# 1.3 Cryptographie asymétrique

NSI Tle - JB Duthoit

## 1.3.1 Un exemple avec *Le puzzle de Merkel*

**Exercice 14.7**

1. Question préliminaire :
   On considère le message codé :

   ```
   secret = '*( (7%#/""1|c|wwsxp~tu}jc/)¯ylqs{y|s%vil&ys~'
   ```

   Décrypter ce message en sachant qu'il a été créé avec une clé "courte" et que le début du message est "identifiant".

2. On imageine dans la suite que Alice veut envoyer un message à Bob, sans que Eve puisse intercepter le message !
   Le puzzle de Merkel fonctionne selon le principe suivant :

   a) Alice va créer un fichier de 1 000 000 de lignes, chaque ligne étant un message du type de la question préliminaire, avec un clé de chiffrement différente et "courte' pour chaque ligne.

   b) Alice envoie ce fichier à Bob. Eve est donc en mesure de l'intercepter.

   c) Bob reçoit le fichier, choisit une ligne au hasard et décrypte le message à l'aide d'un algorithme de force brute (ceci est possible car la clef de chiffrement est courte).
   Il obtient donc un fichier du type :
   *identifiant : 8785452132, clé : sledj#45P9878al*

   d) Bob envoie à Alice, en clair, le numéro d'identifiant. Eve peut intercépter ce message, mais que peut-elle en faire ?

   e) Alice possède bien évidemment le fichier de 1 000 000 de lignes non chiffrées. C'est donc très facile pour elle de connaître la ligne choisie par Bob !

   f) Alice et Bob ont maintenant une clef longue afin de coder leurs futurs échanges (la clef noté après les identifiants).

   ☛ Bien sûr, Eve peut tenter de dechiffrer les lignes, mais cela prendra du temps. On peut considérer que si le dechiffrement d'une ligne prend 1 seconde, il faudra en moyenne 500 000 secondes pour dechiffrer les 1 000 000 de lignes, soit plus de 5 jours !

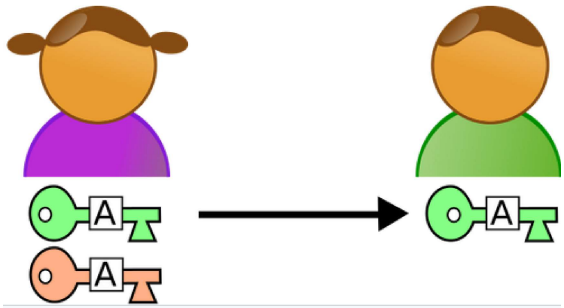
## 1.3.2 Principe du chiffrement asymétrique

### Analogie : la boîte à deux serrures

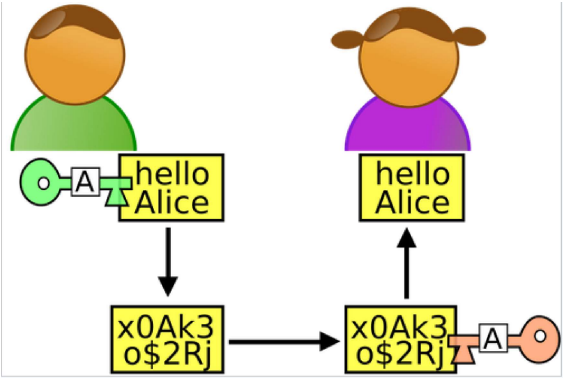
Une autre analogie envisageable serait d'imaginer une boîte avec deux serrures différentes. Lorsque l'on ferme la boîte d'un côté, seule la clef correspondant à l'autre serrure permet l'ouverture de la boîte et vice-versa
Une des clefs est privée et conservée secrète, l'autre est dite publique et un exemplaire peut-être obtenu par quiconque souhaite utiliser la boîte.

Pour chiffrer un message Bob prend la boîte, y place son message, et la ferme à l'aide de la clef publique. Seul le détenteur de la clef privée permettant d'accéder à l'autre serrure, Alice en l'occurrence, sera en mesure de rouvrir la boîte.

### Principe du chiffrement asymétrique



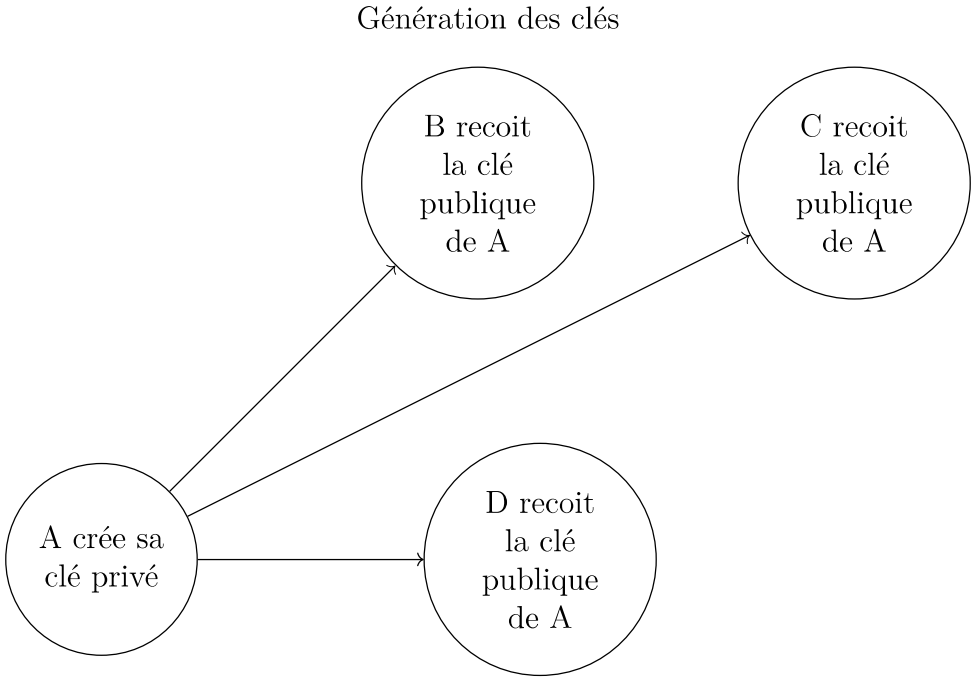

1re étape : Alice génère deux clefs. La clef publique (verte) qu'elle envoie à Bob et la clef privée (rouge) qu'elle conserve précieusement sans la divulguer à quiconque.



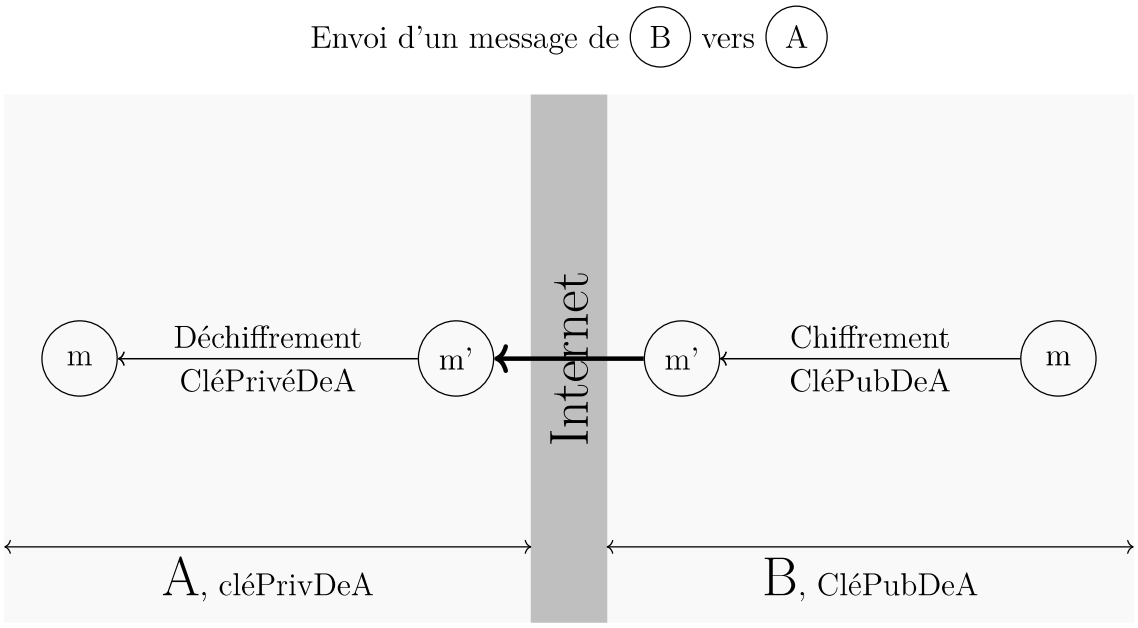

2e et 3e étapes : Bob chiffre le message avec la clef publique d'Alice et envoie le texte chiffré. Alice déchiffre le message grâce à sa clef privée.

Supposons que (A) ait l'envie d'envoyer un message à (B), (C) et (D) de façon sécurisée. (A) doit créer une clé de chiffrement privé (clé privé) et le garde pour lui précieusement. A partir de sa clé privée, il crée une clé publique qu'il diffuse largement.

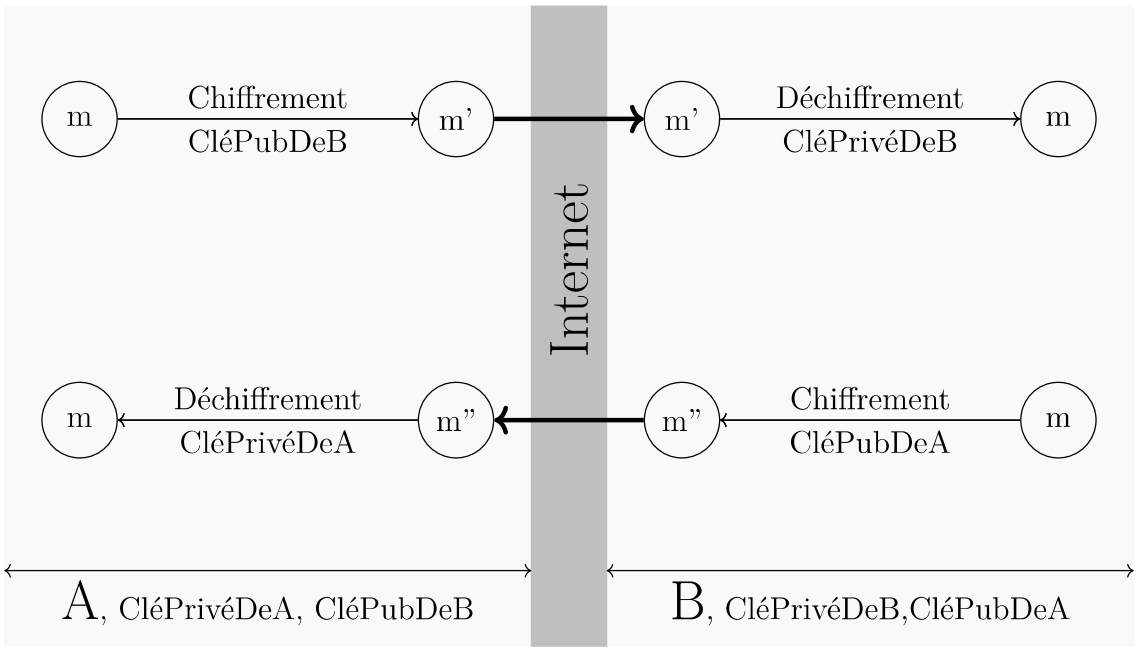
⚠ Bien évidemment, le système repose sur le fait qu'il est impossible de trouver la clé privé à partir de la clé publique.




⚠ La clé privée va servir à chiffrer lors de l'envoi et la clé publique à déchiffrer lors de la réception :



Envoi et réception de message




### 1.3.3 Authentification

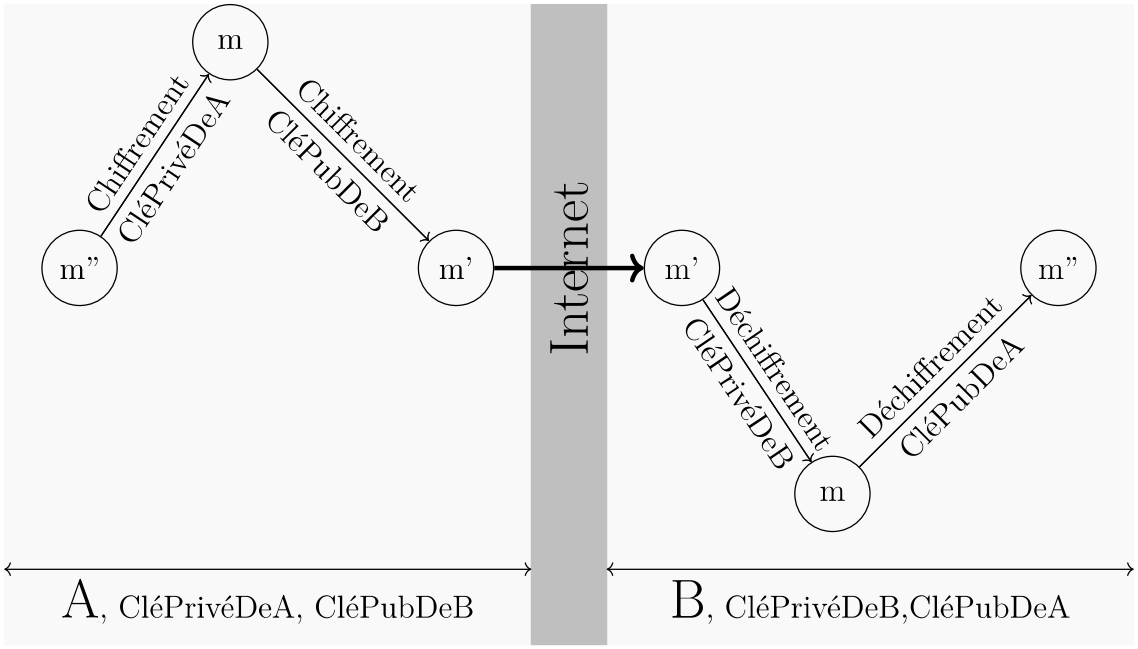
Le chiffrement asymétrique peut servir à authentifier l'expéditeur d'un message :

**Analogie : La boîte à deux serrures...suite !**

Pour signer un message, Alice le place dans la boîte et ferme celle-ci à l'aide de sa clef privée. Ainsi n'importe qui ayant récupéré la clef publique pourra ouvrir la boîte.
Mais comme la boîte a été fermée par la clef privée, cette personne sera assurée que c'est bien Alice, seule détentrice de cette clef, qui aura placé le message dans la boîte et fermé ladite boîte.

**Principe**

Authentification de l'émetteur




Si le récepteur ( B ici) peut déchiffrer grâce à la clé publique de ( A ), c'est bien que le message a été envoyé par ( A ) (le seul à avoir ClePrivéDeA).

☞ Le concept de signature numérique est basé sur cette technique de chiffrement asymétrique.

☞ Le chiffrement asymétrique repose sur des problèmes très difficiles à résoudre dans un sens et faciles à résoudre dans l'autre sens.

### 1.3.4 Un exemple : le RSA

Prenons un exemple : l'algorithme de chiffrement asymétrique RSA est très couramment utilisé, notamment dans tout ce qui touche au commerce électronique.
RSA se base sur la factorisation des très grands nombres premiers. Si vous prenez un nombre premier A (par exemple A = 16813007) et un nombre premier B (par exemple B = 258027589), il facile de déterminer C le produit de A par B (ici on a A x B = C avec C = 4338219660050123). En revanche si je vous donne C (ici 4338219660050123) il est très difficile de retrouver A et B. En tous les cas, à ce jour, aucun algorithme n'est capable de retrouver A et B connaissant C dans un temps "raisonnable". Nous avons donc bien ici un problème relativement facile dans un sens (trouver C à partir de A et B) est extrêmement difficile dans l'autre sens (trouver A et B à partir de C).