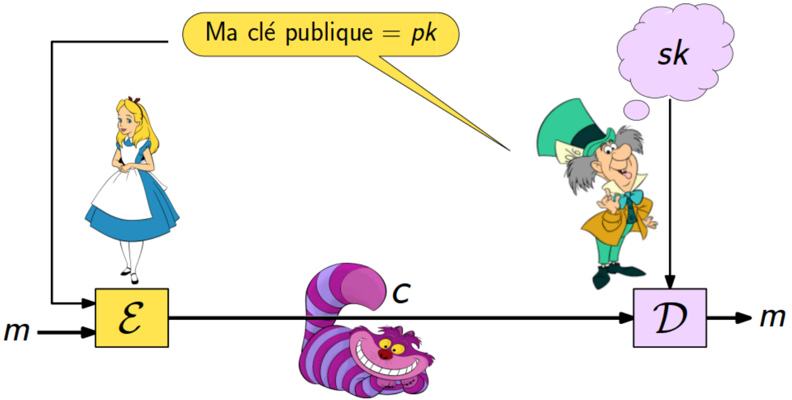
Protocoles cryptographiques. Gestion de clés

Anca Nitulescu
anca.nitulescu@ens.fr

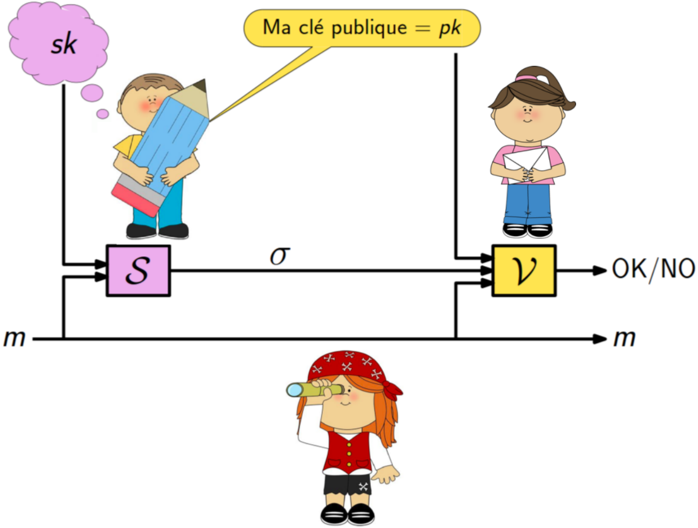
Université Paris 13 Villetaneuse

Cours 10
21/03/2016

Confidentialité - Chiffrement



Authenticité - Signature numérique



Chiffrement et Signature RSA

Génération des clés

$\mathcal{KG}(\ell) = (\mathsf{pk}, \mathsf{sk})$

- Soit $n = p \cdot q$ (p et q premiers)
- L'ordre du groupe multiplicatif $\mathbb{Z}_n^\star = \varphi(n) = (p-1)(q-1)$
- Soit e un entier premier avec $\varphi(n) = (p-1)(q-1)$
- Soit d un entier qui satisfait $d \cdot e = 1 \pmod{\varphi(n)}$

$$d \cdot e + u\varphi(n) = 1 \qquad \text{(Bézout)}$$

clé publique

- $n = pq$: module public
- e : clé de vérification

clé secrète

- $d = e^{-1} \pmod{\varphi(n)}$
- les premiers p et q

Chiffrement RSA

RSA - Génération des clés

- $\mathsf{pk} = e$
- $\mathsf{sk} = d$

RSA - Chiffrement

$\mathcal{E}(\mathsf{pk} = (e, n), m) = C$
$C = m^e \pmod{n}$

RSA - Déchiffrement

$\mathcal{D}(\mathsf{sk} = \mathrm{d}, C) = m$
$m = C^d \pmod{n}$

Signature RSA

σRSA - Génération des clés

- $\mathsf{pk} = e$
- $\mathsf{sk} = d$

σRSA - Signer

$\mathcal{S}(\mathsf{sk} = d, m) = \sigma$
$\sigma = m^d \pmod{n}$

σRSA - Vérifier

$\mathcal{V}(\mathsf{pk}, m, \sigma) = yes/no$
$m \stackrel{?}{=} \sigma^e \pmod{n}$

Chiffrement et Signature ElGamal

ElGamal - Génération des clés

$\mathcal{KG}(\ell) = (\mathsf{pk}, \mathsf{sk})$

- Soit un premier p et le groupe cyclique $\mathbb{Z}_p^\star$
- Soit $g \in \mathbb{Z}_p^\star$ un élément d'ordre $q|(p-1)$.
- Soit une clé secrète $\mathsf{sk} = x$.
- Soit $\mathsf{pk} = g^x \pmod{p}$.

clé publique

- p et g : paramètres publiques
- $\mathsf{pk} = g^x$: clé de vérification

clé secrète

- $\mathsf{sk} = x$
  exposant sécret

Chiffrement ElGamal

ElGamal - Clés

- pk $= g^x$
- sk $= x$

ElGamal - Chiffrement

$\mathcal{E}(\mathrm{pk} = g^x, m) = (C, D)$
$(C, D) = (g^r, (g^x)^r m) \pmod{p}$

ElGamal- Déchiffrement

$\mathcal{D}(\mathrm{sk} = x, (C, D)) = m$
$m = D/C^x \pmod{p}$

Signature ElGamal

σElGamal - Clés

- pk $= g^x$
- sk $= x$

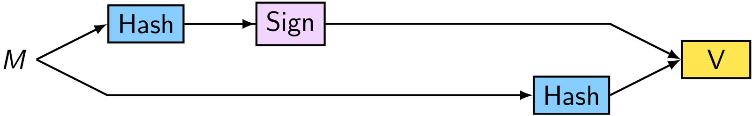
σElGamal - Signer

$\mathcal{S}(\mathrm{sk} = x, m) = \sigma \pmod{q}$
$\sigma = (C, D) = (g^r, (m - xg^r)/r)$

σElGamal - Vérifier

$\mathcal{V}(\mathrm{pk} = g^x, m, \sigma) = yes/no$
$g^m \stackrel{?}{=} C^D (g^x)^C \pmod{p}$

Signatures et Fonctions de hachage



Idée : Hash & Sign

Au lieu de signer le message très long, on signe un condensé du message

Signatures et Fonctions de hachage

Propriétés

Une signature éléctronique :

- est authentique
- est impossible à falsifier (imiter)
- n'est pas réutilisable sur un autre document.
- ne peut pas etre reniée
- facile et rapide à calculer

En plus, avec le hachage :

- Un document signé est inaltérable.

Calculs distribués entre plusieurs parties

Secure two-party computation

- **Problème** : sécurité des calculs distribués entre deux parties
- **But** : permettre à différentes parties de réaliser des calculs, basés sur leurs données privées
- **Résultat du calcul** : connu par les deux parties, mais aucune partie ne puisse déduire les données privées de l'autre.

Alice	fonction F	Bob
entrée a		entrée b

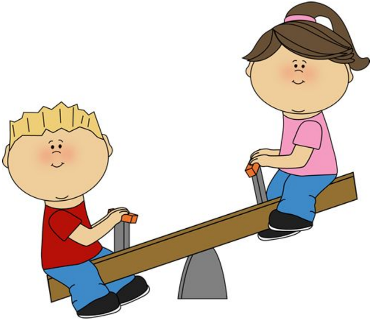
Résultat $\mathsf{F}(a, b)$

Calculs distribués entre plusieurs parties

Exemple - Test d'affinité

- Alice et Bob veulent tester leur compatibilité en couple.
- Ils veulent savoir si leur amour est partagé sans blesser les sentiments de l'autre.
- Chacun a deux choix :
  LOVE / NO-LOVE
- À la fin de leur interaction les deux apprennent si l' amour est réciproque ou non, mais rien de plus.

Test d'affinité



Formellement

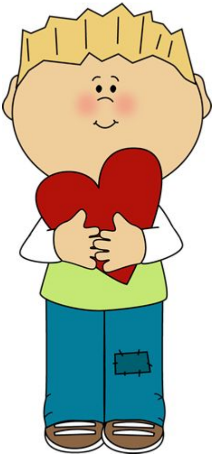
F(love, love) = compatibilité
F(no-love, love) = non-compatibilité
F(love, no-love) = non-compatibilité
F(no-love, no-love) = non-compatibilité

Test d'affinité

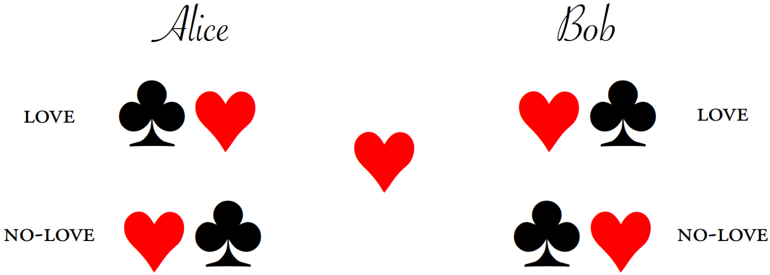
Protocole

On considère 5 cartes à jouer :

- Alice et Bob ont chacun un cœur et un trèfle (♡, ♣)
- Sur la table il y a un cœur ♡, face contre la table
- Alice et Bob mettent leurs cartes sur la table, face cachée.

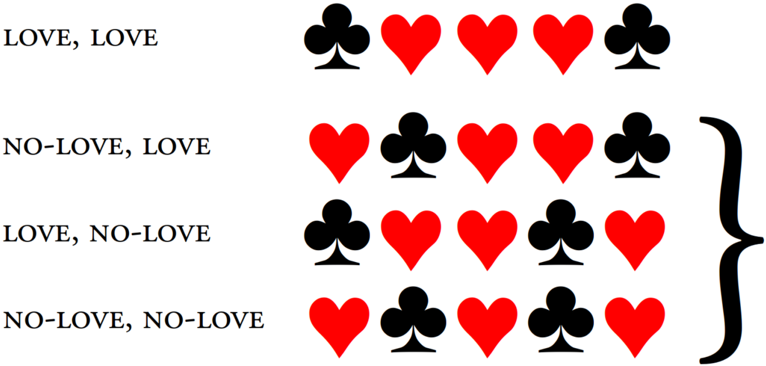


Test d'affinité



Alice et Bob coupent chacun une fois le tas de cartes (en privé). À la fin, seulement s'il y a trois cœur consécutifs, les deux sont compatibles.

Test d'affinité



Les deux coupes répresentent un décalage circulaire qui conserve les 3 cœurs consécutifs.

Calculs distribués entre plusieurs parties

Propriétés

- Chaque entité possède sa partie des données
- À la fin du protocole, chaque participant apprend le résultat du calcul (l'evaluation de la fonction)
- Le calcul est réalisé de manière à ce qu'aucune des parties ne puisse déduire les données de l'autre à partir des résultat du calcul et de ses propres données
- Il suffit qu'un seul participant soit honnête pour que le protocole assure la confidentialité des données privées de Alice et de Bob

Partage du secret

Problème des pirates

Il existe de nombreux cas où il faut partager un secret entre plusieurs personnes.
Par exemple, un trésor partagé par trois pirates.

Partage du secret

Probléme des pirates

- Trois pirates ont enterré un trésor.
- La carte de l'emplacement du trésor est découpée en trois parties.
- Chaque personne detient une partie.
- Il faut les trois parties de la carte pour retrouver l'emplacement du trésor.

Partage du secret

Formellement

Partage de secret à n participants avec seuil k :

- k personnes prises parmi ces n peuvent reconstituer le secret
- $(k-1)$ participants ne peuvent pas reconstituer le secret.

Partage du secret à seuil

Scénario

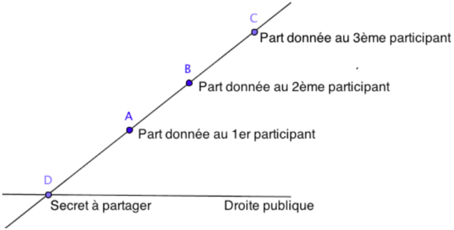
Dans une banque ayant trois responsables, pour éviter la corruption, on peut estimer qu'aucun responsable ne peut ouvrir à lui seul le coffre.
Cependant, il est raisonnable que deux des trois responsables puissent ensemble ouvrir le coffre, notamment si le troisième est indisponible.
On parle alors de partage de secret à seuil.

Partage du secret à seuil

Arme nucléaire

- C'est un tel système qui était en oeuvre en Russie au début des années 1990 pour utiliser l'arme nucléaire.
- Il fallait la participation de deux personnes parmi le président, le ministre de la défense et le chef des armées.

Partage du secret



Système de secret à n participants, avec un seuil égal à 2

- Le secret à partager est constitué par les coordonnées (x, y) d'un point du plan.
- Ce point est défini comme intersection de deux droites.
- On fait publique l'équation d'une droite qui contient le point.
- À chaque participant on donne les coordonnées d'un point sur la deuxième droite.

Partage du secret - Shamir 1979

La protocole de Shamir pour partager un secret

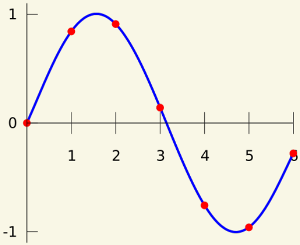
- Il y a n participants, et le seuil pour reconstituer le secret est t participants.
- Le secret à partager est S, un nombre réel.
- On choisit au hasard et de façon uniforme les réels $a_1 \ldots, a_{t-1}$
- On considère le polynôme de degré $t-1$ et des coefficients $a_1 \ldots, a_{t-1}$ et terme libre S :

$$P(X) = S + \sum_{j=1}^{t-1} a_j X^j.$$

Partage du secret - Shamir 1979

La protocole de Shamir pour partager un secret

- Si t participants mettent leurs informations en commun, ils connaissent t points et leurs images par un polynôme de degré $t-1$.
- Par la théorie d'interpolation de Lagrange, on sait reconstituer P, et donc retrouver S.
- On peut démontrer que si on dispose de seulement $t-1$ points sur la courbe de P, on ne peut pas retrouver P



$$P(X) = S + \sum_{j=1}^{3} a_j X^j$$

Preuves sans divulgation

Problème

Trouver Charlie dans une grande image.

Preuve de connaissance

Comment prouver qu'on a trouvé Charlie sans révéler où il est ?

Preuve de connaissance

Preuves sans divulgation

OÙ EST CHARLIE?

Preuve de connaissance

Comment prouver qu'on conaît la solution sans la révéler ?

Deux méthodes

1. photocopier et découper
2. mettre un grand cache avec un trou de la forme de Charlie

Preuves de connaissance

Utilisation - Identification

Identification : prouver son identité ou son appartenance à un groupe

- Accéder à son compte sur un ordinateur partagé entre plusieurs ordinateurs, ou à un réseau ;
- Paiement par CB : prouver qu'on connaît le code confidentiel sans le révéler

Preuves d'identification

Propriétés

1. **Consistante** : si Alice connaît effectivement le secret, tout se passe bien
2. **Significative** : la preuve montre bien qu'Alice connaît le secret
   - Sans connaissance du secret, un tricheur est détecté tôt ou tard
3. **Sans divulgation d'information** : la preuve n'apprend rien de plus que la possession du secret par Alice, et n'est pas transférable
   - Bob n'apprend pas le secret
   - Bob ne peut pas, a posteriori, convaincre un tiers qu'Alice connaissait le secret

Divulgation nulle de connaissance

Contexte

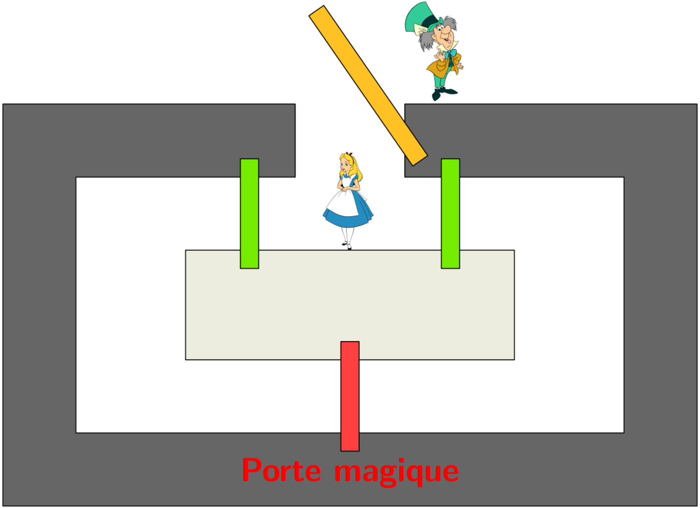
- Le prouveur prétend connaître un secret
- Il veut convaincre le vérifiéur qu'il connaît un tel secret
- Il veut le faire sans transférer cette connaissance au vérifiéur
- Le vérifiéur veut être sûr qu'il a en face de lui quelqu'un qui connaît effectivement le secret
- Les preuves sont interactives et randomisées

Divulgation nulle de connaissance

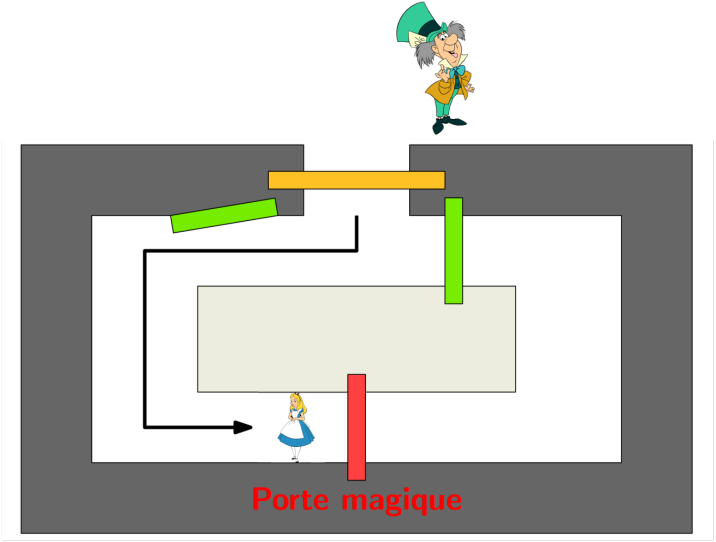
Scénario (La caverne d'Ali Baba)

- Alice entre dans la caverne avec deux couloirs séparés par une porte magique
- Alice veut convaincre Bob qu'elle connaît le secret pour ouvrir la porte magique et passer de l'autre côté
- Bob demande à Alice de sortir à gauche ou à droite (il choisit).
- Alice sort du côté demandé.

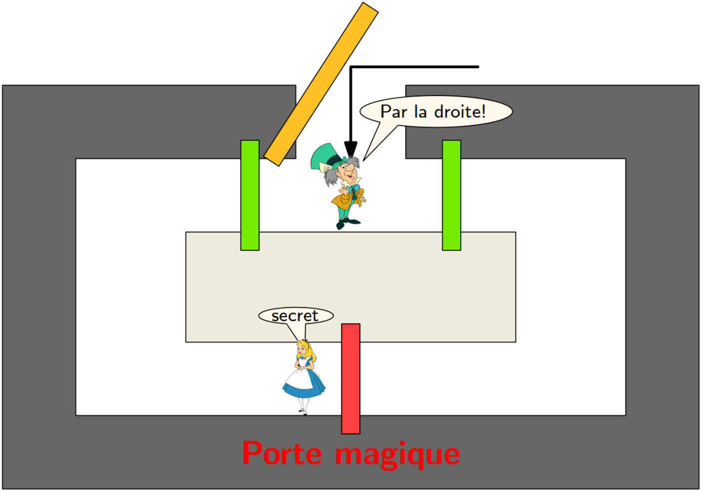
Divulgation nulle de connaissance (ZK)



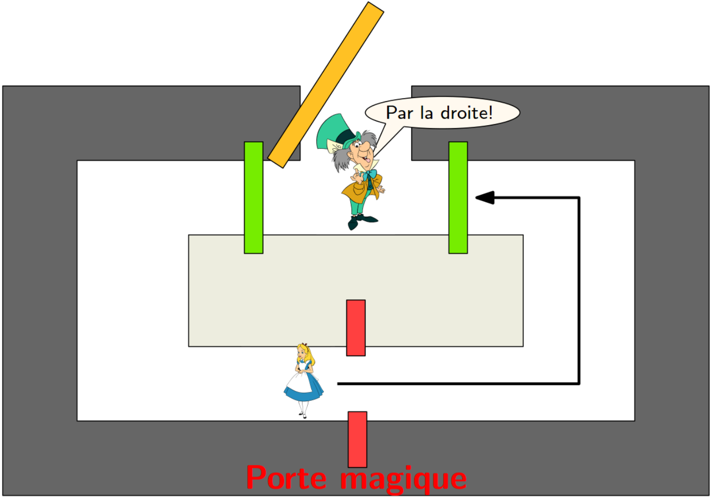
Divulgation nulle de connaissance (ZK)



Divulgation nulle de connaissance (ZK)



Divulgation nulle de connaissance (ZK)



Preuves de connaissance ZK

Propriétés

Avec probabilité $1/2$ Alice a été obligée d'utiliser la clé et la potion magique pour passer de l'autre côté

- Le prouveur connaît le secret
- Si un prouveur est capable de s'authentifier avec probabilité non négligeable :
  - alors il est capable de répondre aux deux défis possibles (droite et gauche)
  - sinon sa probabilité d'être acceptée serait de $1/2$

Preuve de connaissance ZK

Rappel - Racines carrées modulo n

Soit $n = pq$ un module RSA, et $x < n$.

- Si x est un carré modulo p et modulo q, il a deux racines carrées modulo chacun des facteurs et 4 racines modulo n

Factorisation $\Leftrightarrow$ **Racines carrées**

- Si on connaît la factorisation de n, on peut calculer les racines modulo p et q et appliquer le théorème des restes chinois
- Si on a une méthode pour extraire des racines carrées modulo n, on peut factoriser et retrouver p et q

Le protocole d'identification de Fiat-Shamir

Alice, l'utilisateur, veut s'identifier auprès d'un serveur, Bob :

Paramètres

- Alice choisit deux grands nombres premiers p et q et calcule $n = pq$
- Alice choisit ensuite au hasard un nombre entier x entre 1 et $n-1$ et calcule
$$y = x^2 \mod n.$$
- Le couple (n, y) est sa clé publique, et x sa clé secrète.

But

- Alice souhaite prouver à Bob qu'elle connait x (sans le réveler)

Le protocole d'identification de Fiat-Shamir

Public: n, y
Privé: x tel que: $x^2 = y \bmod n$

Alice		Bob
$r \bmod n$		
$t = r^2 \bmod n$	$\xrightarrow{\quad t \quad}$	
		$e \in \{0,1\}$
	$\xleftarrow{\quad e \quad}$	
$s = r/x^e \bmod n$	$\xrightarrow{\quad s \quad}$	
		Vérifier
		$t = s^2 y^e \bmod n$

Le protocole d'identification de Fiat-Shamir

Sécurité

Alice ne connaissant pas x a deux choix :

1. Alice ne triche pas lors de la première étape (calcul et envoi de $t = r^2$) :
   - Si $e = 0$ elle pourra répondre toujours correctement à la question du serveur
   - Si $e = 1$, elle devra choisir un nombre au hasard s, et il n'a pas plus d'une chance sur $n - 1$ de tomber sur r/x.
2. Alice triche lors de l'envoi de t. Dans ce cas, elle peut parier dès le départ sur le bit e que le serveur enverra :
   - Si elle parie $e = 0$, elle envoie effectivement $t = r^2$, puis ensuite $s = r$
   - Si elle parie $e = 1$, elle envoie alors $t = r^2y$, puis ensuite $s = r$ qui vérifie bien $t = s^2y$

Le protocole d'identification de Fiat-Shamir

Sécurité

- Alice, l'utilisateur, a une chance sur deux de faire le bon pari
  - Si elle a fait le mauvais pari, elle a une chance infime de donner la bonne solution.
- Avec un tour de ce protocole, Alice a une probabilité p de faire le bon choix (avec $p \approx 1/2$ si n est grand).
- En répétant ce protocole un certain nombre de fois, le serveur (Bob) pourra s'assurer de l'identité de l'utilisateur.
- **Protocole sans divulgation de connaissance** : quelle que soit la façon dont le serveur utilise le protocole, même en le détournant (par exemple, en ne choisissant pas le bit e au hasard), il ne pourra rien apprendre sur la clé x

Le protocole d'identification de Schnorr

Paramètres

- un nombre premier p
- un deuxième nombre premier q, diviseur de $p-1$
- un générateur g du groupe cyclique d'ordre q de $\mathbb{Z}_p^\star$.
- un entier $x < q$ et on calcule

$$y = g^x \mod n.$$

- la clé publique est (p, q, g, y), le secret est x.

But

- Étant donné y, prouver que l'on connaît x (sans le réveler)

Le protocole d'identification de Schnor

Public: p, q, g, y
Privé: x tel que: $g^x = y \bmod p$

Alice		Bob
$r \bmod q$		
$t = g^r \bmod p$	$\xrightarrow{t}$	
	$\xleftarrow{e}$	$e \in \{0, 1\}$
$s = r - ex \bmod q$	$\xrightarrow{s}$	Vérifier
		$t = g^s y^e \bmod p$

Preuve de connaissance ZK

Conclusions

L'identification est une composante essentielle

- conditionne le bon déroulement d'une transaction
- contrôle d'accès, etc.

Le zero-knowledge est une exigence très forte :

- "sécurité maximale" : on ne révèle que ce qu'il faut
- sécurité accessible en pratique (pour des cas simples)
- outil théorique puissant, nombreuses variante

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

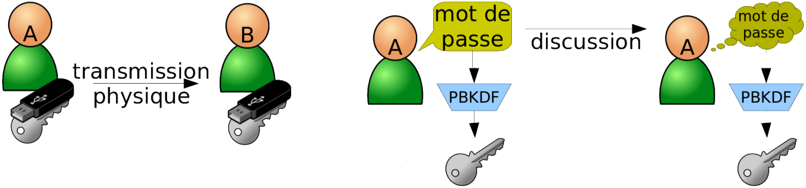
Clé secrètes

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

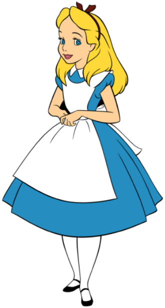
- A choisit la clé, la chiffre à destination de B, qui sera le seul à pouvoir la déchiffrer
- Solution efficace pour la confidentialité

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

Echange de clé Diffie-Hellman

Choisit x

Choisit y



$\text{A}=g^x \longrightarrow$

$\longleftarrow \text{B}=g^y$

calcule B^x

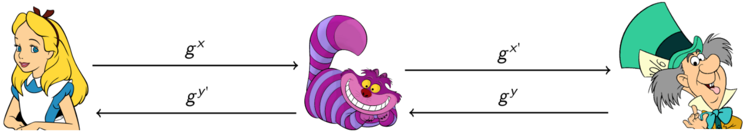
calcule A^y

Clé commune

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

Attaque "Man-in-the-middle"

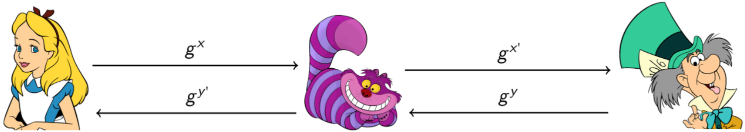
Choisit x Choisit y



Attaque "Man-in-the-middle"

Choisit x

Choisit y



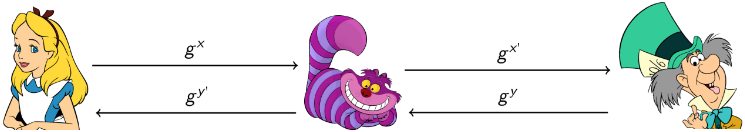
Calcule $g^{xy'}$

Calcule $g^{x'y}$

Attaque "Man-in-the-middle"

Choisit x

Choisit y



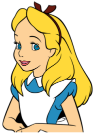
Calcule $g^{xy'}$

Calcule $g^{x'y}$

Ils calculent des clés differentes

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

Solution : Authentification



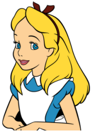
choisit x $\xrightarrow{g^x,\ \mathtt{sign}_A(g^x)}$ vérifie

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

Diffie-Hellman signé

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

Solution : Authentification



choisit x $\xrightarrow{\quad g^x \quad}$

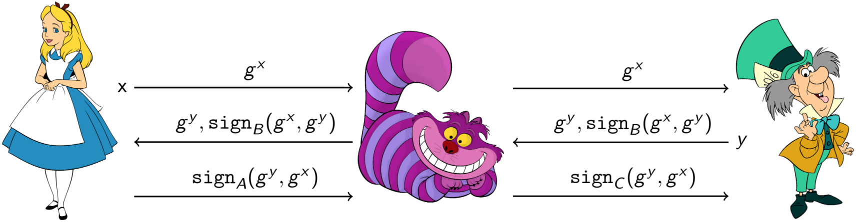
vérifie $\xleftarrow{\quad g^y, \mathtt{sign}_B(g^y, g^x) \quad}$ choisit y

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

Diffie-Hellman signé - V2

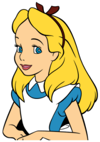
- Evite les attaques par le milieu
- Evite le rejeu : la valeur du déstinataire est aussi signée

Usurpation d'identité



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

Solution : Authentification



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

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

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

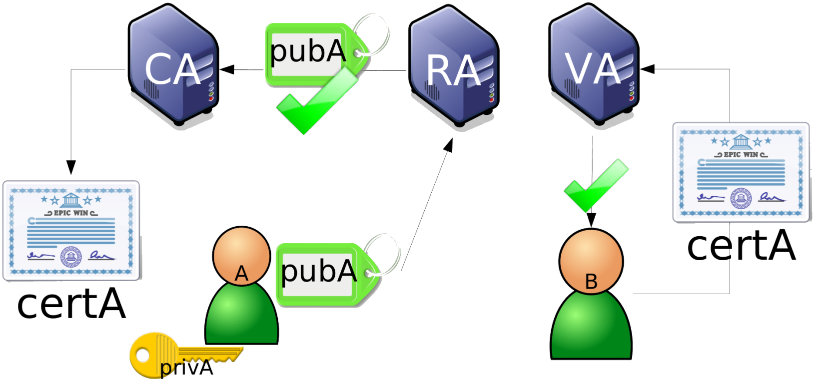
Gestion de clés publiques - PKI

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	Registration Authority	Validation Authority
Émet des certificats signés	Effectue les vérifications d'identités	Confirme qu'un certificat est valide

Gestion de clés - Application