Le chiffre affine

Principe

Le **chiffre affine** est une variante du chiffre de César, très pratique à mettre en œuvre sur un ordinateur car il se réduit à des calculs sur des nombres entiers. On commence par remplacer chaque lettre par son ordre dans l'alphabet, auquel, pour des raisons techniques, on enlève 1 : A devient 0, B devient 1,..., Z devient 25. On choisit ensuite deux nombres entiers a et b qui sont la clé de chiffrement. Le nombre x est alors codé par $y=ax+b$. Ce nombre n'étant pas forcément compris entre 0 et 25, on prend son reste r dans la division par 26. Et ce nombre r est à son tour remplacé par la lettre qui lui correspond.

Exemple

On souhaite coder le mot `ELECTION` avec le choix a=3, b=5.

Message initial	E	L	E	C	T	I	O	N
Étape 1 : en nombres	4	11	4	2	19	8	14	13
Étape 2 : après chiffrement	17	38	17	11	62	29	47	44
Étape 3 : réduction modulo 26	17	12	17	11	10	3	21	18
Message chiffré	R	M	R	L	K	D	V	S

- **Étape 1 :** On remplace les lettres par leur nombre associé : 4,11,4,2,19,8,14,13.

- **Étape 2 :** On calcule pour chaque nombre $ax+b$: Par exemple, pour le premier nombre $x_1=4$, on obtient $y_1=17$. De même, $y_2=38$, $y_3=17$, $y_4=11$, $y_5=62$, $y_6=29$, $y_7=47$, $y_8=44$.

- **Étape 3 :** On prend les restes dans la division par 26, et on trouve : $z_1=17$, $z_2=12$, $z_3=17$, $z_4=11$, $z_5=10$, $z_6=3$, $z_7=21$, $z_8=18$.

- **Étape 4 :** On retranscrit en lettres, remplaçant 17 par R, etc... On trouve `RMRLK DVS`.

Toutes les valeurs de a ne sont pas autorisés pour le chiffrement affine. Imaginons en effet que a=2 et b=3. Alors,

- la lettre A est remplacée par 0, chiffrée en 2*0+3=3, c'est-à-dire que A est chiffrée par D.
- la lettre N est remplacée par 13, chiffrée en 2*13+3=29, dont le reste dans la division par 26 est 3 : N est également remplacé par D.

Ainsi, la valeur a=2 ne convient pas, car deux lettres sont chiffrées de la même façon, et si on obtient un D dans le message chiffré, on ne pourra pas savoir s'il correspond à un A ou à un N.

Avec un peu d'arithmétique, et notamment l'aide du théorème de Bezout, on peut prouver que a convient s'il n'est pas divisible par 2 ou par 13. On peut choisir en revanche pour b n'importe quelle valeur.

Déchiffrement

Pour déchiffrer un message, il faut procéder de la même façon. On commence par transcrire le message en nombres. Pour chaque nombre, on doit inverser la relation $y=ax+b$ (ici, on connait y et on doit retrouver x). On a envie de poser $x=(1/a).y-(b/a)$. C'est presque cela, sauf que l'on fait de l'arithmétique modulo 26. Ce qui remplace $1/a$, c'est l'inverse de a modulo 26, autrement dit un entier a' tel que, lorsqu'on fait le produit aa', on trouve un entier de la forme $1+26k$. On sait qu'un tel entier existe dès que la condition précédente

(2 ne divise pas a, 13 ne divise pas a) est vérifiée. Par exemple, pour $a=3$, on peut choisir $a'=9$ car $9\times3=1+26$.

Cette valeur de a déterminée, on a alors $x=a'y-a'b$, qu'on retranscrit en une lettre comme pour l'algorithme de chiffrement.

a	a^{-1}
1	1
3	9
5	21
7	15
9	3
11	19
15	7
17	23
19	11
21	5
23	17
25	25