Le chiffrement de Hill

Principe de fonctionnement

Contrairement aux chiffrements affines ou de Vigenère, les lettres sont ici codées par groupe de deux, trois, ... Voici un exemple où les lettres sont codées deux à deux, inspiré du travail de Paul Milan.

Etape n°1

On regroupe les lettres par 2. Chaque lettre est ensuite remplacée par un entier selon le même principe que les chiffrements affine ou de Vigenère.

A	B	C	D	E	...	Z
0	1	2	3	4	...	25

Etape n°2

On obtient ainsi des couples d'entiers $(y_1\,;\,y_2)$ tel que :

$$(S_1)\ \begin{cases} y_1 \equiv 11x_1 + 3x_2 \ (26) \\ y_2 \equiv 7x_1 + 4x_2 \ (26) \end{cases}$$

où x_1 correspond à la première lettre et x_2 la seconde et où $0 \leqslant y_1, y_2 \leqslant 25$.

Etape n°3

Les entiers y_1 et y_2 sont enfin transformés en entiers en utilisant le tableau de la première étape.

Exercice n°1 On considère l'équation $23x - 26y = 1$ où x et y sont deux entiers relatifs.

1. Vérifier que le couple $(-9\,;\,-8)$ est solution de cette équation.
2. En déduire toutes les solutions de cette équation.
3. En déduire un entier a tel que $0 \leqslant a \leqslant 25$ et $23a \equiv 1\ (26)$.

Exercice n°2

1. Coder le couple ST.
2. Coder les mots PALACE et RAPACE. Que remarque-t-on ?
3. On s'intéresse maintenant à la procédure de décodage.
   Montrer que tout couple $(x_1\,;\,x_2)$ vérifiant les équations du système (S_1) vérifie aussi les équations du système suivant, noté (S_2) :

$$\begin{cases} 23x_1 & \equiv & 4y_1 + 23y_2 & (26) \\ 23x_2 & \equiv & 19y_1 + 11y_2 & (26) \end{cases}$$

4. A l'aide de l'exercice précédent, montrer que tout couple vérifiant (S_2) vérifie le système ci-dessous, noté (S_3) :

$$\begin{cases} x_1 & \equiv & 16y_1 + y_2 & (26) \\ x_2 & \equiv & 11y_1 + 5y_2 & (26) \end{cases}$$

5. Montrer que tout couple vérifiant (S_3) vérifie aussi (S_1).
6. Décoder alors le mot PFXXKNUW.

> Correction des exercices

Exercice n°1

1. $23 \times (-9) - 26 \times (-8) = 1$. Il s'agit bien d'un couple solution.

2. Soit $(x\,;\,y)$ un couple solution de cette équation. Cela donne $23 \times (-9) - 26 \times (-8) = 1$. Puisque $(-9\,;\,-8)$ est aussi solution, on a
   $23x - 26y = 23 \times (-9) - 26 \times (-8) = 0$ ce qui donne $23(x+9) - 26(y+8) = 0$ soit encore $23(x+9) = 26(y+8)$.

   26 divise $23(x+9)$ et PGCD$(23\,;\,26) = 1$. Alors d'après le théorème de Gauss, il existe un entier relatif k tel que $x + 9 = 26k$.
   On obtient alors $y + 8 = 23k$.
   Les couples solutions sont donc $(-9 + 26k\,;\,-8 + 23k)$.

3. Si $23a \equiv 1\ (26)$ alors il existe un entier relatif b tel que $23a = 1 + 26b$ donc $23a - 26b = 1$.

   $(a\,;\,b)$ est donc solution de notre équation de départ.
   a est de la forme $a = -9 + 26k$ où $k \in \mathbb{Z}$.
   Pour respecter $0 \leqslant a \leqslant 25$, il faut prendre k=1 pour obtenir $a = 17$.

Exercice n°2

1. ST correspond au couple $(18\,;\,19)$.
   On a ensuite $y_1 \equiv 11 \times 18 + 3 \times 19 \equiv 255 \equiv 21\ (26)$ puis $y_2 \equiv 7 \times 18 + 4 \times 19 \equiv 202 \equiv 20\ (26)$
   Le couple $(18\,;\,19)$ a donc pour image le couple $(21\,;\,20)$ qui correspond à VU.

2. On applique le même procédé.
   PA correspond à $(15\,;\,0)$ qui a pour image $(9\,;\,1)$ et qui correspond à (JB).
   LA correspond à $(11\,;\,0)$ qui a pour image $(17\,;\,25)$ et qui correspond à (RZ).
   PA correspond à $(2\,;\,4)$ qui a pour image $(8\,;\,4)$ et qui correspond à (IE).

   RA correspond à $(17\,;\,0)$ qui a pour image $(5\,;\,15)$ et qui correspond à (FP).
   PA correspond à $(15\,;\,0)$ qui a pour image $(9\,;\,1)$ et qui correspond à (JB).
   CE correspond à $(2\,;\,4)$ qui a pour image $(8\,;\,4)$ et qui correspond à (IE).

   La lettre A n'est pas codée de la même façon selon la lettre suivante.

3. L'idée est de supprimer le terme en x_2. On va donc multiplier par 4 la première ligne et la soustraire par 3 fois la seconde.
   On obtient ainsi $44x_1 + 12x_2 - 21x_1 - 12x_2 \equiv 4y_1 - 3y_2\ (26)$ ce qui nous donne $23x_1 \equiv 4y_1 - 3y_2\ (26)$.
   Or $-3 = -26 + 23$ donc $-3y_2 \equiv 23y_2\ (26)$ d'où la première ligne du système (S_2).

   Pour la deuxième ligne, on cherche à supprimer le terme en x_1.
   On va donc multiplier par -7 la première ligne de (S_1) et ajouter 11 fois la deuxième. On obtient ainsi :

$-77x_1 - 21x_2 + 77x_1 + 44x_2 \equiv -7y_1 + 11y_2$ (26) ce qui donne $23x_2 \equiv -7y_1 + 11y_2$ (26).
Or $-7 = -26 + 19$ donc $-7y_1 \equiv 19y_1$ (26) d'où la deuxième ligne du système (S_2).

4. D'après l'exercice n°1, $23a \equiv 1$ (26) $\Leftrightarrow a \equiv 17$ (26) donc :
   $23x_1 \equiv 4y_1 + 23y_2 \Leftrightarrow x_1 \equiv 17(4y_1 + 23y_2)$
   $x_1 \equiv 68y_1 + 391y_2$. Mais $68 \equiv 16$ (26) et $391 \equiv 1$ (26) donc $x_1 \equiv 16y_1 + y_2$.

   $23x_2 \equiv 19y_1 + 11y_2 \Leftrightarrow x_2 \equiv 17(19y_1 + 11y_2)$
   $x_2 \equiv 323y_1 + 187y_2$. Mais $323 \equiv 11$ (26) et $187 \equiv 5$ (26) donc $x_2 \equiv 11y_1 + 5y_2$.

5. Supposons que $(x_1\,;\,x_2)$ soit un couple qui vérifie le système (S_3).
   On a donc $11x_1 + 3x_2 \equiv 11(16y_1 + y_2) + 3(11y_1 + 5y_2) \equiv 209y_1 + 26y_2$ (26).
   Mais $209 \equiv 1$ (26) et $26 \equiv 0$ (26) donc $11x_1 + 3x_2 \equiv y_1$ (26).
   On montre de façon analogue que la deuxième ligne du système (S_1) est vérifiée.

6. PF correspond au couple $(15\,;\,5)$. 15 est la valeur de y_1 et 5 est la valeur de y_2. On utilise ensuite les lignes du système (S_3) pour trouver les valeurs de x_1 et x_2. On trouve alors $x_1 = 11$ et $x_2 = 8$ ce qui donne le couple LI.
   De la même façon, le couple XX est décodé en BE, le couple RT est décodé en couple RT et le couple UW est décodé en couple ES.