D.M : cryptographie

La cryptographie est une science ayant pour objet la protection de messages afin qu'ils ne soient compréhensibles que par l'émetteur et le récepteur. C'est l'un des principaux domaines d'application des mathématiques et l'arithmétique joue un rôle clé. Nous allons voir quelques exemples de chiffrement, c'est-à-dire de transformation d'un message en code secret.

Afin de coder un message on assimile chaque lettre de l'alphabet à un nombre entier comme l'indique le tableau ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Le chiffrement ou cryptage consiste à coder un message. Le déchiffrement consiste à décoder un message codé.

I Chiffrement affine

Le principe :

On se donne une fonction de codage affine f, par exemple : $f(x) = 11x + 8$.
À une lettre du message :

- on lui associe un entier x entre 0 et 25 suivant le tableau ci-dessus
- on calcule $f(x) = 11x + 8$ modulo 26 compris entre 0 et 25 qu'on notera y
- On traduit y par une lettre d'après le tableau ci-dessus

Par exemple, si l'on veut coder la lettre L par la fonction $f(x) = 11x + 8$, on procède de la façon suivante :

- L correspond à $x = 11$. Par suite, $f(11) = 129$
- Or $129 \equiv 25$ [26] et 25 correspond à la lettre Z.
- La lettre L est donc codée par la lettre Z.

Exercice 1

La fonction de codage est définie par la fonction f, définie par : $f(x) = 11x + 8$.

1. Coder la lettre Z.
2. Le but de cette question est de déterminer la fonction de décodage.
   (a) Montrer que pour tous nombres entiers relatifs x et n, on a :

$$11x \equiv n \text{ [26] équivaut à } x \equiv 19n \text{ [26]}$$

   (b) En déduire que la fonction g de décodage est $g(y) = 19y + 4$.
   (c) Décoder la lettre F.

Exercice 2

On a reçu le message suivant : JWPNWMRCFWMY On sait que le chiffrement est affine et que la lettre E est codée par la lettre E et que la lettre J est codée par la lettre N.

Soit la fonction affine f définie par : $f_{a,b}(x) = ax + b$, où a et b sont des entiers naturels compris entre 0 et 25.

1. Démontrer que a et b vérifient le système suivant : $\begin{cases} 4a+b &\equiv 4\ [26] \\ 9a+b &\equiv 13\ [26] \end{cases}$

2.(a) Démontrer que $5a \equiv 9\ [26]$, puis que $a \equiv 7\ [26]$.

(b) En déduire que $b \equiv 2\ [26]$ et que $f_{a,b}$ est définie par $f_{7,2}(x) = 7x+2$.

(c) Démontrer que pour tous relatifs x et z, on a :

$$7x \equiv z\ [26] \text{ équivaut à } x \equiv 15z\ [26]$$

(d) En déduire que la fonction de décodage g est $g_{15,22}(y) = 15y+22$.

(e) Décoder le message.

Exercice 3

1. Déterminer modulo 26 l'opposé d'un nombre compris entre 0 et 25 qui est aussi compris entre 0 et 25.
2. Déterminer tous les entiers compris entre 0 et 25 qui sont sont inversibles modulo 26.
3. Montrer que deux fonctions de chiffrement affine sont distinctes si et seulement si les clés associées sont distinctes. En déduire le nombre total de fonctions de chiffrement possibles
4. Soit a un entier compris entre 0 et 25 inversible modulo 26 et b un entier compris entre 0 et 25.

(a) Déterminer la fonction de déchiffrement associée à $f_{a,b}$.

(b) Déterminer en particulier la fonction de déchiffrement associée à $f_{5,2}$.

II Chiffrement RSA

On se propose d'étudier un système de chiffrement à clé publique.

L'idée est que chaque utilisateur possède deux clés, l'une publique et l'autre privée.

Pour envoyer un message, on le code avec la clé publique, que n'importe qui peut connaître, mais que seul le récepteur peut déchiffrer avec sa clé privée. L'avantage est que la clé privée ne circule jamais par les moyens de communication.

L'un de ces procédés est le système RSA du nom de trois mathématiciens, Rivest, Shamir, Adleman, qui l'ont mis au point en 1978.

Mais son usage ne s'est généralisé qu'à la fin des années 1990 avec l'arrivée d'internet.

En effet, ce procédé nécessite l'utilisation de très grands nombres premiers comme on va le voir.

1. **Propriété fondamentale** $n = pq$ est le produit de deux nombres premiers p et q distincts.

   n pose $m = (p-1)(q-1)$ et on note c un nombre premier avec m.

   On note x un nombre entier naturel.

(a) Démontrer qu'il existe des nombres entiers d et k tels que $cd = km+1$ (c'est-à-dire $cd \equiv 1\ [m]$).

(b)
- **Cas où x est non divisible par p**

  Démontrer que $x^{p-1} \equiv 1\ [p]$.

  En déduire que $x^{km} \equiv 1\ [p]$, puis que $x^{cd} \equiv x\ [p]$.
- **Cas où x est divisible par p**

  Démontrer que $x^{cd} \equiv x\ [p]$.

(c) Démontrer de façon analogue que pour tout nombre entier x, $x^{cd} \equiv x\ [q]$.

(d) En déduire que pour tout nombre entier naturel x, $x^{cd} \equiv x\ [n]$.

Le principe :

- Pour chiffrer un message(cartes bancaires, Internet, ...), on choisit deux nombres premiers p et q très grands et on calcule $n = pq$.
  On pose $m = (p-1)(q-1)$.
  On cherche deux nombres entiers naturels c et d tels que $cd \equiv 1\ [m]$.
- Les messages x seront des nombres entiers appartenant à $\{0; 1; \ldots; n-1\}$.
  Le codage de ce message consiste à calculer $C(x) \equiv x^c\ [n]$.
  Le décodage consiste à calculer $D(y) \equiv x^c\ |n]$.
  On a bien $D(C(x)) \equiv x^{cd} \equiv x\ [n]$.
- Pour chiffrer un message, on a besoin de connaître c et n.
  Le couple $(n; c)$ est appelé **la clé publique** car elle est connue de tous et répertoriée dans un annuaire.
  Pour déchiffrer, il faut connaître d et n.
  d est appelé **la clé privée** car elle n'est connue que par la personne qui reçoit le message codé.

2. **Application**

Alexandre veut choisir une clé publique $(n; c)$ et sa clé privée d.

Il prend $p = 5$, $q = 11$ et donc $n = 55$ (p et q sont choisis petits, contrairement à la réalité, pour la simplicité des calculs).

(a) Démontrer qu'il peut choisir $c = 9$ et $d = 9$.

(b) Les lettres de l'alphabet sont chiffrées par des entiers de 0 à 26.

Paul qui connaît la clé publique d'Alexandre, crypte le message : « VIVE LES MATHS » et lui envoie.

Quel message crypté Alexandre reçoit ? Comment le décode-t-il ?

Remarques :

- Les nombres premiers p et q doivent demeurer cachés car leur connaissance entraîne celle de $m = (p-1)(q-1)$, puis celle de d en résolvant l'équation de Bézout $cd - km = 1$ (ce qui est possible car c est dans l'annuaire).
- Le système RSA 1024 bits correspond à un nombre $n = pq$ de l'ordre de $2^{1024} \approx 10^{308}$ s'écrivant avec 309 chiffres décimaux.
- Dans la pratique, les messages ne sont pas codés lettre par lettre mais par bloc de lettres. Un bloc de 2 lettres donnant un bloc numérique de 4 chiffres.

BONUS : Théorème des restes chinois

III Le théorème chinois

Soient m et n deux entiers naturels premiers entre eux.

Démonter que si a et b sont des entiers alors le système

$$\begin{cases} x & \equiv & a\ [m] \\ x & \equiv & b\ [n] \end{cases}$$

admet une unique solution modulo mn.

IV Application

Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les partager également, et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent,et six d'entre eux sont tués.Un nouveau partage donnerait au cuisinier 4 pièces. Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ?