

Exercice

En utilisant le chiffrement affine avec $a=17$ et $b=-2$, donner le codage et le décodage du mot :
BONJOUR

Correction :

$$a=17 \text{ et } b=-2$$

$E(x)=y$ est **le reste de la division euclidienne** de $17x-2$ par 26 .

$$E(x) \equiv 17x - 2 \pmod{26}$$

$$0 \leq E(x) \leq 25$$

$$\text{Pgcd}(17;26)=1$$

On détermine **une solution particulière** de l'équation : $17u + 26v = 1$

En utilisant le logiciel Xcas :

$$\text{iabcuv}(17,26,1)$$

On obtient **$(-3;2)$** .

$$\text{On a, } y \equiv ax + b \pmod{26} \quad a=17$$

$$17x \equiv y - b \pmod{26}$$

$$17x - 26k = y - b$$

Une solution particulière de cette équation est **$(-3(y-b) ; -2(y-b))$** .

$$\text{Donc, } x \equiv -3(y-b) \pmod{26} \quad b=-2$$

$$x \equiv -3y - 6 \pmod{26}$$

$$\text{ou } x \equiv 23y + 20 \pmod{26}$$

$D(y)$ est **le reste de la division euclidienne** de $23y+20$ par 26 .

$$D(y) \equiv 23y + 20 \pmod{26}$$

$$0 \leq D(y) \leq 25$$

$$\boxed{D(y) = D[E(x)] = x}$$

Exemple :

	B	O	N	J	O	U	R
x	01	14	13	09	14	20	17
$17x-2$	15	236	219	151	236	338	287
y	15	02	11	21	02	00	01
	P	C	L	V	C	A	B
$23y+20$	365	66	273	503	66	20	43
D(y)	01	14	13	09	14	20	17