Exercice 1

A U est associé le nombre 20.

$9\times 20+5=185=26\times 7+3$

3 est associé à la lettre D.

Donc U est codé par D.

On a $9\times 3=27\equiv 1[26]$.

Démontrons l'équivalence : $9m+5\equiv p[26]\Leftrightarrow m\equiv 3p-15[26]$.

On a :

$9m+5\equiv p[26]$	$m\equiv 3p-15[26]$
$\Rightarrow 27m+15\equiv 3p[26]$	$\Rightarrow 9m\equiv 27p-135[26]$
$\Rightarrow m+15\equiv 3p[26]$	$\Rightarrow 9m\equiv p-5[26]$
$\Rightarrow m\equiv 3p-15[26]$	$\Rightarrow 9m+5\equiv p[26]$

A B est associé le nombre 1.

$3\times 1-15\equiv 14[26]$

14 est associé à la lettre O.

Donc B est décodé par O.

Exercice 2

1. a) $6^{10}=60466176=11\times 5496925+1$, donc $6^{10}\equiv 1[11]$.

b) $6\equiv 1[5]$, donc $6^{4}\equiv 1[5]$.

c) $6^{40}=(6^{10})^{4}\equiv 1[11]$ d'après a) $6^{40}=(6^{4})^{10}\equiv 1[5]$ d'après b).

d) D'après c), 5 divise $6^{40}-1$ et 11 divise $6^{40}-1$, de plus PGCD(11, 5) = 1, donc, par un théorème du cours, $5\times 11=55$ divise $6^{40}-1$.

2. a) PGCD(65, 40) = 5. Si l'équation (E) admet une solution (x, y), alors 5 divise 65x – 40y, donc 5 divise 1, ce qui est absurde.

b) PGCD(40, 17) = 1, par le théorème de Bézout, il existe u et v entiers relatifs tels que $17u+40v=1$; le couple (u, -v) est donc solution de (E').

c) Par l'algorithme d'Euclide

$40=17\times 2+6$

$17=6\times 2+5$

$6=5\times 1+1$

	1	0
	0	1
2	1	-2
2	-2	5
1	3	-7

Ainsi on a : $40(3)+17(-7)=1$, soit $17(-7)-40(-3)=1$, le couple (-7, -3) est une solution de (E').

d)) Pour tous x et y $\in\mathbb{Z}$, on a :

$17x-40y=1$

$\Leftrightarrow 17x-40y=17(-7)-40(-3)$

$\Leftrightarrow 17(x+7)=40(y+3)\qquad(1)$

40 divise 17(x + 7) et PGCD(17 , 40) = 1, donc, d'après le théorème de Gauss, 40 divise x + 7 ; il existe donc $k\in Z$ tel que x + 7 = 40k. Il vient alors, en remplaçant dans (1), $17\times 40k=40(y+3)$, soit y + 3 = 17k.

Les solutions sont donc :

$$\begin{cases} x=-7+40k \\ y=-3+17k, k\in Z \end{cases}$$

$17x_0\equiv 1[40]$ équivaut à : il existe m entier relatif tel que $17x_0=1+40m$. D'après la résolution ci-dessus, on en déduit que x_0 est de la forme -7 + 40k, où $k\in\mathbb{Z}$. Il existe une seule valeur de x_0, entier naturel inférieur à 40, c'est 33.