7.11 1) La signature d'Alice est $s \equiv m^{d_A} \mod n_A$, ici $s \equiv 111^{147} \mod 253$.

x	reste r	n	$111^{2^n} \mod 253$	contribution (si $r = 1$)
147	1	0	111	111
73	1	1	$111^2 \equiv -76$	-76
36	0	2	$(-76)^2 \equiv -43$	
18	0	3	$(-43)^2 \equiv 78$	
9	1	4	$78^2 \equiv 12$	12
4	0	5	$12^2 \equiv -109$	
2	0	6	$(-109)^2 \equiv -10$	
1	1	7	$(-10)^2 \equiv 100$	100

$111^{147} \equiv 111 \cdot (-76) \cdot 12 \cdot 100 \equiv 89 \mod 253$

Alice obtient ainsi la signature $s = 89$.

2) Alice envoie à Bob le message m et la signature s encodés au moyen de la clé publique de Bob. Elle lui envoie donc le message codé $m^{e_B} \mod n_B$ et la signature codée $s^{e_B} \mod n_B$.

(a) Le message codé sera en l'occurrence $111^5 \mod 247$:

x	reste r	n	$111^{2^n} \mod 247$	contribution (si $r = 1$)
5	1	0	111	111
2	0	1	$111^2 \equiv -29$	
1	1	2	$(-29)^2 \equiv 100$	100

$111^5 \equiv 111 \cdot 100 \equiv 232 \mod 247$

Le message codé transmis à Bob est donc 232.

(b) La signature codée sera dans ce cas $89^5 \mod 247$:

x	reste r	n	$89^{2^n} \mod 247$	contribution (si $r = 1$)
5	1	0	89	89
2	0	1	$89^2 \equiv 17$	
1	1	2	$17^2 \equiv 42$	42

$89^5 \equiv 89 \cdot 42 \equiv 33 \mod 247$

La signature codée transmise à Bob est ainsi 33.

3) Bob utilise sa clé privée pour décoder le message et la signature transmis par Alice sous forme codée.

   (a) Pour décrypter le message, Bob calcule $232^{173} \mod 247$:

x	reste r	n	$232^{2^n} \mod 247$	contribution (si $r = 1$)
173	1	0	232	(-15)
86	0	1	$(-15)^2 \equiv -22$	
43	1	2	$(-22)^2 \equiv -10$	(-10)
21	1	3	$(-10)^2 \equiv 100$	100
10	0	4	$100^2 \equiv 120$	
5	1	5	$120^2 \equiv 74$	74
2	0	6	$74^2 \equiv 42$	
1	1	7	$42^2 \equiv 35$	35

   $232^{173} \equiv (-15) \cdot (-10) \cdot 100 \cdot 74 \cdot 35 \equiv 111 \mod 247$

   Bob obtient bien le message en clair $m = 111$.

   (b) Pour décrypter la signature, Bob calcule $33^{173} \mod 247$:

x	reste r	n	$33^{2^n} \mod 247$	contribution (si $r = 1$)
173	1	0	33	33
86	0	1	$33^2 \equiv 101$	
43	1	2	$101^2 \equiv 74$	74
21	1	3	$74^2 \equiv 42$	42
10	0	4	$42^2 \equiv 35$	
5	1	5	$35^2 \equiv -10$	-10
2	0	6	$(-10)^2 \equiv 100$	
1	1	7	$100^2 \equiv 120$	120

   $33^{173} \equiv 33 \cdot 74 \cdot 42 \cdot (-10) \cdot 120 \equiv 89 \mod 247$

   Bob obtient bien la signature en clair $s = 89$.

4) Pour vérifier l'authenticité du message, c'est-à-dire que le message a bien été envoyé par Alice, Bob doit contrôler que $m = s^{e_\mathrm{A}} \mod n_\mathrm{A}$.

   Dans cet exemple, Bob calcule $89^3 \mod 253$.

   Puisqu'il trouve $89^3 \equiv 111 = m \mod 253$, il conclut que c'est bien Alice qui a envoyé le message.