7.13 La signature du message nécessite de connaître la clé privée d'Alice.
Il faut donc au préalable factoriser 437. Il n'y a guère de méthode connue autre que celle qui consiste à tester les diviseurs premiers.

$437 \equiv 1 \not\equiv 0 \mod 2 : 2 \nmid 437$
$437 \equiv 2 \not\equiv 0 \mod 3 : 3 \nmid 437$
$437 \equiv 2 \not\equiv 0 \mod 5 : 5 \nmid 437$
$437 \equiv 3 \not\equiv 0 \mod 7 : 7 \nmid 437$
$437 \equiv 8 \not\equiv 0 \mod 11 : 11 \nmid 437$
$437 \equiv 8 \not\equiv 0 \mod 13 : 13 \nmid 437$
$437 \equiv 12 \not\equiv 0 \mod 17 : 17 \nmid 437$
$437 \equiv 0 \mod 19 : 19 \mid 437$
On trouve ainsi la factorisation $437 = 19 \cdot 23$.

$\varphi(437) = (19-1)(23-1) = 396$
La clé privée d vérifie la congruence $17\,d \equiv 1 \mod 396$.

Résolvons l'équation diophantienne $17\,x + 396\,y = 1$:

$$\begin{aligned} 396 &= 17 \cdot 23 + 5 && \Longrightarrow && 5 = 396 - 17 \cdot 23 \\ 17 &= 5 \cdot 3 + 2 && \Longrightarrow && 2 = 17 - 5 \cdot 3 \\ 5 &= 2 \cdot 2 + 1 && \Longrightarrow && 1 = 5 - 2 \cdot 2 \\ 2 &= 1 \cdot 2 \end{aligned}$$

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - (17 - 5 \cdot 3) \cdot 2 = 17 \cdot (-2) + 5 \cdot 7 \\ &= 17 \cdot (-2) + (396 - 17 \cdot 23) \cdot 7 = 396 \cdot 7 + 17 \cdot (-163) \end{aligned}$$

À partir de la solution particulière $x_0 = -163$ et $y_0 = 7$, on déduit la solution générale :

$$\begin{cases} x = -163 + \frac{396}{1}\,k = -163 + 396\,k \\ y = \quad 7 - \frac{17}{1}\,k = \quad 7 - 17\,k \end{cases} \quad \text{où } k \in \mathbb{Z}$$

La condition $1 < x < \varphi(n) = 396$ implique $k = 1$.
On conclut que $d = -163 + 396 = 233$.

La signature du message vaut $s = 100^{233} \mod 437$:

x	reste r	n	$100^{2^n} \mod 437$	contribution (si $r = 1$)
233	1	0	100	100
116	0	1	$100^2 \equiv -51$	
58	0	2	$(-51)^2 \equiv -21$	
29	1	3	$(-21)^2 \equiv 4$	4
14	0	4	$4^2 \equiv 16$	
7	1	5	$16^2 \equiv -181$	-181
3	1	6	$(-181)^2 \equiv -14$	-14
1	1	7	$(-14)^2 \equiv 196$	196

$100^{233} \equiv 100 \cdot 4 \cdot (-181) \cdot (-14) \cdot 196 \equiv 156 \mod 437$
La signature du message est ainsi $s = 156$.