Tutorial 11 Solutions

1 (a) $n = 11 \times 13 = 143$, $\phi(n) = 10 \times 12 = 120$

$$120 = 37 \times 3 + 9$$
$$37 = 9 \times 4 + 1$$

$$\therefore \quad 1 = 37 - 9 \times 4 = (1)37 + (-4)9$$
$$= 37 - 4(120 - 37 \times 3) = (-4)120 + (13)37$$

$$\therefore \quad 1 \equiv 13 \times 37 \pmod{120}$$

$$\therefore \quad e = 13.$$

(b) $25^{13} \equiv 25 \times (25^2)^6 \equiv 25 \times 53^6$
$\equiv 25 \times (53^2)^3 \equiv 25 \times 92^3$
$\equiv 25 \times 92 \times (92^2)^1 \equiv 12 \times 27^1$
$\equiv 12 \times 27 \equiv 38 \pmod{143}$

Similarly, $5^{13} \equiv 70$, $19^{13} \equiv 6 \pmod{143}$

So A receives $(38, 70, 6)$.

(c) $27^{37} \equiv 27 \times (27^2)^{18} \equiv 27 \times 14^{18}$
$\equiv 27 \times (14^2)^9 \equiv 27 \times 53^9$
$\equiv 27 \times 53 \times (53^2)^4 \equiv 1 \times 92^4$
$\equiv (92^2)^2 \equiv 27^2 \equiv 14 \pmod{143}$

Similarly, $119^{37} \equiv 15 \pmod{143}$

So A decrypts to $(14, 15)$, or NO.

2 (a) $40^{30} \equiv (40^2)^{15} \equiv 48^{15}$

$\equiv 48 \times (48^2)^7 \equiv 48 \times 73^7$

$\equiv 48 \times 73 \times (73^2)^3 \equiv 12 \times 91^3$

$\equiv 12 \times 91 \times 91^2 \equiv 25 \times 36$

$\equiv 27 \pmod{97}$

So $\beta = 27$.

(b) $40^7 \equiv 40 \times (40^2)^3 \equiv 40 \times 48^3$

$\equiv 40 \times 48 \times 48^2 \equiv 77 \times 73 \equiv 92 \pmod{97}$

$27^7 \equiv 27 \times (27^2)^3 \equiv 27 \times 50^3$

$\equiv 27 \times 50 \times 50^2 \equiv 89 \times 75 \equiv 79 \pmod{97}$

$\therefore 10 \times 27^7 \equiv 14 \pmod{97}$

$e(10,7) = (40^7, 10 \times 27^7) \equiv (92, 14) \pmod{97}$

$e(1,7) = (40^7, 1 \times 27^7) \equiv (92, 79) \pmod{97}$

A receives $(92,14), (92,79)$.

(c) $d(92,39) = 39 \times (92^{30})^{-1} = 14$

$d(91,92) = 92 \times (91^{30})^{-1} = 5$

$d(51,59) = 59 \times (51^{30})^{-1} = 5$

A decrypts to $(14,05,09)$ or NEE.