Exo 1

$n = 221$, $e = 3$

1- Encodage de message $x = 12$ (2pts)

$x = 12$.

$y = x^e \bmod 4$

$= 12^3 \bmod 221$

$= 181$

donc le message $\boxed{y = 181}$

2- $m = 192$ (4pts)

* La factorisation de n.

on a : $n = p \cdot q$

et $m = (p-1)\cdot(q-1)$

$= p \cdot q - p - q + 1$ —— (1)

$p \cdot q = 221$

$\Rightarrow p = 221/q$

à partir (1) :

$(221/q)\cdot q - (221/q) - q + 1 = m = 192$

$221 - \frac{221}{q} - q + 1 = 192$

$-\frac{221}{q} - q + 30 = 0$

$-q^2 + 30q - 221 = 0$

$\Delta = 4$, $q_1 = \frac{-15-2}{-1} = 17$, $q_2 = \frac{-15+2}{-1} = 13$

donc : $\boxed{p = 17}$ et $\boxed{q = 13}$

ou : $\boxed{p = 13}$ et $\boxed{q = 17}$

* La clé privée de Bob (2 pts)

$d.e \bmod m = 1$

$d = (1+km)/e$

- $k=0 \Rightarrow d = 1/3$; $k=1 \Rightarrow d = 1+192/3 = 193/3$;

$k=2 \Rightarrow d = 385/3$; $k=3 \Rightarrow d = 577/3$; $k=4 \Rightarrow d = 769/3$;

$k=5 \Rightarrow d = 961/3$; $k=6 \Rightarrow$ ..... Impossible

car 192 et divisible sur 3.

on ne peut pas trouver d.

Exo 2 :

la clé publique : (35, 5)

donc, $n = 35$, $e = 5$

* le message chiffré envoyé : $C = 10$.

donc on a un décryptage :

$M = C^d \bmod n$ (2 pts)

* La valeur de d

$n = 35 \Rightarrow p = 7$ et $q = 5$

$m = (p-1)(q-1) = 24$

$d = (1+km)/e$ (2 pts)

- $k=0 \Rightarrow d = 1/5$; $k=1 \Rightarrow d = 25/5 = 5$.

donc $d = 5$

$M = 10^5 \bmod 35$

$\boxed{M = 5}$ (2 pts)

EXO3:

$n = 119$, $e = 7$

* La représentation de message "SIE":

S → 18
I → 08 ⇒ 180, 804 ← la taille de bloc
E → 04
x_1 x_2

(2 pts)

$Y_1 = X_1^e \bmod n$

$= 180^7 \bmod 119$

$= (61)^7 \bmod 119$

$= 61 . (61^2)^3 \bmod 119 = 61 . (32)^3 \bmod 119$

$= 61 . (43) \bmod 119 = 5$

donc $\boxed{Y_1 = 5}$ (1 pts)

$Y_2 = X_2^e \bmod n$

$= (804)^7 \bmod 119 = (90)^7 \bmod 119$

$= 90 . (90^2)^3 \bmod 119 = 90 . (8)^3 \bmod 119$

$= 90 . 36 \bmod 119 = 27$

donc $\boxed{Y_2 = 27}$ (1 pts)

donc le nouveau message : 005027

00 → A
50 mod 26 = 24 → Y
27 mod 26 = 01 → B

(2 pts)

donc Alice retrouve le message : AYB