Compléments sur la méthode RSA

Malika More
(malika.more@iut.u-clermont1.fr)
Jean Mailfert - Gisèle Provost

1A - IUT Info - Clermont 1

Arithmétique et Cryptographie

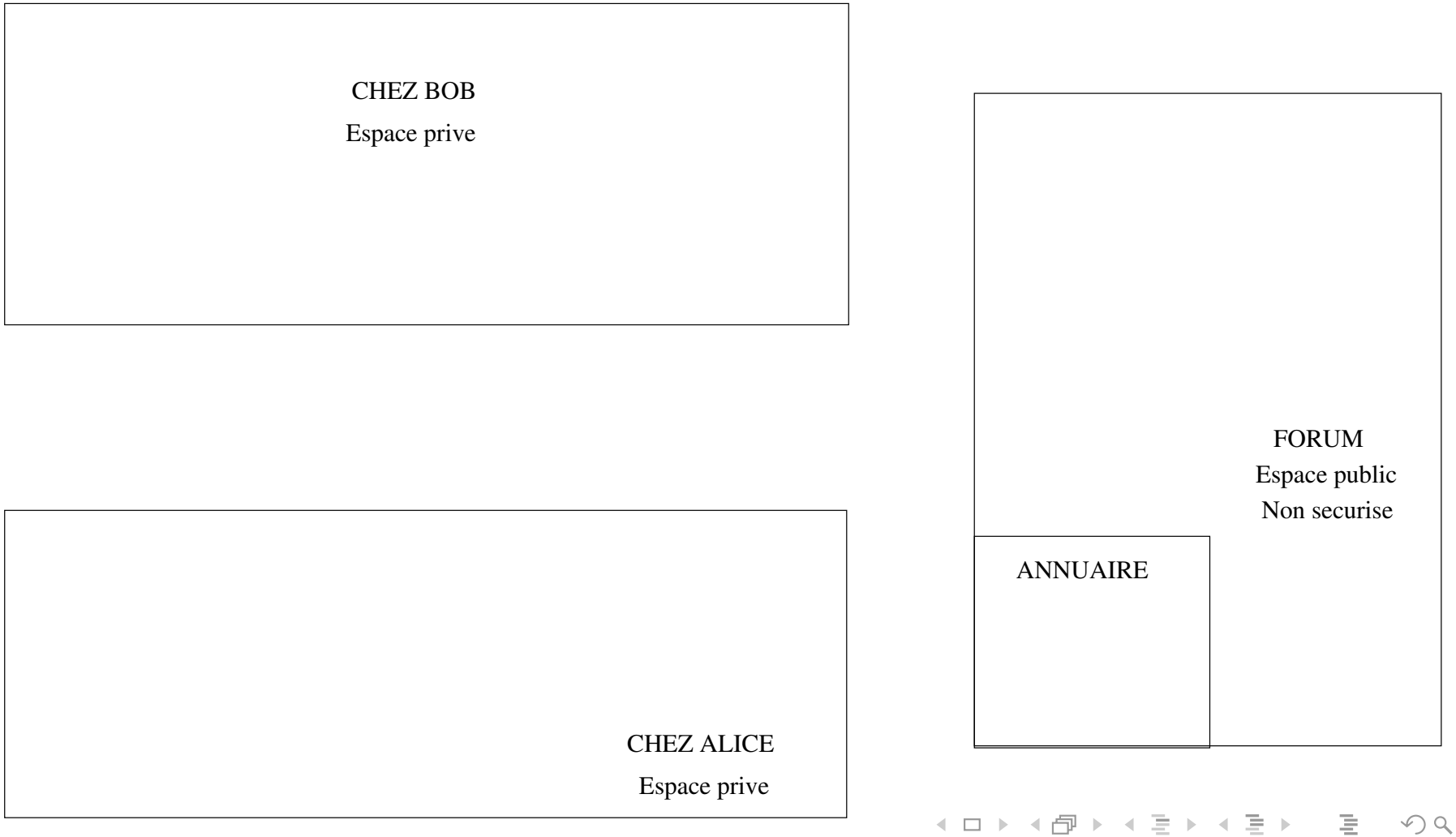
Année 2011-2012

Important

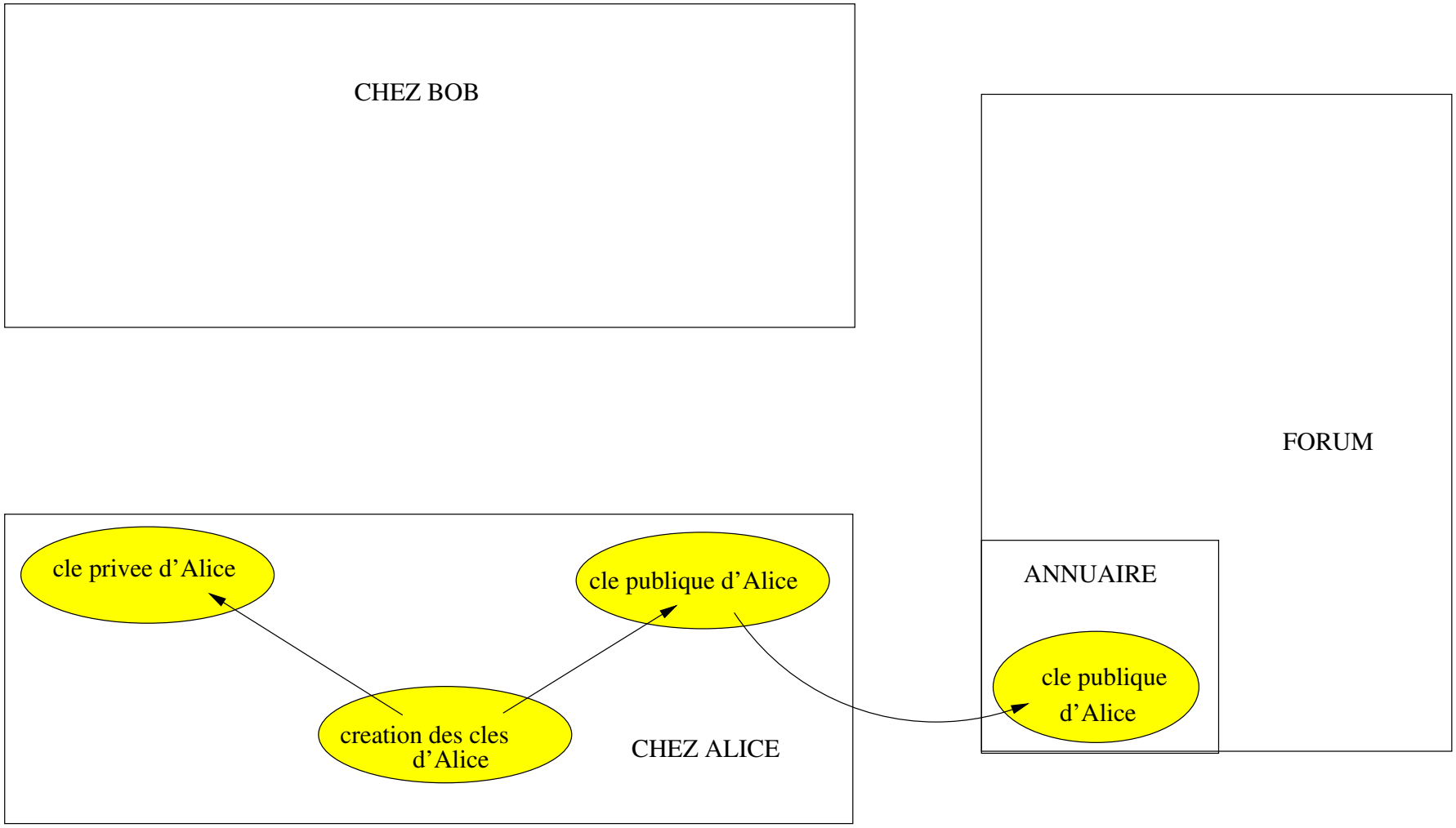
- Les transparents du cours et d'autres documents et informations sont disponibles sur la page du cours sur l'ENT
- Il est très fortement recommandé d'apporter une calculatrice en cours et en TD d'arithmétique

Plan du cours

Contexte


CHEZ BOB
Espace prive
FORUM
Espace public
Non securise
ANNUAIRE
CHEZ ALICE
Espace prive

Alice fabrique ses clés



Alice fabrique ses clés

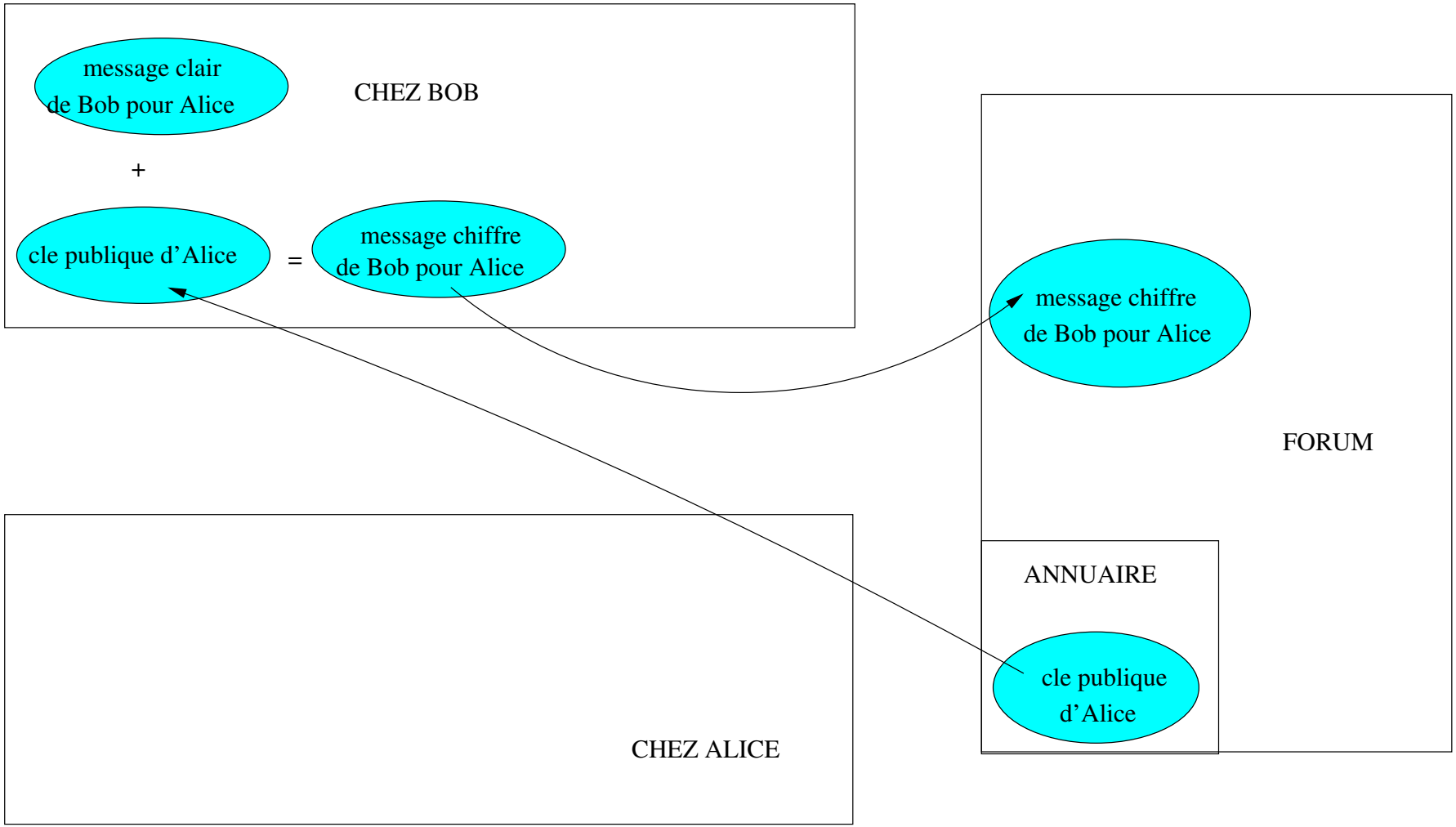
1. Alice choisit deux nombres premiers p_A et q_A et calcule le **module $\mathbf{N_A} = p_A \times q_A$**
2. Alice calcule $\varphi(N_A) = (p_A - 1)(q_A - 1)$ et choisit un **compliqueur $\mathbf{E_A}$** premier avec $\varphi(N_A)$
3. Alice calcule le **faciliteur $\mathbf{D_A}$**, inverse de E_A modulo $\varphi(N_A)$
4. Alice rend **publics $\mathbf{N_A}$** et **$\mathbf{E_A}$** mais garde **privés $\mathbf{D_A}$**, ainsi que $\varphi(N_A)$, p_A et q_A

Alice fabrique ses clés

Exemple

- Alice choisit $p_A = 11$ et $q_A = 17$
- Alice calcule le module $N_A = 11 \times 17 = 187$ et $\varphi(N_A) = 10 \times 16 = 160$
- Alice choisit le compliqueur $E_A = 13$, qui est premier avec $\varphi(N_A)$
- Alice calcule le faciliteur $D_A = E_A^{-1} \mod \varphi(N_A) = 13^{-1} \mod 160 = 37$
- Alice rend publics $E_A = 13$ et $N_A = 187$ et garde secrets $D_A = 37$, ainsi que p_A, q_A et $\varphi(N_A)$

Bob envoie un message secret à Alice



Bob envoie un message secret à Alice

1. Bob vérifie que son message **M** est acceptable : $\mathbf{M} < \mathbf{N_A}$
2. Bob calcule le *cryptogramme* de ce message

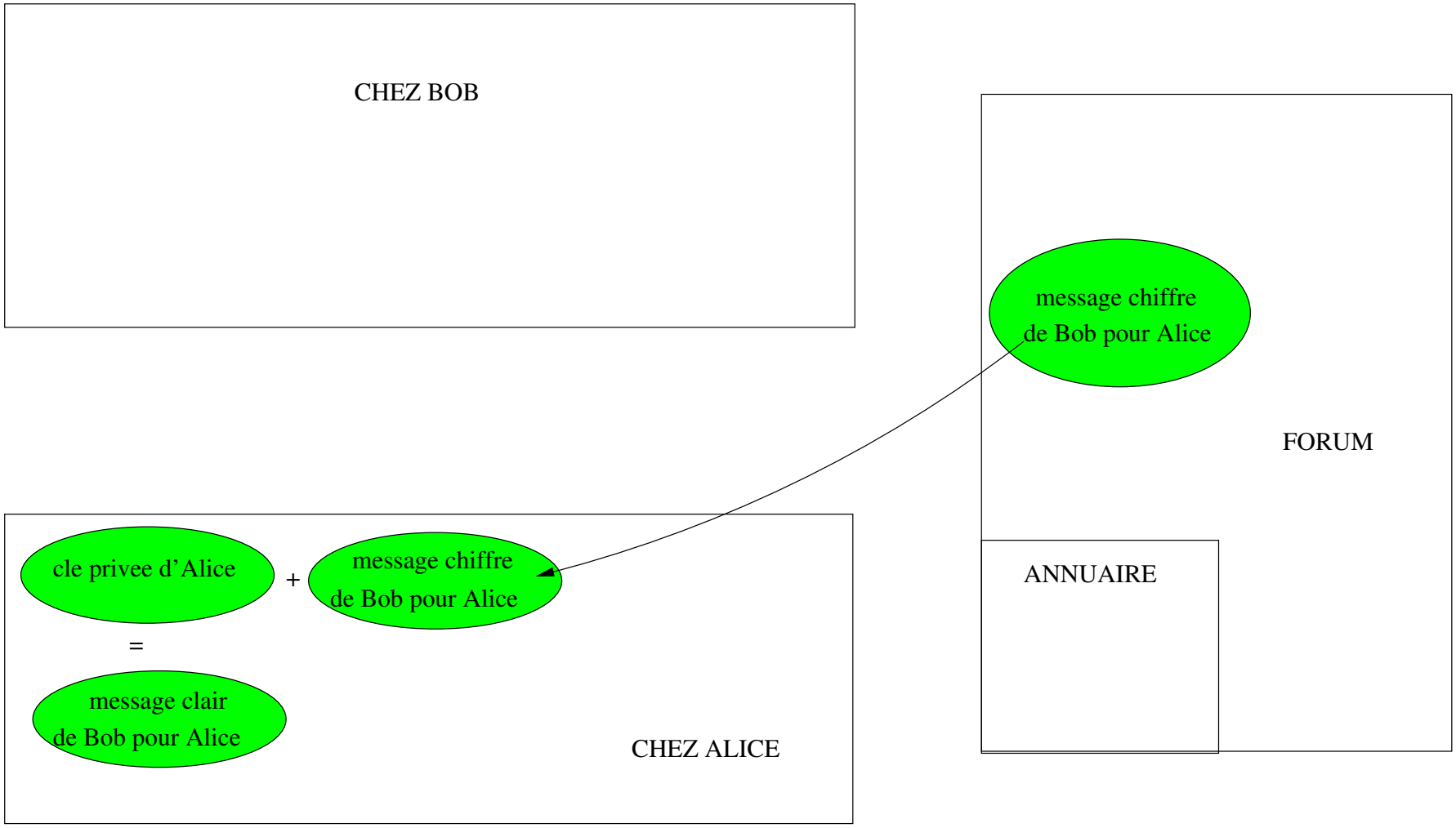
$$\mathbf{C} = \mathbf{M}^{\mathbf{E_A}} \mod \mathbf{N_A}$$

3. Bob envoie le cryptogramme **C** à Alice

Exemple

- Bob vérifie que son message $M = 4$ est acceptable : $4 < 187$
- Bob calcule le cryptogramme $C = 4^{13} \mod 187 = 174$
- Bob envoie le cryptogramme 174 à Alice

Alice reçoit un message secret



Alice reçoit un message secret

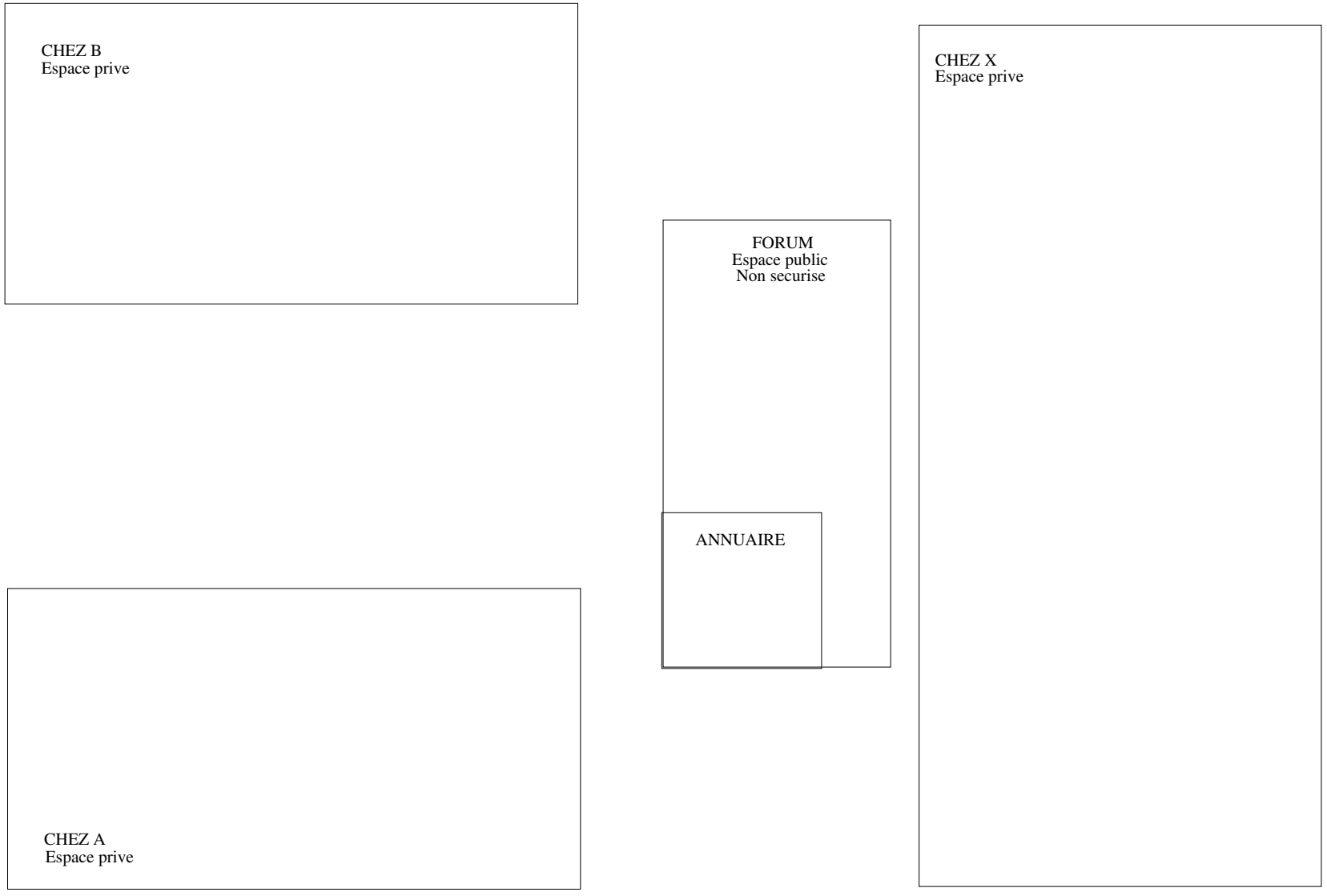
1. Alice reçoit le cryptogramme $\mathbf{C}$
2. Alice déchiffre le cryptogramme $\mathbf{C}$ en calculant
$$\mathbf{C}^{\mathbf{D_A}} \mod \mathbf{N_A}$$
3. Elle retrouve le message $\mathbf{M}$ envoyé par Bob

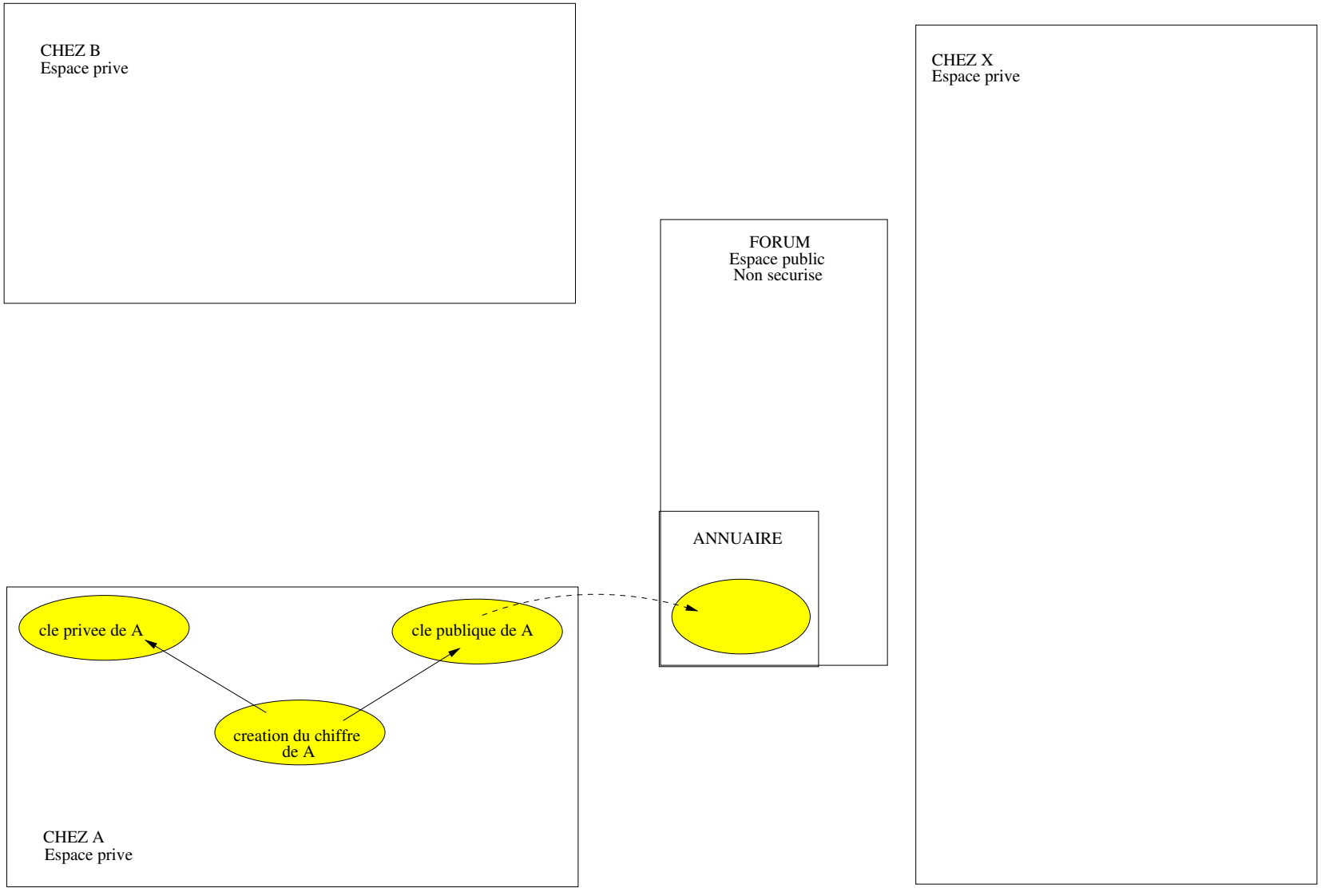
Exemple

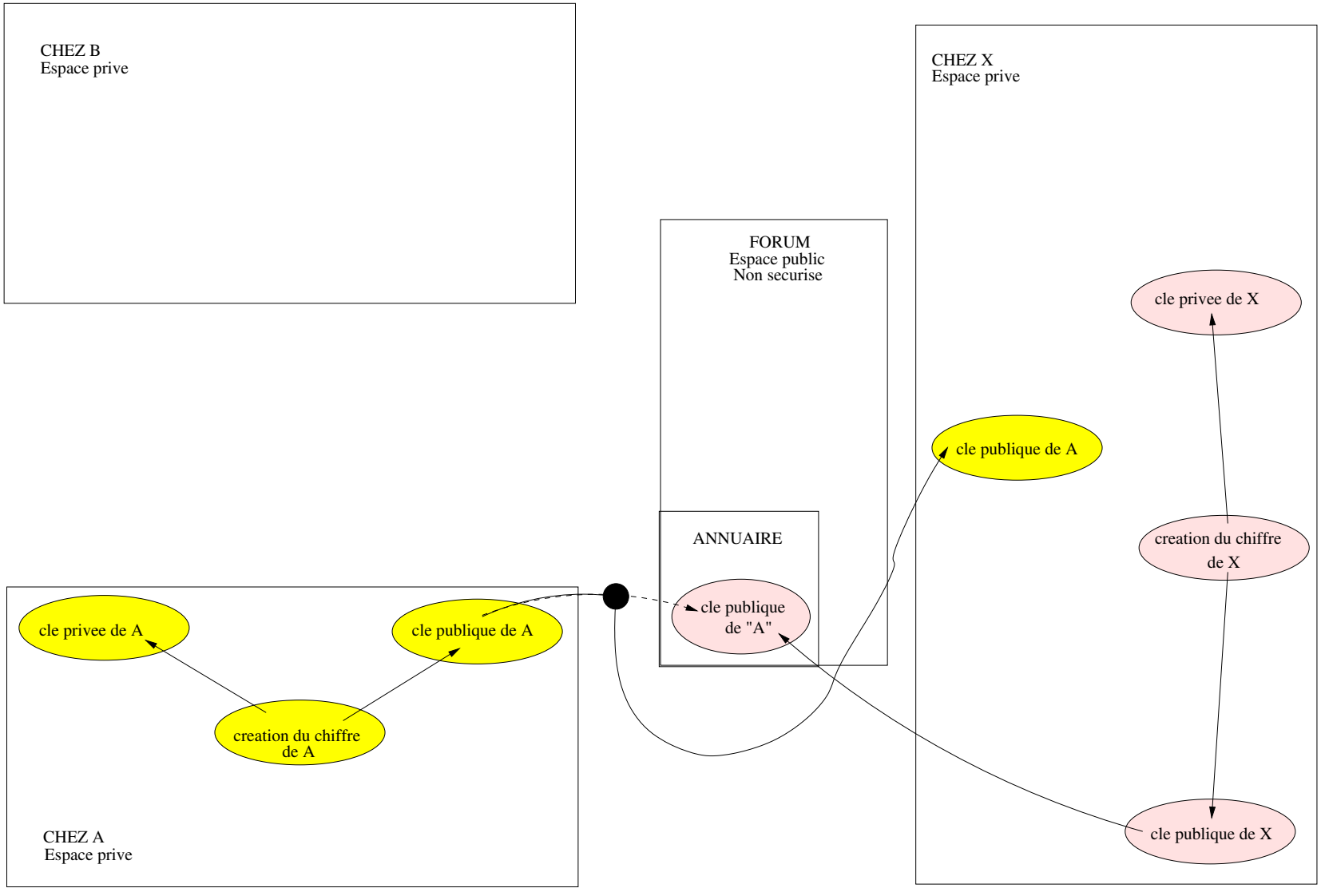
- Alice reçoit le cryptogramme $C = 174$
- Alice déchiffre le cryptogramme en calculant $M' = 174^{37} \mod 187 = 4$
- Alice a retrouvé le message $M = 4$ envoyé par Bob

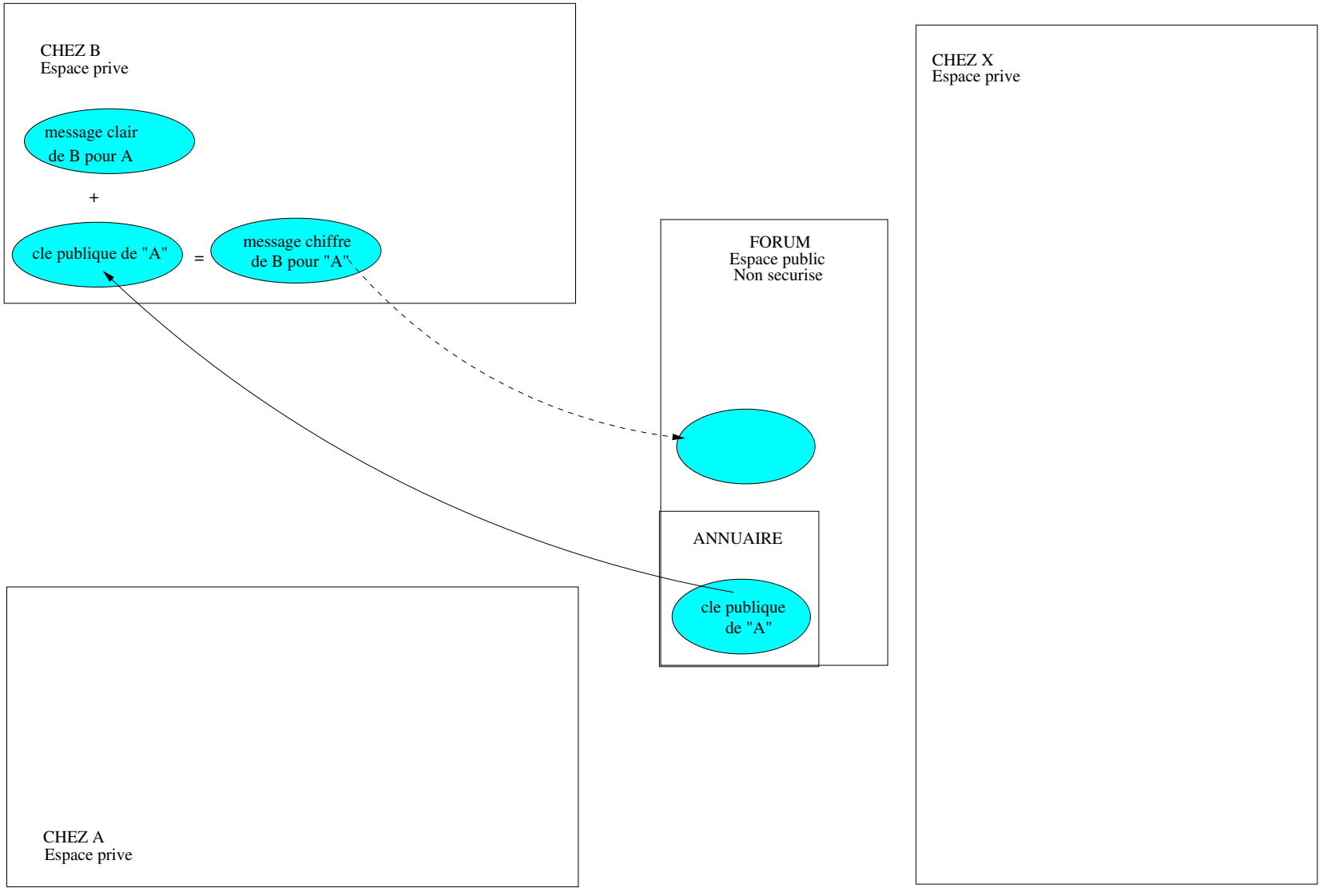
Contexte

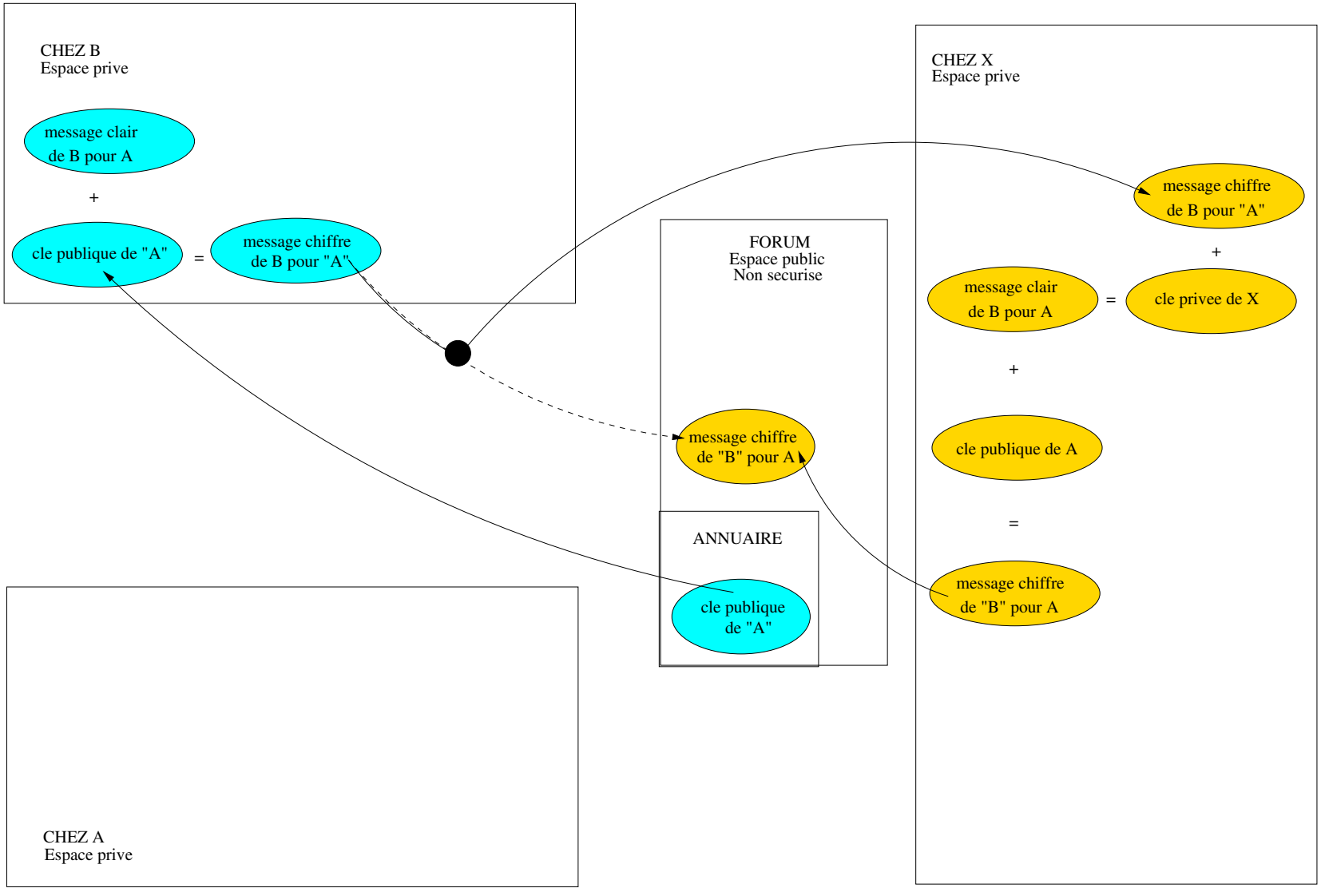
Dans cette partie, on présente une attaque des cryptosystèmes à clé publique qui permet d'espionner Alice et Bob à leur insu.

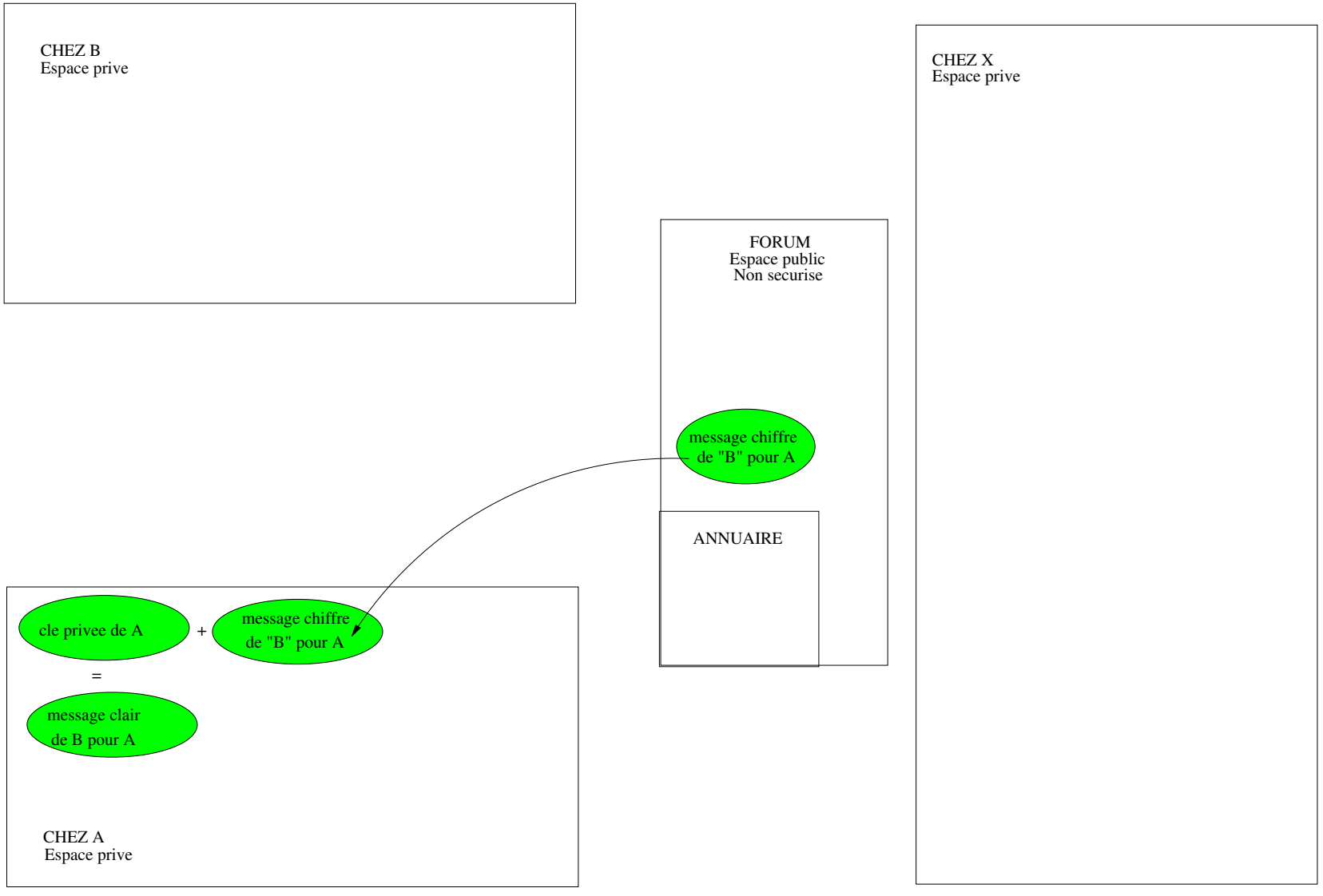

CHEZ B
Espace prive
CHEZ X
Espace prive
FORUM
Espace public
Non securise
ANNUAIRE
CHEZ A
Espace prive


CHEZ B
Espace prive
CHEZ X
Espace prive
FORUM
Espace public
Non securise
ANNUAIRE
cle privee de A
cle publique de A
creation du chiffre
de A
CHEZ A
Espace prive


CHEZ B
Espace prive
CHEZ X
Espace prive
FORUM
Espace public
Non securise
cle privee de X
cle publique de A
ANNUAIRE
creation du chiffre
de X
cle publique
de "A"
cle privee de A
cle publique de A
creation du chiffre
de A
cle publique de X
CHEZ A
Espace prive

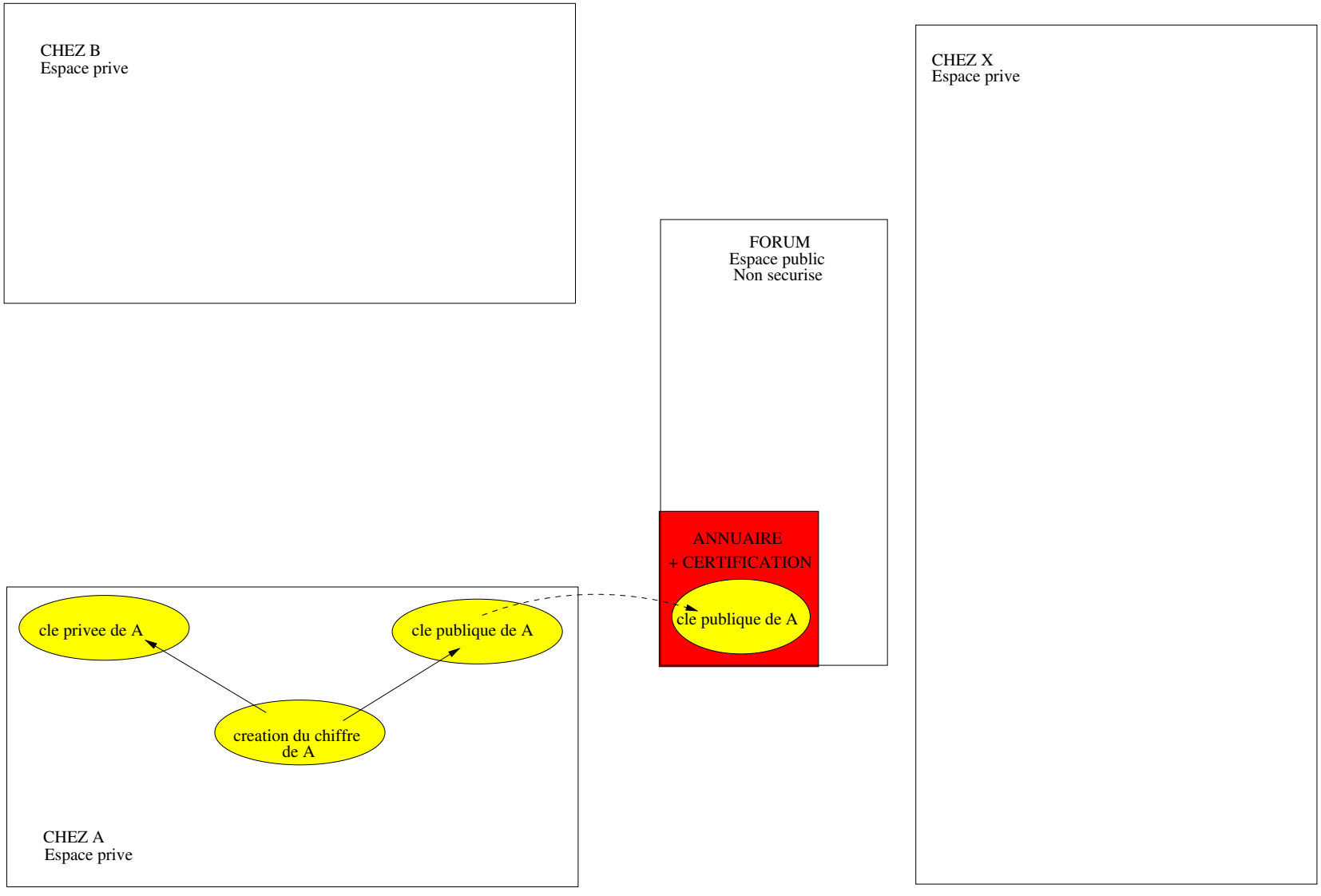

CHEZ B
Espace prive
message clair
de B pour A
+
cle publique de "A"
=
message chiffre
de B pour "A"
FORUM
Espace public
Non securise
ANNUAIRE
cle publique
de "A"
CHEZ X
Espace prive
CHEZ A
Espace prive


CHEZ B
Espace prive
message clair
de B pour A
+
cle publique de "A"
=
message chiffre
de B pour "A"
FORUM
Espace public
Non securise
message chiffre
de "B" pour A
ANNUAIRE
cle publique
de "A"
CHEZ X
Espace prive
message chiffre
de B pour "A"
+
message clair
de B pour A
=
cle privee de X
+
cle publique de A
=
message chiffre
de "B" pour A
CHEZ A
Espace prive


CHEZ B
Espace prive
CHEZ X
Espace prive
FORUM
Espace public
Non securise
message chiffre
de "B" pour A
ANNUAIRE
cle privee de A
+
message chiffre
de "B" pour A
=
message clair
de B pour A
CHEZ A
Espace prive

Certification

Pour éviter cette attaque, on fait appel à une autorité de certification qui garantit l'identité du dépositaire des clés publiques


CHEZ B
Espace prive
CHEZ X
Espace prive
FORUM
Espace public
Non securise
ANNUAIRE
+ CERTIFICATION
cle publique de A
cle privee de A
cle publique de A
creation du chiffre
de A
CHEZ A
Espace prive

À vous de jouer !

La clé publique RSA d'Alice est constituée du module $N_A = 187$ et du compliqueur $E_A = 13$, et sa clé privée du faciliteur $D_A = 37$. Bob souhaite envoyer le message $M = 4$ à Alice en utilisant la méthode RSA.
Malheureusement, Alice et Bob ignorent qu'Alice a subi une attaque de l'homme au centre de la part de Mr X., dont la clé publique RSA est constituée constituée du module $N_X = 91$ et du compliqueur $E_X = 5$, et la clé privée du faciliteur $D_X = 29$.

1. Quel est le calcul effectué par Bob pour chiffrer son message ?
2. Quels sont les calculs effectués par Mr X. ?
3. Quel est le calcul effectué par Alice pour déchiffrer le cryptogramme qu'elle a reçu ?

1. Bob chiffre son message avec la clé publique de Mr X. Il calcule donc $C = M^{E_X} \mod N_X$, soit $4^5 \mod 91 = 23$. Ensuite, il tente de déposer le cryptogramme C dans l'espace public.
2. Mr X. intercepte le cryptogramme C. Il le déchiffre avec sa propre clé privée, en calculant $C^{D_X} \mod N_X$, soit $23^{29} \mod 91 = 4$, et il retrouve le message M de Bob. Ensuite, Mr X. chiffre le message M avec la clé publique d'Alice, il calcule donc $M^{E_A} \mod N_A$, soit $C' = 4^{13} \mod 187 = 174$. Pour finir, il dépose le cryptogramme C' dans l'espace public.
3. Alice récupère le cryptogramme C' qui lui est destiné. Elle le déchiffre avec sa clé privée, en calculant $C^{D_A} \mod N_A$, soit $174^{37} \mod 187 = 4$, et elle retrouve bien le message M de Bob.

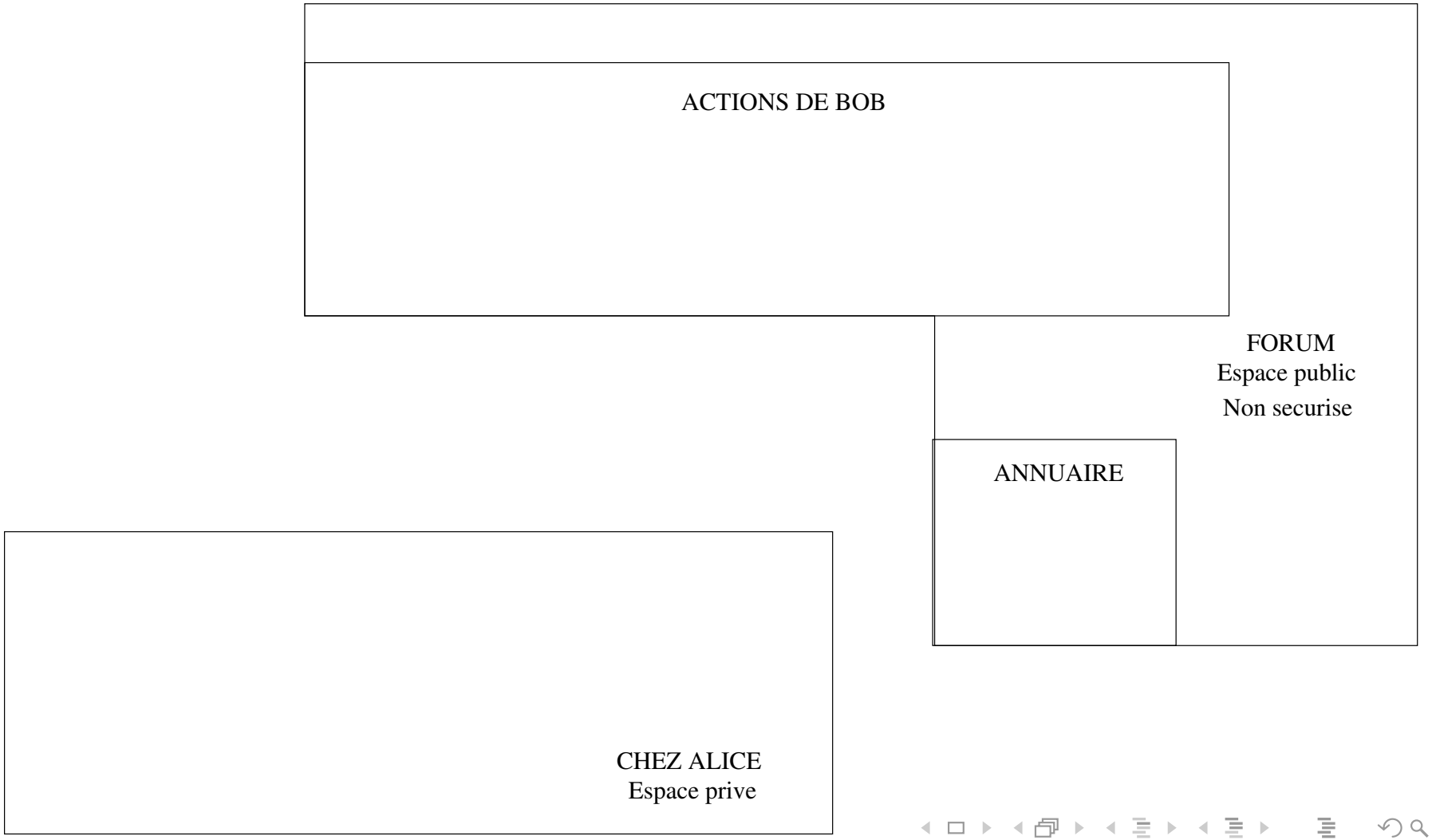
Une autre utilisation de RSA

Voici un exemple montrant une autre utilisation de la méthode RSA, largement répandue dans le domaine du commerce électronique.

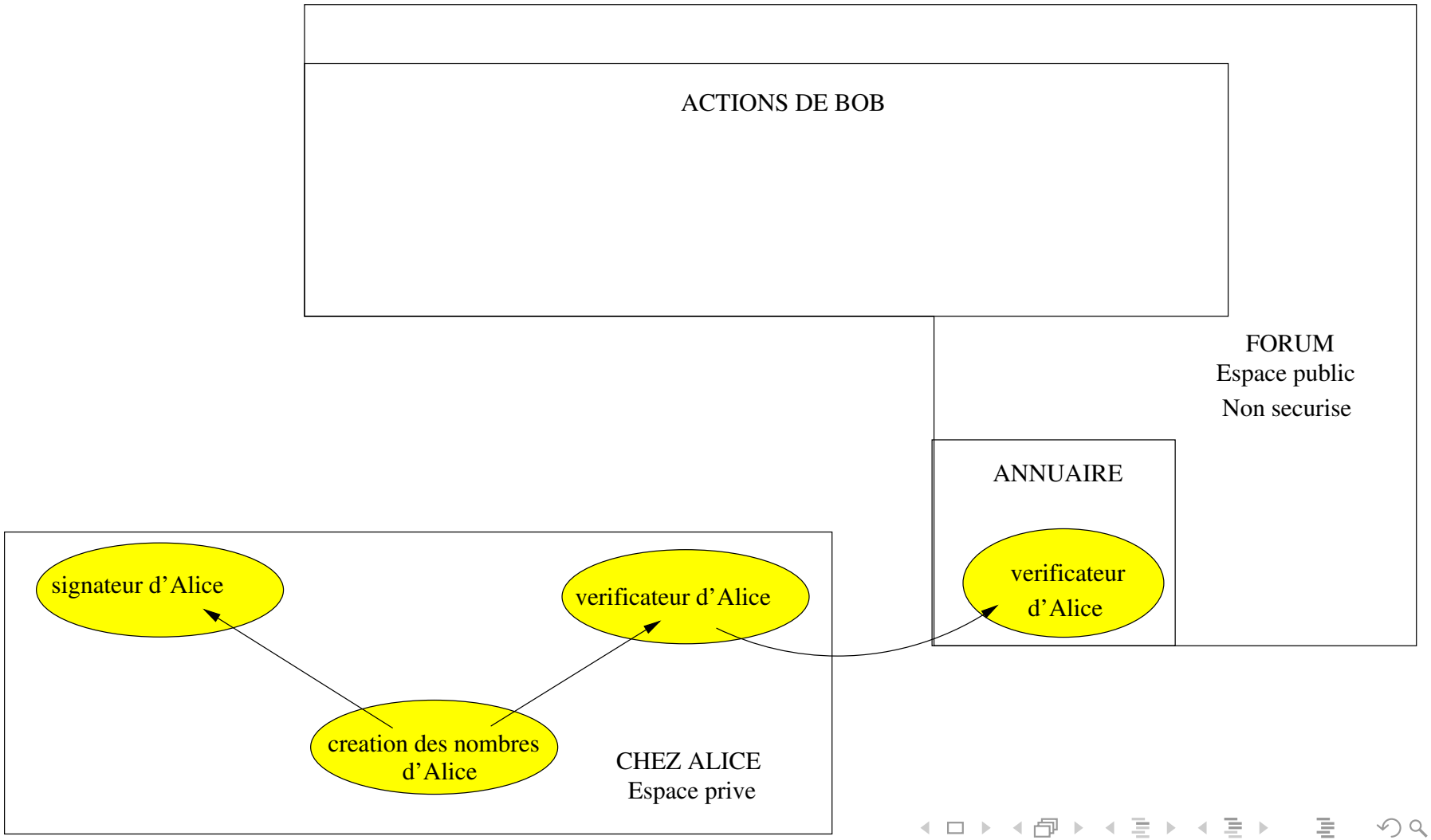
Exemple

Alice vote en ligne et transmet son vote à Bob à qui elle fait entière confiance pour organiser le décompte des bulletins. Par contre, Bob doit pouvoir être certain lorsqu'il reçoit le message d'Alice qu'il s'agit bien de son bulletin et pas de celui de quelqu'un qui se fait passer pour Alice. Le protocole utilisé est largement inspiré de celui du RSA pour le chiffrement/déchiffrement.

Préparation



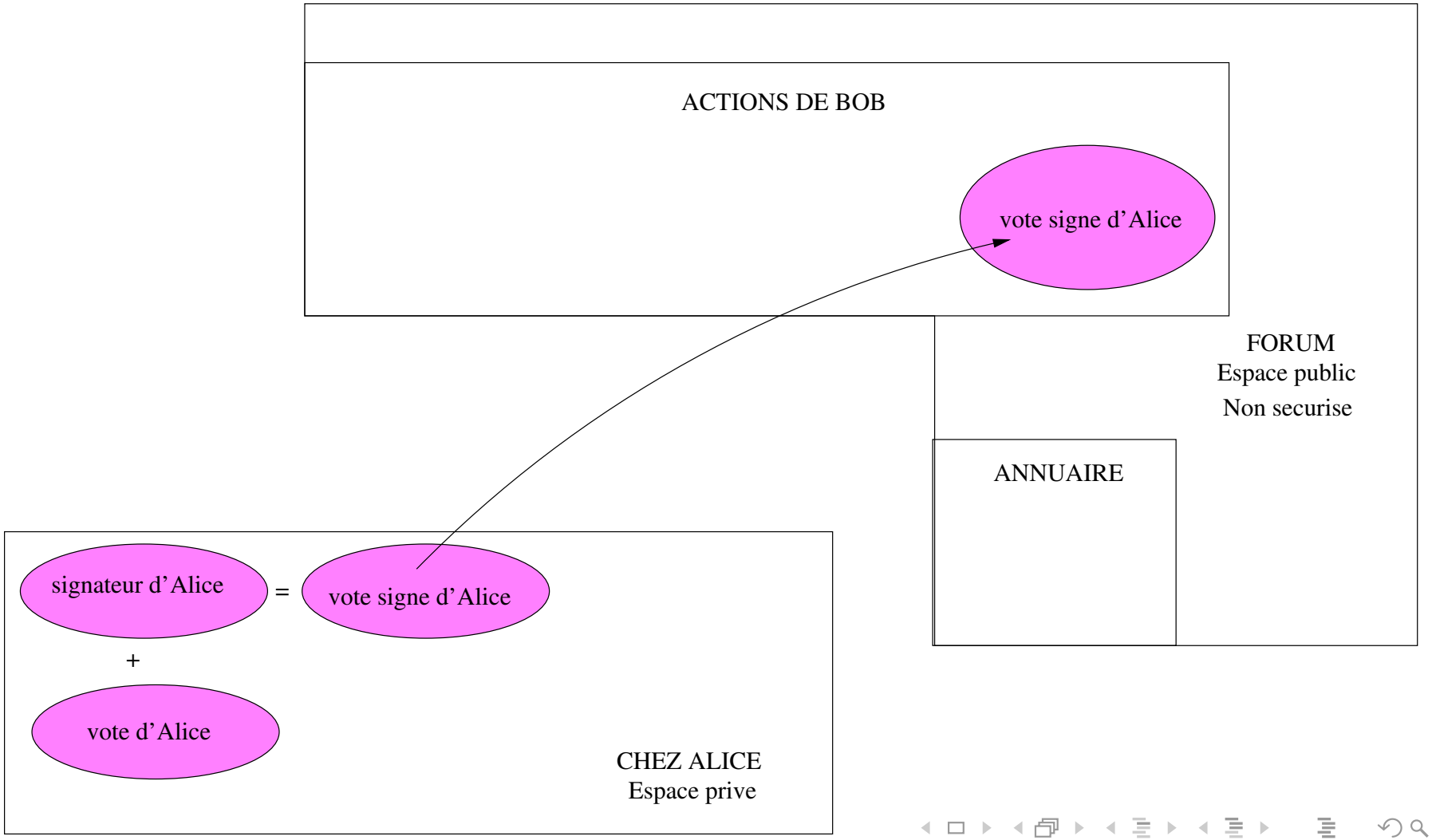
Préparation



Préparation

1. Alice choisit deux nombres premiers secrets p_A et q_A et calcule le **module** $\mathbf{N_A} = p_A \times q_A$
2. Alice calcule $\varphi(N_A) = (p_A - 1)(q_A - 1)$ et choisit un **vérificateur** $\mathbf{v_A}$ premier avec $\varphi(N_A)$
3. Alice calcule le **signateur** $\mathbf{s_A}$, inverse de v_A modulo $\varphi(N_A)$
4. Alice rend publics N_A et v_A mais garde privés s_A, et aussi $\varphi(N_A)$, p_A et q_A

Signature du vote



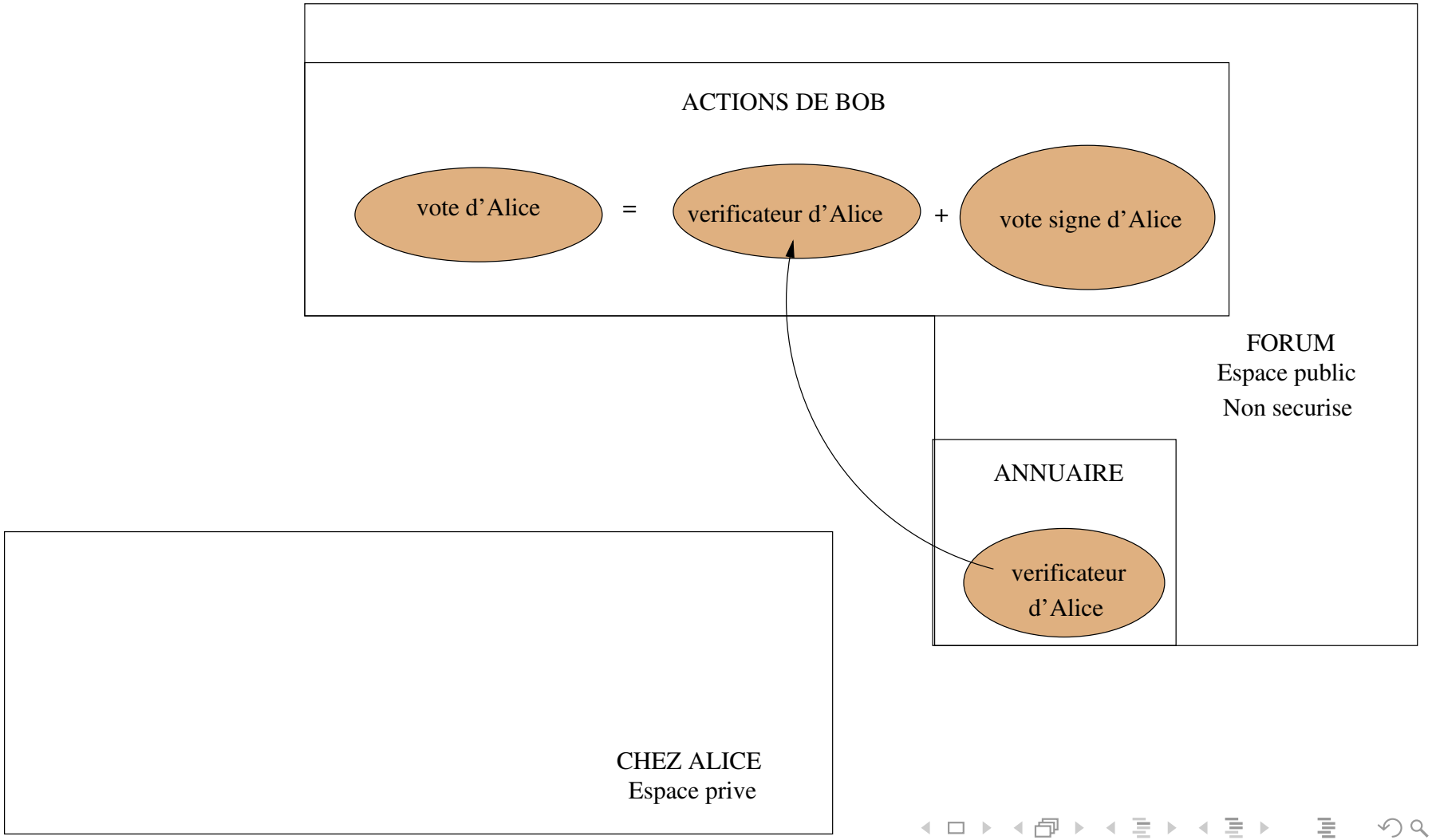
Signature du vote

1. Alice choisit son vote (message) $\mathbf{M} < \mathbf{N_A}$
2. Alice calcule le *signé* de ce message

$$\mathbf{S} = \mathbf{M}^{s_A} \mod \mathbf{N_A}$$

3. Alice envoie la paire $(\mathbf{M}, \mathbf{S})$ à Bob

Vérification du vote



Vérification du vote

1. Bob calcule

$$\mathbf{S}^{\mathbf{v_A}} \mod \mathbf{N_A}$$

2. Il vérifie que le résultat est égal à **M**.

À vous de jouer !

Alice choisit $p_A = 23$, $q_A = 47$ et $v_A = 675$. Argumentez que ses choix sont corrects et mettez en œuvre la partie **Préparation** du protocole de signature. (*Attention à bien détailler vos calculs*)

1. Les nombres p_A et q_A sont bien premiers.
   Alice calcule le module $N_A = 23 \times 47 = 1081$

2. Ensuite Alice calcule $\varphi(N_A) = (p_A - 1) \times (q_A - 1) = 1012$.
   Alice a choisi $v_A = 675$ comme vérificateur. Ce choix est correct si le vérificateur est premier avec 1012. Calculons le pgcd avec la méthode d'Euclide.

$$\begin{array}{rcrcrcr} & & & & & & 1012 \\ & & & & & & 675 \\ 1012 & - & 675 & \times & 1 & = & 337 \\ 675 & - & 337 & \times & 2 & = & 1 \\ 337 & - & 1 & \times & 337 & = & 0 \end{array}$$

3. Ensuite, Alice doit calculer l'inverse s_A de v_A modulo 1012. Il suffit donc d'étendre le calcul précédent d'une colonne.

$$\begin{array}{rcrcrcr} & & & & & & 0 \\ & & & & & & 1 \\ 0 & - & 1 & \times & 1 & = & -1 \\ 1 & - & (-1) & \times & 2 & = & 3 \end{array}$$

donc $3 \times 675 \equiv 1 \mod 1012$ soit $s_A = 3$.

4. Alice rend public uniquement le vérificateur v_A et le module N_A.

À vous de jouer !

Alice choisit de voter $V = 959$ car elle trouve que ce nombre est cool bien que non premier. Argumentez que ce choix est correct et mettez en œuvre la partie **Signature du vote** du protocole. (*Attention à bien détailler vos calculs*)

1. Le choix du message est correct car
   $V = 959 < 1081 = N_B$

2. Pour calculer le signé, Alice utilise son signateur $s_A = 3$. Elle calcule $959^3 \mod 1081$ en faisant une exponentiation rapide. Comme $3 =_{binaire} 11$ on fait le produit des valeurs correspondants à 1 et 0 élévations au carré successives pour obtenir le résultat.

puissances de 2	2^0	2^1
élévation au carré	959	831

   D'où un signé de $959 \times 831 = 232 \mod 1081$

3. Alice envoie la paire $(959, 232)$ à Bob

À vous de jouer !

Mettez en œuvre la partie **Vérification du vote** du protocole.
(*Attention à bien détailler vos calculs*)

1. Bob reçoit le couple $(M, S) = (959, 232)$.

2. Il calcule $S^{v_A} \mod 1081$ à l'aide d'une exponentiation rapide :

puissances de 2	2^0	2^1	2^2	2^3	2^4
élévations au carré	232	855	269	1015	32

puissances de2	2^5	2^6	2^7	2^8	2^9
élévations au carré	1024	6	36	215	823

Comme $675 =_{binaire} 1010100011$ on fait le produit des valeurs correspondants à $9, 7, 5, 1$ et 0 élévations au carré successives. D'où un résultat

$$M' = 823 \times 36 \times 1024 \times 855 \times 232 \mod 1081 = 959$$

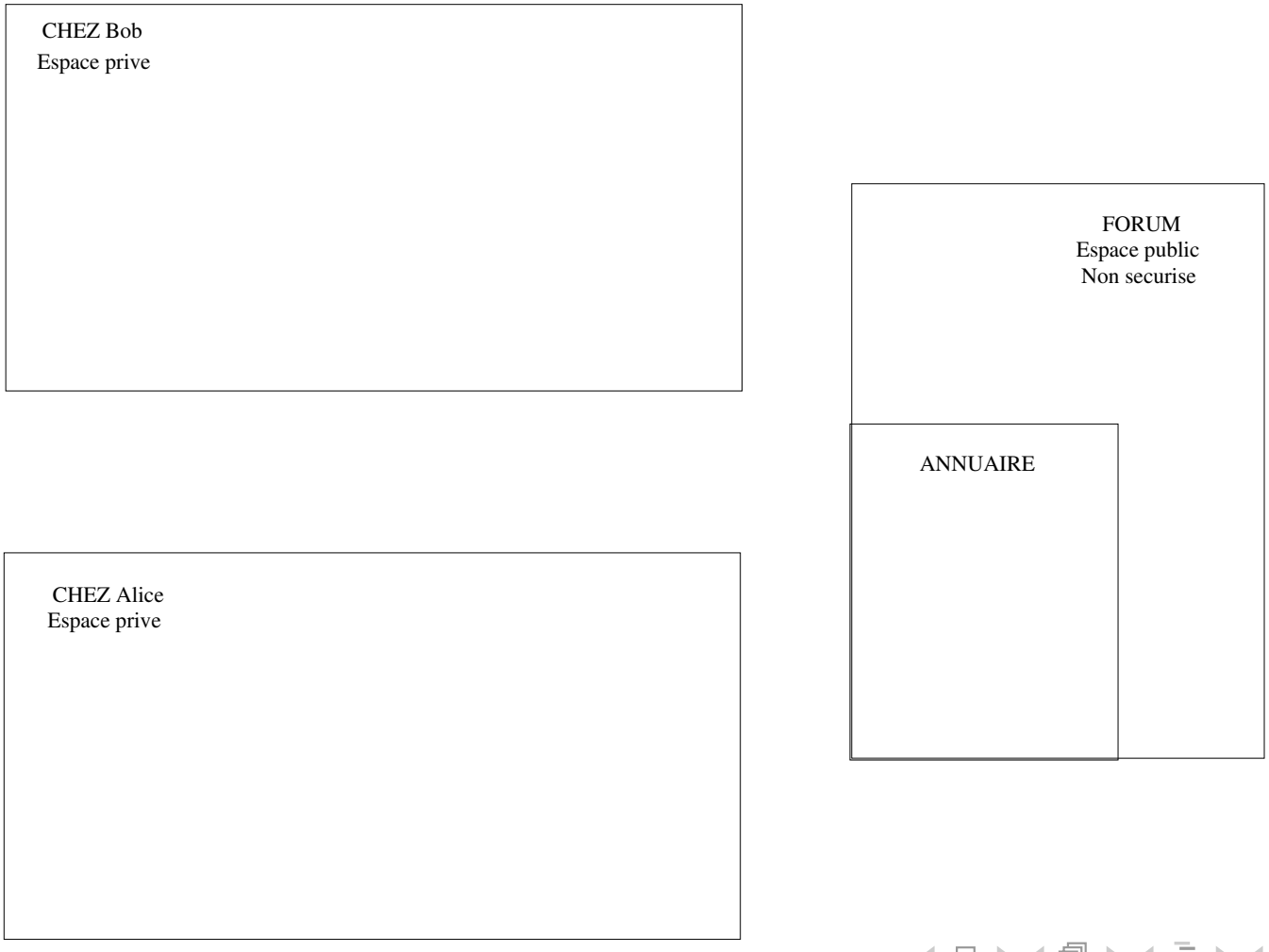
3. Bob retrouve bien le message d'Alice, ce qui garantit qu'Alice a bien envoyé un vote pour 959.

Chiffrer et signer en même temps ?

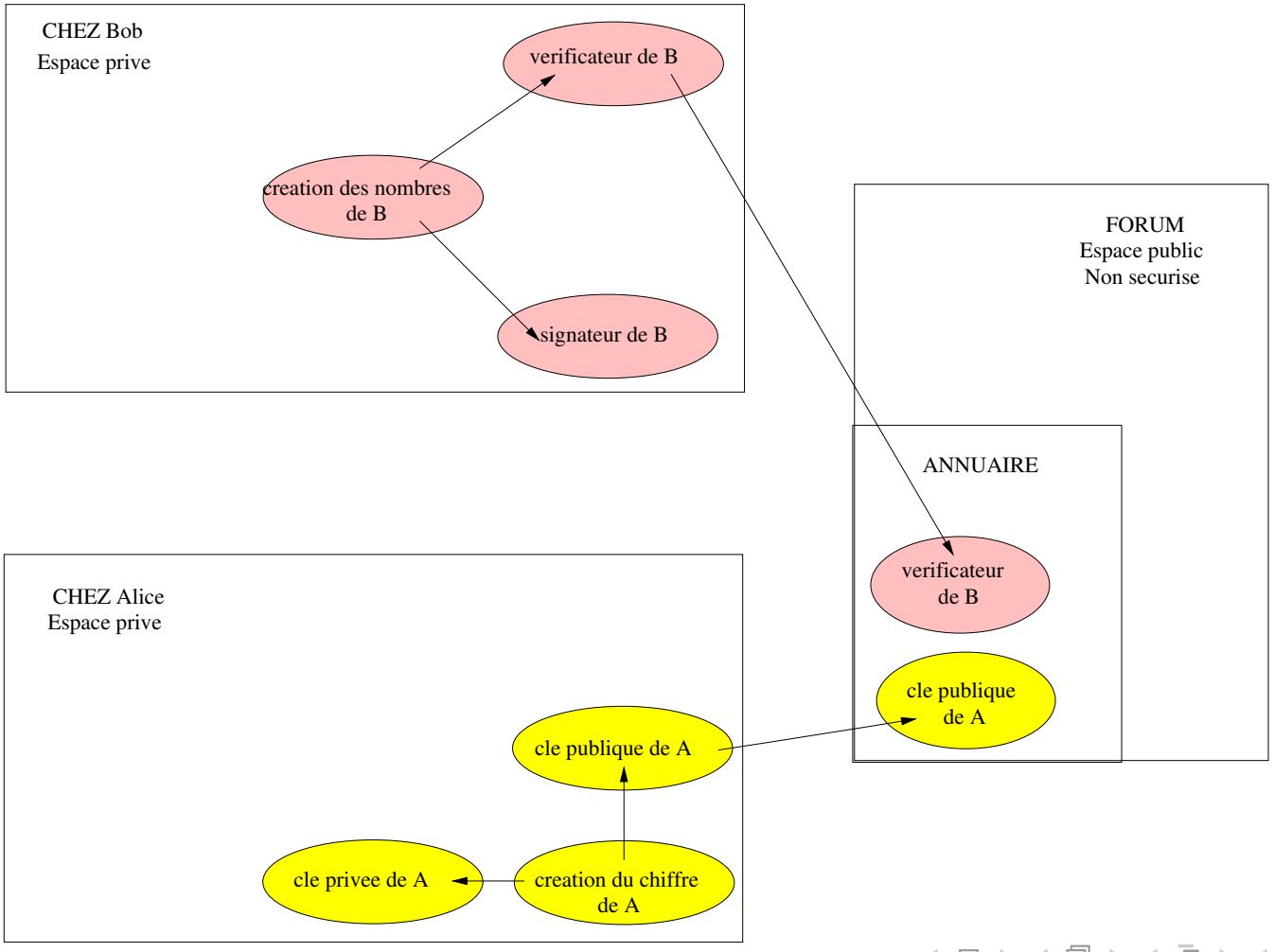
Voici une façon de combiner chiffrement et signature pour un même message :

- Bob envoie à Alice un message chiffré avec la clé publique d'Alice, puis signé avec son propre signateur (de Bob)
- Alice vérifie que l'expéditeur est bien Bob, en utilisant le vérificateur de Bob, puis elle déchiffre le message en utilisant sa propre clé privée (d'Alice)

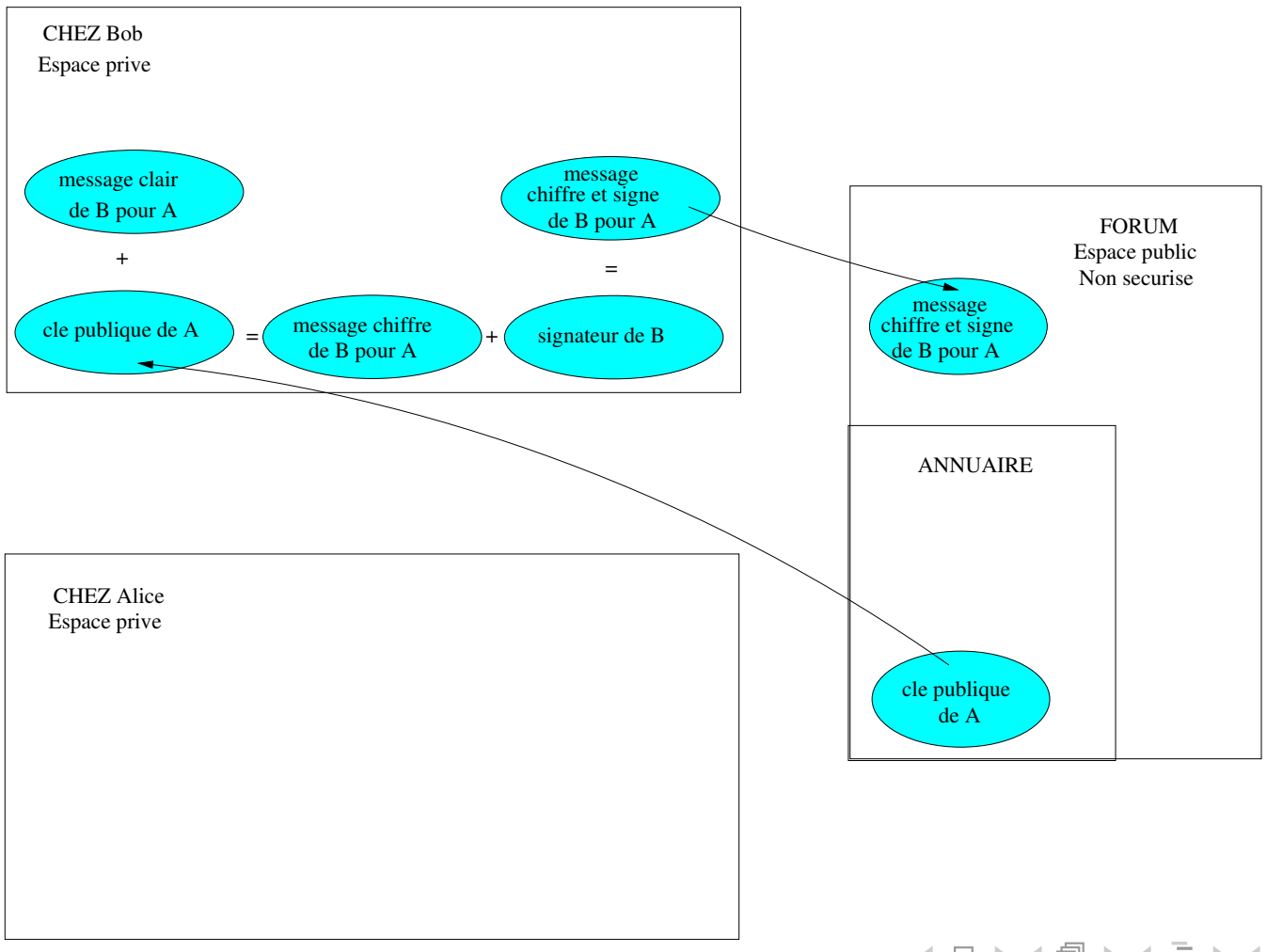
Contexte


CHEZ Bob
Espace prive
FORUM
Espace public
Non securise
ANNUAIRE
CHEZ Alice
Espace prive

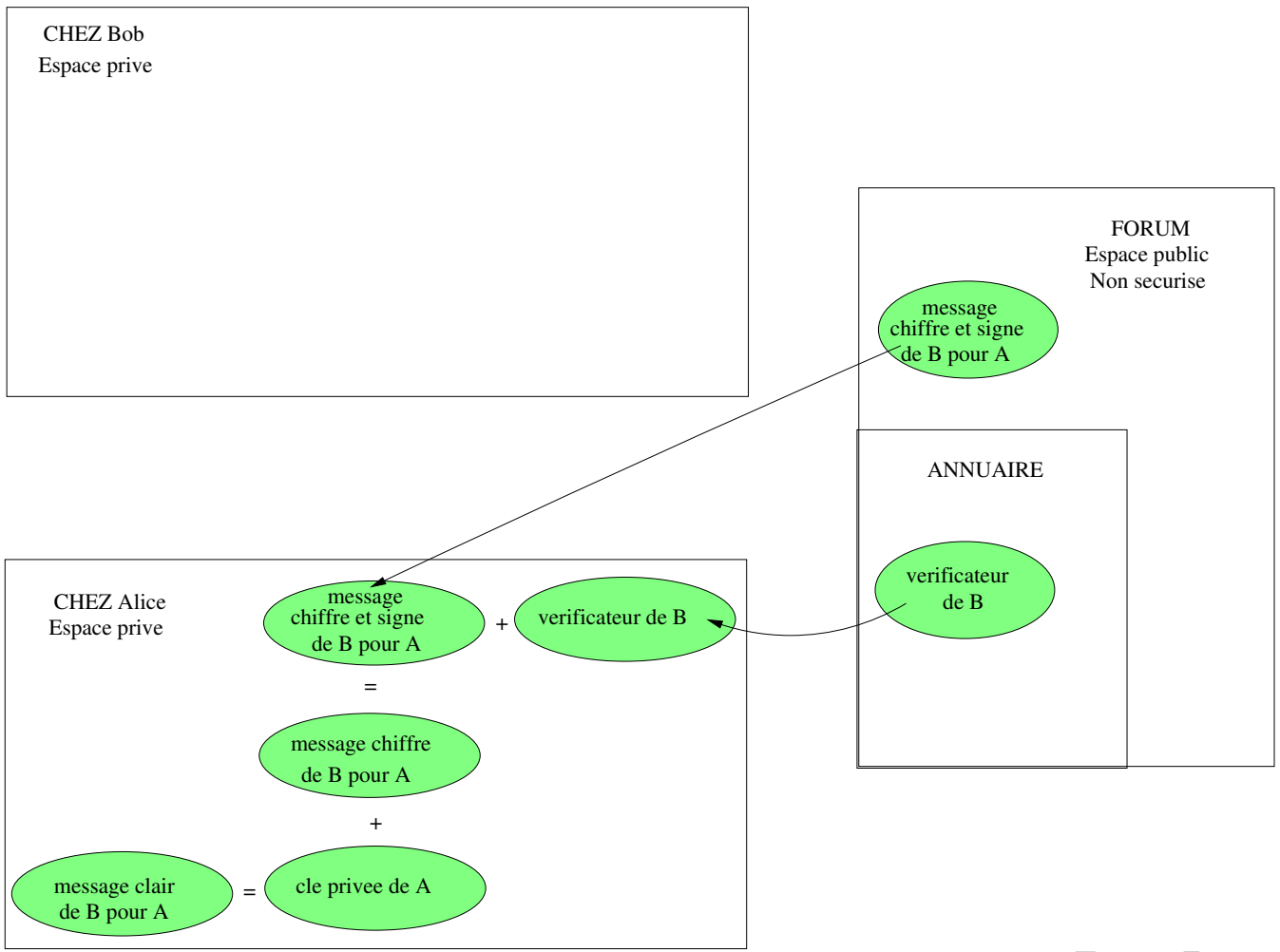
Préparation



Bob chiffre un message pour Alice et le signe



Alice reçoit un message chiffré et signé



Le retour de Mr X.

- On a vu comment se prémunir contre les attaques du type « homme au centre »
- On a dit que la sécurité théorique de la méthode RSA repose sur la difficulté de factoriser un produit de deux grands nombres premiers inconnus.
- Cependant, personne ne sait si une attaque de RSA qui ne reposerait pas sur la factorisation ne serait pas efficace !
- Par ailleurs, voici un exemple montrant qu'une mauvaise utilisation de RSA peut créer des failles de sécurité.

Exemple

Pour leurs chiffres RSA respectifs, Bob et Charlie ont choisi le même module $N = 221$. Le compliqueur de Bob est $E_B = 169$ et le compliqueur de Charlie est $E_C = 83$. Mr X a découvert qu'Alice a envoyé le même message M sous la forme du cryptogramme $C_B = 29$ à Bob et $C_C = 74$ à Charlie.

1. Trouver deux nombres positifs U et V tels que $E_B U - E_C V = 1$.
2. Montrer que $M^{E_B U} = M^{E_C V} \times M$.
3. Calculer $(C_B)^U \mod N$ et $(C_C)^V \mod N$.
4. Calculer $\left((C_C)^V\right)^{-1} \mod N$.
5. Expliquez comment Mr X peut découvrir quel est le message M.
6. Quelle est l'erreur commise par Bob et Charlie ?

1. Si les nombres U et V existent, c'est-à-dire si E_B et E_C sont premiers entre eux, on peut les calculer en utilisant l'algorithme d'Euclide étendu.

$$\begin{array}{r|r|r} 169 & 1 & 0 \\ 83 & 0 & 1 \\ 169 - 83 \times 2 = 3 & 1 - 0 \times 2 = 1 & 0 - 1 \times 2 = -2 \\ 83 - 3 \times 27 = 2 & 0 - 1 \times 27 = -27 & 1 - (-2) \times 27 = 55 \\ 3 - 2 \times 1 = 1 & 1 - (-27) \times 1 = 28 & -2 - 55 \times 1 = -57 \\ 2 - 1 \times 2 = 0 & & \end{array}$$

On a donc

$$169 \times 28 - 83 \times 57 = 1$$

d'où $U = 28$ et $V = 57$

2. On vient de voir que $E_B U - E_C V = 1$, ce qui s'écrit aussi $E_B U = E_C V + 1$. On peut donc écrire $M^{E_B U} = M^{E_C V + 1} = M^{E_C V} \times M$ (c'est bien $=$ et pas $\equiv$)
3. Il suffit de faire le calcul, on trouve

$$(C_B)^U \mod N = 29^{28} \mod 221 \equiv 55$$

$$(C_C)^V \mod N = 74^{57} \mod 221 \equiv 79$$

4. On calcule de même

$$\left((C_C)^V\right)^{-1} \mod N = 79^{-1} \mod 221 \equiv 14$$

5. On a vu que $M^{E_B U} = M^{E_C V} \times M$. En passant au modulo, on obtient

$$M^{E_B U} \equiv M^{E_C V} \times M \mod N$$

Or, pour chiffrer son message M, Alice a calculé $C_B = M^{E_B} \mod N$ et $C_C = M^{E_C} \mod N$. Par conséquent, on peut écrire

$$(C_B)^U \equiv (C_C)^V \times M \mod N$$

En multipliant les deux membres par $\left((C_C)^V\right)^{-1} \mod N$, on obtient

$$\left((C_C)^V\right)^{-1} \times (C_B)^U \equiv M \mod N$$

Il ne reste plus qu'à calculer

$$M = 14 \times 55 \mod 221 = 107$$

Mr X. a découvert que le message envoyé par Alice était $M = 107$

6. L'erreur de Bob et Charlie est d'avoir choisi le même module (et aussi des compliqueurs premiers entre eux...) Et en plus Alice leur a envoyé le même message...

La factorisation

- Étant donné un entier n, il s'agit simplement de trouver un diviseur de n.
- On sait qu'il suffit de tester tous les nombres premiers jusqu'à $\sqrt{n}$.
- Ce n'est pas très difficile en théorie, mais en pratique le problème est surtout de disposer de suffisamment de temps.

Pourquoi la factorisation prend-elle du temps ?

L'objectif de cette partie est d'estimer le nombre d'essais nécessaires (dans le pire des cas) pour trouver un diviseur d d'un entier n, en fonction du nombre de chiffres de l'écriture décimale de n.

Notation

Pour tout $x \geq 1$, on note $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x.
Ainsi, on a $\pi(2) = 1$, $\pi(3) = \pi(4) = 2$, $\pi(5) = \pi(6) = 3$, etc.

- Que valent $\pi(50)$ et $\pi(100)$?
  - On compte sur la table des nombres premiers :
  - $\pi(50) = 15$ et $\pi(100) = 25$

- Que peut-on dire de la limite de $\pi(x)$ lorsque x tend vers $+\infty$?
  - Il y a une infinité de nombres premiers.
  - Par conséquent, on a $\lim_{+\infty} \pi(x) = +\infty$

- Soit n un entier inférieur à 10000 qui n'est pas premier. Combien de nombres d faut-il tester au maximum pour trouver un diviseur de n ?
  - On est sûr de trouver (au moins) un diviseur premier $\leq \sqrt{n} < \sqrt{10000} = 100$, donc il suffit de tester tous les nombres premiers inférieurs à $\sqrt{n} < 100$

- Quel rapport avec la fonction $\pi(x)$?
  - Il y a $\pi(\sqrt{n}) \leq \pi(100)$ nombres premiers inférieurs à $\sqrt{n}$
  - Une borne supérieure sur le nombre d'essais à effectuer est donc $\pi(100)$

On admet qu'on a l'encadrement suivant pour $x \geq 55$:

$$\frac{x}{\ln x + 2} < \pi(x) < \frac{x}{\ln x - 4}$$

- Vérifier cette propriété pour $n = 546$.
  - Sur la table des nombres premiers, on compte $\pi(546) = 100$
  - On calcule $\ln 546 \approx 6,3$
  - On en déduit $\frac{n}{\ln n + 2} = \frac{546}{8,3} \approx 66$ et $\frac{n}{\ln n - 4} = \frac{546}{2,3} \approx 237$
  - L'encadrement obtenu

    $$66 < 100 < 237$$

    est correct, quoique pas très précis

Déterminer un majorant du nombre α d'essais à effectuer pour trouver un diviseur d'un entier N non premier de 10, 50, et 100 chiffres décimaux.

- On rappelle que si k est le nombre de chiffres de l'écriture décimale d'un entier n, alors $\ln n \approx 2,3 \times (k-1)$.
  - D'après ce qu'on a vu
    $$\alpha \leq \pi(\sqrt{N}) < \frac{\sqrt{N}}{\ln \sqrt{N} - 4} = \frac{\sqrt{N}}{\frac{1}{2} \ln N - 4}$$
  - Pour un nombre N de $k = 10$ chiffres, on a $10^9 \leq N < 10^{10}$, donc $\alpha < \frac{10^5}{\frac{2,3 \times 9}{2} - 4} \approx 19230$
  - Pour $k = 50$ chiffres, on a $\alpha < \frac{10^{25}}{\frac{2,3 \times 49}{2} - 4} \approx 1,91\ 10^{23}$
  - Pour $k = 100$ chiffres, on a $\alpha < \frac{10^{50}}{\frac{2,3 \times 99}{2} - 4} \approx 9,1\ 10^{47}$

- Actuellement, on recommande d'utiliser des clés RSA de 2048 bits, c'est-à-dire environ 700 chiffres décimaux. Conclusion ? À titre de comparaison, on estime que le nombre d'atomes de la Terre est d'environ 10^{50}, et le nombre d'atomes dans l'univers de l'ordre de 10^{80}.

- À retenir : la factorisation des grands nombres prends du temps parce-qu'il y a énormément de diviseurs potentiels

Consignes pour l'examen

- Calculatrices fortement recommandées
- Téléphones portables interdits, même pour savoir l'heure
- Formulaire autorisé
  - Feuille A4
  - Recto-verso
  - Manuscrit
  - Non photocopié
  - Signé

Au programme à l'examen

- Arithmétique
  - Calcul modulaire
  - Inverse modulaire
  - Identité de Bézout
  - Équations $ax = b$
  - Utilisation du théorème de Fermat
- Chiffrements affines
- Méthodes Sac-à-dos et RSA
  - Fabriquer les clés
  - Chiffrer
  - Déchiffrer

PAS au programme à l'examen

- Équations diophantiennes
- Chiffrements par substitution et analyse des fréquences
- Sécurité et signature

FIN