7.6 1) $n = 3 \cdot 11 = 33 \qquad \varphi(n) = (3-1)\cdot(11-1) = 20$

Pour crypter le message, il faut calculer $5^7 \mod 33$:
$5^7 \equiv 5^2 \cdot 5^2 \cdot 5^2 \cdot 5 \equiv (-8)\cdot(-8)\cdot(-8)\cdot 5 \equiv 64 \cdot (-40) \equiv (-2)\cdot(-7) \equiv 14$
On a donc obtenu pour message crypté : $c = 14$.

Pour décrypter le message, il faut disposer de la clé privée d, c'est-à-dire résoudre la congruence $7\,d \equiv 1 \mod 20$.
On devine immédiatement que $d = 3$.

On décrypte le code $c = 14$, en calculant $14^3 \mod 33$:
$14^3 \equiv 14^2 \cdot 14 \equiv (-2)\cdot 14 \equiv 5 \mod 33$
On retrouve bien le message $m = 5$.

2) $n = 7 \cdot 11 = 77 \qquad \varphi(n) = (7-1)\cdot(11-1) = 60$

Pour crypter le message, il faut calculer $8^{17} \mod 77$:

x	reste r	n	$8^{2^n} \mod 77$	contribution (si $r = 1$)
17	1	0	8	8
8	0	1	$8^2 \equiv (-13)$	
4	0	2	$(-13)^2 \equiv 15$	
2	0	3	$15^2 \equiv -6$	
1	1	4	$(-6)^2 \equiv 36$	36

$8^{17} \equiv 8 \cdot 36 \equiv 57 \mod 77$
On a donc obtenu pour message crypté : $c = 57$.

Pour décrypter le message, il faut disposer de la clé privée d, c'est-à-dire résoudre la congruence $17\,d \equiv 1 \mod 60$.
À cette fin, résolvons l'équation diophantienne $17\,x + 60\,y = 1$:

$$\begin{aligned} 60 &= 17\cdot 3 + 9 &\Longrightarrow\quad 9 &= 60 - 17\cdot 3 \\ 17 &= 9\cdot 1 + 8 &\Longrightarrow\quad 8 &= 17 - 9\cdot 1 \\ 9 &= 8\cdot 1 + 1 &\Longrightarrow\quad 1 &= 9 - 8\cdot 1 \\ 8 &= 1\cdot 8 \end{aligned}$$

$$\begin{aligned} 1 &= 9 - 8\cdot 1 \\ &= 9 - (17 - 9\cdot 1)\cdot 1 = 17\cdot(-1) + 9\cdot 2 \\ &= 17\cdot(-1) + (60 - 17\cdot 3)\cdot 2 = 60\cdot 2 + 17\cdot(-7) \end{aligned}$$

À partir de la solution particulière $x_0 = -7$ et $y_0 = 2$, on déduit la solution générale :

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

La condition $1 < x < \varphi(n) = 60$ implique $k = 1$.
On conclut que $d = -7 + 60 = 53$.

Il reste maintenant à calculer $57^{53} \mod 77$:

x	reste r	n	$57^{2^n} \mod 77$	contribution (si $r=1$)
53	1	0	57	57
26	0	1	$57^2 \equiv 15$	
13	1	2	$15^2 \equiv -6$	-6
6	0	3	$(-6)^2 \equiv 36$	
3	1	4	$36^2 \equiv -13$	-13
1	1	5	$(-13)^2 \equiv 15$	15

$57^{53} \equiv 57 \cdot (-6) \cdot (-13) \cdot 15 \equiv (-34) \cdot 36 \equiv 8 \mod 77$

On retrouve ainsi bien le message initial $m = 8$.

3) $n = 17 \cdot 31 = 527 \qquad \varphi(n) = (17-1)(31-1) = 480$

Le message codé est $c = 2^7 \equiv 128 \mod 527$.

Pour décrypter le message, il faut disposer de la clé privée d, c'est-à-dire résoudre la congruence $7\,d \equiv 1 \mod 480$.

Utilisons cette fois-ci la formule $d = 7^{\varphi(480)-1} \mod 480$.

De $480 = 2^5 \cdot 3 \cdot 5$, on tire que $\varphi(480) = 480\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 128$.

x	reste r	n	$7^{2^n} \mod 480$	contribution (si $r=1$)
127	1	0	7	7
63	1	1	$7^2 \equiv 49$	49
31	1	2	$49^2 \equiv 1$	1
15	1	3	$1^2 \equiv 1$	1
7	1	4	$1^2 \equiv 1$	1
3	1	5	$1^2 \equiv 1$	1
1	1	6	$1^2 \equiv 1$	1

$d \equiv 7^{127} \equiv 7 \cdot 49 \cdot 1^5 \equiv 343 \mod 480$

Le décryptage du message se résume au calcul $128^{343} \mod 527$.

x	reste r	n	$128^{2^n} \mod 527$	contribution (si $r=1$)
343	1	0	128	128
171	1	1	$128^2 \equiv 47$	47
85	1	2	$47^2 \equiv 101$	101
42	0	3	$101^2 \equiv 188$	
21	1	4	$188^2 \equiv 35$	35
10	0	5	$35^2 \equiv 171$	
5	1	6	$171^2 \equiv 256$	256
2	0	7	$256^2 \equiv 188$	
1	1	8	$188^2 \equiv 35$	35

$128^{343} \equiv 128 \cdot 47 \cdot 101 \cdot 35 \cdot 256 \cdot 35 \equiv 2 \mod 527$

Comme prévu, on retrouve bien le message initial.