7.5 On rappelle qu'à l'exercice 7.2, on a trouvé que Bob a pour clé publique $(253, 3)$ et pour clé secrète $(11, 23, 147)$.

1) Pour décrypter 13, il faut calculer $13^{147} \mod 253$:

x	reste r	n	$13^{2^n} \mod 253$	contribution (si $r = 1$)
147	1	0	13	13
73	1	1	$13^2 \equiv -84$	-84
36	0	2	$(-84)^2 \equiv -28$	
18	0	3	$(-28)^2 \equiv 25$	
9	1	4	$25^2 \equiv 119$	119
4	0	5	$119^2 \equiv -7$	
2	0	6	$(-7)^2 \equiv 49$	
1	1	7	$49^2 \equiv 124$	124

$$13^{147} \equiv \underbrace{13 \cdot (-84)}_{\equiv -80} \cdot \underbrace{119 \cdot 124}_{\equiv 82} \equiv -80 \cdot 82 \equiv 18 \mod 253$$

Le 13 est ainsi décodé en 18.

2) Pour décrypter 00, il faut calculer $0^{147} \equiv 0 \mod 253$.

3) Pour décrypter 66, il faut calculer $66^{147} \mod 253$:

x	reste r	n	$66^{2^n} \mod 253$	contribution (si $r = 1$)
147	1	0	66	66
73	1	1	$66^2 \equiv 55$	55
36	0	2	$55^2 \equiv -11$	
18	0	3	$(-11)^2 \equiv 121$	
9	1	4	$121^2 \equiv -33$	-33
4	0	5	$(-33)^2 \equiv 77$	
2	0	6	$77^2 \equiv 110$	
1	1	7	$110^2 \equiv -44$	-44

$$66^{147} \equiv \underbrace{66 \cdot 55}_{\equiv -80} \cdot \underbrace{(-33) \cdot (-44)}_{\equiv 82} \equiv 88 \cdot (-66) \equiv 11 \mod 253$$

Le 66 est ainsi décodé en 11.

4) Pour décrypter 157, il faut calculer $157^{147} \mod 253$:

x	reste r	n	$157^{2^n} \mod 253$	contribution (si $r = 1$)
147	1	0	157	157
73	1	1	$157^2 \equiv 108$	108
36	0	2	$108^2 \equiv 26$	
18	0	3	$26^2 \equiv -83$	
9	1	4	$(-83)^2 \equiv 58$	58
4	0	5	$58^2 \equiv 75$	
2	0	6	$75^2 \equiv 59$	
1	1	7	$59^2 \equiv -61$	-61

$$157^{147} \equiv \underbrace{157 \cdot 108}_{\equiv 5} \cdot \underbrace{58 \cdot (-61)}_{\equiv 4} \equiv 5 \cdot 4 \equiv 20 \mod 253$$

Le 157 est ainsi décodé en 20.

5) Pour décrypter 28, il faut calculer $28^{147} \mod 253$:

x	reste r	n	$28^{2^n} \mod 253$	contribution (si $r = 1$)
147	1	0	28	28
73	1	1	$28^2 \equiv 25$	25
36	0	2	$25^2 \equiv 119$	
18	0	3	$119^2 \equiv -7$	
9	1	4	$(-7)^2 \equiv 49$	49
4	0	5	$49^2 \equiv 124$	
2	0	6	$124^2 \equiv -57$	
1	1	7	$(-57)^2 \equiv -40$	-40

$$28^{147} \equiv \underbrace{28 \cdot 25}_{\equiv -59} \cdot \underbrace{49 \cdot (-40)}_{\equiv 64} \equiv (-59) \cdot 64 \equiv 19 \mod 253$$

Le 28 est ainsi décodé en 19.

Le message crypté 13 00 66 157 28 est donc décodé en 18 00 11 20 19.

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Il signifie SALUT.