PKI - Gestion de clés

Anca Nitulescu
anca.nitulescu@ens.fr

Ecole Normale Supérieure, Paris

Cours 8

Gestion de clés

Importance des clés

- Détiennent tous les secrets
- Servent de lien entre les acteurs

Gestion des clés

- Collaboration entre plusieurs acteurs
- Besoin de sécurité sur la circulation des clés

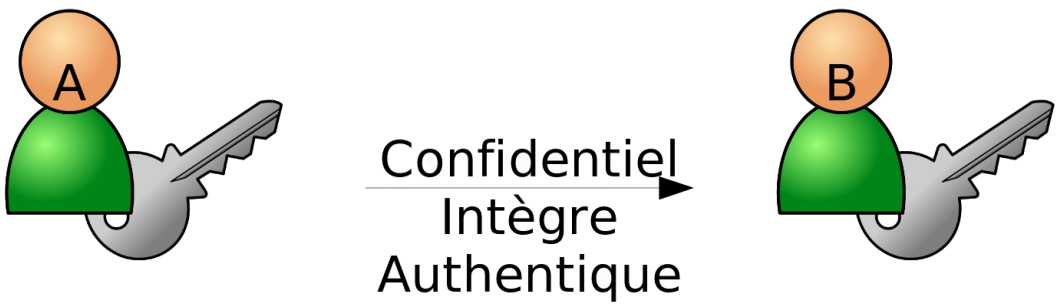
Gestion de clés

Clé secrètes

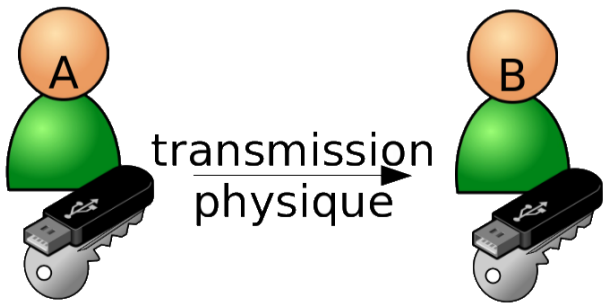
La sécurité des échanges dépend presque exclusivement de la sécurité de la clé

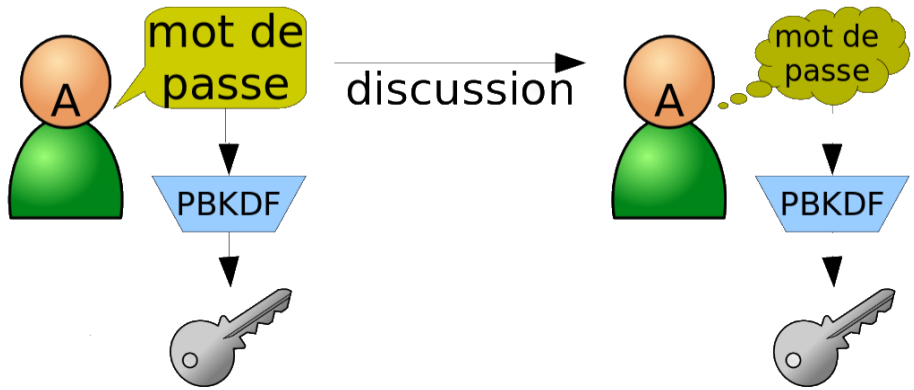
La transmission d'une clé secrète doit :

- être confidentielle
- être intègre et authentique



Clés secrètes





Transmission physique

- On s'échange la clé physiquement
- Pas de problème d'authenticité

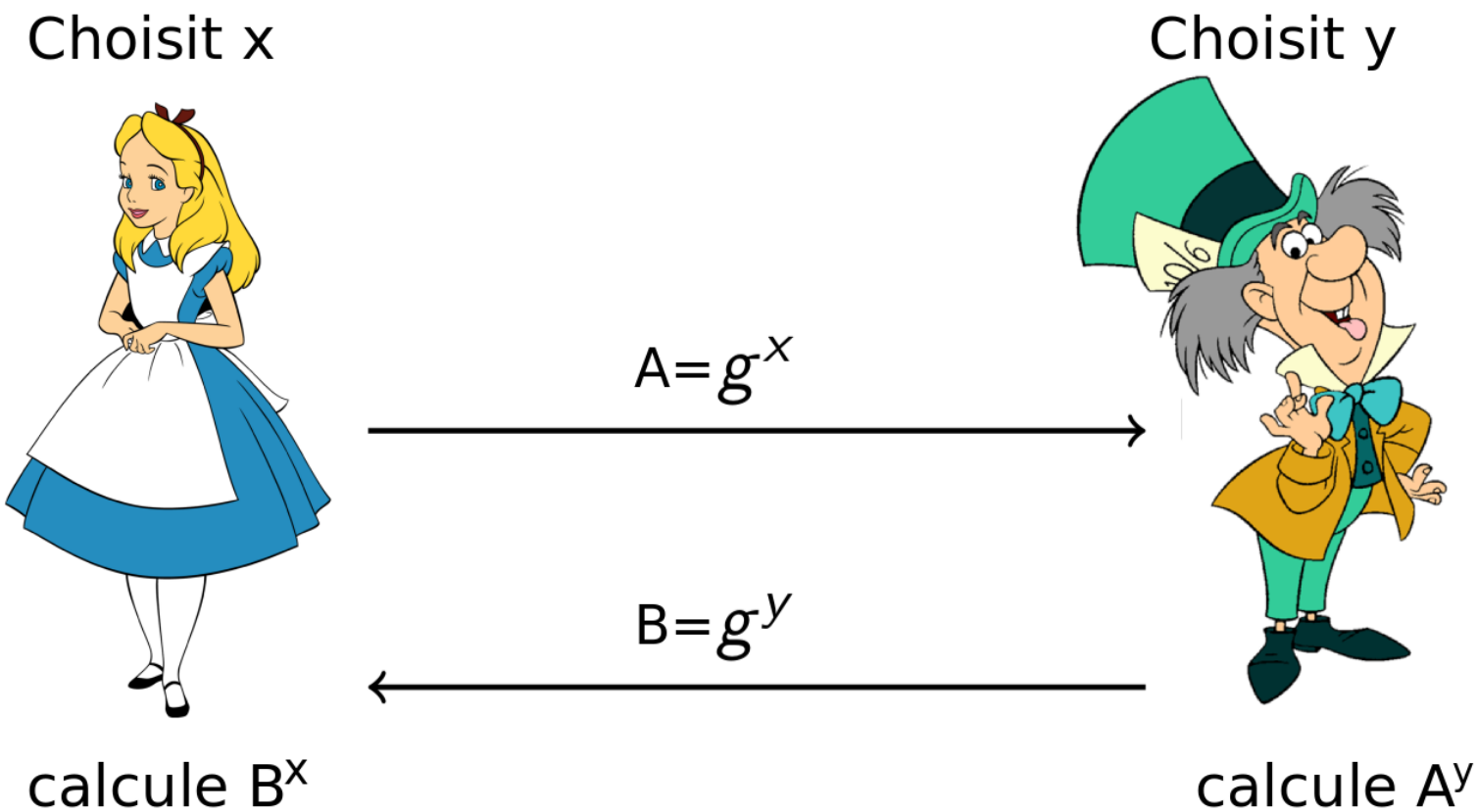
Clés secrètes

Autre solution : chiffrement asymétrique

- A choisit la clé, la chiffre à destination de B, qui sera le seul à pouvoir la déchiffrer
- Solution efficace pour la confidentialité

Reste le problème de l'authenticité de la clé publique !

Echange de clé Diffie-Hellman



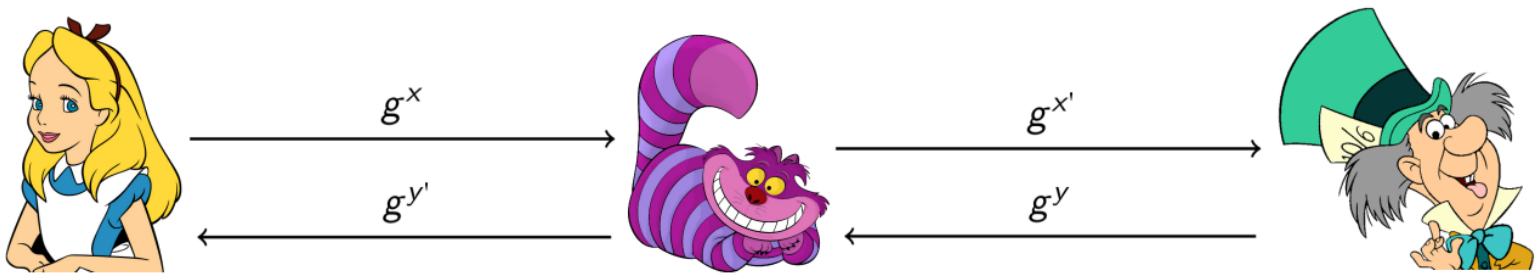
Clé commune

$$B^x = (g^y)^x = A^y = (g^x)^y = g^{xy}$$

Attaque "Man-in-the-middle"

Choisit x

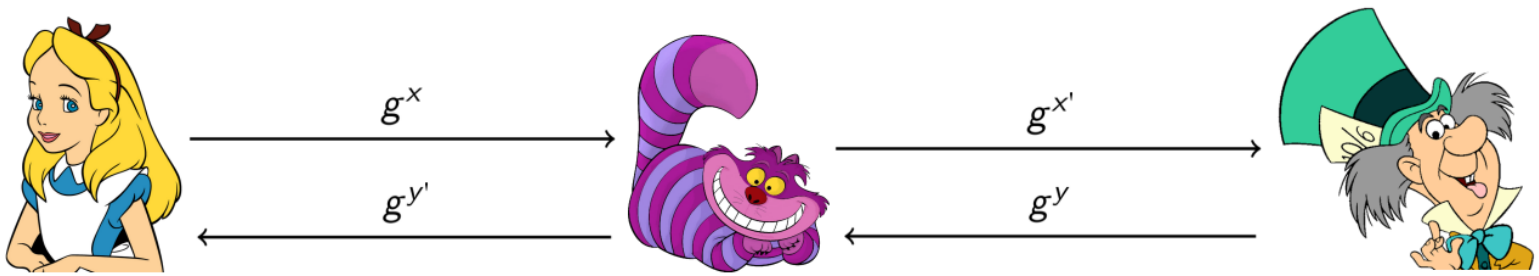
Choisit y



Attaque "Man-in-the-middle"

Choisit x

Choisit y



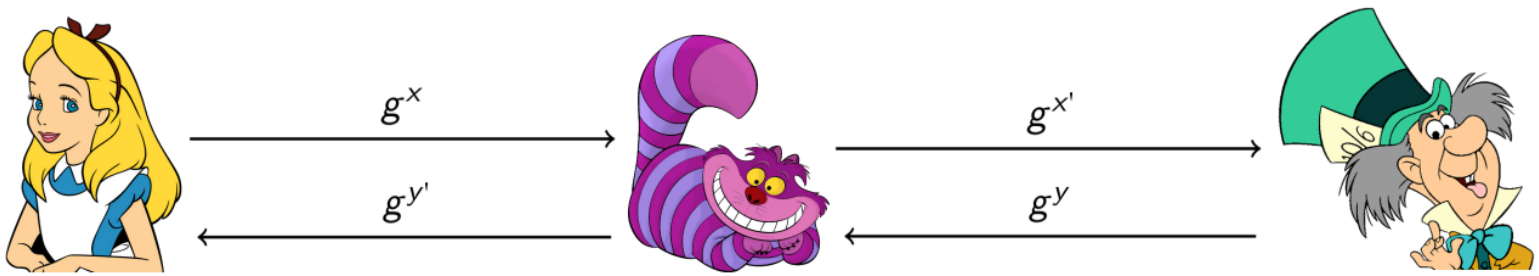
Calcule $g^{xy'}$

Calcule $g^{x'y}$

Attaque "Man-in-the-middle"

Choisit x

Choisit y



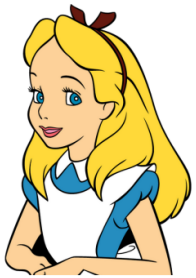
Calcule $g^{xy'}$

Calcule $g^{x'y}$

Ils calculent des clés differentes

$$g^{xy'} \neq g^{x'y}$$

Solution : Authentification



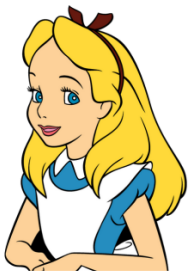
choisit x —— $g^x, \mathtt{sign}_A(g^x)$ ——→ vérifie

vérifie ←—— $g^y, \mathtt{sign}_B(g^y)$ —— choisit y

Diffie-Hellman signé

1. **Evite les attaques par le milieu**
   - impossible pour un attaquant de fournir $\mathrm{sign}_A(g^{x'})$
2. **Rejeu possible**
   - si un couple $(g^x, \mathrm{sign}_A(g^x))$ est capturé, il peut être utilisé indéfiniment pour s'authentifier comme Alice.

Solution : Authentification



choisit x —— g^x ——→

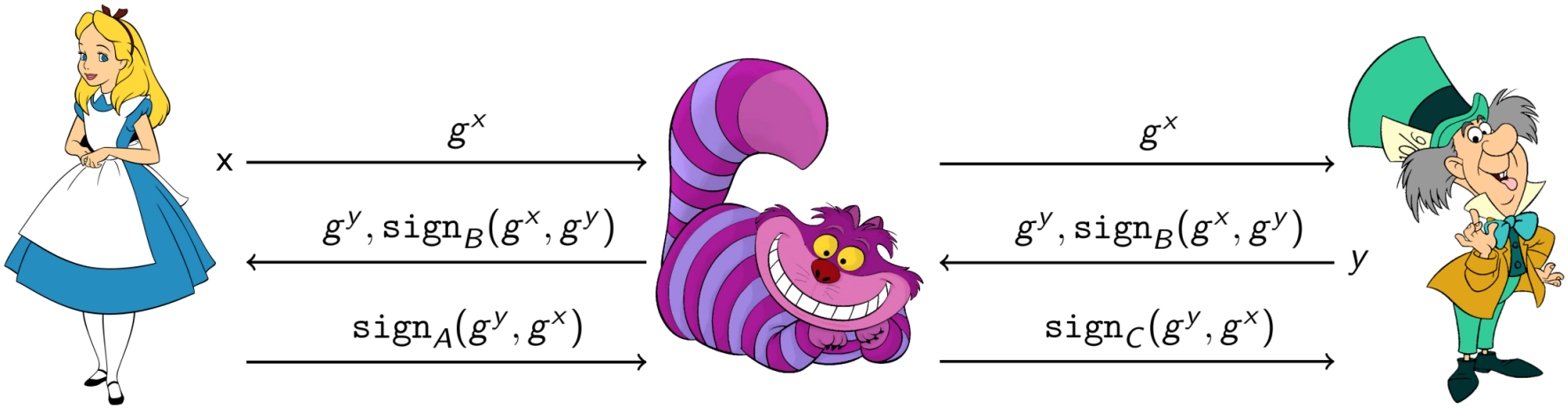
vérifie ←—— $g^y, \mathtt{sign}_B(g^y, g^x)$ —— choisit y

—— $\mathtt{sign}_A(g^x, g^y)$ ——→ vérifie

Diffie-Hellman signé - V2

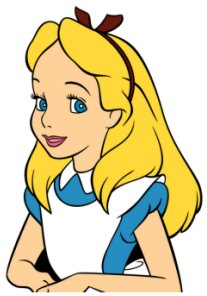
- Evite les attaques par le milieu
- Evite le rejeu : la valeur du déstinataire est aussi signée

Usurpation d'identité



Tous les messages envoyés par Alice sont vus par Bob comme venant de Cheshire.

Solution : Authentification



choisit x $\xrightarrow{A, g^x}$

$\xleftarrow{B, g^y, \mathtt{sign}_B(B, g^y, g^x, A)}$ choisit y

vérifie $\xrightarrow{A, \mathtt{sign}_A(A, g^x, g^y, B)}$ vérifie

Diffie-Hellman signé - V3

- Evite l'usurpation d'identité.

Gestion de clés publiques

Certificats

Un certificat X.509 contient :

- L'organisme émetteur du certificat
- Le détenteur du certificat
- Les dates de validité
- Les dates du détenteur
- La clé publique
- La signature

Certificats

L'émetteur

L'émetteur est «l'autorité de confiance» qui signe le certificat, après avoir vérifié l'identité du détenteur

Le détenteur

Le détenteur est l'entité qui «possède» la clé publique (et la clé privée associée)

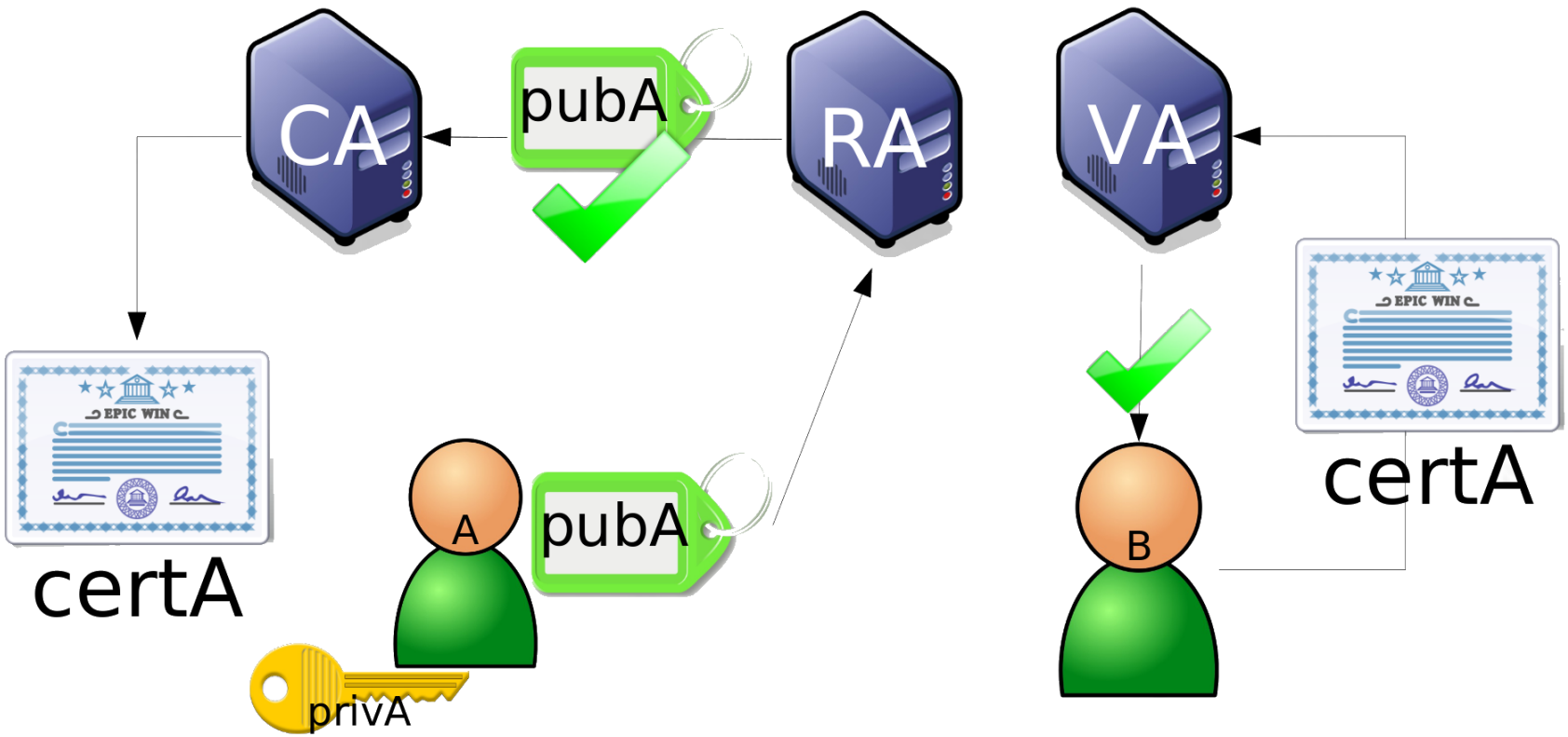
Gestion de clés publiques - PKI

Principe d'une PKI

PKI : Annuaire de clés authentifiées

En pratique, il s'agit d'une collaboration entre plusieurs intervenants : les « autorités » et les utilisateurs.

Gestion de clés - Schéma PKI



Les « Autorités »

Rôle des autorités

En théorie, ce système répond au problème d'authenticité des clés

Certificate Authority

Émet des certificats signés

Registration Authority

Effectue les vérifications d'identités

Validation Authority

Confirme qu'un certificat est valide

Gestion de clés - Application