7.14 1) (a) Le professeur doit crypter le message $m = 4$ avec la clé publique du secrétariat, c'est-à-dire calculer $4^7 \mod 77$:

x	reste r	n	$4^{2^n} \mod 77$	contribution (si $r = 1$)
7	1	0	4	4
3	1	1	$4^2 \equiv 16$	16
1	1	2	$16^2 \equiv 25$	25

$4^7 \equiv 4 \cdot 16 \cdot 25 \equiv 60 \mod 77$

Le professeur transmet au secrétariat le message codé 60.

(b) Pour déterminer la signature envoyée par le professeur, il faut connaître sa clé privée.

$n_\mathrm{P} = 15 = 3 \cdot 5 \qquad \varphi(n_\mathrm{P}) = (3-1)(5-1) = 8$

La clé privée d_P du professeur satisfait la congruence $3\,d_\mathrm{P} \equiv 1 \mod 8$.

Comme $3 \cdot 3 \equiv 1 \mod 8$, on trouve immédiatement $d_\mathrm{P} = 3$.

La signature du message du professeur vaut $s \equiv 4^3 \equiv 4 \mod 15$.

Le professeur doit encore crypter la signature pour la transmettre au secrétariat, donc calculer $4^7 \mod 77$. Ce calcul est le même que celui qui lui a permis de coder le message. Le professeur envoie donc au secrétariat la signature codée 60.

2) Pour décrypter le message reçu par le secrétariat, on a besoin de sa clé privée.

$n_\mathrm{S} = 77 = 7 \cdot 11 \qquad \varphi(n_\mathrm{S}) = (7-1)(11-1) = 60$

La clé privée d_S du secrétariat vérifie la congruence $7\,d_\mathrm{S} \equiv 1 \mod 60$.

Afin d'obtenir d_S, résolvons l'équation diophantienne $7\,x + 60\,y = 1$:

$$\begin{aligned} 60 &= 7 \cdot 8 + 4 &\quad\Longrightarrow\quad & 4 = 60 - 7 \cdot 8 \\ 7 &= 4 \cdot 1 + 3 &\quad\Longrightarrow\quad & 3 = 7 - 4 \cdot 1 \\ 4 &= 3 \cdot 1 + 1 &\quad\Longrightarrow\quad & 1 = 4 - 3 \cdot 1 \\ 3 &= 1 \cdot 3 \end{aligned}$$

$$\begin{aligned} 1 &= 4 - 3 \cdot 1 \\ &= 4 - (7 - 4 \cdot 1) \cdot 1 = 7 \cdot (-1) + 4 \cdot 2 \\ &= 7 \cdot (-1) + (60 - 7 \cdot 8) \cdot 2 = 60 \cdot 2 + 7 \cdot (-17) \end{aligned}$$

À partir de la solution particulière $x_0 = -17$ et $y_0 = 2$, on déduit la solution générale :

$$\begin{cases} x = -17 + \frac{60}{1}\,k = -17 + 60\,k \\ y = \quad 2 - \frac{7}{1}\,k = \quad 2 - \quad 7\,k \end{cases} \quad \text{où } k \in \mathbb{Z}$$

La condition $1 < x < \varphi(n) = 60$ implique $k = 1$.

On conclut que $d_\mathrm{S} = -17 + 60 = 43$.

(a) Pour décrypter le message et la signature, il faut calculer $41^{43} \mod 77$:

x	reste r	n	$41^{2^n} \mod 77$	contribution (si $r = 1$)
43	1	0	41	-36
21	1	1	$(-36)^2 \equiv -13$	-13
10	0	2	$(-13)^2 \equiv 15$	
5	1	3	$15^2 \equiv -6$	-6
2	0	4	$(-6)^2 \equiv 36$	
1	1	5	$36^2 \equiv -13$	-13

$41^{43} \equiv (-36) \cdot (-13) \cdot (-6) \cdot (-13) \equiv 6 \mod 77$

Le secrétariat obtient pour message $m = 6$ et pour signature $s = 6$.

(b) Pour vérifier que le message a bien été envoyé par le professeur, le secrétariat doit s'assurer que $6^3 \equiv 6 \mod 15$.

Puisque cette congruence est bien vérifiée, le message a bel et bien été envoyé par le professeur.

3) Pour décrypter le message, le secrétariat calcule $12^{43} \mod 77$:

x	reste r	n	$12^{2^n} \mod 77$	contribution (si $r = 1$)
43	1	0	12	12
21	1	1	$12^2 \equiv -10$	-10
10	0	2	$(-10)^2 \equiv 23$	
5	1	3	$23^2 \equiv -10$	-10
2	0	4	$(-10)^2 \equiv 23$	
1	1	5	$23^2 \equiv -10$	-10

$12^{43} \equiv 12 \cdot (-10) \cdot (-10) \cdot (-10) \equiv 12 \mod 77$

Le message obtenu par le secrétariat est donc $m = 12$.

Pour décrypter la signature, le secrétariat calcule $27^{43} \mod 77$:

x	reste r	n	$27^{2^n} \mod 77$	contribution (si $r = 1$)
43	1	0	27	27
21	1	1	$27^2 \equiv 36$	36
10	0	2	$36^2 \equiv -13$	
5	1	3	$(-13)^2 \equiv 15$	15
2	0	4	$15^2 \equiv -6$	
1	1	5	$(-6)^2 \equiv 36$	36

$27^{43} \equiv 27 \cdot 36 \cdot 15 \cdot 36 \equiv 48 \mod 77$

Le secrétariat obtient par conséquent la signature $s = 48$.

Pour s'assurer de l'authenticité du message, le secrétariat doit encore calculer $48^3 \mod 15$. Comme $48^3 \equiv 12 = m \mod 15$, le secrétariat conclut que le message a bien été envoyé par le professeur.