A chaque lettre de l'alphabet, on associe un entier naturel x.

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

Le code associé à x est l'entier naturel y tel que : $0 \leq y \leq 25$ et $y \equiv a\,x + b$ [26], $a \neq 0$.
Le couple d'entiers $(a\,;\,b)$ est la clé de codage du chiffrement affine.

Stanislas intercepte le message crypté suivant : TU SATUMT NHMTTU.
Il n'*a* pas la clé mais pense la retrouver à l'aide du premier mot car il espère que celui-ci est LE.

a. Montrer que la clé $(a\,;\,b)$ vérifierait alors le système : $\begin{cases} 11\,a + b \equiv 19 \quad [26] \\ 4\,a + b \equiv 20 \quad [26] \end{cases}$.

b. En déduire que $7\,a \equiv -1 \quad [26]$

c. Déterminer un couple $(u\,;\,v)$ tels que $7\,u + 26\,v = 1$ et en déduire une valeur de a qui convient.

d. Décoder le message.

CORRECTION

a. à T on associe $y = 19$, à L on associe $x = 11$
Si T est la lettre codée correspondant à L alors $19 \equiv a \times 11 + b$ [26]
à U on associe $y = 20$, à E on associe 4
Si U est la lettre codée correspondant à E alors $20 \equiv a \times 4 + b$ [26]
a et b sont donc solutions du système : $\begin{cases} 11\,a + b \equiv 19 \quad [26] \\ 4\,a + b \equiv 20 \quad [26] \end{cases}$.

b. Si a et b sont solutions du système : $\begin{cases} 11\,a + b \equiv 19 \quad [26] \\ 4\,a + b \equiv 20 \quad [26] \end{cases}$, alors par différence terme à terme :
$11\,a + b - (4\,a + b) \equiv 19 - 20 \quad [26]$ soit $7\,a \equiv -1 \quad [26]$

c. 26 et 7 sont premiers entre eux donc d'après le théorème de Bézout, il existe deux entiers u et v tels que $7\,u + 26\,v = 1$
$11 \times 7 = 77$ et $26 \times 3 = 78$ donc $-11 \times 7 + 26 \times 3 = 1$ donc $u = -11$ et $v = 3$ sont solutions de $7\,u + 26\,v = 1$

$\begin{cases} 7\,u + 26\,v = 1 \\ 7\,a + 26\,b = 1 \end{cases}$ où $\alpha = -11$ et $\beta = 3$ donc par différence terme à terme : $7\,(u - \alpha) + 26\,(v - \beta) = 0$ donc $7\,(u - a) = -26\,(v - \beta)$
7 divise $-26\,(v - \beta)$, or 7 et 26 sont premiers entre eux donc d'après le théorème de Gauss, 7 divise $v - \beta$
Il existe un entier relatif k tel que $v - \beta = 7\,k$ donc $v = 7\,k + v$
En remplaçant dans $7\,(u - a) = -26\,(v - \beta)$ alors $u - a = -26\,k$ donc $u = -26\,k + a$
$a = -11$ et $\beta = 7$ donc $u = -26\,k - 11$ et $v = 7\,k + 3$, $k \in \mathbb{Z}$.

Vérification

Soit $u = -26\,k + 3$ et $v = 7\,k - 11$, $k \in \mathbb{Z}$, alors $7\,u + 26\,v = 7\,(-26\,k - 11) + 26\,(7\,k - 3) = -11 \times 7 + 26 \times 3 = 1$

Les solutions de $7\,u + 26\,v = 1$ sont $u = -26\,k - 11$ et $v = 7\,k + 3$, $k \in \mathbb{Z}$.

On cherche a tel que $7\,a \equiv -1 \quad [26]$ et $0 \leq a \leq 25$
$7\,a \equiv -1 \quad [26] \Leftrightarrow$ il existe q $(q \in \mathbb{Z})$ tel que $7\,a = -1 + 26\,q$ soit $-7\,a + 26\,q = 1$ donc $-a = -26\,k - 11$ $(k \in \mathbb{Z})$

soit $a = 26\,k + 11$ $(k \in \mathbb{Z})$, $0 \leq a \leq 25$ donc $a = 11$

$\begin{cases} 11\,a + b \equiv 19 \quad [26] \\ 4\,a + b \equiv 20 \quad [26] \end{cases}$ et $a = 11$ donc $4 \times 11 + b \equiv 20 \quad [26]$ or $44 = 26 + 18$ donc $b + 18 \equiv 20 \quad [26]$ donc $b \equiv 2 \quad [26]$
$0 \leq b \leq 25$ donc $b = 2$

Le code associé à x est l'entier naturel y tel que : $0 \leq y \leq 25$ et $y \equiv 11\,x + 2 \quad [26]$
Il s'agit de décoder le message donc de déterminer x en fonction de y
$11\,x \equiv y - 2 \quad [26]$ or $7 \times 11 = 77$ donc $7 \times 11 \equiv -1 \quad [26]$ donc $7 \times 11\,x \equiv 7\,(y - 2) \quad [26]$
$-x \equiv 7\,(y - 2) \quad [26]$ donc $x \equiv -7\,(y - 2) \quad [26]$
$-7 \equiv 19 \quad [26]$ donc $x \equiv 19\,y + 14 \quad [26]$

Lettre codée	T	U	S	A	T	U	M	T	N	H	M	T	T	U
codage y	19	20	18	0	19	20	12	19	13	7	12	8	19	20
décodage $x \equiv 19\,y + 14 \quad [26]$	11	4	18	14	11	4	8	11	1	17	8	10	11	4
Lettre décodée	L	E	S	O	L	E	I	L	B	R	I	L	L	E

Le message décodé est LE SOLEIL BRILLE