'Euclide** :

Soit b et c deux entiers. Si un nombre premier p divise le produit bc, alors p divise b ou c.
Indication : utiliser le théorème de Bézout.

Exercice 52

Prouver le **petit théorème de Fermat** :

Si p est premier et si a est premier avec p, alors $a^{p-1} \equiv 1 \mod p$.

Exercice 53

Reformulation du théorème de Fermat-Euler.
Soit $n \in \mathbb{N}^*$. Montrer que

$$(a)_n \in (\mathbb{Z}/n\mathbb{Z})^* \implies (a)_n^{\varphi(n)} = (1)_n.$$

Preuve (du théorème de Fermat-Euler)

4.2.3 Système RSA

Ce système inventé en 1977 par **Rivest**, **Shamir** et **Adleman** est fondé sur la difficulté de factoriser des grands nombres (même avec un ordinateur bien sûr !), et la fonction à sens unique utilisée est une fonction « puissance ». En voici le principe.

La **clé secrète** est constituée de deux « grands » nombres premiers distincts p et q.

La **clé publique** est constituée du produit $n = pq$, ainsi que d'un entier e inversible modulo $\varphi(n)$. (Autrement dit, e et $\varphi(n)$ sont premiers entre eux.)

Le chiffrement d'un message, représenté par un élément $M \in \mathbb{Z}/n\mathbb{Z}$, se fait par la « simple » transformation :

$$M \longmapsto M^e.$$

Pour déchiffrer, il faut savoir calculer la fonction réciproque. Il se trouve que celle-ci est simplement :

$$M \longmapsto M^d,$$

où d est l'inverse de e modulo $\varphi(n)$.

L'expéditeur ne connaît que la clé publique, c'est-à-dire les nombres e et n. Seul le destinataire connaît la **clé privée** d.

Reformulons ces dernières lignes à l'aide d'un théorème :

Théorème

Soit p et q deux premiers distincts, $n = pq$ et e un entier inversible modulo $\varphi(n)$. (Autrement dit, $(e)_{\varphi(n)} \in (\mathbb{Z}/\varphi(n)\mathbb{Z})^*$.)

Soit les fonctions

$$\begin{aligned} \mathrm{E} : \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ M &\longmapsto M^e \end{aligned}$$

et

$$\begin{aligned} \mathrm{D} : \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ M &\longmapsto M^d \end{aligned}$$

où d est l'inverse de e modulo $\varphi(n)$. (Autrement dit, $(e)_{\varphi(n)} \cdot (d)_{\varphi(n)} = (1)_{\varphi(n)}$.)

On a

$$(\mathrm{D} \circ \mathrm{E})(M) = M \text{ pour tout } M \in \mathbb{Z}/n\mathbb{Z}.$$

Preuve

Soit $M = (m)_n \in \mathbb{Z}/n\mathbb{Z}$.
D'abord on a $(\mathrm{D} \circ \mathrm{E})(M) = \mathrm{D}(\mathrm{E}(M)) = \mathrm{D}(M^e) = (M^e)^d = M^{ed}$.

Il s'agit donc de prouver que $M^{ed} = M$. On peut bien sûr supposer $d > 0$ et $e > 0$.

I. Supposons $M \in (\mathbb{Z}/n\mathbb{Z})^*$.

Avec cette hypothèse, vu le théorème de Fermat-Euler, on a $m^{\varphi(n)} \equiv 1 \mod n$. Or $ed = 1 + k\varphi(n)$ pour un $k \in \mathbb{N}$. D'où :

$$m^{ed} = m^{1+k\varphi(n)} = m\left(m^{\varphi(n)}\right)^k \equiv m \mod n.$$

II. Supposons $M \notin (\mathbb{Z}/n\mathbb{Z})^*$.

Si $m \equiv 0 \mod p$ et $m \equiv 0 \mod q$, alors $m \equiv 0 \mod n$ et le résultat est immédiat.

Supposons alors $m \equiv 0 \mod p$ et m non congru à 0 modulo q. (Le cas $m \equiv 0 \mod q$ et m non congru à 0 modulo p est analogue : il suffit d'échanger les rôles de p et q.)

En utilisant l'égalité $\varphi(n) = \varphi(p)\varphi(q)$ on obtient :

$$m^{\varphi(n)} = m\left(m^{\varphi(q)}\right)^{\varphi(p)} \equiv 1 \mod q.$$

Alors on a pour un $k \in \mathbb{N}$:

$$m^{ed} = m^{1+k\varphi(n)} = m\left(m^{\varphi(q)}\right)^{k\varphi(p)} \equiv m \mod q.$$

On a donc $m^{ed} \equiv m \mod q$ et $m^{ed} \equiv 0 \mod p$ car par hypothèse $m \equiv 0 \mod p$.

Autrement dit, il existe trois entiers α, β, γ tels que

$$\begin{aligned} m^{ed} &= m + \alpha q \\ m^{ed} &= \beta p \\ m &= \gamma p \end{aligned}$$

D'où

$$\beta p = \gamma p + \alpha q \text{ ou encore } p(\beta - \gamma) = \alpha q.$$

Si $\beta = \gamma$ alors $\alpha = 0$, $m^{ed} = m$ et par suite $M^{ed} = M$.

Si $\beta \neq \gamma$ alors $p \mid \alpha$ (voir l'exercice 51), autrement dit $\alpha = \delta p$ pour un entier δ.

On a alors

$$m^{ed} = m + \delta pq \text{ ou encore } m^{ed} \equiv m \mod pq,$$

ce qui prouve que $M^{ed} = M$. □

Dans les exercices qui suivent, les nombres premiers p et q choisis ne sont pas grands afin de faciliter les calculs.

Exercice 54

Soit $p = 2$, $q = 5$ et $n = pq$.

1. Vérifier que p et q sont des premiers distincts.
2. Calculer $\varphi(n)$.
3. Prouver que $(3)_{\varphi(n)} \in (\mathbb{Z}/\varphi(n)\mathbb{Z})^*$.
4. Quel est l'inverse de 3 modulo $\varphi(n)$?
5. On considère le message $M = (8)_n$. En utilisant le système RSA (et la clé publique 3), chiffrer le message M, puis déchiffrer le message trouvé. Quel message doit-on obtenir ?
6. Bernard a obtenu le message chiffré $(7)_n$. Quel était le message en clair ?

Exercice 55

Si n est un nombre naturel, la $n^{\text{ème}}$ puissance d'un nombre a est, par définition, le produit de n facteurs égaux à a. Ainsi, d'après cette définition, le calcul de a^n nécessite $n-1$ multiplications. On peut cependant obtenir le même résultat en effectuant moins d'opérations. Voici, à titre d'exemple, l'évaluation de a^{35} :

- On écrit l'exposant n comme somme de puissances de 2. Ici, $35 = 32 + 2 + 1$;
- on calcule ensuite les puissances paires de a : $a^2 = a \cdot a$, $a^4 = a^2 \cdot a^2$, $a^8 = a^4 \cdot a^4$, $a^{16} = a^8 \cdot a^8$, $a^{32} = a^{16} \cdot a^{16}$;
- on multiplie pour terminer les « bons » carrés : $a^{35} = a^{32} \cdot a^2 \cdot a^1$. Le nombre de multiplications nécessaires dans ce cas est 7, au lieu de 34.

1. Combien de multiplications nécessite cet algorithme pour calculer chacune des puissances suivantes : a^{10}, a^{61}, a^{1000} ?
2. Calculer $835^{25} \mod 1073$.
3. Calculer le reste de la division de la division de 54^{171} par 11.
4. Trouver $x \in \{0; \ldots; 86\}$ tel que $(31)_{87}^{111} = (x)_{87}$.

Exercice 56

1. À l'aide de l'algorithme d'Euclide, calculer le plus grand diviseur commun des nombres 15612 et 125. Puis écrire une égalité de Bézout.
2. En déduire l'inverse de $(125)_{15612}$ dans $\mathbb{Z}/15612\mathbb{Z}$.

Exercice 57

Calculer l'inverse de $(39)_{10000}$ dans $\mathbb{Z}/10000\mathbb{Z}$.

Exercice 58

Trouver, si possible, deux entiers u et v vérifiant :

1. $121u - 25v = 5$
2. $377u + 3159v = 1$

Exercice 59

Soit $p = 11$, $q = 17$ et $n = pq$.

1. Vérifier que p et q sont des premiers distincts.
2. En écrivant une égalité de Bézout, montrer que $(21)_{\varphi(n)} \in (\mathbb{Z}/\varphi(n)\mathbb{Z})^*$ et calculer l'inverse de 21 modulo $\varphi(n)$.
3. Chiffrer le message $M = (123)_n$ à l'aide de la clé publique 21.
4. Bob a obtenu le message chiffré $(100)_n$. Quel était le message en clair ?

Exercice 60

En utilisant le système RSA, Fernand dit « le parrain de Namur » doit envoyer le message TUE JO à Raoul dit « la gâchette facile », sans que personne ne le sache. Pour ce faire, Raoul construit sa clé publique en choisissant : $p = 37$, $q = 43$ et $e = 5$.

1. Vérifier que la clé e est licite pour que Fernand puisse coder son message à l'aide du système RSA.
2. Par un calcul, Raoul choisit 605 pour sa clé privée. Montrer que ce choix est correct.

   Alors Raoul envoie les deux nombres pq et 5 à Fernand pour que ce dernier puisse lui envoyer le message de manière confidentielle. D'abord Fernand convertit le message en nombres, en associant à chaque lettre sa position dans l'alphabet. Ainsi,

   $$\text{T} = 20,\ \text{U} = 21,\ \text{E} = 05,\ \text{J} = 10 \text{ et } \text{O} = 15.$$

   Il obtient un message M qu'il sépare en blocs de 3 chiffres ; il obtient alors

   $$002\ 021\ 051\ 015.$$

   Ensuite, Fernand utilise la clé publique e pour chaque bloc.
3. Quel message codé Fernand obtient-il ?

   Fernand peut maintenant envoyer son message à Raoul par courrier électronique.
4. Vérifier que le message que Raoul décodera à l'aide de sa clé privée est bien TUE JO.
5. Quel est l'intérêt de découper un message en blocs de 3 chiffres plutôt qu'en blocs de 2 chiffres ?

Exercice 61

Échanger avec un camarade un message chiffré à l'aide du système RSA.

Exercice 62

Soit n un entier produit de deux premiers distincts et supposons que l'on connaisse la valeur de $\varphi(n)$.

1. Expliquer comment on peut alors calculer l'exposant d (en supposant que l'on connaisse n (voir le système RSA)).
2. Montrer que la connaissance de $\varphi(n)$ entraîne celle des deux nombres premiers et donc la factorisation de n.

Remarques

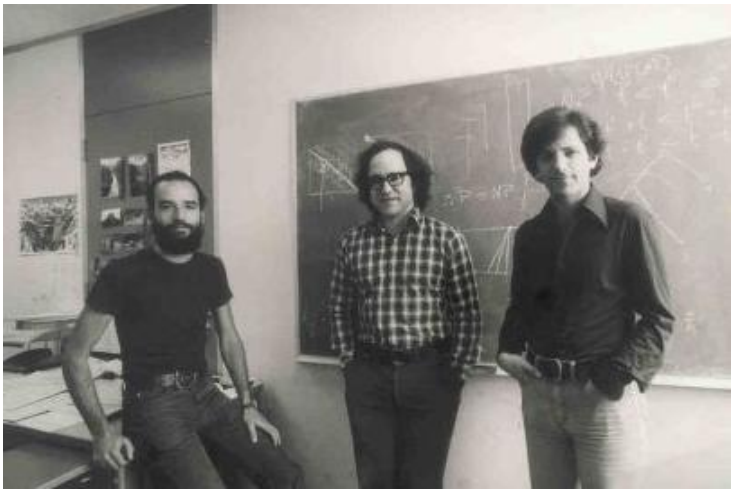
1. Comme on ne sait pas factoriser efficacement les grands entiers, le cryptanalyste ne sait pas accéder à $\varphi(n)$ et à l'exposant caché d. (Voir l'exercice précédent.)
2. On peut se demander si le cryptanalyste ne pourrait pas obtenir l'exposant secret d par un moyen détourné, sans passer par $\varphi(n)$. Il n'en n'est rien : on peut montrer que si le cryptanalyste sait trouver un entier congru à d modulo $\varphi(n)$, alors il sait aussi factoriser n.
3. L'exposant d donne un algorithme pour calculer la fonction de déchiffrement. Mais peut-être il y en a d'autres ? Bien que cela paraisse très improbable, on ne sait pas prouver formellement que savoir inverser la fonction $M \mapsto M^e$ (voir le système RSA) implique la connaissance de la factorisation de n.

Terminons ce chapitre par quelques considérations pratiques :

Pour passer à une réalisation pratique du système, quelques questions restent en suspens. Euclide a démontré qu'il existe une infinité de nombres premiers (ouf ! pour le système cryptographique RSA), mais comment choisit-on concrètement de grands premiers p et q ? De quelle taille faut-il les prendre ? Pour quelles garanties de sécurité ?

La meilleure méthode pour disposer de deux premiers p et q consiste à les prendre au hasard. Pour cela, on prend des entiers aléatoires et on teste leur primalité. Les manières de faire sont nombreuses. Disons simplement que les mathématiques utilisées sont variées et complexes, et qu'un ordinateur « bêtement » programmé ne suffit pas.

Depuis près de 30 ans, le système RSA a résisté à toutes les attaques des cryptanalystes du monde. C'est ainsi que le système RSA est l'algorithme de choix pour chiffrer les transactions par cartes de crédit sur Internet, pour assurer la sécurité du courrier électronique ou pour authentifier les appels téléphoniques.



Ronald **R**ivest Adi **S**hamir et Leonard **A**dleman

Bibliographie

Gilles Zémor, *Cours de cryptographie*, Cassini, Paris 2000