EXERCICE 1 (8 PTS):

Soit l'annuaire des clés publiques suivant :

Entité	Clé publique (e , n)
Bob	(**x** , 33)
Alice	(17 , 33)

1. x peut-il être égale à 8 ? justifier **(1 pts)**

Note : Dans ce qui suit $x = 3$.

PARTIE 1 : CHIFFREMENT RSA (4 PTS)

Oscar est entrai d'écouter le canal, a un instant t il reçoit le message $M = 5$ se dirigeant vers **Alice**.

1. Déterminer le message clair (**3 pts)**
2. Où réside-t-elle la complexité de l'algorithme **RSA** ? (**1 pts)**

PARTIE 2 : SIGNATURE RSA (4 PTS)

1. Rappeler le fonctionnement de la signature **RSA**. (**0.5 pts)**
2. **Bob** a pour clé privé $d = 7$. Vérifier que ce choix convient. (**0.5 pts)**
3. **Bob** signe le message $m = 30$ par la signature $\sigma = 24$. Vérifier que cette signature est correcte (**2 pts)**

EXERCICE 2 (6 PTS):

I. Deux personnes **Alice** et **Bob** désirent échanger **une clé de session**, pour cela ils utilisent **l'algorithme d'échange de deffie Hellman**

1. Rappeler le schéma d'échange **(1 pts)**
2. Quelle sont les informations que peut récupérer **Oscar** ? (**1 pts)**
3. On suppose que le générateur $g = 16$ et $p = 157$ et que **Alice** génère le nombre aléatoire $a = 4$ et **Bob** génère le nombre aléatoire $b = 79$.
    a. calculer la clé de session (**1 pts)**.

II. On utilise maintenant **El-Gamal**

1. Rappeler le schéma d'envoi d'un message m de **Bob** vers **Alice** **(1 pts)**
2. On suppose que le générateur $g = 16$ et $p = 157$ et que **Alice** génère le nombre aléatoire $a = 4$ et **Bob** génère le nombre aléatoire $b = 79$, et **Bob** désire communiquer le message $m = 100$. **Décrire tout le processus** (calculer les valeurs intermédiaire). (**2 pts)**

EXERCICE 3 (3 PTS):

Note : La clé publique RSA est (e, n), la clé privé est (d, n)

PARTIE 1 : SIGNATURE RSA SANS HACHAGE

Alice envoie à **Bob** deux couples (message, signature) : (m_1, σ_1) et (m_2, σ_2).

Montrer qu'**Oscar** (en récupérant ses deux couples) peut construire une signature valide σ du message $m1 * m2$ **(1 pts)**

PARTIE 2 : SIGNATURE RSA AVEC HACHAGE

Alice envoie à **Bob** un couple (message, signature) : (m, σ).

1. Donner σ en fonction du haché du message $H(m)$, d et n **(1 pts)**
2. On suppose que H n'est pas résistante à la seconde pré-image. **Oscar** récupère la signature valide σ d'un message m. Montrer comment Oscar peut construire une signature valide pour un message différent de m. **(1 pts)**

EXERCICE 4 (3 PTS)

1. Donner les propriétés que doit satisfaire une fonction d'hachage ? **(1 pts)**
2. Expliquer brièvement l'algorithme d'hachage MD5 **(2 pts)**

Solution Sujet Securité :

exercice 01

1. on a $n = 33 \Rightarrow p = 11 \quad q = 3$

$\Rightarrow \varphi(n) = (11-1)(3-1) = 20.$

on a x admet un inverse dans $\mathbb{Z}/_{20}\mathbb{Z}$

ssi $pgcd(x, \underbrace{\varphi(n)}_{20}) = 1$

dans ce cas $x = 8$ or $pgcd(8, \varphi(33))$

$= pgcd(8, 20) = 4 \neq 1$ ainsi x

ne peut pas être égal a 8.

Partie 01 : Chiffrement RSA :

- $C = 5$ depuis Bob vers Alice

$\Rightarrow$ que Bob a crypter le Message M avec

la clé publique de Alice $e = 17$.

1. Trouvons d'abord la clé privé de Alice d

on a d est l'inverse de e dans $\mathbb{Z}/_{20}\mathbb{Z}$

$\Rightarrow d \times e \equiv 1 [20]$

- $d \times 17 \equiv 1 \, [20] \iff \text{pgcd}(17, 20) = 1$

- $20 = 1 \times \underline{17} + \underline{3}$
- $17 = 5 \times \underline{3} + \underline{2}$
- $3 = 1 \times \underline{2} + \underline{1}$

- on a besoin de trouver $d \times 17 + k \times 20 = 1$

- $1 = 3 - 1 \times \underline{2}$
- $1 = 3 - 1 \times (17 - 5 \times 3)$

  $= 6 \times \underline{3} - 1 \times \underline{17}$
- $1 = 6 \times (20 - 1 \times 17) - 1 \times 17$
- $= 6 \times 20 - 7 \times 17$

$\Rightarrow 1 = 6 \times 20 - 7 \times 17 \;/\; \begin{matrix} k = 6 \\ d = ? \end{matrix}$

$1 = 6 \times 20 - 17 \times 20 + 17 \times 20 - 17 \times 07$

$1 = -11 \times 20 + 13 \times 20$

$\Rightarrow d = 13$ inverse modulaire de 17

Maintenant calculons le Message claire

- $M = C^d \bmod n$

$M = 5^{13} \bmod 33$

→ utilisons l'algorithme indien par le calcul d'exponentiel Modulaire :

- $13 = 1101$

$b_0 = 1$ $r = 1^2 \times 5 \bmod 33 = 5$

$b_1 = 1$ $r = 5^2 \times 5 \bmod 33 = 26$

$b_2 = 0$ $r = 26^2 \bmod 33 = 16$

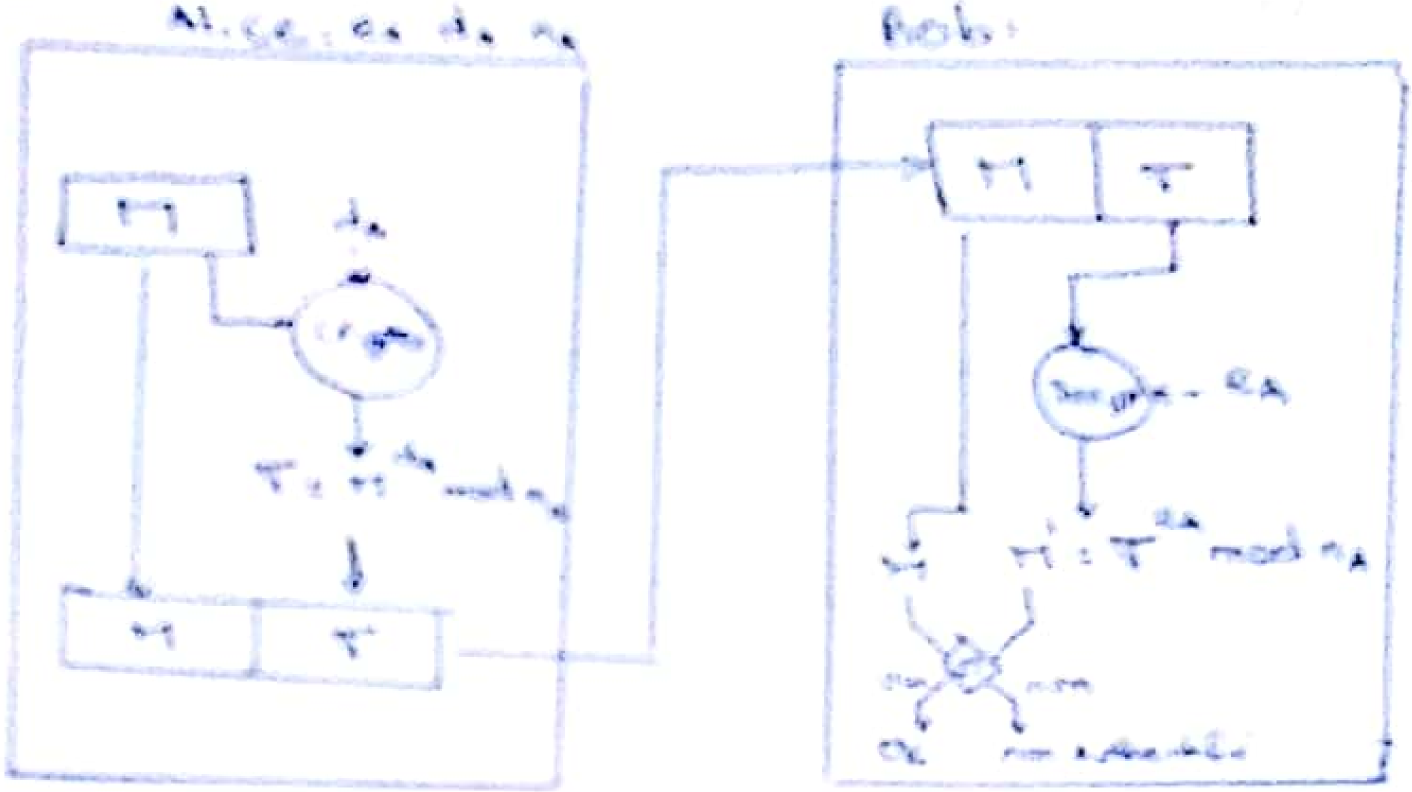
$b_3 = 1$ $r = 16^2 \times 5 \bmod 33 = 26$

$\Rightarrow \boxed{M = 26}$ Message claire

2. La Complexité de l'algorithme de RSA reside dans la decomposition du semi-premier n (trouver p et q tq $p \times q = n$)

Partie 2 : Signature RSA (e : clé publique, d : clé privé)

1.



Rappel : RSA → Chiffrer (Dechiffrer (M)) = M

2. bob : clé privé = 7

on a $e_B = 3$ et $d_B = 7$ on a $\varphi(n) = 20$

$3 \times 7 \equiv 1 \, [20] \Rightarrow d$ est bien l'inverse de e

3. $M_{Bob} = 30$ et $T_{Bob} = 24$

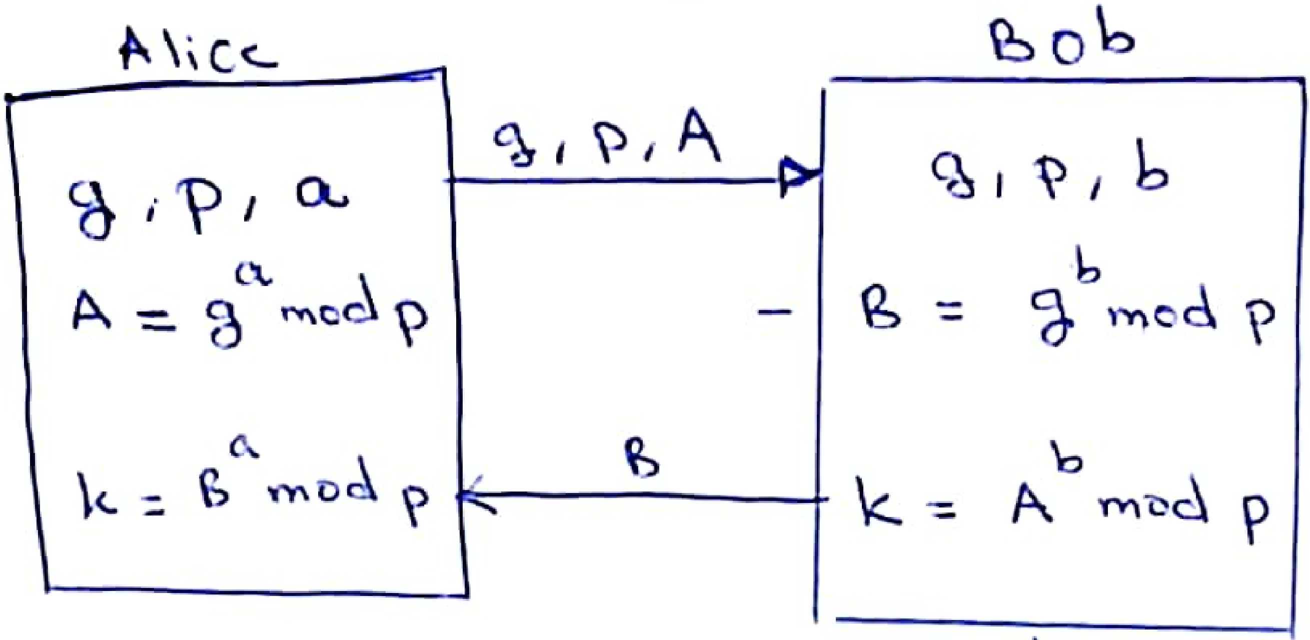
valider la signature revient à calculer :

$M' = T_{Bob}^{3} \bmod n_B = 24^{3} \bmod 33 = 30$

$\Rightarrow M_{Bob} = M' \Rightarrow$ Signature Valide

Exercice 2 :

1. schéma d'échange Diffie-Hellman :



note : clé de session : $k = g^{ab} \bmod p$

2. Informations que peut récupérer Oscar :

- g, p, A, B (Dans le canal d'échange)

3. clé de Session :

$$k = g^{ab} \bmod p = 16^{316} \bmod 157$$

plusieurs méthodes de calcule suivirent la plus simple étant d'utiliser le thm de fermat : car 157 premier :

$$a^{p-1} \bmod p = 1$$

- $316 = (157 - 1) \times 2 + 4$

$$= 16^4 \times (16^{(157-1)})^2 \bmod 157$$

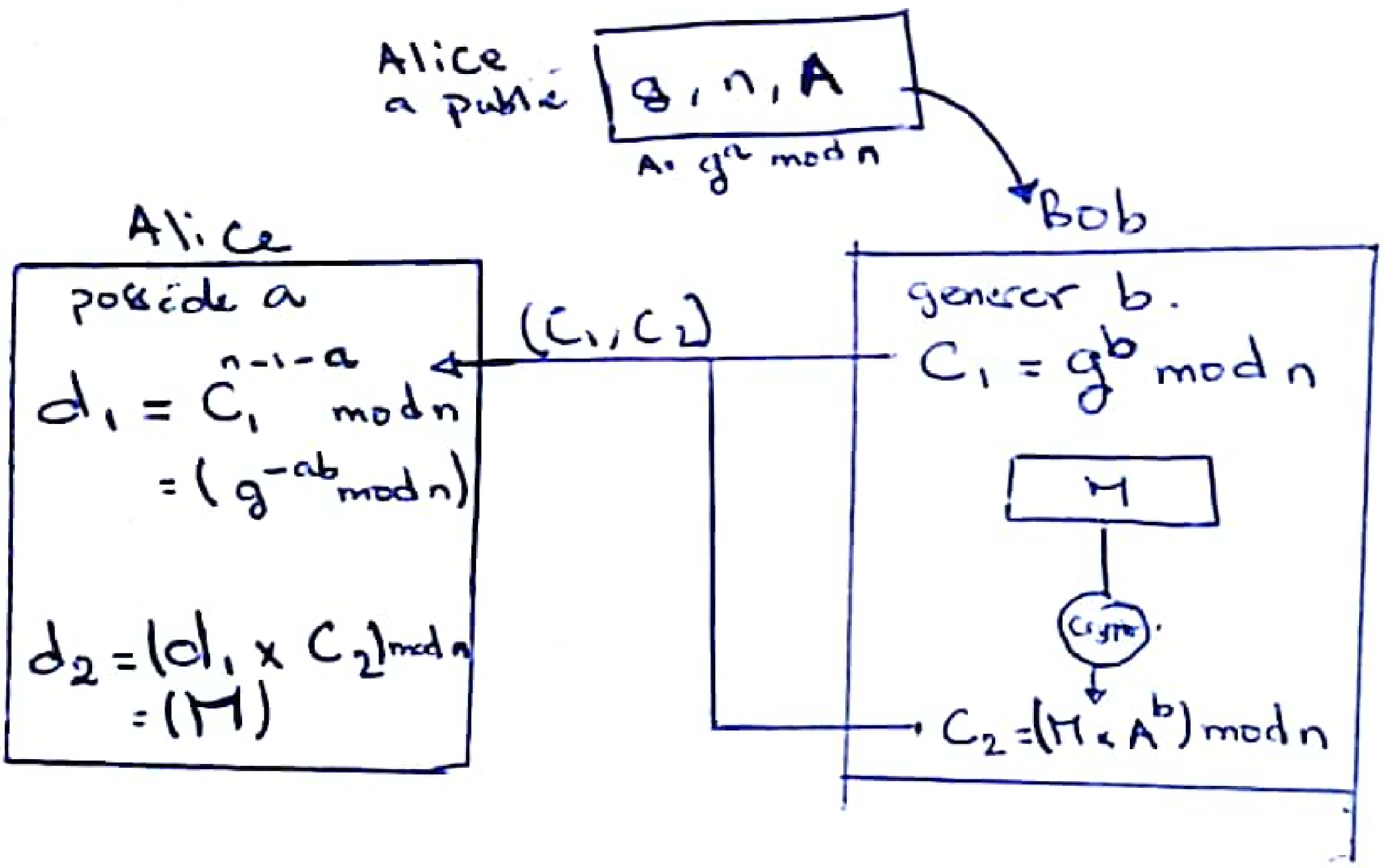
$$= (16^4 \bmod 157)(16^{157-1} \bmod 157)^2 \bmod 157$$

$$= 16^4 \bmod 157$$

$$= 67$$

ainsi clé de session $k = 67$

II. EL-GAMAL :



2. on a : $g = 16$ $n = 157$ $a = 4$ $b = 79$ A=

+ on a aussi au préalable : $A = 16^4 \bmod 157 = 67$

1. bob : Former C_1, C_2 :

$C_1 = g^b \bmod n = 16^{79} \bmod 157 = 16$

(en fait on applique l'algorithme indien avec $79 = (1001111)_2$)

$C_2 = (M \times A^b) \bmod 157$

$= (100 \times (67^{79} \bmod 157)) \bmod 157$

calculé de la même façon

$= (100 \times 67) \bmod 157$

$= 106$

2. Alice : d_1, d_2

$d_1 = C_1^{n-1-a} \bmod 157$

$= 16^{157-1-4} \bmod 157 = 16^{152} \bmod 157$

$= 75$ (indien)

$d_2 = (d_1 \times C_2) \bmod 157$

$= \boxed{100} = M$

Exercice 03

On a Alice envoit (m_1, σ_1) ; (m_2, σ_2) qu'oscar intercepte :

on a : $\sigma_1 = m_1^d \mod n$ et $\sigma_2 = m_2^d \mod n$

$\Rightarrow \sigma_1 \times \sigma_2 = m_1^d \mod n \times m_2^d \mod n$

$= (m_1 \times m_2)^d \mod n$

ainsi $\sigma = \sigma_1 \times \sigma_2$ est une signature valide pour le msg : $m_1 \times m_2$

II. Signature RSA avec Hachage :

1- $\sigma = (H(m))^d \mod n$

2- puisque H n'est pas resistante a la seconde pré image :

∘ oscar intercepte (m, σ)

oscar peut calculer m' tq $H(m') = H(m)$

il constitue alors le couple (m', σ) qui est cohérent car σ signature valide pour m'

exercice 04

revoir le cours