7.2 1) $n = p\,q = 11 \cdot 23 = 253$
$\varphi(n) = (p-1)\,(q-1) = (11-1) \cdot (23-1) = 10 \cdot 22 = 220$

2) $\text{pgcd}(2, 220) = 2 \neq 1$

$\text{pgcd}(3, 220) = 1$
$e = 3$ est le plus petit exposant d'encodage RSA que Bob peut choisir.

3) d est solution de la congruence $e\,d \equiv 1 \mod \varphi(n)$, ici $3\,d \equiv 1 \mod 220$.

(a) **1re méthode**
Résolvons l'équation diophantienne $3\,x + 220\,y = 1$.

Appliquons l'algorithme d'Euclide pour calculer $\text{pgcd}(3, 220)$:
$220 = 3 \cdot 73 + 1 \qquad \Longrightarrow \qquad 1 = 220 - 3 \cdot 73$
$3 = 1 \cdot 3$

À partir de la solution particulière $x_0 = -73$ et $y_0 = 1$, on déduit la solution générale :
$$\begin{cases} x = -73 + \frac{220}{1}\,k = -73 + 220\,k \\ y = \quad 1 - \quad \frac{3}{1}\,k = \quad 1 - \quad 3\,k \end{cases} \quad \text{où } k \in \mathbb{Z}$$

La condition $1 < x < \varphi(n) = 220$ implique $k = 1$.
On conclut que $d = -73 + 220 = 147$.

(b) **2e méthode**
En utilisant l'exercice 7.11, on obtient $d \equiv 3^{\varphi(220)-1} \mod 220$

Sachant que $220 = 2^2 \cdot 5 \cdot 11$, on en déduit que :
$\varphi(220) = 220\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{11}\right) = 80.$

Utilisons l'algorithme d'exponentiation binaire pour calculer $3^{79} \mod 220$:

x	reste r	n	$3^{2^n} \mod 220$	contribution (si $r = 1$)
79	1	0	3	3
39	1	1	$3^2 \equiv 9$	9
19	1	2	$9^2 \equiv 81$	81
9	1	3	$81^2 \equiv -39$	-39
4	0	4	$(-39)^2 \equiv -19$	
2	0	5	$(-19)^2 \equiv -79$	
1	1	6	$(-79)^2 \equiv 81$	81

$3^{79} \equiv 3 \cdot 9 \cdot 81 \cdot (-39) \cdot 81 \equiv 147 \mod 220$
On conclut également que $d = 147$.

4) clé publique : $(253, 3)$
clé secrète : $(11, 23, 147)$