Les protocoles de sécurité sur Internet et la logique de la connaissance

Qu'est-ce qu'un protocole ?

Un protocole est un ensemble de règles que des logiciels utilisent pour communiquer.

Qu'est-ce que la sécurité ?

La sécurité sur le Web cherche à garantir les propriétés suivantes :

– confidentialité, y compris l'absence de fuite d'information,

– intégrité,

– disponibilité.

Qu'est-ce que la sécurité ?

La sécurité sur le Web cherche à garantir les propriétés suivantes :

– confidentialité, y compris l'absence de fuite d'information,
– intégrité,
– disponibilité.

et à mettre en œuvre trois fonctions :

– l'authentification,
– la non répudiation.
– la prévention du déni de service

Les protocoles de sécurité et les rôles

Souvent, pour illustrer un protocole de sécurité, on raconte une histoire, où tous les personnages jouent un rôle.

Comme dans la Commedia dell'Arte, leur rôle est attaché à leur nom.

Alice,
Bob,
Carole,
Dave,

sont les principaux acteurs.

Ève enregistre tout.

Mallory est malicieuse

Trent est très écouté,

c 'est un tiers de confiance

ou un garant.

Quelques maximes

Tout le monde se méfie de tout le monde.

Quelques maximes

Tout le monde se méfie de tout le monde.

Un protocole doit être robuste à toute attaque (sécurité).

Quelques maximes

Tout le monde se méfie de tout le monde.

Un protocole doit être robuste à toute attaque (sécurité).

Il est très difficile de prédire la robustesse d’un protocole.

Quelques maximes

Tout le monde se méfie de tout le monde.

Un protocole doit être robuste à toute attaque (sécurité).

Il est très difficile de prédire la robustesse d'un protocole.

En général, son inventeur explique pourquoi il le croit robuste et le propose à la communauté des experts qui essaient de trouver des attaques. S'il résiste, il est considéré comme bon.

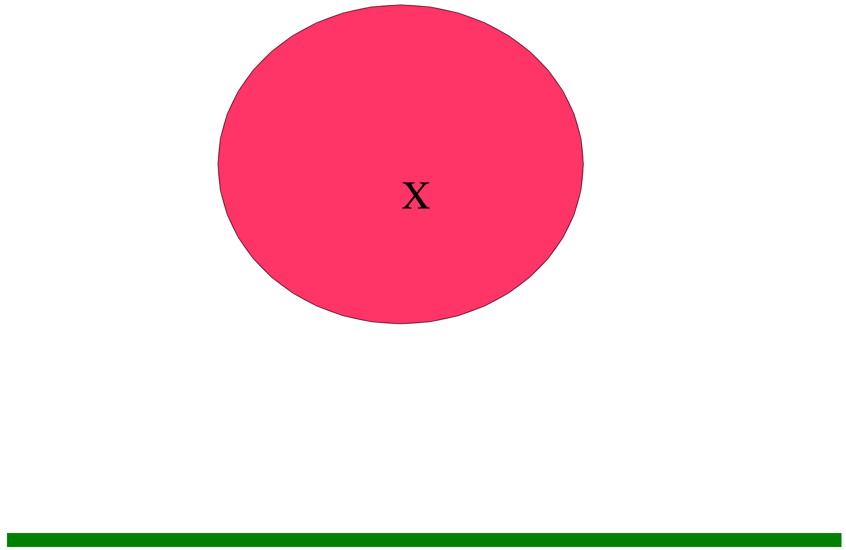
Jouer à pile ou face sur Internet

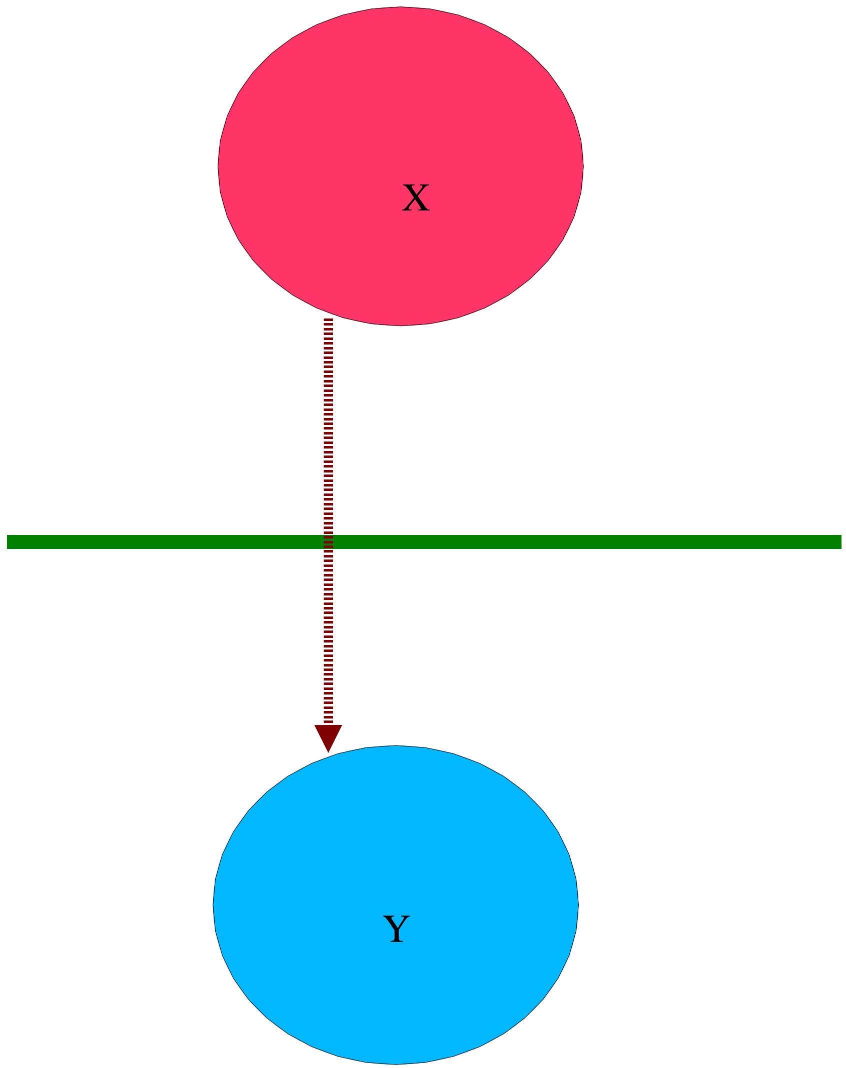
Un protocole extrêmement simple à la base des mécanisme de signature électronique.

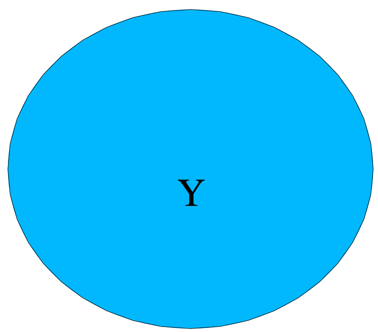
Fonctions à sens unique

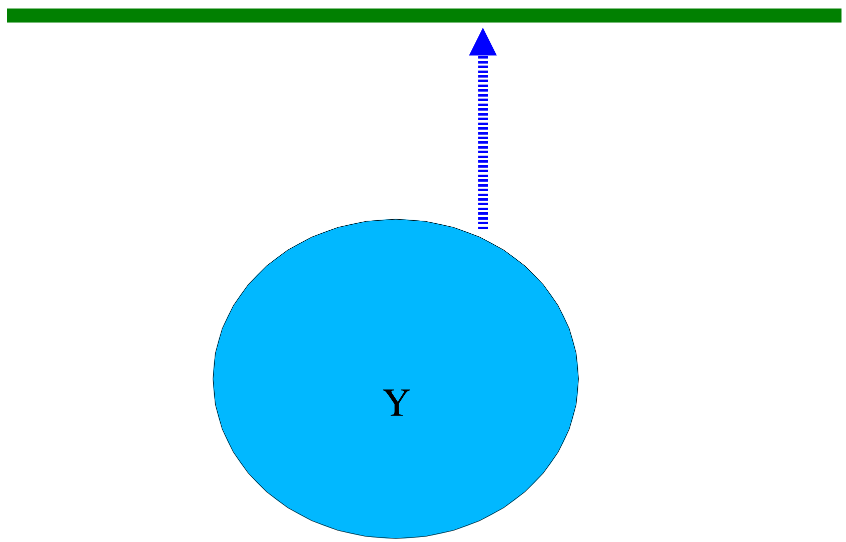
Une fonction à sens unique $SensUnique$ est une fonction pour laquelle

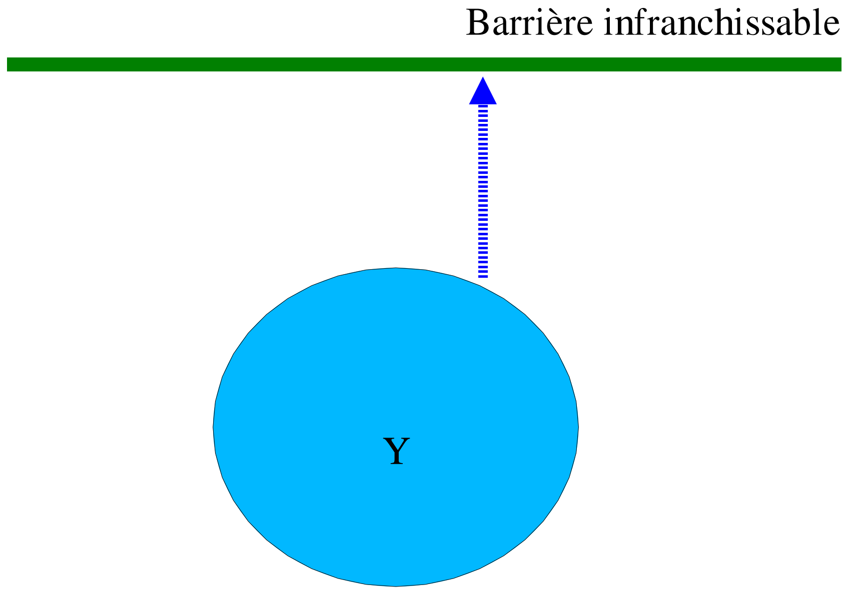
- on peut **calculer** $y = SensUnique(x)$ quand on connaît x,
- mais on ne peut pas **calculer** x quand on connaît y.

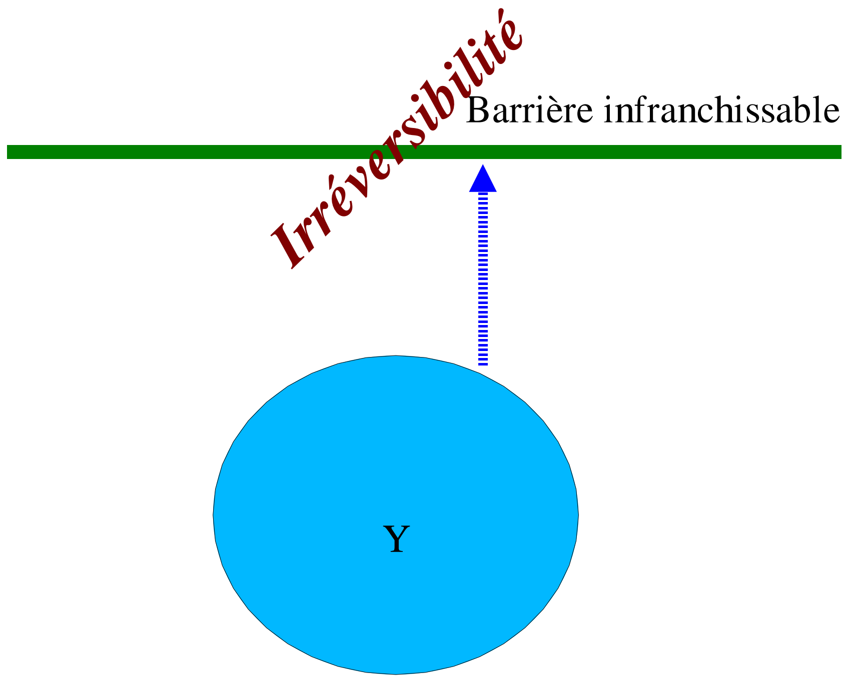

x


X
Y


Y


Y


Barrière infranchissable
Y


Irréversibilité
Barrière infranchissable
Y

Protocole pile ou face à base de fonction à sens unique

– Alice choisit un nombre x au hasard.

Protocole pile ou face à base de fonction à sens unique

- Alice choisit un nombre x au hasard.
- Alice calcule $y = SensUnique(x)$.
- Alice envoie y à Bob.

Protocole pile ou face à base de fonction à sens unique

– Alice choisit un nombre x au hasard.

– Alice calcule $y = SensUnique(x)$.

– Alice envoie y à Bob.

– Bob devine si x est pair ou impair.

Protocole pile ou face à base de fonction à sens unique

- Alice choisit un nombre x au hasard.
- Alice calcule $y = SensUnique(x)$.
- Alice envoie y à Bob.
- Bob devine si x est pair ou impair.
- Bob communique sa prédiction à Alice.
- Si Bob a correctement deviné, le résultat final est pile, sinon c'est face.

Protocole pile ou face à base de fonction à sens unique

– Alice choisit un nombre x au hasard.

– Alice calcule $y = SensUnique(x)$.

– Alice envoie y à Bob.

– Bob devine si x est pair ou impair.

– Bob communique sa prédiction à Alice.

– Si Bob a correctement deviné, le résultat final est pile, sinon c'est face.

– Alice annonce le résultat et envoie x à Bob.

– Bob vérifie que $y = SensUnique(x)$.

Clés de chiffrement

Clés publiques et clés privées

Dans un système de clés asymétriques, on peut distinguer :

- une clé publique :
  - tout le monde peut m'envoyer des messages chiffrés (ou cryptés) que je serai le seul à déchiffrer.

Clés publiques et clés privées

Dans un système de clés asymétriques, on peut distinguer :

- une clé publique :
  - tout le monde peut m'envoyer des messages chiffrés (ou cryptés) que je serai le seul à déchiffrer.
- une clé privée :
  - je peux déchiffrer des messages que l'on m'envoie chiffrés avec ma clé publique,
  - je peux chiffrer des messages avec ma clé privée que mes destinataires déchiffreront avec ma clé publique (signature).

Le protocole de Needham-Schroeder

Quelques notations pour les protocoles

– $Un \rightarrow Deux : Message$

L'agent Un envoie un message $Message$ à l'agent $Deux$.

Quelques notations pour les protocoles

- $Un \rightarrow Deux : Message$

  L'agent Un envoie un message $Message$ à l'agent $Deux$.

- $\{M\}_{Ka}$

  le contenu M est chiffré par la clé K_a.

Quelques notations pour les protocoles

- $Un \rightarrow Deux : Message$

  L'agent Un envoie un message $Message$ à l'agent $Deux$.
- $\{M\}_{Ka}$

  le contenu M est chiffré par la clé K_a.
- N_a est un nonce créé par le l'agent a.

Quelques notations pour les protocoles

- $Un \rightarrow Deux : Message$

  L'agent Un envoie un message $Message$ à l'agent $Deux$.
- $\{M\}_{Ka}$

  le contenu M est chiffré par la clé K_a.
- N_a est un nonce créé par le l'agent a.

  c'est nombre spécialement créé pour cet instance du protocole,

  comme garantie de fraîcheur.

Le protocole de Needham-Schroeder

1. $Alice \rightarrow Bob :$ $\{Na, A\}_{Kb}$

2. $Bob \rightarrow Alice :$ $\{Na, Nb\}_{Ka}$
3. $Alice \rightarrow Bob :$ $\{Nb\}_{Kb}$

Une attaque du protocole de Needham-Schroeder

1. $Alice \rightarrow Mallory: \quad \{Na, A\}_{Km}$
1. $Mallory \rightarrow Bob: \quad \{Na, A\}_{Kb}$
2. $Bob \rightarrow Mallory: \quad \{Na, Nb\}_{Ka}$
2. $Mallory \rightarrow Alice: \quad \{Na, Nb\}_{Ka}$
3. $Alice \rightarrow Mallory: \quad \{Nb\}_{Km}$
3. $Mallory \rightarrow Bob: \quad \{Nb\}_{Kb}$

Où est la faute ?

On a mal perçu ce que savait chaque agent.

Où est la faute ?

On a mal perçu ce que savait chaque agent.

On a oublié le rôle d’un agent malveillant.

Où est la faute ?

On a mal perçu ce que savait chaque agent.

On a oublié le rôle d’un agent malveillant.

Il faut formaliser précisément cette connaissance.

Logique de la connaissance

Qu'est-ce que la logique de la connaissance ?

- La logique de la connaissance ou logique épistémique est la logique qui formalise
  - "l'agent i sait que p", noté $K_i(p)$,
  - "p est une connaissance commune", noté $C(p)$.

La connaissance commune

$C(p)$ formalise des phrases comme

- "C'est un fait bien connu que p, sauf des fous."
- "L'agent i sait que l'agent j sait que l'agent i sait que l'agent j sait que, etc.".

La connaissance commune

$C(p)$ formalise des phrases comme

– “C’est un fait bien connu que p, sauf des fous.”

– “L’agent i sait que l’agent j sait que l’agent i sait que , etc.”.

On a besoin d’une modalité E, dite de “connaissance partagée”,

“Tout le monde sait que p”,

$$E_G(p) = \bigwedge_{i \in G} K_i(p).$$

La connaissance commune

$C(p)$ formalise des phrases comme

– "C'est un fait bien connu que p, sauf des fous."

– "L'agent i sait que l'agent j sait que l'agent i sait que , etc.".

On a besoin d'une modalité E, dite de "connaissance partagée",

"Tout le monde sait que p",

$$E_G(p) = \bigwedge_{i \in G} K_i(p).$$

La connaissance commune n'est pas la connaissance partagée.

Les trois sages et leurs chapeaux

Le problème

Le roi dit

- Vous êtes trois sages.
- Je vous bande les yeux.
- Je vous mets des chapeaux sur la tête

  parmi lesquels il y a au plus deux chapeaux rouges.
- En regardant, les chapeaux des autres, devinez si vous avez un chapeau rouge ou non sur la tête.

Conclusion

Le problème (suite)

Le premier dit : Je ne sais pas.

Le deuxième dit : Je ne sais pas.

Le troisième dit : Je sais.

Comment a-t-il fait ?

En résumé

Nous avons vu

– les protocoles

En résumé

Nous avons vu

– les protocoles

– la cryptographie et le chiffrement,

En résumé

Nous avons vu

- les protocoles
- la cryptographie et le chiffrement,
- les clés : publiques, privées, symétriques,

En résumé

Nous avons vu

- les protocoles
- la cryptographie et le chiffrement,
- les clés : publiques, privées, symétriques,
- les fonctions a sens unique,

En résumé

Nous avons vu

– les protocoles

– la cryptographie et le chiffrement,

– les clés : publiques, privées, symétriques,

– les fonctions a sens unique,

– les nonces, la fraîcheur.

Il faut retenir

La sécurité ne réside pas seulement dans le chiffrement,

mais aussi dans la qualité du protocole.

Il faut retenir

La sécurité ne réside pas seulement dans le chiffrement,

mais aussi dans la qualité du protocole.

Or définir un bon protocole est difficile.