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.

A 1. Supposons que (a ; b) et (a' ; b') soient deux clés telles que $a \equiv a'$ [26] et $b \equiv b'$ [26]. Démontrez que les codes obtenus avec ces deux clés de codage sont les mêmes.
On peut donc choisir les entiers naturels a et b tels que $1 \leq a \leq 25$ et $0 \leq b \leq 25$.
2. *a*. Ainsi, en théorie, de combien de clés de codage dispose-t-on ?
b. Choisissons la clé (4 ; 3). Recopiez et compléter le tableau ci-contre (le tableau en question est un tableau où il faut coder le mot palace.)
Si vous souhaiter déchiffrer le mot codé, quelle problème rencontrez vous?

B. Pour être utilisable, un chiffrement doit coder deux nombres différents à l'aide de deux nombres différents.
X et x' sont deux entiers naturels compris enter 0 et 25, y et y' sont leurs codes respectifs avec la clé (a ; b) telle que $1 \leq a \leq 25$ et $0 \leq b \leq 25$.
1. Pourquoi les propositions: "si $x \neq x'$, alors $y \neq y'$" et "si $y = y'$, alors $x = x'$" sont-elles équivalentes ?
2. Démontrez que, si $y = y'$, alors $a\,(x - x') \equiv 0$ [26].
3. Avec le théorème de Gauss, déduisez-en que si a est premier avec 26, alors $x = x'$.
4. Conclusion. Donnez une condition suffisante pour que le chiffrement soit utilisable. De combien de clés "utilisables" dispose-t-on? Que penser de la sûreté de cette technique de chiffrement?

CORRECTION

A 1. $y \equiv a\,x + b$ [26], or $a \equiv a'$ [26] donc $a\,x \equiv a'\,x$ [26]
$b \equiv b'$ [26] et $a\,x \equiv a'\,x$ [26] donc par addition terme à terme : $a\,x + b \equiv a'\,x + b'$ [26], donc $y \equiv y'$ [26].
$0 \leq y \leq 25$ et $0 \leq y' \leq 25$ donc $-25 \leq y - y' \leq 25$
Le seul multiple de 26 compris entre – 25 et 25 est 0 donc $y - y' = 0$ soit $y = y'$
Les codes obtenus avec ces deux clés de codage sont les mêmes.

2. *a*. $1 \leq a \leq 25$ donc on a 25 choix possibles pour a
$0 \leq b \leq 25$ donc on a 26 choix possibles pour b.
Il existe donc 25×26 clés possibles soit 650 clés possibles.

b.

	P	A	L	A	C	E
x	15	0	11	0	2	4
$4\,x + 3$	63	3	47	3	11	19
y	11	3	21	3	11	19
	L	D	V	D	L	T

PALACE est codé en LDVDLT

Décodage : $y \equiv 4\,x + 3$ [26] donc $4\,x \equiv y - 3$ [26]
$y - 3$ prend a priori toutes les valeurs comprises entre 0 et 25 en particulier il se peut que $y = 4$ or $4\,x \equiv 1$ [26] $\Leftrightarrow 4\,x = 26\,k + 1$ ($k \in \mathbb{Z}$) $\Leftrightarrow 2\,(2\,x - 13\,k) = 1$ ce qui est impossible puisque 1 n'est pas pair.

B. 1. Les propositions: "si $x \neq x'$, alors $y \neq y'$" et "si $y = y'$, alors $x = x'$" sont la négation l'une de l'autre donc sont équivalentes.

2. Si $y = y'$, alors $a\,x + b \equiv a\,x' + b$ [26] donc $a\,(x - x') \equiv 0$ [26].

3. $a\,(x - x') \equiv 0$ [26] donc 26 divise $a\,(x - x')$
26 et a sont premiers entre eux donc d'après le théorème de Gauss, 26 divise $x - x'$.
$0 \leq x \leq 25$ et $0 \leq x' \leq 25$ donc $-25 \leq x - x' \leq 25$
Le seul multiple de 26 compris entre – 25 et 25 est 0 donc $x - x' = 0$ soit $x = x'$.

4. si $y = y'$ et si a est premier avec 26, alors $x = x'$ donc si a est premier avec 26 et si $x \neq x'$ (question 1) alors $y \neq y'$ donc le chiffrement est utilisable si a est premier avec 26.

Tous les nombres pairs ne sont pas multiples de 26 donc $a = 2\,k + 1$
Il existe 12 nombres impairs compris entre 1 et 25
Parmi ces nombres impairs, il faut exclure 13 qui n'est pas premier avec 26.
a peut donc prendre 11 valeurs.
on a 1 choix possibles pour a et 26 choix possibles pour b donc il existe donc 11×26 clés possibles soit 286 clés possibles.
Le faible nombre de clés possibles rend ce chiffrement peu sûr.