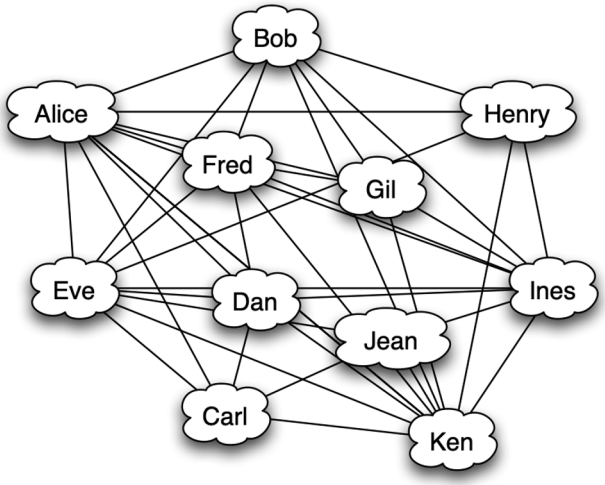
Gestion des clés

- Problématiques:
  - Le nombre énorme de **clés symétriques** à gérer
- Des échanges chiffrés avec **n** personnes nécessitent **nx(n-1)/2**

Remarque:

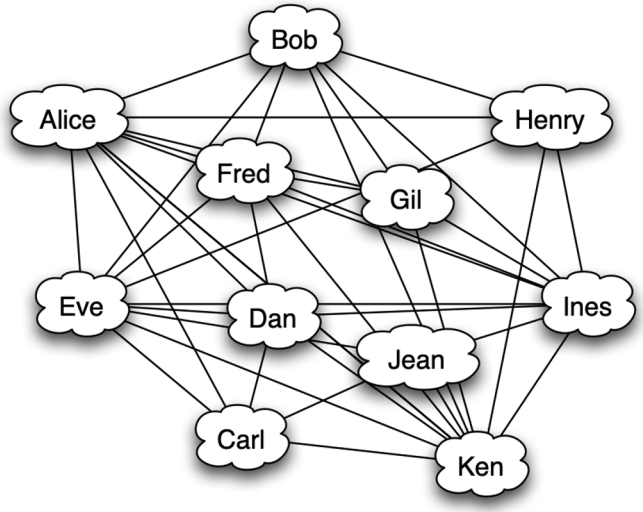
- Si **n** intervenants veulent s'échanger des informations en utilisant des **clés asymétriques** sans l'aide d'un tiers, chaque intervenant doit avoir une clé publique unique connue de tous. Donc, **n** clés sont suffisantes.



Gestion des clés

La gestion des clés concerne:

- La distribution de clés cryptographiques,
- Les mécanismes utilisés pour l'association identité–clé
- La génération, la maintenance et la révocation de clés.
- Le stockage sécurisé à long terme des clés de déchiffrement (obligation légale).



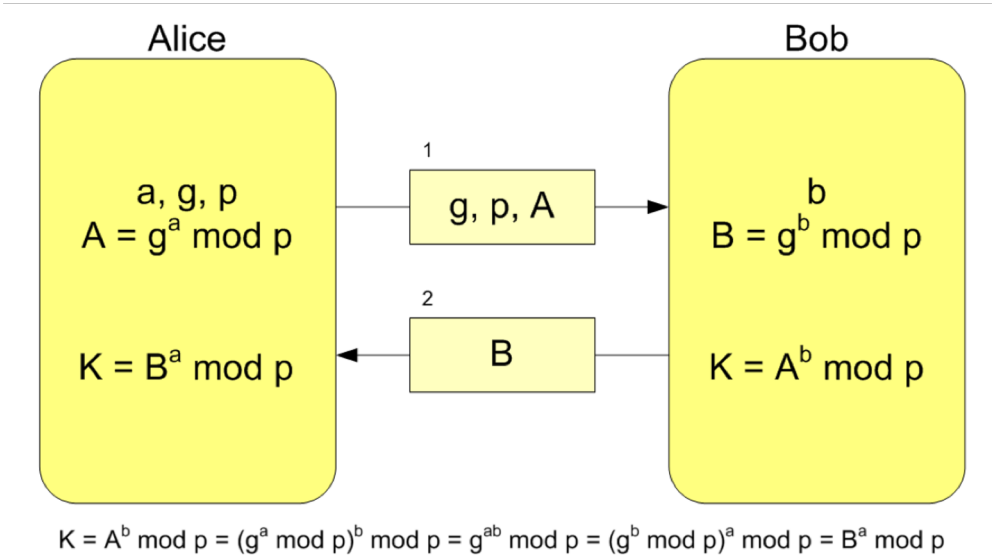
Gestion des clés

- Problématiques:
  - Distribution des clés publiques de façon authentifiée, confidentielle.
  - Association d'une clé publique à une (représentation d'une) identité ?
  - Représentation d'une identité (nommage) ?
  - Sécurisation de la création des identités ?
  - Limitation des dégâts provoqués par la perte d'une clé secrète ?

Gestion des clés

L’échange de clés

- 1976 **Diffie, Hellman et Merkle** publient le premier schéma d’échange Whitfield Diffie and Martin E. Hellm de clés.
- Basé sur la difficulté du logarithme discret.



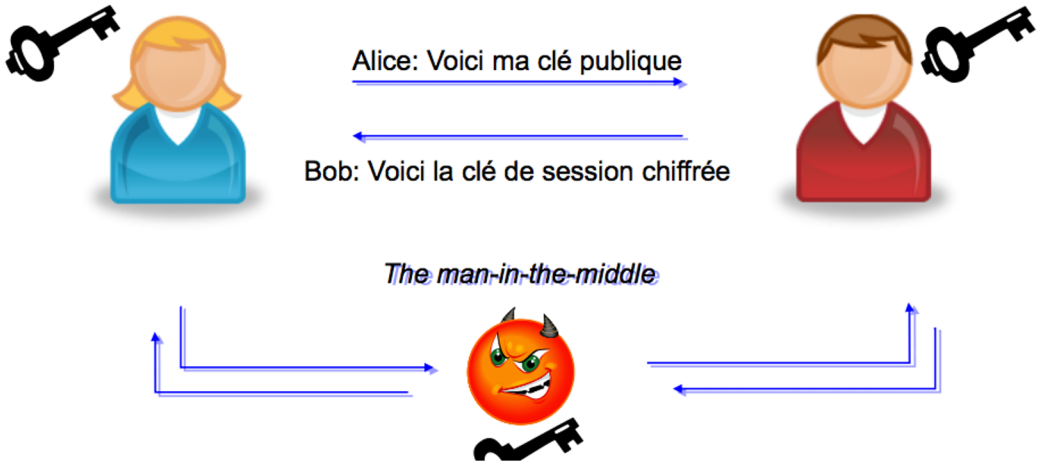
Gestion des clés

Echange de clés Diffie-Hellman :

- Alice et Bob choisissent un modulo **p** (de préférence un grand nombre premier) et un entier **g** ; **p** et g ne sont pas secrets.
- Alice choisit un nombre secret **a**. Bob choisit un nombre secret **b**.
- Alice calcule $\mathbf{A} \equiv \mathbf{g}^{\mathbf{a}} \bmod \mathbf{p}$ et le transmet à Bob. Bob calcule $\mathbf{B} \equiv \mathbf{g}^{\mathbf{b}} \bmod \mathbf{p}$ et le transmet à Alice. **A** et **B** ne sont pas secrets.
- Alice reçoit **B** et calcule $\mathbf{K}_{ab} \equiv (\mathbf{B})^{\mathbf{a}} \equiv (\mathbf{g}^{\mathbf{b}})^{\mathbf{a}} \bmod \mathbf{p} \equiv \mathbf{g}^{\mathbf{ba}} \bmod \mathbf{p}$.
- Bob reçoit **A** et calcule $\mathbf{K}_{ab} \equiv ((\mathbf{A})^{\mathbf{b}} \equiv (\mathbf{g}^{\mathbf{a}})^{\mathbf{b}} \bmod \mathbf{p} \equiv \mathbf{g}^{\mathbf{ba}} \bmod \mathbf{p}$.
- Alice et Bob disposent maintenant d'une clé commune $\mathbf{K}_{ab}$ dont ils peuvent se servir pour chiffrer leur correspondance.
- Un attaquant passif qui écoute les échanges connaît **p, A, B**, mais il ne connaît ni **a** ni **b**: il ne peut pas calculer (facillement) la clé $\mathbf{K}_{ab}$.

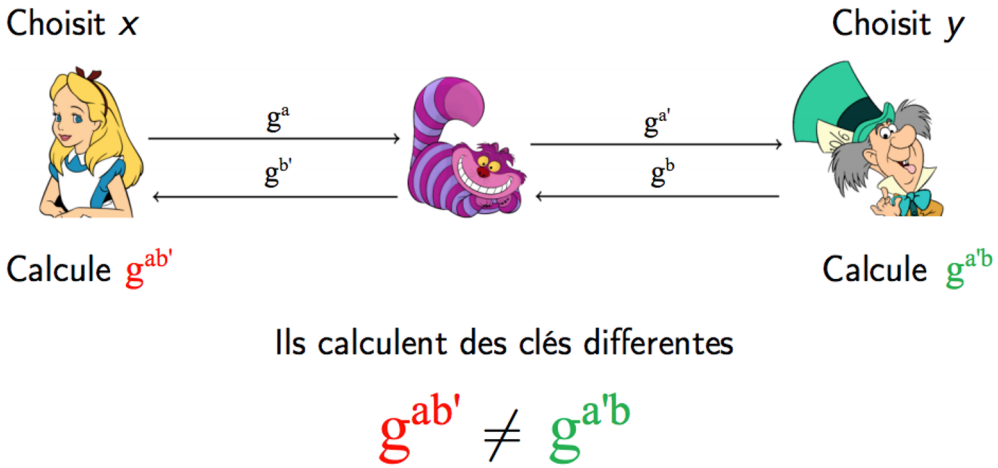
Gestion des clés

- Attaque Man-In-The-Middle:
  - Lorsque deux intervenants veulent échanger des informations pour échanger une clé de session grâce à RSA, ils se doivent d'authentifier leur partenaire.



Gestion des clés

- Attaque Man-In-The-Middle:
  - Cette attaque repose sur l'interception de ga et gb, ce qui est facile puisqu'ils sont échangés en clair ; l'élément g étant supposé connu par tous les attaquants. Pour retrouver les nombres a et b et ainsi casser complètement l'échange, il faudrait calculer le logarithme discret de ga et gb, ce qui est impossible en pratique.



Gestion des clés

- Attaque Man-In-The-Middle:
  - Mais un attaquant peut se placer entre Alice et Bob, intercepter la clé ga envoyée par Alice et envoyer à Bob une autre clé ga', se faisant passer pour Alice. De même, il peut remplacer la clé gb envoyée par Bob à Alice par une clé gb', se faisant passer pour Bob. L'attaquant communique ainsi avec Alice en utilisant la clé partagée gab' et communique avec Bob en utilisant la clé partagée ga'b, Alice et Bob croient communiquer directement. C'est ce que l'on appelle « attaque de l'homme du milieu ».
  - Alice et Bob croient ainsi avoir échangé une clé secrète alors qu'en réalité ils ont chacun échangé une clé secrète avec l'attaquant, l'homme du milieu.

Infrastructure à clé publique

- L'infrastructure à clé publique ou Public key infrastructure (PKI) est un modèle hiérarchique qui se repose sur une autorité certifiant les clés des divers intervenants.
- Le rôle de l'autorité de certification (Certification Authority ou CA) est de s'assurer de la validité de la correspondance entre un nom d'une personne et une clé publique.
  - Le CA émet des certificats X.509 aux personnes qu'elle a pu authentifier.
  - Voir Exemple sur Firefox ou google
- Une personne faisant confiance à un CA devrait pouvoir identifier toutes les personnes authentifiées par ce CA.

Infrastructure à clé publique

- En résumé , c'est système permettant aux agents de reconnaître quelle clé publique appartient à qui.

- Services fournis par la PKI :
  - Vérification d'identité et création de certificats
  - Révocation des clés
  - Test d'appartenence de certificats
  - Recouvrement des clés de déchiffrement
- Composants d'une PKI :
  - Autorité de certification (CA).
  - Autorité d'enregistrement (RA).
  - Autorité de dépot (Repository).
  - Autorité de recouvrement.

Infrastructure à clé publique

- **Autorité d'enregistrement (RA) :**
  – Vérifie l'identité du demandeur de certificat.
- **Autorité de certification (CA) :**
  – Signe les certificats.
  – Signe les révocations de certificats.
  – Peut être la même que la RA.
-

Infrastructure à clé publique

- **Autorité de dépot (Repository) :**
  – Maintient les certificats dans un répertoire public de certificats.
  – Maintient une liste de révocation de certificats (CRL) dans le répertoire des certificats. La CRL est vérifiée activement par les clients ou par les services de validation.
- **Autorité de recouvrement :**
  – Protège certaines clés privées pour récupération ultérieure.
- **Clients**.

Infrastructure à clé publique

Client et Mode d'emploi

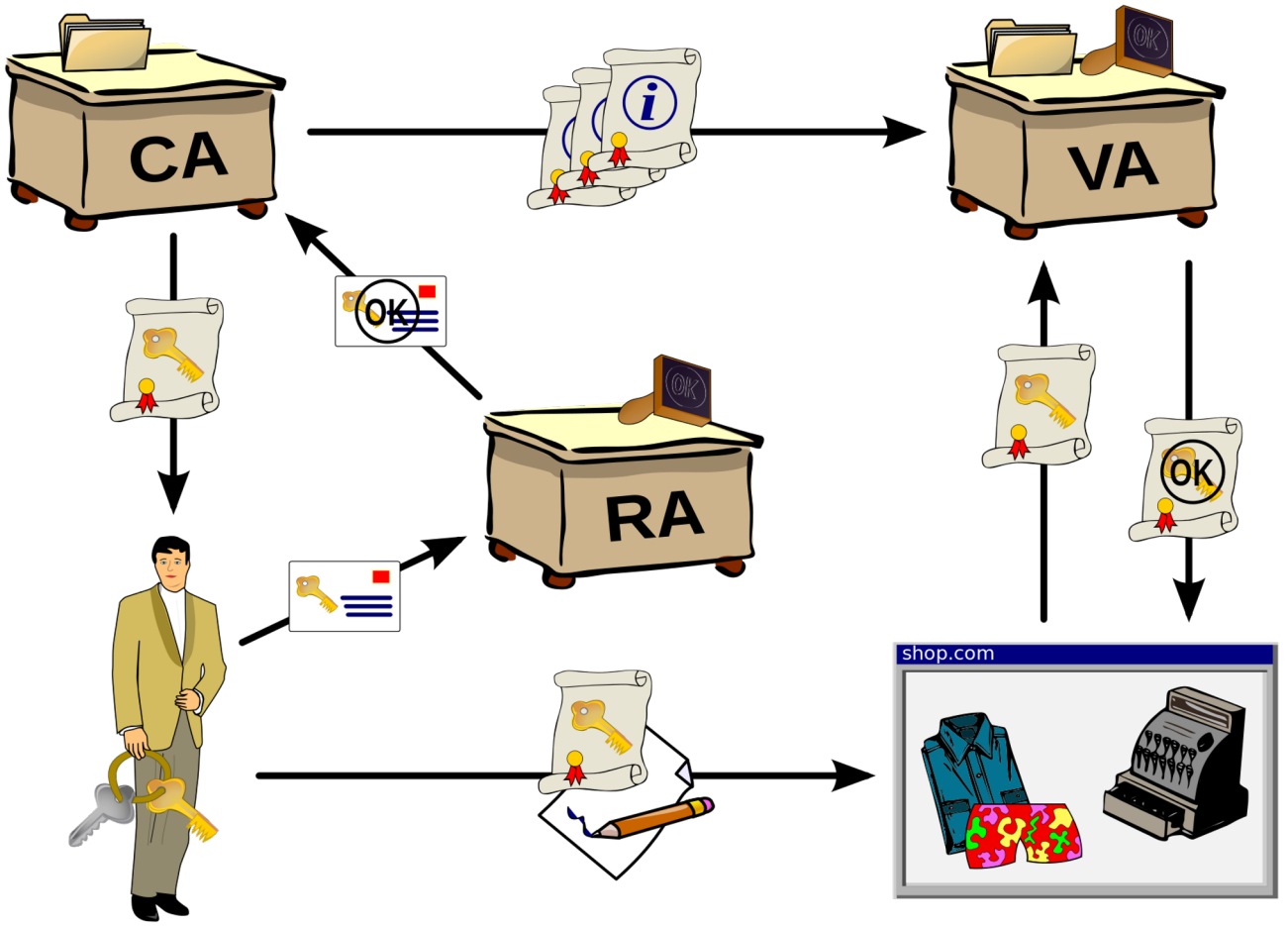
- Actions à entreprendre par **Alice** pour joindre la PKI :
  – Génération de sa paire clé privée/clé publique.
  – Transport de sa clé publique à la RA :
    - Certificate Signing Request – divers formes.
  – La RA vérifie qu'Alice est bien celle qui prétend l'être (à définir selon les implémentations !) et informe la CA.
  – La CA délivre le certificat stipulant "Cette clé 'K_A appartient bien à Alice".
  – Le Repository récupère et stocke ce certificat, mis à disposition pour tout le monde

Infrastructure à clé publique

Client et Mode d'emploi

- Maintenant **Bob** peut récupérer (soit chez le Repository, soit d'une autre manière !) le certificat d'Alice
  – Si **Bob** fait confiance à la **CA**, il peut accepter comme valide le certificat, et authentifier diverses conversations avec Alice.
- Celà implique bien sûr la possesion de la **clé publique de la CA**, pour bien vérifier la signature digitale sur le certificat !

Infrastructure à clé publique



Certificat numérique

- Un certificat à clé publique est un certificat numérique qui lie l'identité d'un système à une clé publique, et éventuellement à d'autres informations;

- C'est une structure de donnée signée numériquement qui atteste sur l'identité du possesseur de la clé privée correspondante à une clé publique.

-

Certificat numérique

- Un certificat est signé numériquement par une autorité de certification (CA) à qui font confiance tous les usagers et dont la clé publique est connue par tous d'une manière sécurisée.

- Ainsi, afin de publier sa clé publique, son possesseur doit fournir un certificat de sa clé publique signé par l'autorité de certification.

- Après vérification de la signature apposée sur le certificat en utilisant la clé publique de l'autorité de certification, le récepteur peut déchiffrer et vérifier les signatures de son interlocuteur dont l'identité et la clé publique sont inclus dans le certificat.

Certificat numérique

Certificat X509

- Certificate
  - Version
  - Serial Number
  - Algorithm ID
  - Issuer
  - **Validity**
    - **Not Before**
    - **Not After**
  - **Subject**
  - Subject Public Key Info
    - Public Key Algorithm
    - **Subject Public Key**
  - Issuer Unique Identifier (Optional)
  - Subject Unique Identifier (Optional)
  - Extensions (Optional)
- Certificate Signature Algorithm
- **Certificate Signature**

Identification de la personne

Signature du contenu par le CA