Principe de la cryptographie à clé publique

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

1A - IUT Info - Clermont 1

Arithmétique et Cryptographie

Année 2011-2012

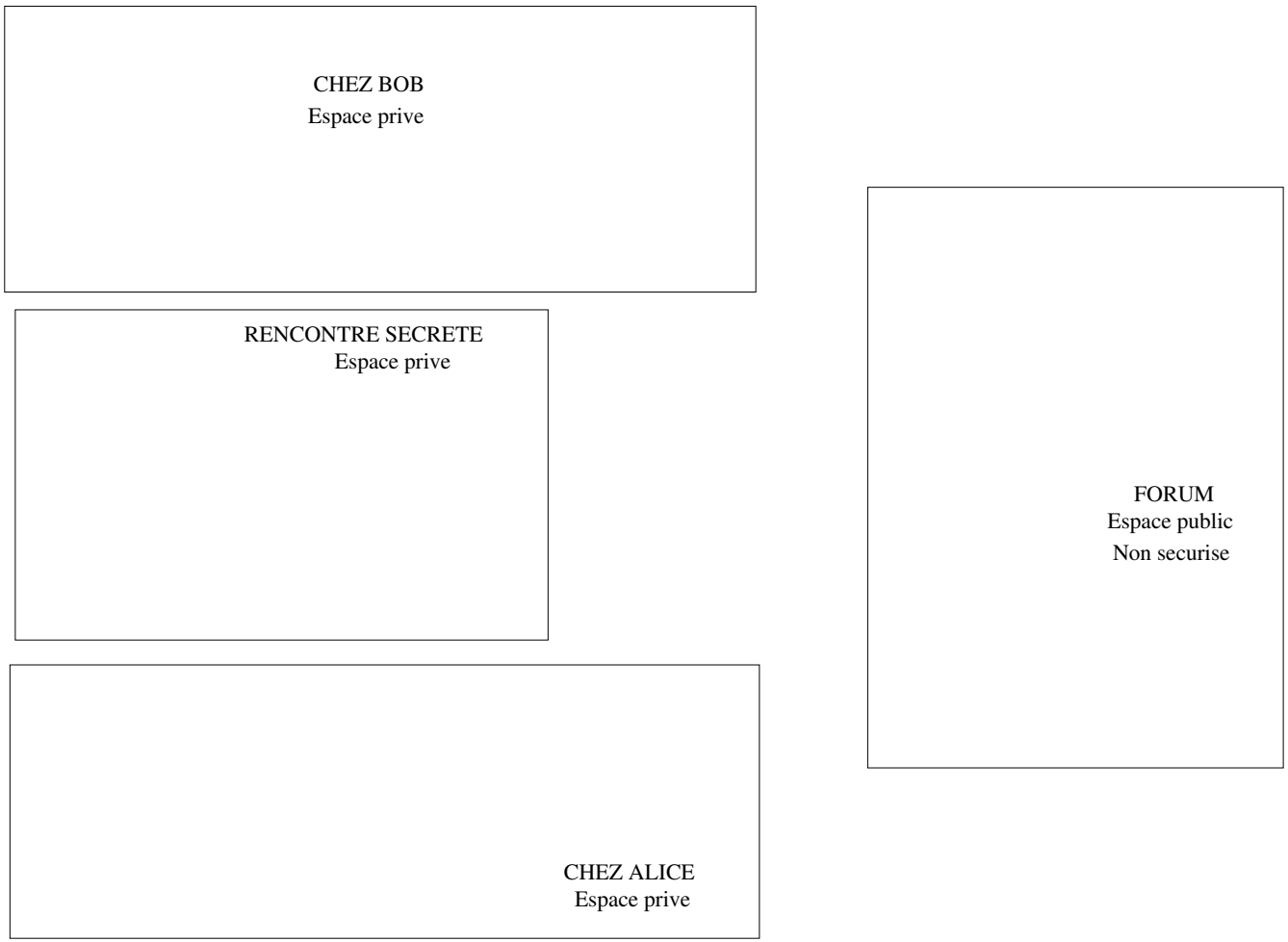
1 Cryptosystème à clés secrètes

2 Cryptosystème à clé publique

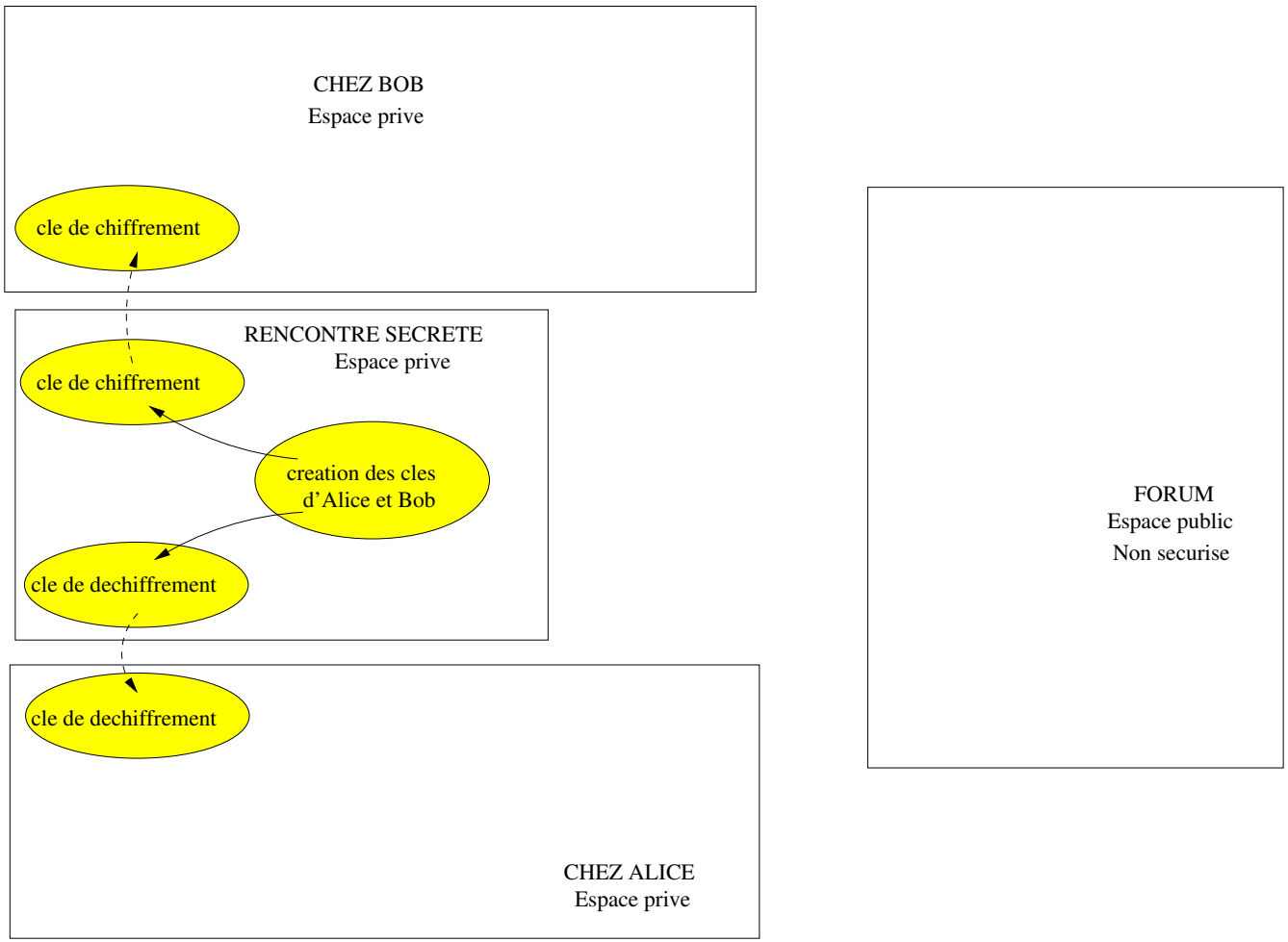
Cryptographie à clé secrète

- Méthodes utilisées jusqu'aux années 1970
- Notion fondamentale
  - Chaque correspondant est en possession de deux clés secrètes, l'une utilisée pour chiffrer et l'autre pour déchiffrer
- Inconvénient majeur
  - Nécessite un canal sûr pour communiquer ces clés, et donc un contact préalable

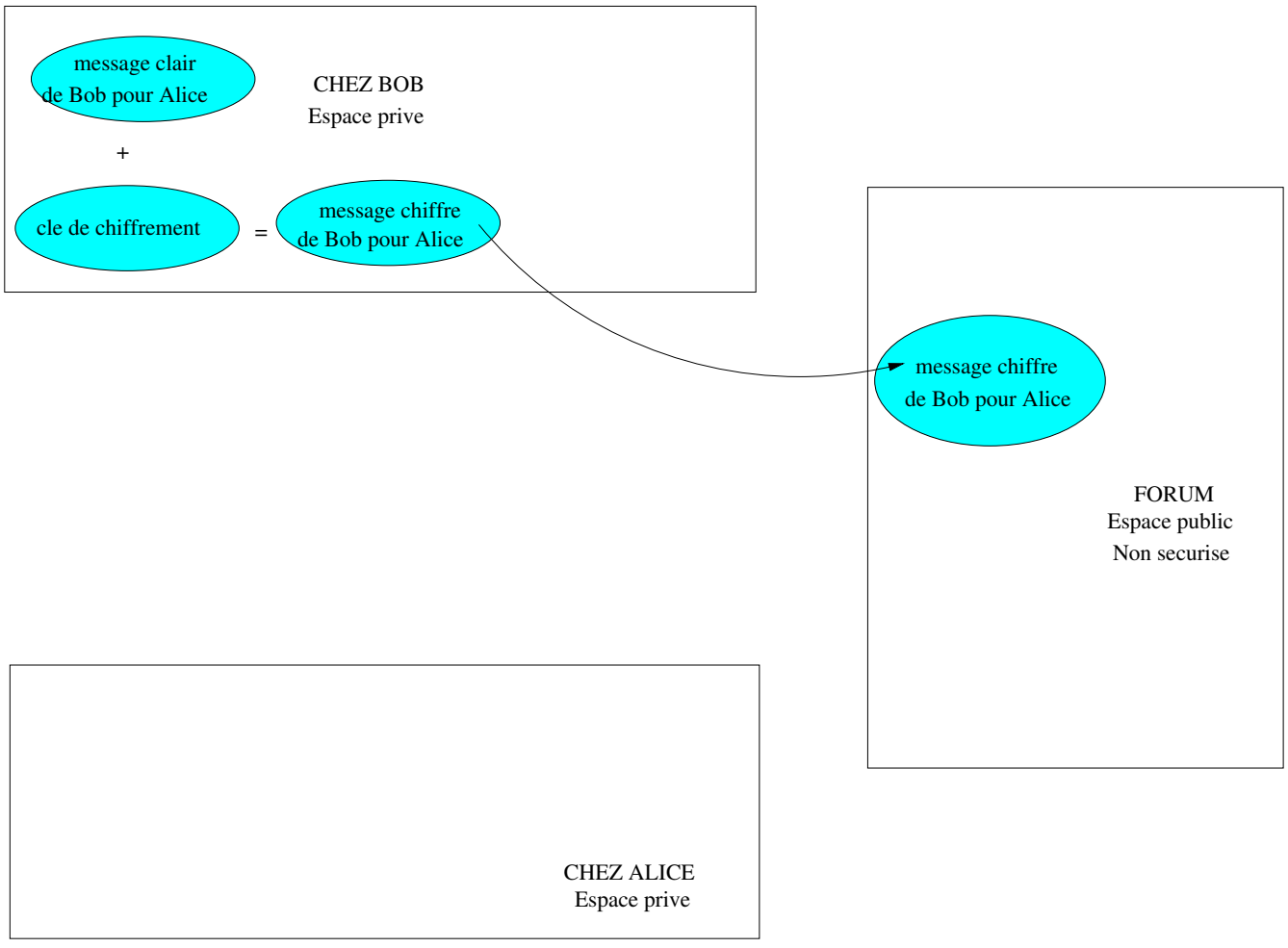
Contexte


CHEZ BOB
Espace prive
RENCONTRE SECRETE
Espace prive
CHEZ ALICE
Espace prive
FORUM
Espace public
Non securise

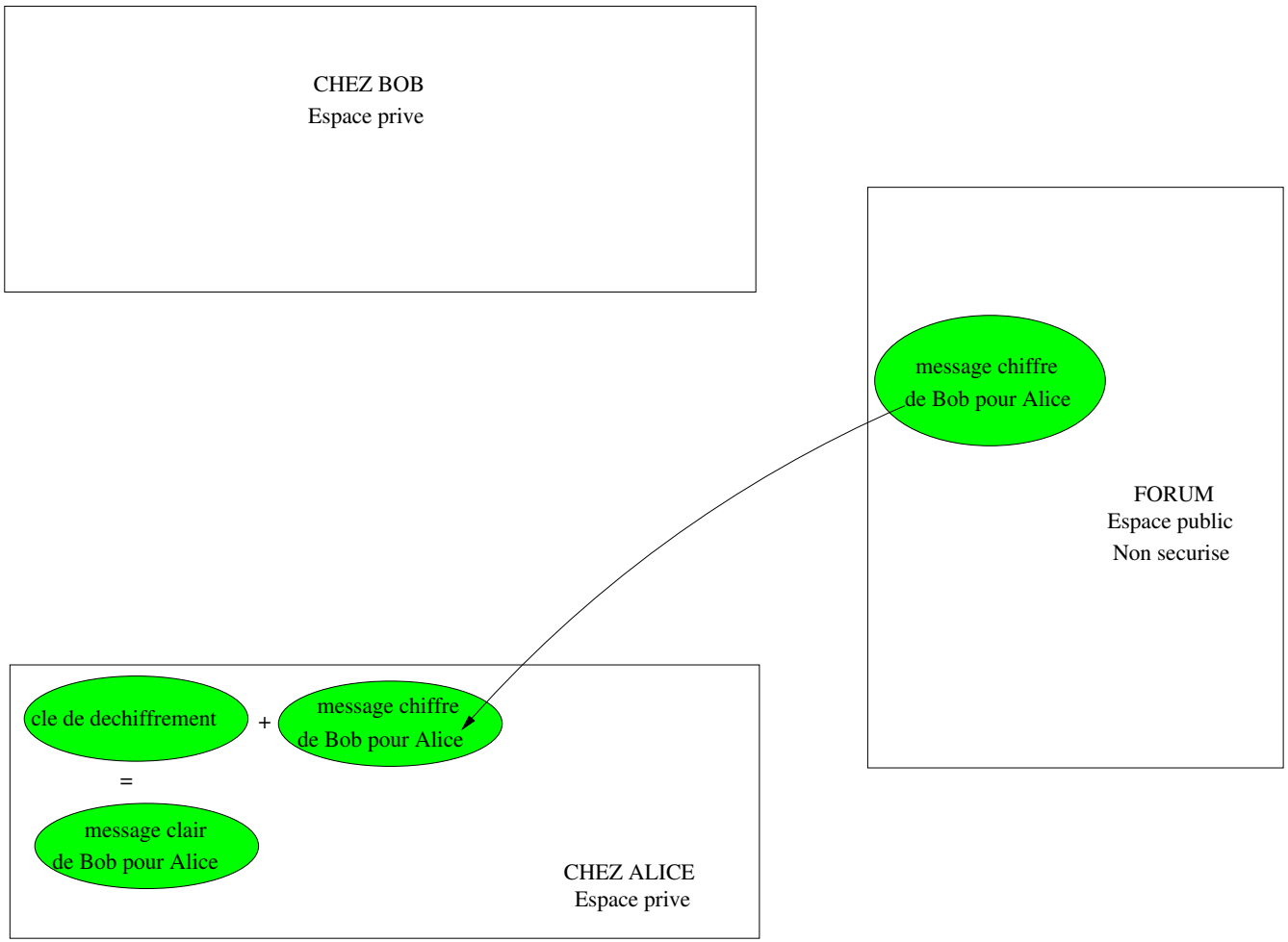
Alice et Bob se rencontrent en secret



Bob envoie un message secret à Alice



Alice reçoit un message secret



1 Cryptosystème à clés secrètes

2 Cryptosystème à clé publique

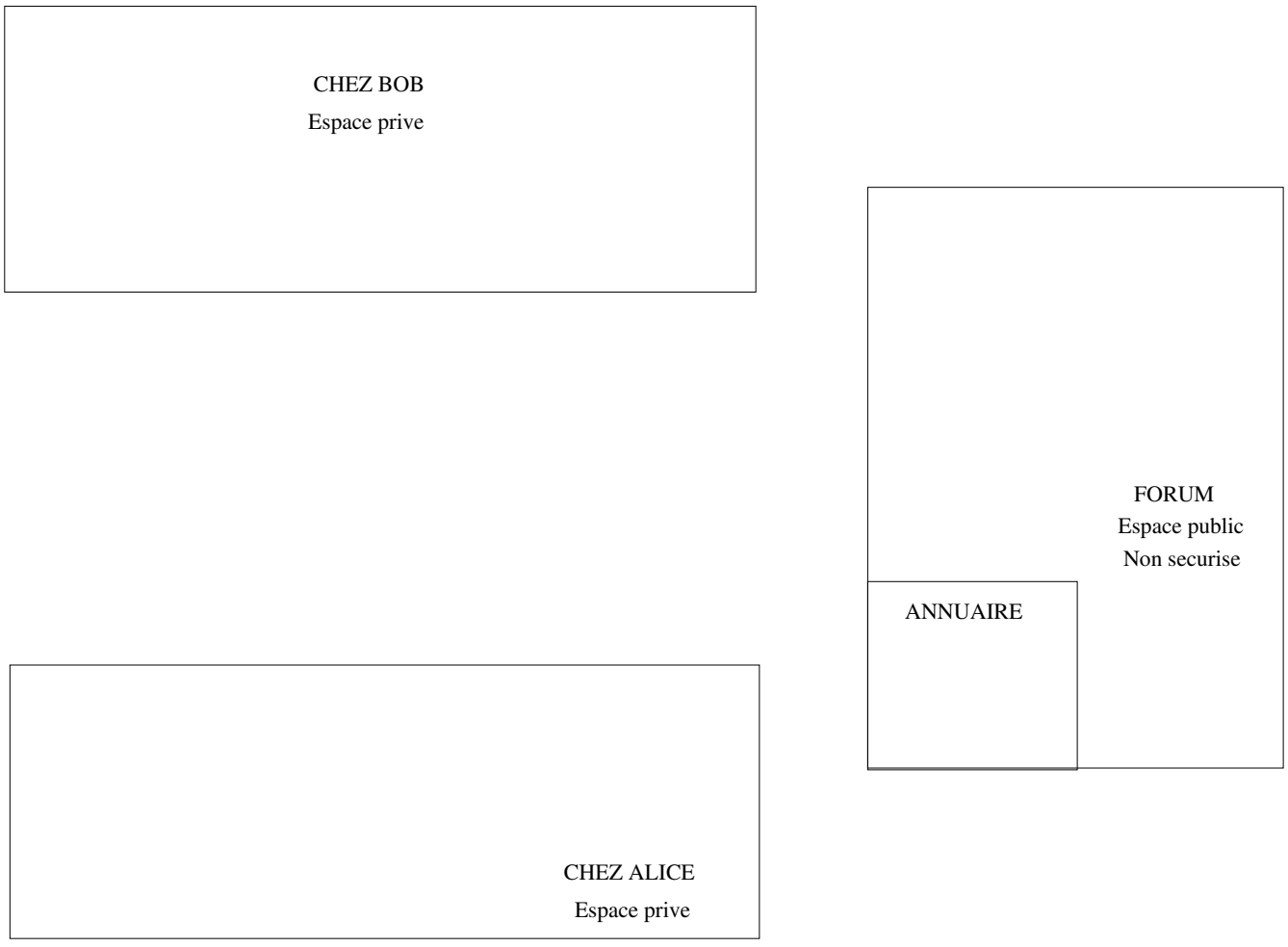
Cryptographie à clé publique

- Un concept inédit (1976, Diffie-Hellman)
  - Une clé publique pour chiffrer
  - Une clé privée pour déchiffrer
  - *Aucun contact préalable n'est nécessaire pour communiquer*
- Lien mathématique entre ces deux clés
  - *Fonction trappe à sens unique*.
  - Calculer aisément la clé de chiffrement en connaissant la clé de déchiffrement
  - Opération inverse *pratiquement* impossible.
- Rôle fondamental de l'ordinateur
  - On utilise des problèmes mathématiques que l'on ne sait pas résoudre *rapidement*
  - Par exemple la factorisation de grands nombres pour la méthode RSA

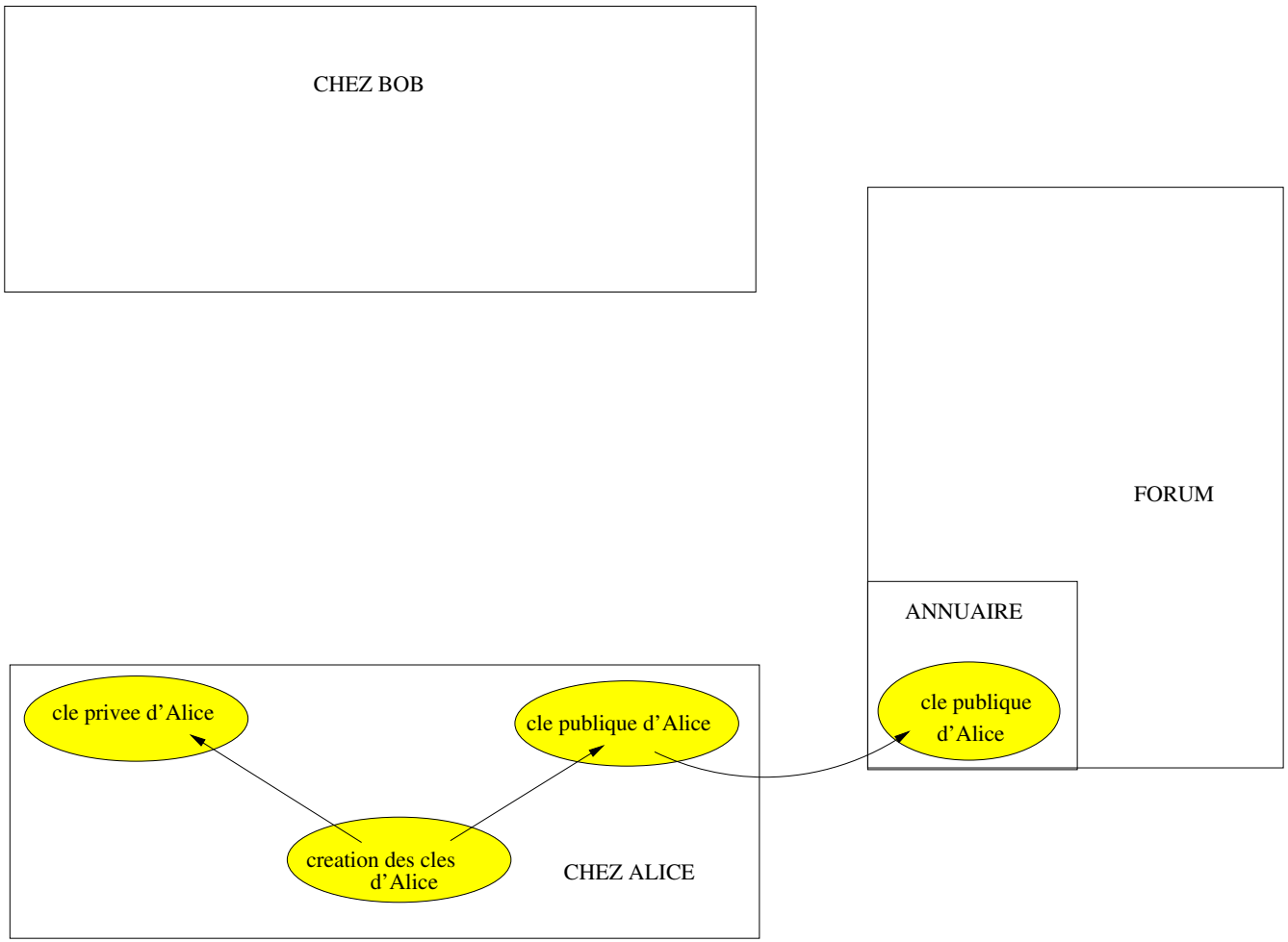
La fonction trappe à sens unique de RSA

- Actuellement, on recommande d'utiliser des clés RSA de 2048 bits, c'est-à-dire environ 700 chiffres décimaux.
- Si on dispose de deux nombres, même de 350 chiffres chacun, on peut *calculer leur produit* très rapidement avec n'importe quel ordinateur.
- Par contre, les meilleurs algorithmes de connus, tournant sur les meilleurs ordinateurs actuels, sont incapables de *factoriser un produit* de deux nombres premiers aléatoires de 350 chiffres chacun.
- Encore faut-il que les nombres premiers soient suffisamment aléatoires, mais c'est une autre histoire.

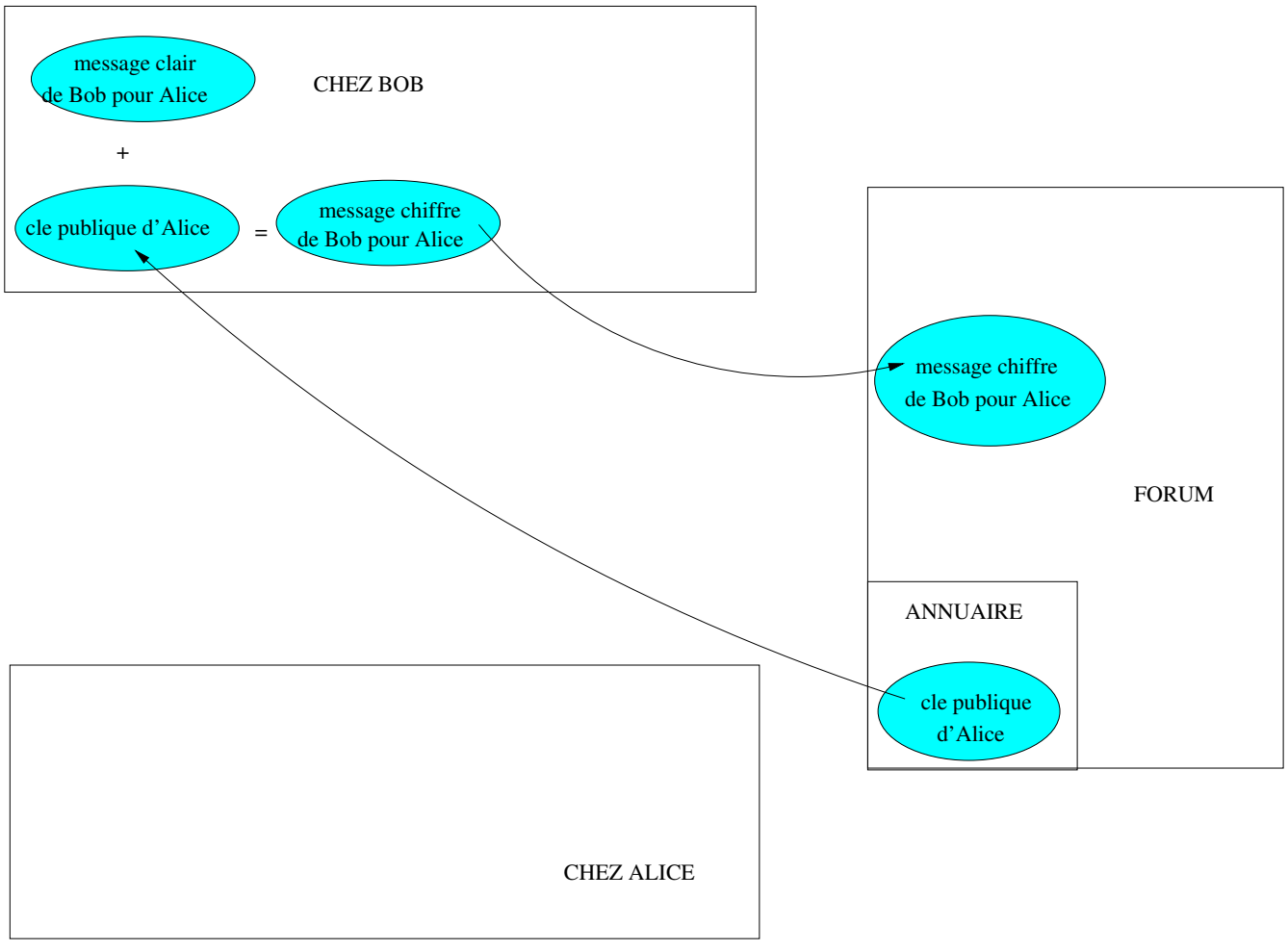
Contexte


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

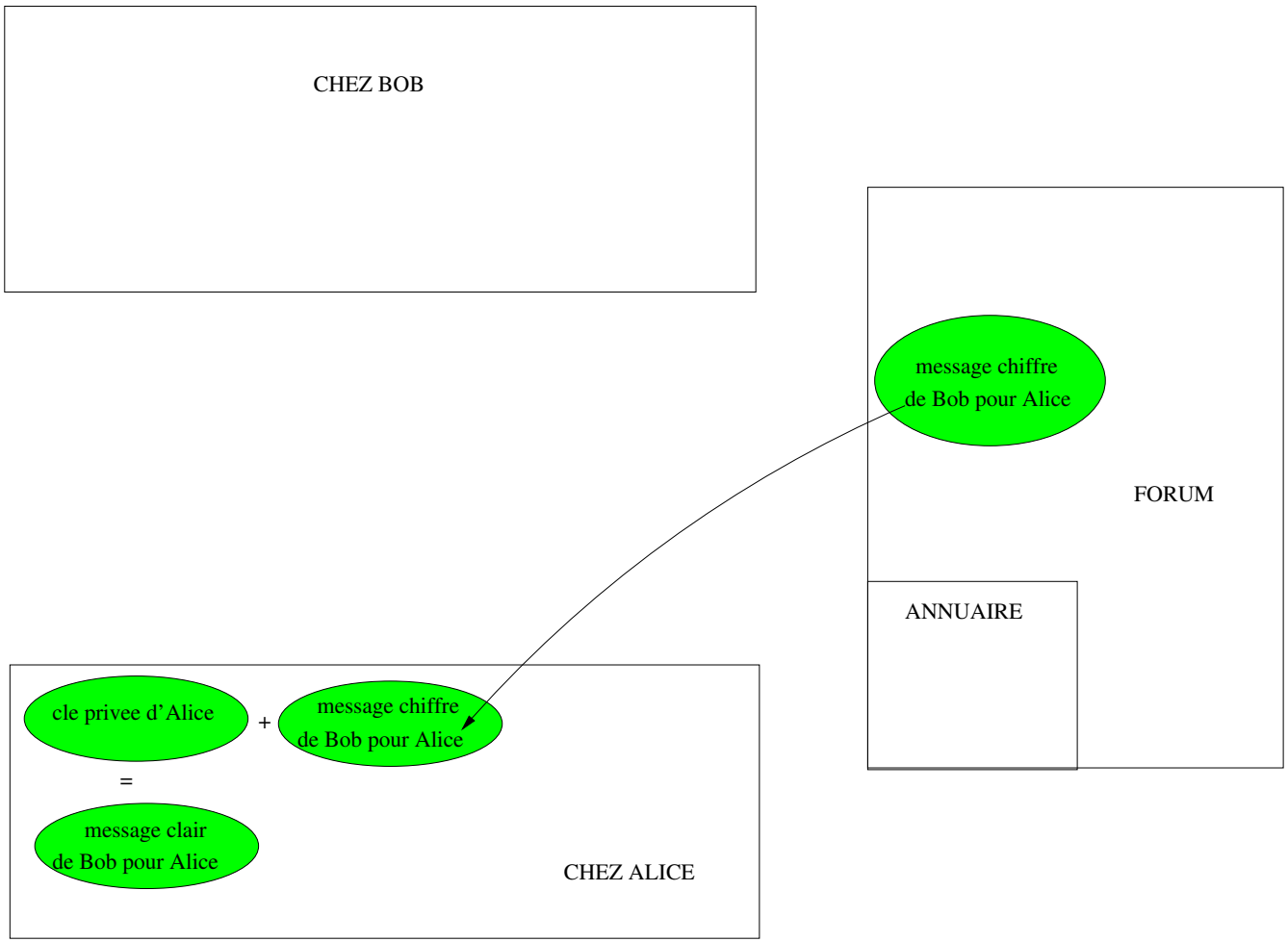
Alice fabrique ses clés



Bob envoie un message secret à Alice



Alice reçoit un message secret



FIN