Le chiffrement affine

I. Principe général

À chaque lettre de l'alphabet, on fait correspondre son rang entre 0 et 25 au sens large (et pas de 1 à 26).

Tableau de correspondance :

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

On choisit deux entiers a et b compris entre 0 et 25 (avec $a \neq 0$).

On dit que le couple (a ; b) est la clé de cryptage affine (on retiendra que le codage affine fonctionne avec une clé constituée de deux nombres).

On calcule le reste y de la division euclidienne de $ax+b$ par 26.

On note la lettre de l'alphabet correspondant à y.

$$x \xrightarrow{\text{codage}} y \equiv ax+b \ [26] \ *$$
$$y \xrightarrow{\text{décodage}} x$$

* Cette écriture est employée abusivement pour dire que y est le reste de la division euclidienne de $ax+b$ par 26.

La clé doit être tenue secrète : seul l'émetteur et le récepteur la connaissent.

Point info :

Pendant la guerre des Gaules, Jules César utilisait un tel procédé ($y \equiv x+3$ [26]) pour envoyer des messages chiffrés à Cicéron au Sénat.
Le procédé employé par Jules César constituait en un décalage de trois lettres : il était à la fois simple à coder et à décoder.

II. Étude d'un exemple

On prend la clé $(a\,;b)=(17\,;16)$.

1°) Codons le mot ALICE.

Le codage est symbolisé par : $y \equiv 17x+16$ [26].

A = 0 $\quad 17\times 0+16=16 \rightarrow$ Q

L = 11 $\quad 17\times 11+16=203$ et $203\equiv 21$ [26] $\rightarrow$ V

I = 8 $\quad 8\times 17+16=152$ et $152\equiv 22$ [26] $\rightarrow$ W

C = 2 $\quad 2\times 17+16=50$ et $50\equiv 24$ [26] $\rightarrow$ Y

E = 4 $\quad 4\times 17+16=84$ et $84\equiv 6$ [26] $\rightarrow$ G

ALICE donne en codage QVWYG.

On pourrait constituer une table de cryptage pour lire rapidement plutôt que de calculer ou bien utiliser un tableur.
On peut aussi utiliser un programme qui code directement la phrase qu'on lui donne.

2°) Décodons le mot YTILBQOG.

Pour envoyer des messages à Cicéron qui était resté en poste de Sénat à Rome.

Avec un tel système de cryptage, la clé (a ; b) doit être tenu secrète par l'émetteur et le récepteur.

Une première piste

codage : $y=17x+16$

décodage : $x=\dfrac{y-16}{17}$ (cette relation donne la bijection réciproque de la fonction $x \mapsto 17x + 16$)

En modulo, on ne peut pas avoir de fraction.

Cette piste n'aboutit donc pas.

Une autre piste

Il faut chercher un « inverse » en nombre 17 modulo 26 c'est-à-dire un entier naturel a (compris entre 0 et 25) au sens large tel que $a\times 17\equiv 1$ [26].
On essaie tous les entiers naturels à partir de 0 et l'on trouve que l'entier 23 convient c'est-à-dire qu'il vérifie

$23\times 17\equiv 1$ [26].

Nous verrons qu'il y a un moyen beaucoup plus rapide utilisant l'égalité de Bezout.

Fin de la recherche

Nous allons partir de $y \equiv 17x+16$ [26].
En multipliant les deux membres de cette congruence par 23, on obtient :

$23y \equiv 17x \times 23+16 \times 23$ [26]

Or $23 \times 17 \equiv 1$ [26] et $23 \times 16 \equiv 4$ [26].

Donc on obtient : $23y \equiv x+4$ [26] et par suite, $23y \equiv x+4$ [26] d'où $x \equiv 23y-4$ [26].

Cette relation nous définit la « fonction de décodage » : $x \mapsto 23x-4$ [26].

Il s'agit d'un chiffrement affine de clé $(c\,;d)=(23\,;-4)$.

III. Utilisation d'outils informatiques : automatisation des calculs

1°) Tableur

On peut passer sur tableur pour effectuer codage et décodage d'un message.

Point info

Dans un tableur Excel, on obtient le code ASCII d'un caractère en tapant : $=\text{CODE}(\ldots)-65$.

Pour retrouver la lettre à partir du rang, on tape : $=\text{CAR}(\ldots\ +\ 65)$.

Voir fichier Excel correspondant.

2°) On peut aussi utiliser un programme.

Voir fichier en langage C.

IV. Problème de la clé de codage

Il n'y a pas de $26 \times 26 = 26^2$ clés de codage possible.
Il y en a moins.

On essaie la clef (14 ; 3).

On rentre l'alphabet ABCDEFGHIKLMNOPQRSTUVWXYZ.
On voit que deux lettres différentes sont codées par la même lettre et qu'il y a une boucle.

On peut essayer plusieurs clefs similaires.

Comment faut-il choisir la clé de codage pour obtenir un bon chiffrement affine ?

V. Choix de la clé pour le codage

Nous allons étudier le problème suivant : toutes les clés conviennent-elles ?

La réponse est non, ainsi que nous allons le voir…

On considère le cryptage affine défini par $y \equiv ax+b$ [26] avec x et y compris entre 0 et 25 au sens large et a et b des entiers donnés.

On se propose de démontrer que « Deux lettres distinctes sont cryptées par deux lettres distinctes si et seulement si $\text{PGCD}(a\,;26)=1$ ».

Démonstration :

1er cas : a est premier avec 26 c'est-à-dire $\text{PGCD}(a\,;26)=1$

Supposons que x et x' soient deux entiers compris entre 0 et 25 au sens large tels que
$a \times x+b \equiv a \times x'+b$ [26] (1).

$ax+b$ correspond au codage de la lettre associé à x ;
$ax'+b$ correspond au codage de la lettre associée à x'.

Démontrons qu'alors $x=x'$.

(1) $\Leftrightarrow$ $a \times x \equiv a \times x'$ [26]

$\Leftrightarrow$ $a \times (x-x') \equiv 0$ [26]

$\Leftrightarrow 26 \mid a(x-x')$

$\Leftrightarrow 26 \mid x-x'$ (théorème de Gauss car a et 26 sont premiers entre eux*)

$\Leftrightarrow x-x'=0$ car $x-x'$ est compris entre – 25 et + 25 sens large et le seul multiple de 26 dans [– 25 ; + 25] est 0

*On pourrait croire qu'il y a une rupture de chaîne équivalence ; on pourra vérifier aisément qu'il n'en est rien.

On a démontré que $a \times x+b \equiv a \times x'+b$ [26] $\Leftrightarrow$ $x=x'$.

Par contraposée, on a démontré que $a \times x+b \not\equiv a \times x'+b$ [26] $\Leftrightarrow$ $x \neq x'$.

2e cas : a n'est pas premier avec 26 c'est-à-dire $\text{PGCD}(a\,;26) \neq 1$

Posons $d=\text{PGCD}(a\,;26)$.
Nous savons que $d>0$.
On note k l'entier naturel tel que $k \times d = 26$.
Démontrons que les lettres correspondant à 0 et k sont codées par la même lettre.
c'est-à-dire que $a \times 0+b \equiv a \times k+b$ [26].

On sait que $d \mid a$.
Donc $kd \mid ak$.
Or $kd = 26$ d'où $26 \mid ak$.
Donc $0 \equiv ak$ [26].

D'où $a\times 0+b\equiv a\times k+b$ [26].
Cette congruence permet de dire que la lettre « A » associé à 0 est codée par la même lettre que la lettre associée à *k*. Ce qui nous montre que, dans ce cas, le codage n'est pas bon.

Pour aller plus loin : les applications injectives

Définition :

Soit *f* une application d'un ensemble *E* dans un ensemble *F*.
On dit que *f* est **injective** pour exprimer que pour tout couple $(x\,;x')$ d'éléments de *E*, on a :

$f(x)=f(x')\Rightarrow x=x'$

ce qui est équivalent par contraposée : $x\neq x'\Rightarrow f(x)=f(x')$

Commentaires :

L'ensemble d'arrivée *F* n'intervient pas dans la définition

Exemples :

Les fonctions affines non constantes, « cube », « racine carrée », $x\mapsto x^{2p+1}$ avec $p\in\mathbb{N}$ sont injectives.

Contre-exemple :

$f:\mathbb{R}\to\mathbb{R}$ n'est pas injective.
$x\mapsto x^2$

En revanche, la restriction de la fonction *f* à $\mathbb{R}_+$ est injective.

Cas particulier des fonctions réelles :

1. I est un intervalle non vide de $\mathbb{R}$.

Une fonction $f:I\to\mathbb{R}$ où strictement monotone est injective.
La réciproque est fausse.

La continuité n'intervient pas pour la monotonie.

2. Une fonction paire, ou plus généralement, une fonction dont la courbe représentative admet une droite d'équation $x=a$ pour axe de symétrie n'est pas injective.

Retour sur les clés de cryptage possibles

On doit avoir $\text{PGCD}(a\,;26)=1$ avec $0<a\leqslant 25$ (on avait dit au début que $a\neq 0$ pour une clé de cryptage affine).

Combien de choix avons-nous ?

a peut prendre les valeurs 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25. Il y a donc 12 valeurs possibles pour a.
Pour b, il y a 26 valeurs possibles.

Au total, il y a donc $12\times 26=312$ clefs possibles.

VI. Problème de décodage

1°) Principe général

Dans le problème de décodage nous sommes amenés à résoudre l'« équation » $ax+b\equiv y$ [26] où l'inconnue est x et y est donné.

(1) $\Leftrightarrow ax\equiv y-b$ [26]

Pour poursuivre on cherche un « inverse » à a modulo 26, c'est-à-dire un entier a' tel que $aa'\equiv 1$ [26].

a et 26 étant premiers entre eux, d'après le théorème de Bézout, il existe deux entiers *u* et *v* tel que $au+26v=1$.

On « congrut » la relation modulo 26.

On a donc : $au\equiv 1$ [26] car $26\equiv 0$ [26].

On peut donc choisir : $a'=u$.

Ainsi, on peut trouver un inverse à *a* modulo 26. Il suffit de prendre le coefficient *a* de l'égalité de Bezout.

(1) $\Rightarrow a'ax\equiv a'(y-b)$ [26]
$\Rightarrow x\equiv a'(y-b)$ [26]
$\Rightarrow x\equiv a'y-a'b$ [26]

Conclusion :

Le décodage s'effectue par un chiffrement affine de clé $(c\,;d)=(a'\,;-a'b)$.

2°) Exemple

On prend la clé $(a\,;b)=(17\,;16)$.
Déterminer la clé de décodage $(c\,;d)$.

On utilise la calculatrice pour trouver les coefficients de Bezout de 17 et 26.
On obtient $a'=-3$.
On congrut modulo 26 de façon à obtenir un entier entre 0 et 25 au sens large.
On obtient $c=23$.
On calculer ensuite $d=22$ ou $d=-3$ (comme on veut).
On donne à la personne la clé de codage. À elle de trouver ensuite la clé de décodage.