Communications sécurisées : les problèmes

Université de Franche-Comté

Pierre-Cyrille Héam

Sécurité – Fiabilité

- **Fiabilité** : le logiciel fonctionne comme il est sensé le faire.
  - Fonctionnelle : *Quand j'appuie sur le frein, la voiture ralenti*,
  - Quantitative : *Sur le plat, la voiture peut atteindre les 160 km/h*,
  - Robustesse : *Si un pneu éclate à moins de 100 km/h, le contrôle du véhicule est maintenu*.
  - ...
- **Sécurité** : Fiabilité face à un ou plusieurs adversaires malveillants et intelligents.

Sécurité des communications

On va au ciné ?

Comment Penny peut-elle dire un secret à Leonard sans que Sheldon, dans la pièce, ne sache de quoi il retourne ?

Les solutions

- La **stéganographie** : cacher le message.
  - nécessite une méthode secrète : difficile à large échelle,
  - utilisation massive peu discrete et surcharge du traffic.
- La **cryptographie** : chiffrer le message en utilisant un code/chiffre.
- Il faut aussi des **protocoles** pour mettre en œuvre, à large échelle, la cryptographie.

Cadre de travail

La poste malhonnête (ça n'est pas la réalité) :

- Les personnes qui envoient les messages/colis/lettres sont chez elles et tout passe par la poste (le réseau est ouvert),
- Les postiers sont suceptibles d'ouvrir tous les messages non cachetés (chiffrés),
- Les postiers peuvent fabriquer de fausses lettres/colis/messages,
- Certains postiers sont malhonnêtes, (le réseau n'est pas sûr)
- Les postiers n'ouvrent pas les colis/lettres cachetés (la cryptographie est parfaite).

Comment faire ?

On va au ciné ?

Penny et Leonard sont dans des pièces séparées, sans moyen de communication autre que les messages qui transitent par Sheldon.

Plan

Three Pass Shamir Protocol

Three Pass Shamir Protocol

Three Pass Shamir Protocol

Three Pass Shamir Protocol

Attack on the Three Pass Shamir Protocol

Attack on the Three Pass Shamir Protocol

Attack on the Three Pass Shamir Protocol

Attack on the Three Pass Shamir Protocol

Diffie Hellman

171, 452327,

171, 452327

171, 452327,

171, 452327,

Diffie Hellman

171, 452327,

X_p

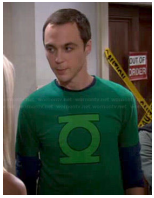
171, 452327, 31827

X_p = reste de

$171^{31827}/452327$

171, 452327,

Diffie Hellman



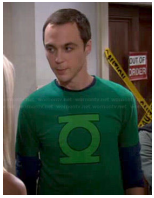
171, 452327, X_p,

171, 452327, 31827

X_p = reste de $171^{31827}/452327$

171, 452327, X_p

Diffie Hellman

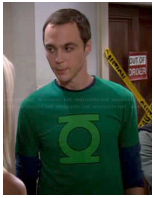


171, 452327, X_p,

171, 452327, 31827
X_p = reste de
$171^{31827}/452327$

171, 452327, X_p
289567

Diffie Hellman



171, 452327, X_p,

171, 452327, 31827

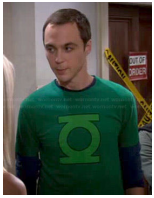
X_p = reste de $171^{31827}/452327$

171, 452327, X_p

289567

X_L = reste de $171^{289567}/452327$

Diffie Hellman



171, 452327, X_p,X_L

X_L

171, 452327, 31827
X_p = reste de
$171^{31827}/452327$
X_L

171, 452327, X_p
289567
X_L = reste de
$171^{289567}/452327$

Diffie Hellman

171, 452327, 31827
X_p = reste de $171^{31827}/452327$
X_L

171, 452327, X_p,X_L

171, 452327, 289567
X_L = reste de $171^{289567}/452327$
X_P

Diffie Hellman

171, 452327, 31827
X_p = reste de $171^{31827}/452327$
X_L

$X_p^{289567}/452327$ et $X_L^{31827}/452327$ ont le même reste

171, 452327, X_p,X_L

171, 452327, 289567
X_L = reste de $171^{289567}/452327$
X_P

Nouveaux Problèmes

- Fraîcheur,
- Rejeux,
- Authentification,
- Partage de clés,
- Chiffrement assymétrique lourd (sur le plan algorithmique).

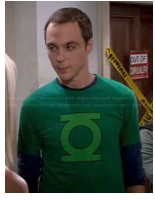
Idées : sessions avec des validités temporaires, avec authentification et mise en commun d'une clé symétrique partagée ; en s'appuyant sur le chiffrement asymétrique (type RSA).

Plan

Chiffrement assymétrique

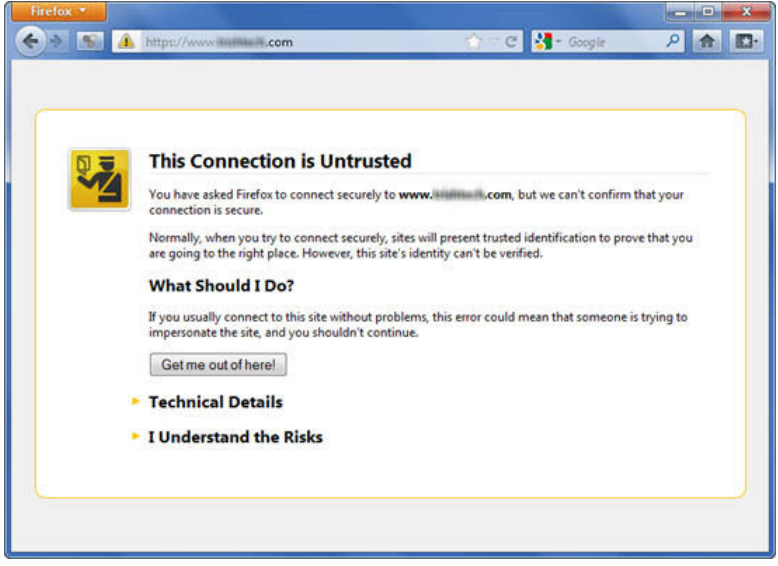
Une clé pour chiffrer (publique) et une clé pour déchiffrer (privée).

Je veux un cadena de Leonard.



Authentification

Exception IE ou Mozzilla :



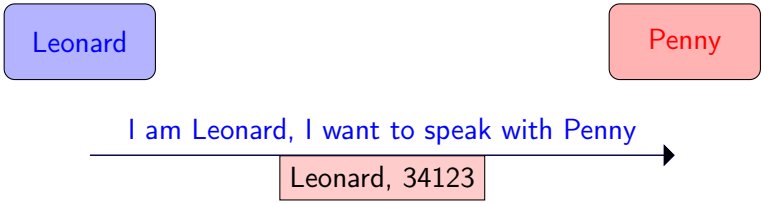
Comment Leonard sait-il que le message vient bien de Penny ?

Comment Leonard sait-il que le message vient bien de Penny ?

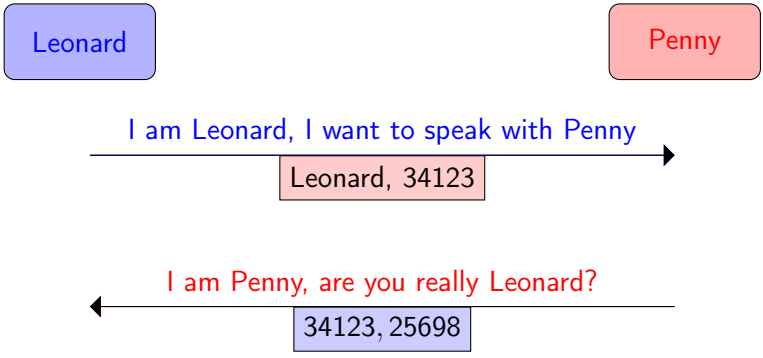
Indication : Si Penny envoie un message avec un nombre aléatoire chiffré avec le cadena de Leonard, s'il lui renvoie un message avec ce nombre, elle sait que seul Léonard est sencé connaître ce nombre.

NSPK

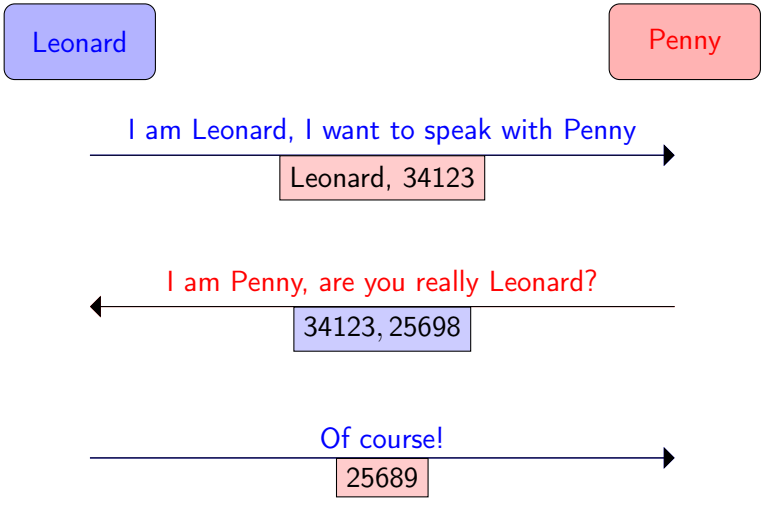
NSPK


Leonard
Penny
I am Leonard, I want to speak with Penny
Leonard, 34123

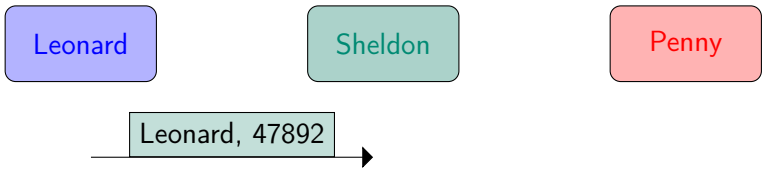
NSPK


Leonard
Penny
I am Leonard, I want to speak with Penny
Leonard, 34123
I am Penny, are you really Leonard?
34123, 25698

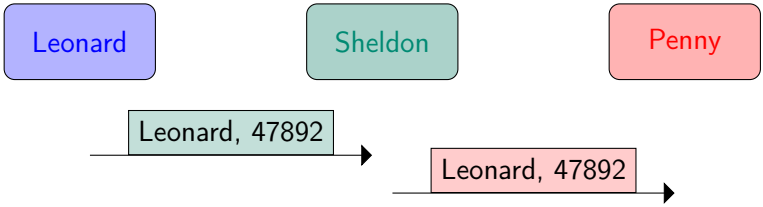
NSPK


Leonard
Penny
I am Leonard, I want to speak with Penny
Leonard, 34123
I am Penny, are you really Leonard?
34123, 25698
Of course!
25689

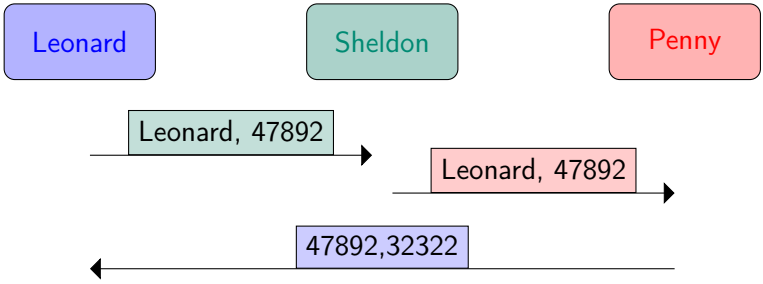
NSPK



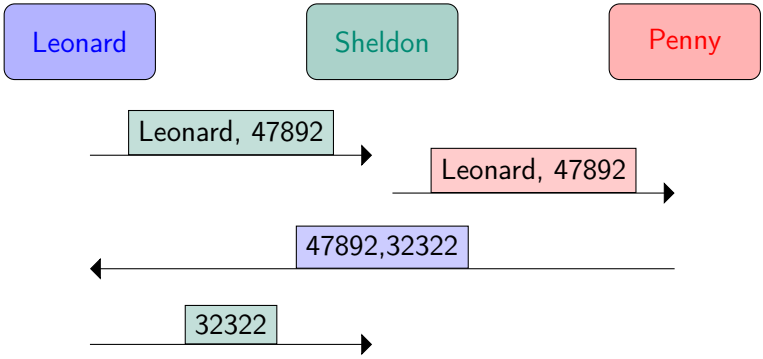
NSPK



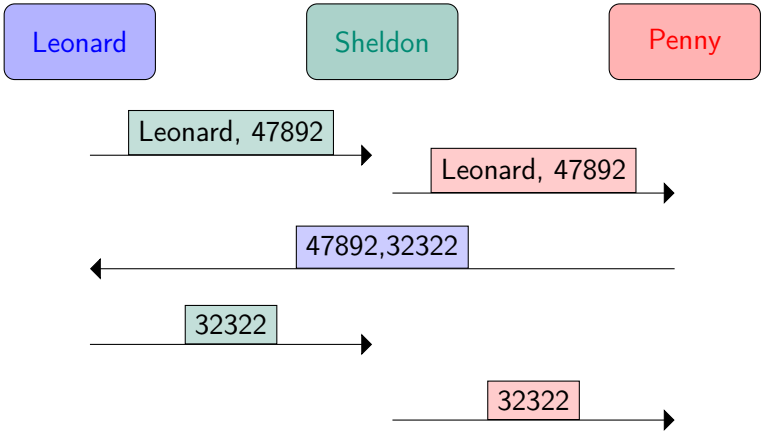
NSPK


Leonard
Sheldon
Penny
Leonard, 47892
Leonard, 47892
47892,32322

NSPK


Leonard
Sheldon
Penny
Leonard, 47892
Leonard, 47892
47892,32322
32322

NSPK



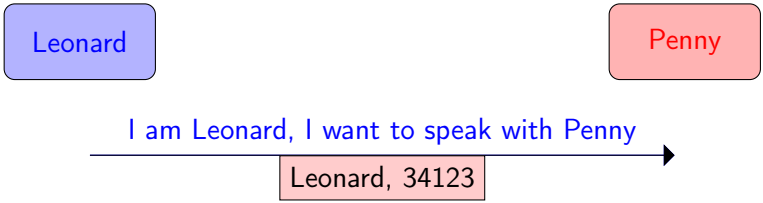
Penny croit communiquer avec Leonard mais parle en fait avec Sheldon.

NSPK-Lowe

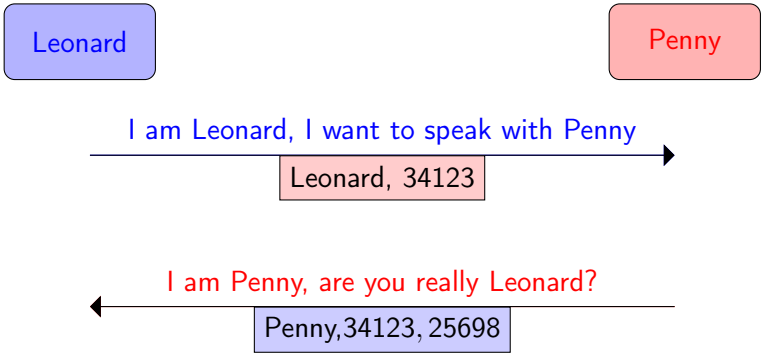
Leonard

Penny

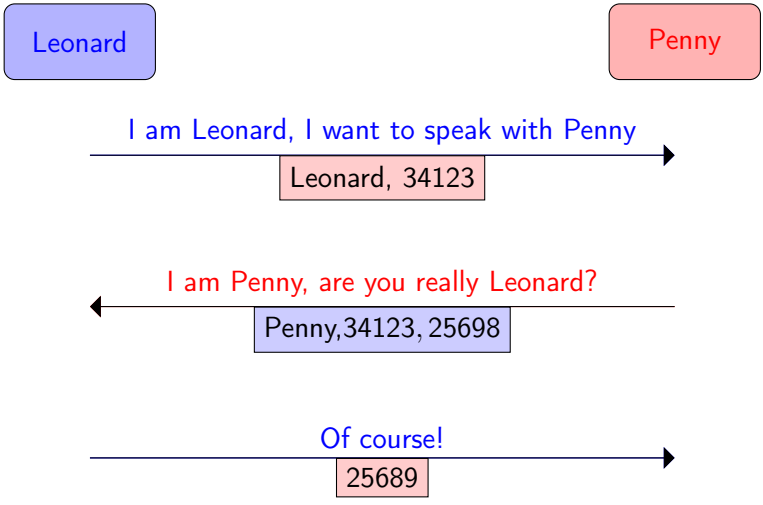
NSPK-Lowe


Leonard
Penny
I am Leonard, I want to speak with Penny
Leonard, 34123

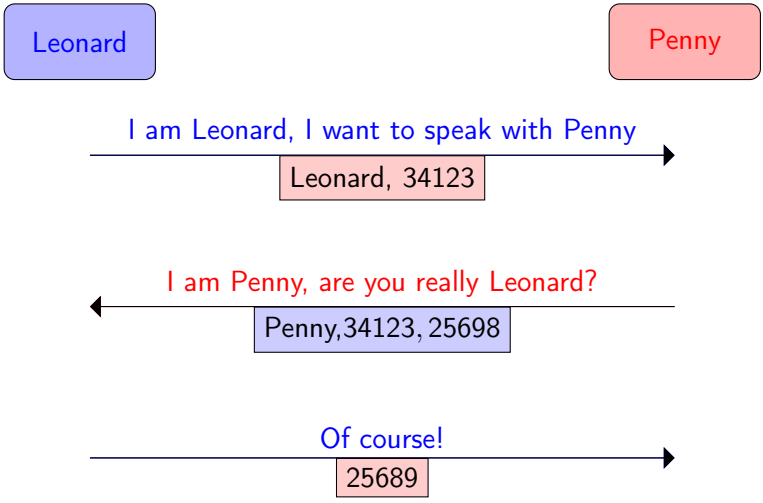
NSPK-Lowe


Leonard
Penny
I am Leonard, I want to speak with Penny
Leonard, 34123
I am Penny, are you really Leonard?
Penny,34123, 25698

NSPK-Lowe


Leonard
Penny
I am Leonard, I want to speak with Penny
Leonard, 34123
I am Penny, are you really Leonard?
Penny,34123, 25698
Of course!
25689

NSPK-Lowe



On peut **démontrer** qu'il n'y a pas de faille.

Notations - Remarques

On écrit plus succintement le protocole ainsi :

$A \rightarrow B$: $\{A, N_A\}_{PK_B}$
$B \rightarrow A$: $\{B, N_A, N_B\}_{PK_A}$
$A \rightarrow B$: $\{N_B\}_{PK_B}$

- Le nonce (*number used once*) N_B est ensuite utilisé comme clé secrète pour la session entre A et B.
- On souhaite minimiser les chiffrements à clés publiques (coûteux en ressources).

NSPK-Lowe avec serveur

- Il y a trois agents, A, B et S.
- A et B connaissent la clé publique de S.

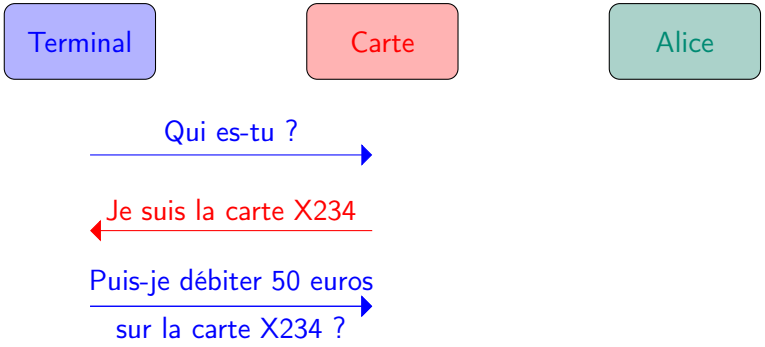
NSPK-Lowe avec serveur

- Il y a trois agents, A, B et S.
- A et B connaissent la clé publique de S.

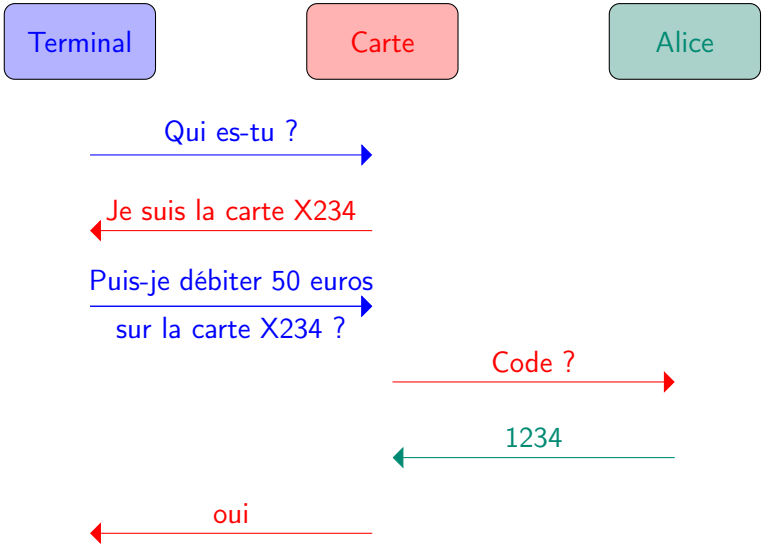
$A \to S$: $\{A, B\}$
$S \to A$: $\{B, PK_B\}_{PK_S^{-1}}$
$A \to B$: $\{A, N_A\}_{PK_B}$
$B \to S$: $\{B, A\}$
$S \to B$: $\{A, PK_A\}_{PK_S^{-1}}$
$B \to A$: $\{B, N_A, N_B\}_{PK_A}$
$A \to B$: $\{N_B\}_{PK_B}$

Plan

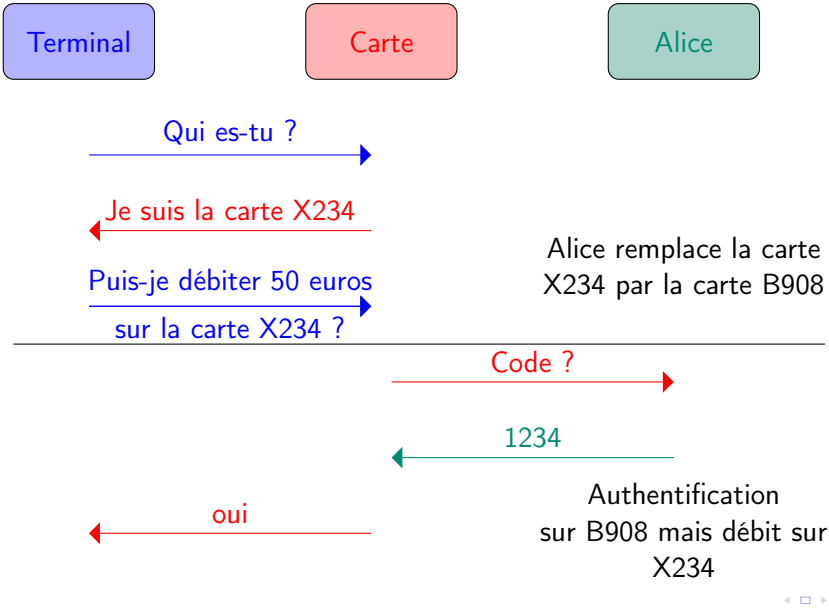
Carte Bleue


Terminal
Carte
Alice
Qui es-tu ?
Je suis la carte X234
Puis-je débiter 50 euros
sur la carte X234 ?

Carte Bleue


Terminal
Carte
Alice
Qui es-tu ?
Je suis la carte X234
Puis-je débiter 50 euros
sur la carte X234 ?
Code ?
1234
oui

Carte Bleue


Terminal
Carte
Alice
Qui es-tu ?
Je suis la carte X234
Alice remplace la carte X234 par la carte B908
Puis-je débiter 50 euros sur la carte X234 ?
Code ?
1234
Authentification sur B908 mais débit sur X234
oui

TCP

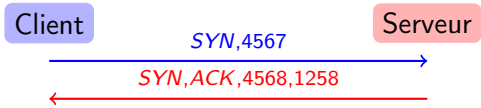
- Pour transmettre de l'information sur internet, les messages sont découpés en paquets transportés par le protocole IP.
- Les paquets paquets IP ne suivent pas tous nécessairement la même route et leur ordre peut être mélangé. Il peut s'en perdre aussi.
- TCP est le protocole chargé de gérer tout cela.

Pour cela TCP utilise :

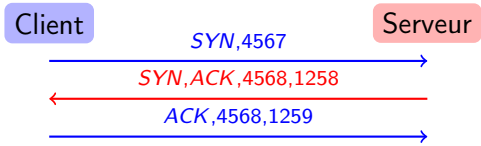
- des numéros de messages,
- des accusés de réceptions,
- procède en trois phases : ouverture de la session, transfert, clôture.

TCP

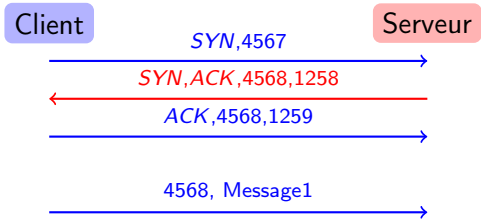
TCP



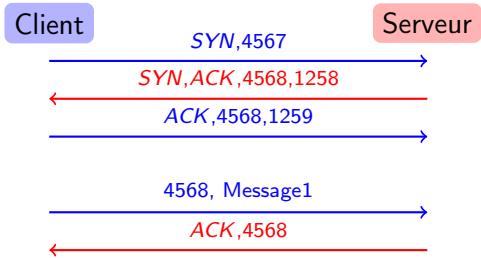
TCP



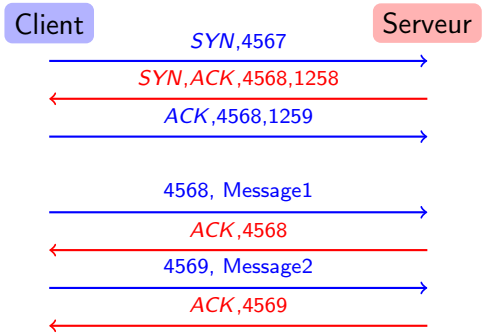
TCP


Client
Serveur
SYN,4567
SYN,ACK,4568,1258
ACK,4568,1259
4568, Message1

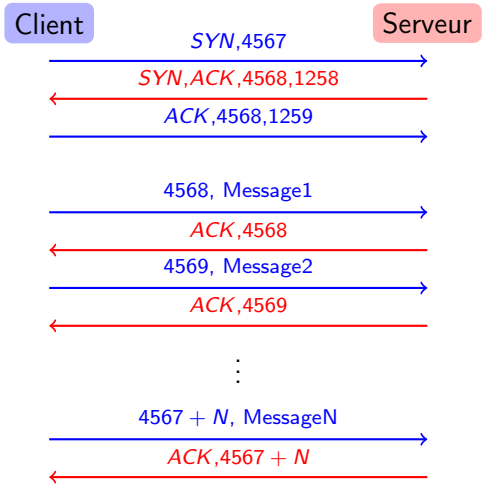
TCP


Client
Serveur
SYN,4567
SYN,ACK,4568,1258
ACK,4568,1259
4568, Message1
ACK,4568

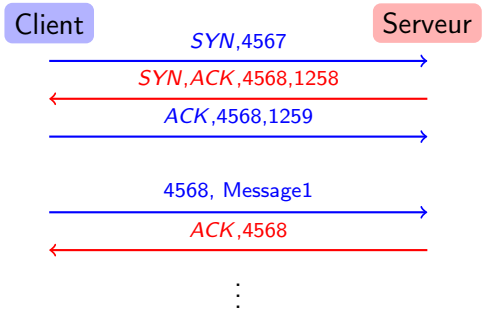
TCP


Client
Serveur
SYN,4567
SYN,ACK,4568,1258
ACK,4568,1259
4568, Message1
ACK,4568
4569, Message2
ACK,4569

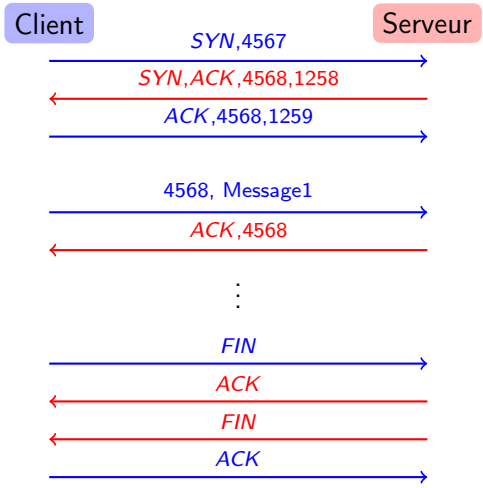
TCP


Client
Serveur
SYN,4567
SYN,ACK,4568,1258
ACK,4568,1259
4568, Message1
ACK,4568
4569, Message2
ACK,4569
4567 + N, MessageN
ACK,4567 + N

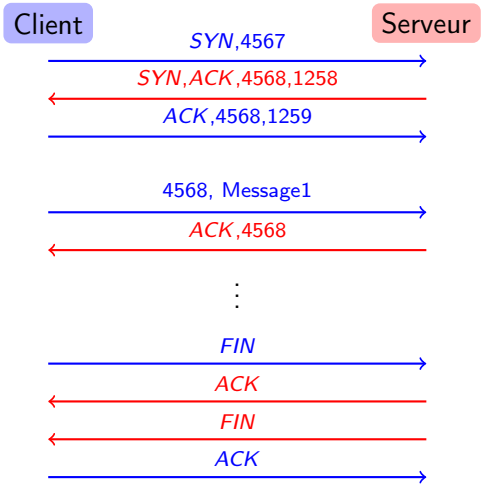
TCP


Client
Serveur
SYN,4567
SYN,ACK,4568,1258
ACK,4568,1259
4568, Message1
ACK,4568

TCP


Client
Serveur
SYN,4567
SYN,ACK,4568,1258
ACK,4568,1259
4568, Message1
ACK,4568
FIN
ACK
FIN
ACK

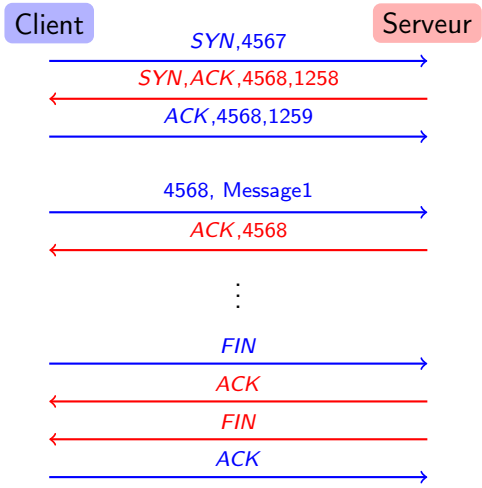
TCP



Attaque dite de *Mitnick*

- Envoi de demande d'ouverture de connexion par le premier message à un serveur.
- Sans faire la troisième étape : la connexion est dite semi-ouverte.
- Le nombre de connexions semi-ouvertes est limité : on bloque le serveur par un `deni de service`.

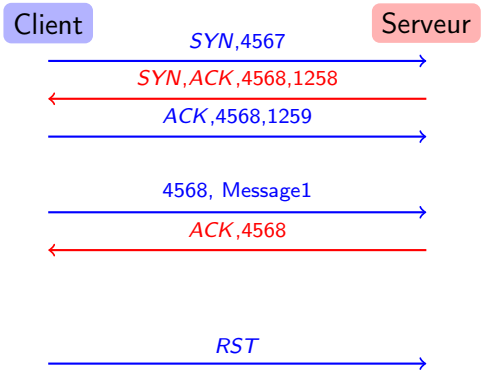
TCP



Attaque dite de *Morris*

- Detection d'une ouverture TCP.
- Prédiction du numéro de séquence si le générateur est mauvais,
- envoi de fausses données (avec les bons numéros de séquence).

TCP



Attaque dite de *Joncheray*
L'attaquant peut espionner le poste du client.

- Detection d'une ouverture TCP.
- Envoi d'un message de rupture brutale (avec l'IP du client).
- Récupération des données, possibilité de faire un *man in the middle*.

Les protocoles de vote

1. L'urne doit être publique (transparente),
2. Seuls les inscrits votent et doivent être identifiés,
3. Chacun doit vérifier que les votes viennent d'inscrits, et que chaque inscrit a voté au plus une fois,
4. Tout le monde doit pouvoir vérifier le comptage final,
5. L'urne ne doit pas permettre de savoir qui a voté quoi,
6. Chaque votant doit pouvoir vérifier que son vote est dans l'urne et non modifié,
7. Un votant ne doit pas pouvoir prouver son vote à un tiers,
8. Les autorités peuvent être malhonnêtes.

Propriétés

1. Secret fort,
2. Secret faible,
3. Authentification,
4. Non répudiation,
5. *time stamp*,
6. Intégrité,
7. Vote,
8. ...

Vérification Automatiques

- La plupart des propriétés sont indécidables si on en borne pas le nombre de sessions.
- La plupart des propriétés sont décidables si on borne le nombre de sessions, mais la complexité est élevée.
- Il existe des outils comme AVISPA ou ProVerif.

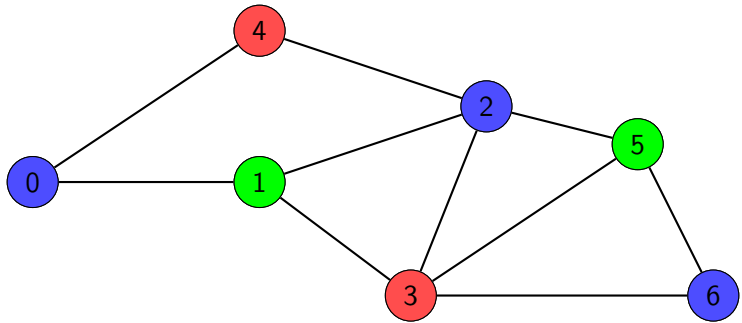
Objectif

Objectif : prouver que je connais un secret M sans rien dévoiler sur M. (prouver son identité sans la donner, non-répudiation, votes)

Illustration : Comment prouver à un aveugle que je sais différencier par la vue deux balles parfaitement identiques au toucher ?

3-COLOR

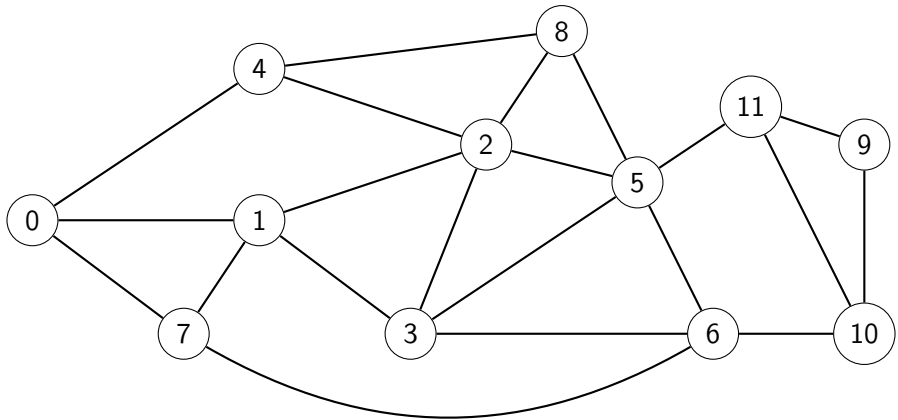
Données : Un graphe non orienté G.
Sortie : S'il existe, un 3-coloriage du graphe (deux sommets vosins n'ont pas la même couleur).



Protocole

Objectif

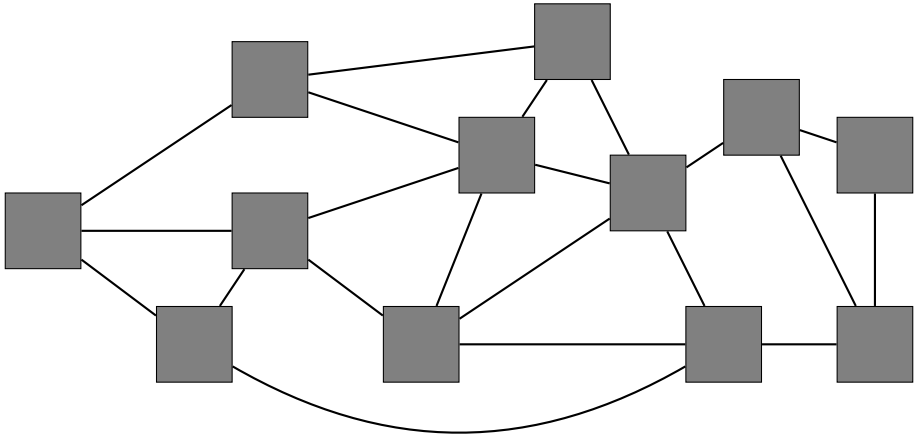
Alice connaît un 3-coloriage pour un graphe de très grande taille. Elle veut prouver à/convaincre Bob qu'elle connaît ce coloriage, mais sans le lui donner.



Protocole

Objectif

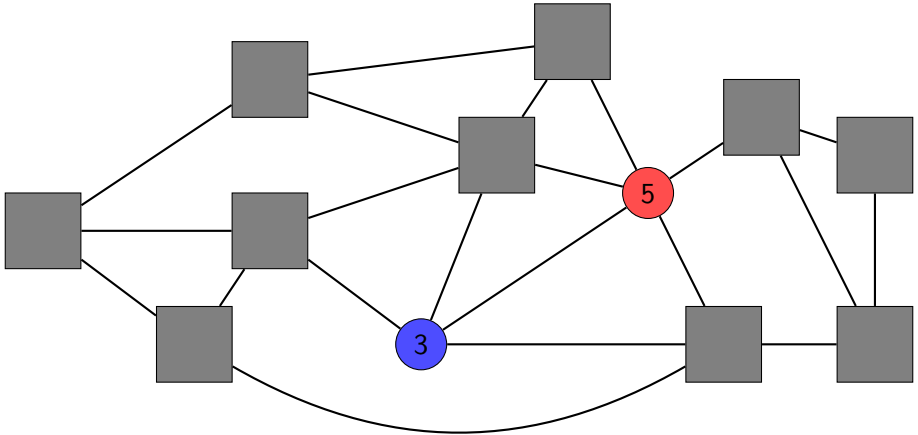
Alice connaît un 3-coloriage pour un graphe de très grande taille. Elle veut prouver à/convaincre Bob qu'elle connaît ce coloriage, mais sans le lui donner.



Protocole

Objectif

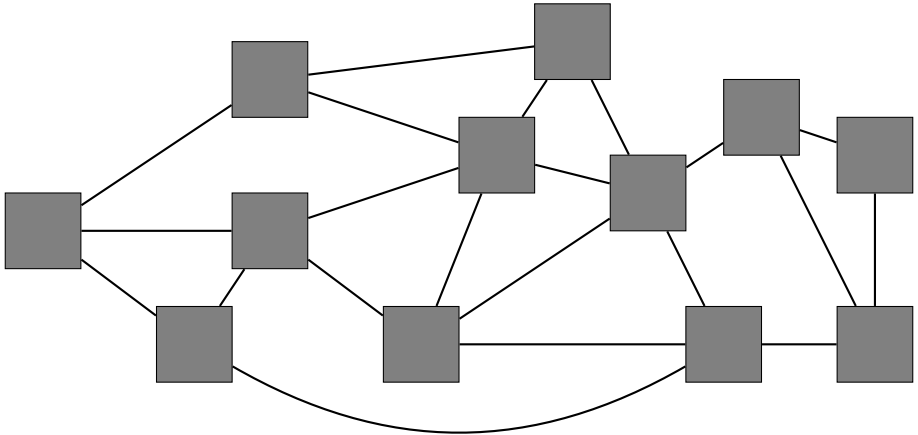
Alice connaît un 3-coloriage pour un graphe de très grande taille. Elle veut prouver à/convaincre Bob qu'elle connaît ce coloriage, mais sans le lui donner.



Protocole

Objectif

Alice connaît un 3-coloriage pour un graphe de très grande taille. Elle veut prouver à/convaincre Bob qu'elle connaît ce coloriage, mais sans le lui donner.



Plan

Conclusion

La sécurité c'est compliqué :

- Conception (beaucoup de mathématiques pour garantir qu'il n'y a pas certaines attaques),
- Mise en œuvre complexes,
- Moindre relachement : faille.