Chiffrement affine

On définit chaque lettre par un nombre compris entre 0 et 25

On utilise une fonction de hachage

$f : [\![0, 25]\!] \to [\![0, 25]\!]$

$x \mapsto f(x) = 17x + 22 \ (26)$

Rem les outils

- congruences dans $\mathbb{Z}$
- théorème de Bézout
- Algo d'Euclide

A chiffrement - on calcule pour chaque lettre $f(x)$

B Déchiffrement.

idée $y = 17x + 22 \ (26)$

on cherche u tel que $17u = 1 \ (26)$ pour remplacer

$uy = 17xux + ux22 \ (26)$ $y = 17x + 22 \ (26)$ par $17uy = 17x + 22 \ (26)$

$uy = x + 22u \ (26)$ puis $uy = x + 17^{-1} \cdot 22 \ (26)$

$x = uy - 22u \ (26)$

(inverse) (on cherche l'inverse de 17 !)

$17u = 1 \ (26)$ par Bézout $\exists v$ tq $17u - 26v = 1$

17 et 26 sont premiers entre eux. donc (u, v) existent dans $\mathbb{Z}$.

Algo d'Euclide pour remonté $\to$ $17 \times (-3) - 26(-2) = 1$

$(u, v) = (-3, -2)$

donc $u = -3 + 26k$ $\quad k \in \mathbb{Z}$.

$v = -2 + 17k$

Une seule valeur vérifie $0 \leq u \leq 25$ $\to$ $u = 23$

donc $17 \times 23 = 1 \ (26)$

Soit g la fonction de déchiffrage

$$y = f(x) \ (26) \iff x = g(y) \ (26)$$

$17 \times 23 = 1 \ (26)$ soit $y = 17x + 22 \ (26)$

$$\iff 23y = 23 \times 17x + 506 \ (26)$$

$$\iff 23y - 506 = x \ (26)$$

$$(-506 = -19 \times 26 - 12)$$

$$\iff 23y + 14 = x \ (26)$$

$$g : y \mapsto 23y + 14$$

chiffrement de Hill

chiffrement polygraphique, on chiffre les lettres par paquets

Ex avec un regroupement de deux lettres.

$$f : (x_1, x_2) \mapsto (y_1, y_2)$$

Ex $y_1 = 9x_1 + 4x_2 \ (26)$

$y_2 = 5x_1 + 7x_2 \ (26)$

Déchiffrement : on doit trouver $g : (y_1, y_2) \mapsto (x_1, x_2)$

Par résolution du système $43x_1 = 7y_1 - 4y_2 \ (26)$

$$43x_2 = -5y_1 + 9y_2 \ (26)$$

On pose $\begin{cases} 3_1 = 7y_1 - 4y_2 \ (26) \\ y_2 = -5y_1 + 5y_2 \ (26) \end{cases}$

On doit chercher l'inverse de 43 dans $\mathbb{Z}/26\mathbb{Z}$, soit par Bézout, comme 43 et 26 sont premiers entre eux

$$43u = 1 \ (26) \Rightarrow u = -3 \ (26) \text{ ou } u = 23 \ (26)$$

Par multiplication par u dans $43 x_1 = z_1 \ (26)$
$43 x_2 = z_2 \ (26)$

on obtient $\begin{cases} x_1 = 5y_1 + 12y_2 \ (26) \\ x_2 = 15y_1 + 25y_2 \ (26) \end{cases}$

Généralisation $f : \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$

avec $y_i = \sum_{j=1}^{n} d_j x_j \quad \forall i$

On a une matrice carré H telle que $f\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = H \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

$H \in \mathcal{M}_n(\mathbb{N})$ est la matrice de chiffrement.

On cherche alors $DH = I \ (26)$ avec D matrice de déchiffrement.

Une matrice de décryptage existe ssi le déterminant de la matrice de chiffrement H est premier avec 26.