Routage & Sécurité

Nour EL MADHOUN

Enseignante-Chercheuse à l'ISEP

nour.el-madhoun@isep.fr

Plan

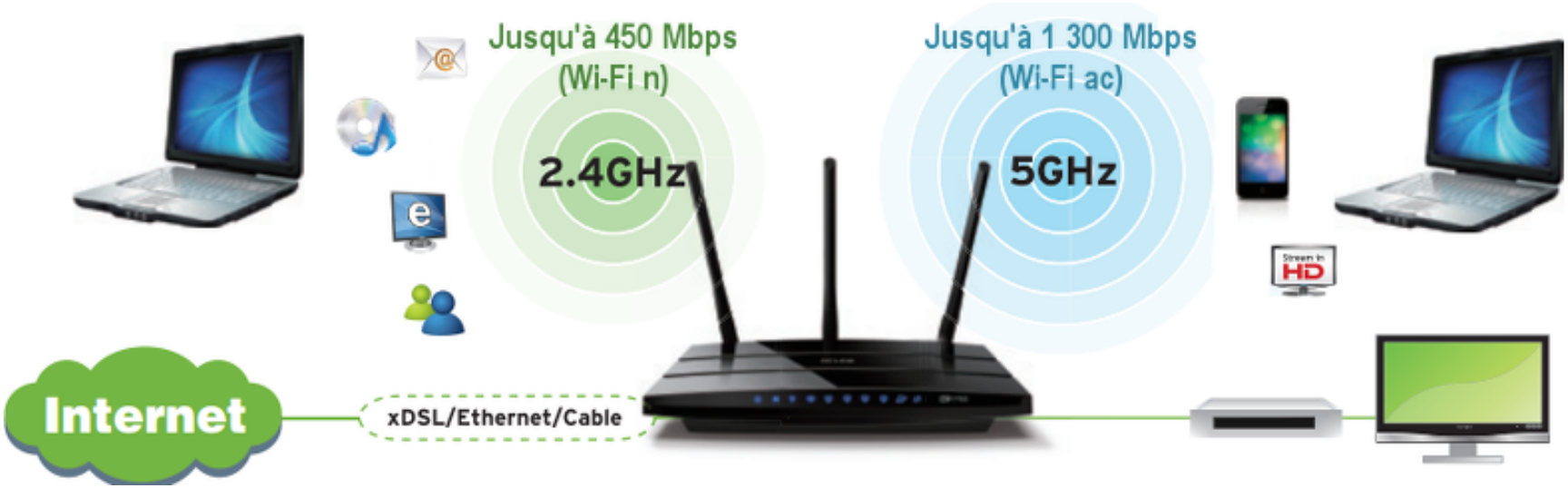
Partie 1: Routage

Partie 2: Sécurité

Partie 1: Routage

Les réseaux (Rappel)

Les réseaux (Rappel)

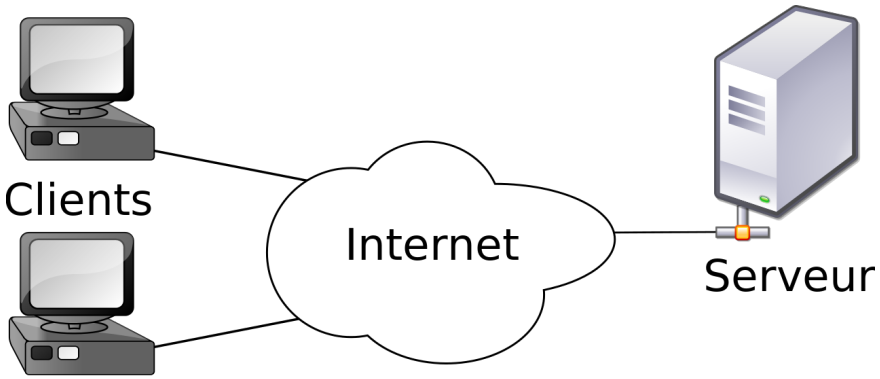


Les réseaux (Rappel)

- ✓ Les réseaux ont pour fonction:
  - de **transporter des informations** afin de **réaliser des services** pouvant se trouver n'importe **où sur le globe**.

- ✓ Une série d'équipements **matériels et de processus logiciels** sont mis en œuvre pour **assurer ce transport:**
  - depuis **les câbles ou les ondes radio** dans lesquels **circulent les données jusqu'aux protocoles** permettant de les traiter.

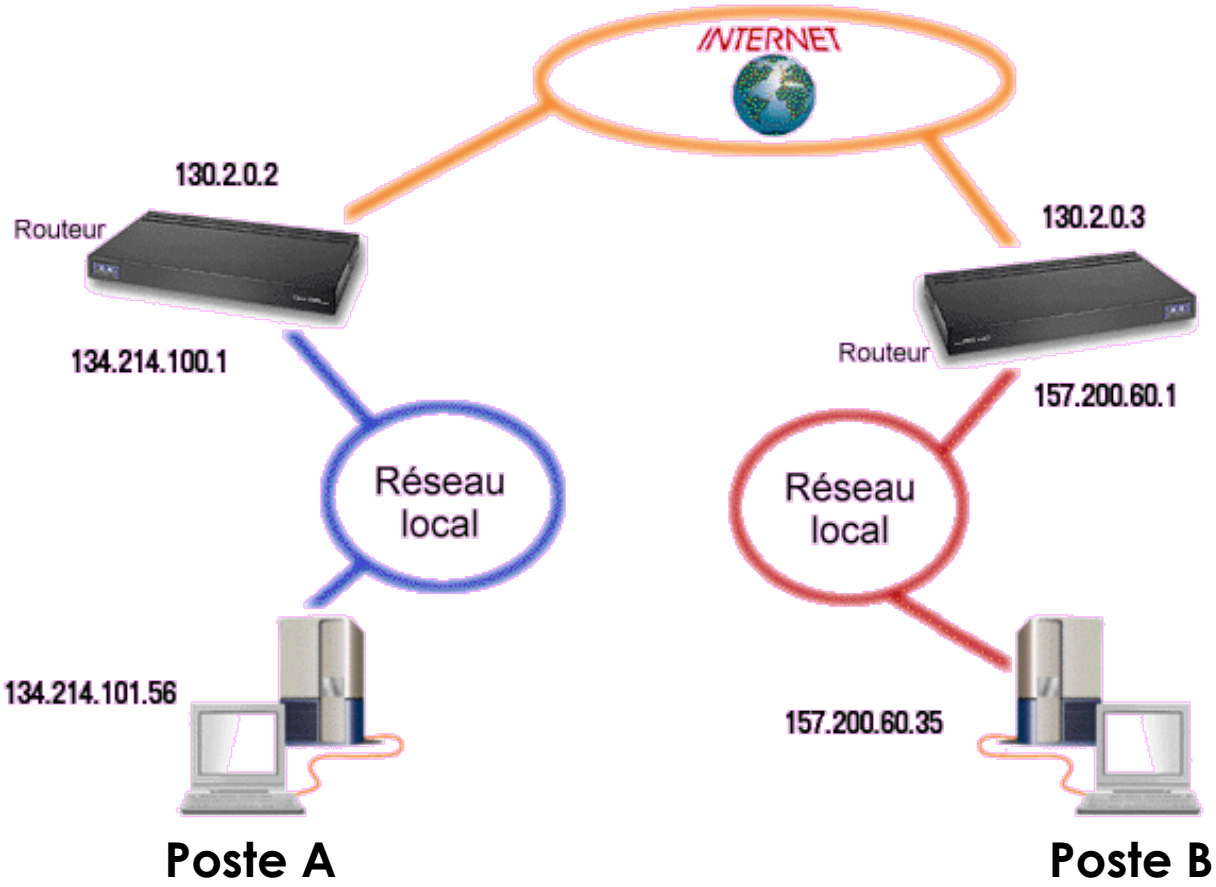
Les réseaux (Rappel)



Modèle1: Client/Serveur

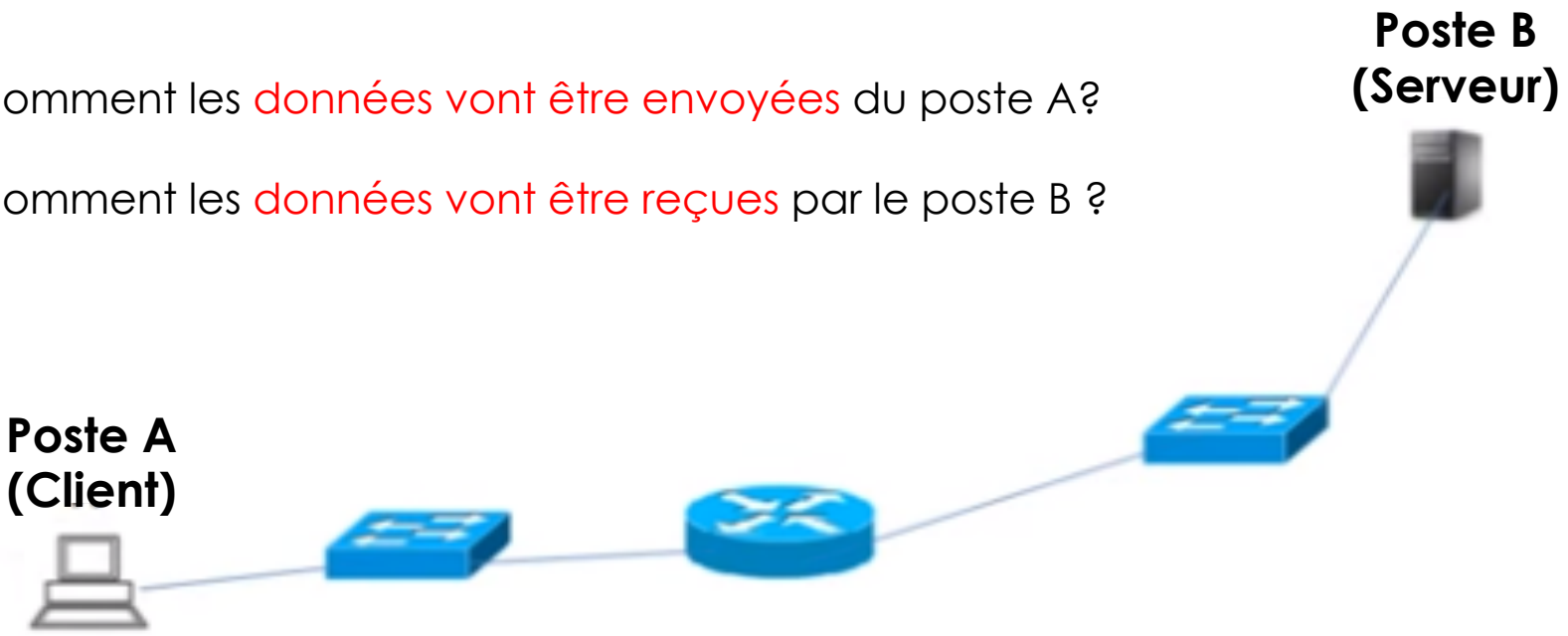
Modèle 2: Pair à Pair

Les réseaux (Rappel)

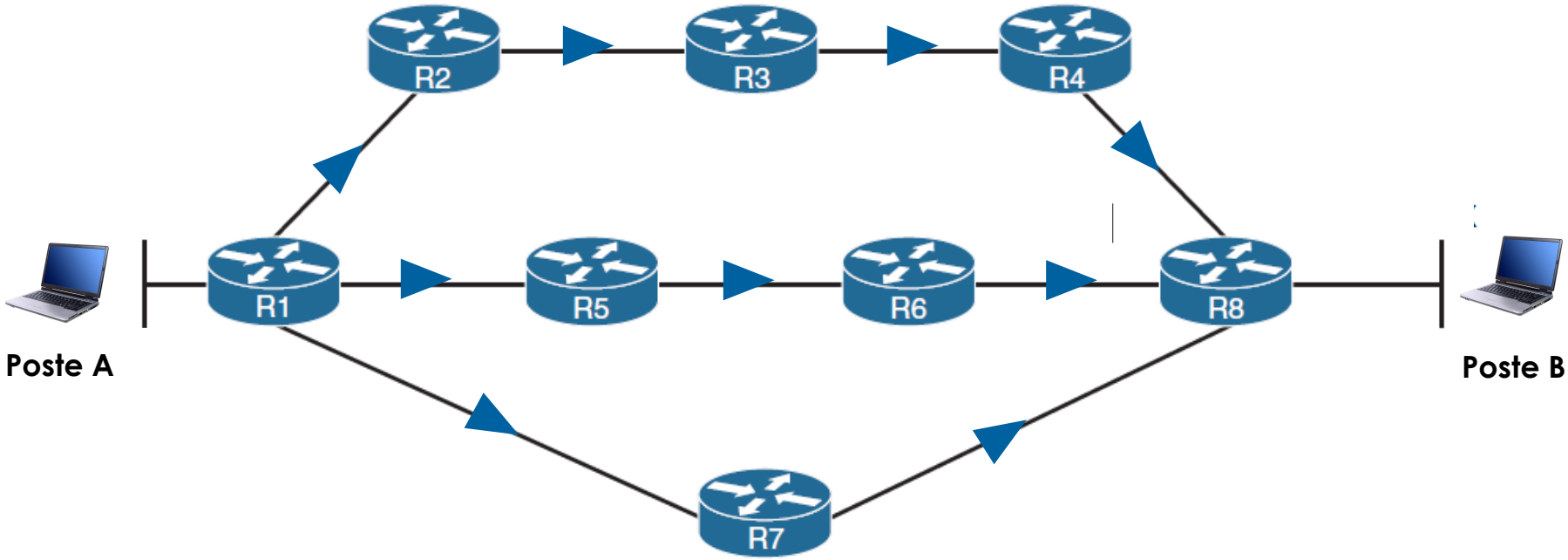


Les réseaux (Rappel)

- Comment les données vont être envoyées du poste A?
- Comment les données vont être reçues par le poste B ?



Les réseaux (Rappel)



- Comment les données vont être envoyées du poste A?
- Comment les données vont être reçues par le poste B ?
- Quel chemin vont prendre les données ?

→ **Solution: Routage**

Le routage: définition

- ✓ Le **routage** est un **mécanisme** par lequel les données transmises sur le réseau d'un **expéditeur à un ou plusieurs destinataires**.

- ✓ Le **routage** est un **mécanisme** par lequel **des chemins sont sélectionnés** dans **un réseau** pour **acheminer les données** d'un **expéditeur** jusqu'à **un ou plusieurs destinataires**.

Le routage: définition

✓ Plusieurs protocoles de routage existent, on s'intéresse:

- Protocole RIP (Routing Information Protocol)

- Protocole OSPF (Open Shortest Path First)

Protocole RIP

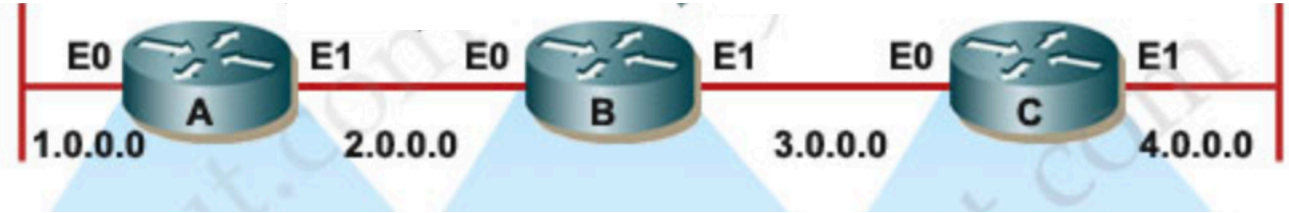
- ✓ Protocole à **vecteur de distance:**

  - Le couple **« adresse IP/Distance »** est appelé **« vecteur de distance »**
  - **Distance** : **nombre de sauts** (routeurs) pour atteindre une destination ou un réseau

- ✓ Un routeur RIP construit **sa table de routage** en fonction **des vecteurs de distance**

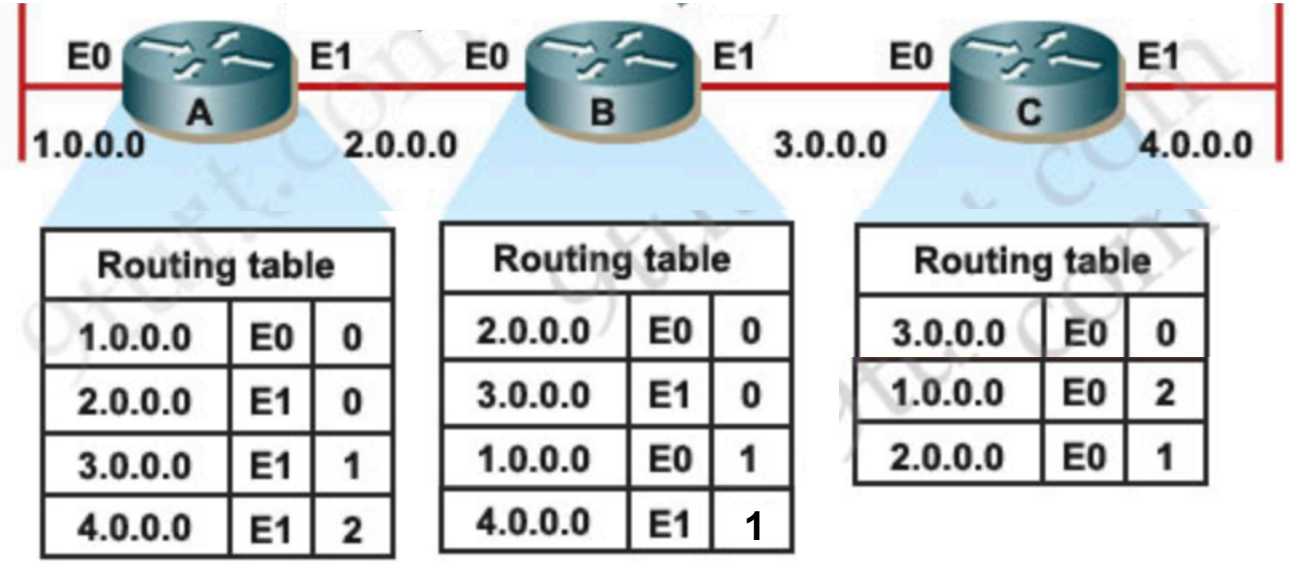
Protocole RIP

✓ Exemple:



Protocole RIP

✓ Exemple:



Routing table		
1.0.0.0	E0	0
2.0.0.0	E1	0
3.0.0.0	E1	1
4.0.0.0	E1	2

Routing table		
2.0.0.0	E0	0
3.0.0.0	E1	0
1.0.0.0	E0	1
4.0.0.0	E1	1

Routing table		
3.0.0.0	E0	0
1.0.0.0	E0	2
2.0.0.0	E0	1

Protocole OSPF

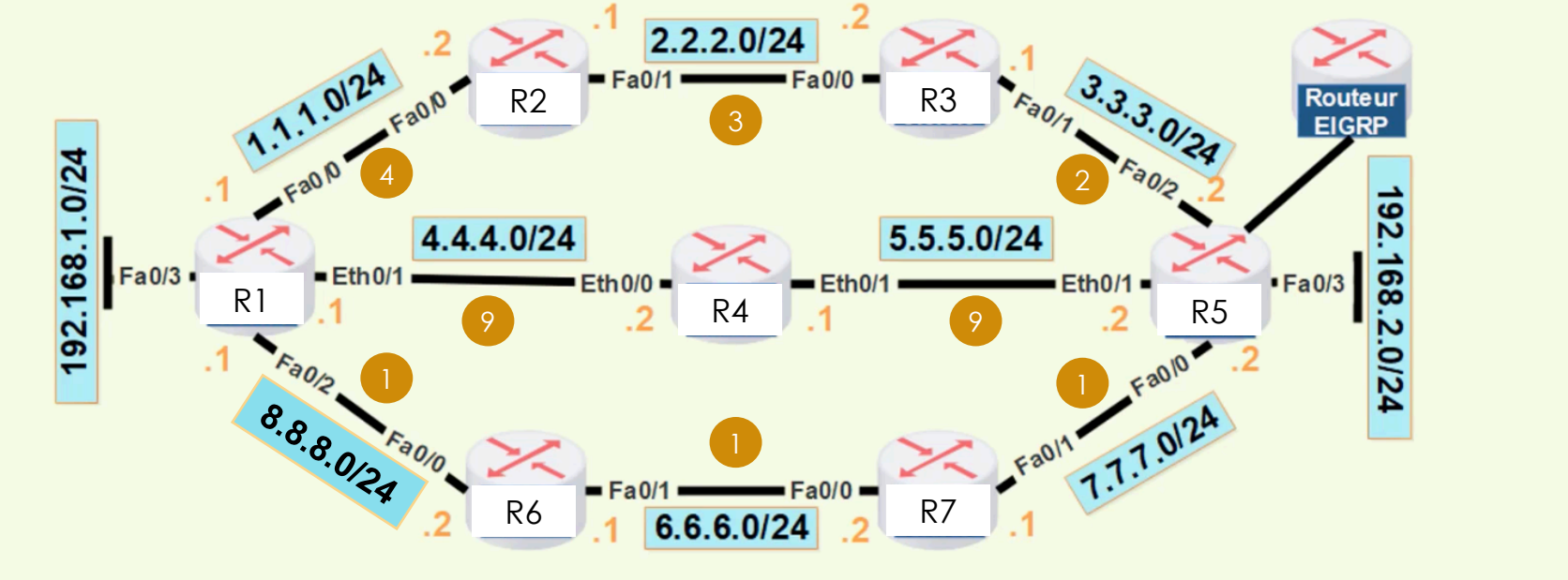
- ✓ Protocole à **état des liens:**

  - Etat de liens: chaque lien a **un coût**

- ✓ Les routeurs OSPF collectent l'ensemble **des coûts des liens** et **construisent les tables de routage avec le plus court chemin** (somme des coûts plus petite): **Dijkstra**

Protocole OSPF

✓ Exemple:



Partie 2: Sécurité

Problèmes

- Réseaux Internet globalement ouvert
  - Explosion d'Internet
    - Développement des applications web amplifiant le vecteur d'attaques
    - Vulnérabilités exploitées par les pirates
  - Codes malveillants
    - De milliers de nouveaux codes malveillants par an
    - Virus, vers, spywares, etc.

Motivations d'un attaquant

- La rancune
- L'argent
- Un réseau se vante de la sécurité de son système: le défi
- La curiosité
- L'engagement politique

Cibles

- N'importe quel système informatique peut être piraté:
  - Les banques
  - Les serveurs militaires
  - Les universités
  - Les fournisseurs d'accès Internet

Propriétés de sécurité

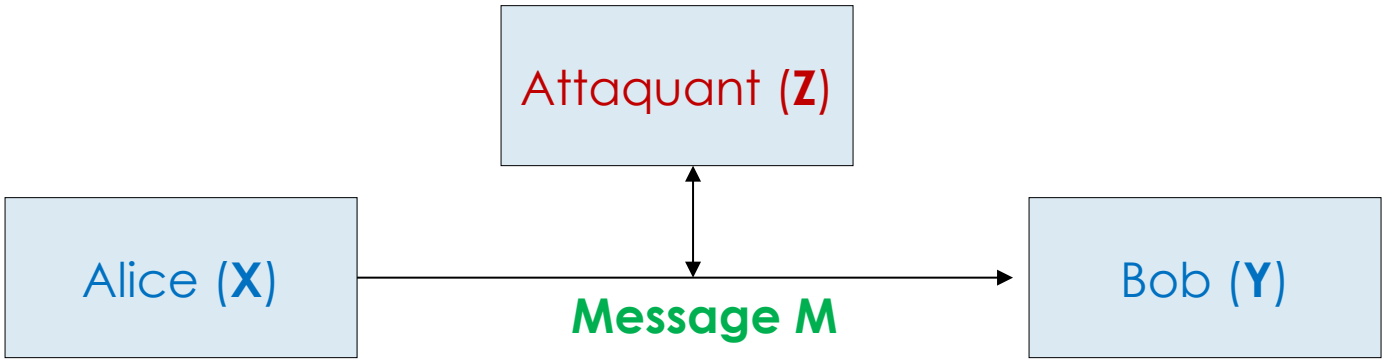
- Confidentialité
- Intégrité
- Authentification
- Non-Répudiation

« Propriétés de la sécurité informatique »

Critères Fondamentaux

Propriétés de sécurité

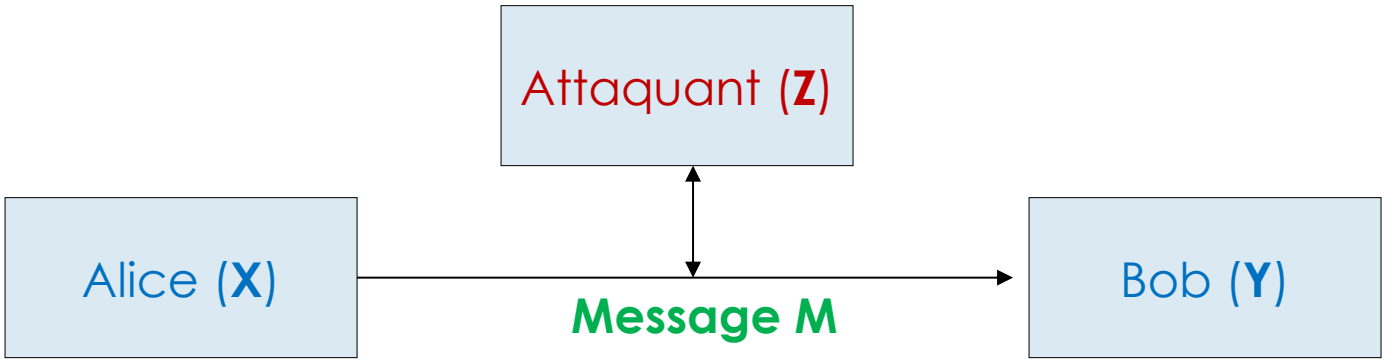
- Confidentialité:



✓ Empêcher Z d'intercepter et lire le contenu du **M**
✓ Seulement X et Y qui peuvent comprendre le contenu du **M**

Propriétés de sécurité

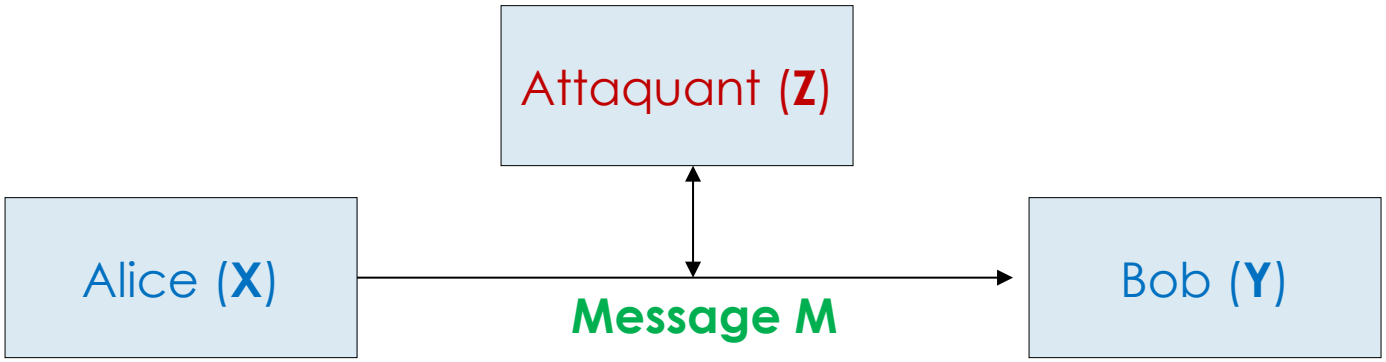
- Intégrité:



- ✓ Empêcher **Z** de modifier le contenu du **M**
- ✓ Le contenu du **M** n'est pas modifié, d'une manière malveillante ou accidentelle, lors de la transmission

Propriétés de sécurité

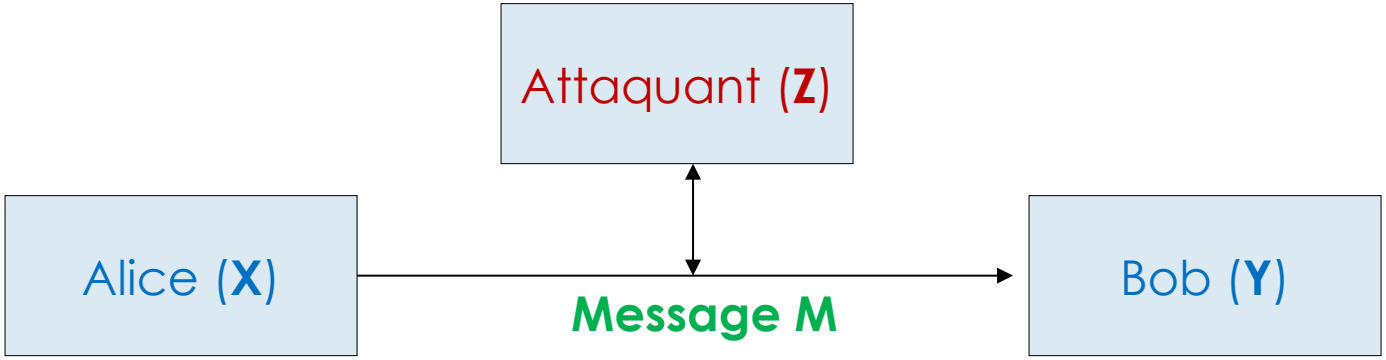
- Authentification



- ✓ Empêcher **Z** de prendre l'identité de **X** ou **Y**
- ✓ **X** doit s'authentifier auprès du **Y**
- ✓ **Y** doit s'authentifier auprès du **X**

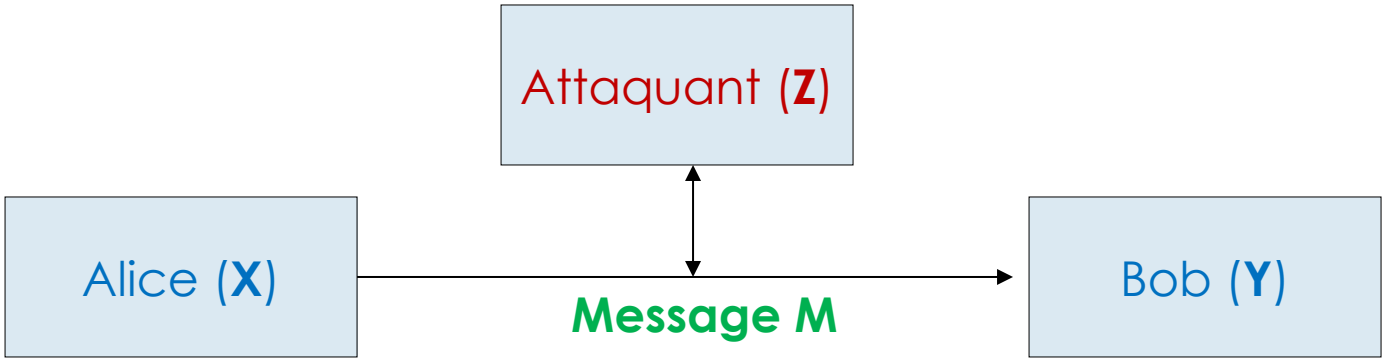
Propriétés de sécurité

- Non-Répudiation



- ✓ **X** ne pas nier qu'il a envoyé **M**
- ✓ **Y** ne pas nier qu'il a reçu **M**

Propriétés de sécurité

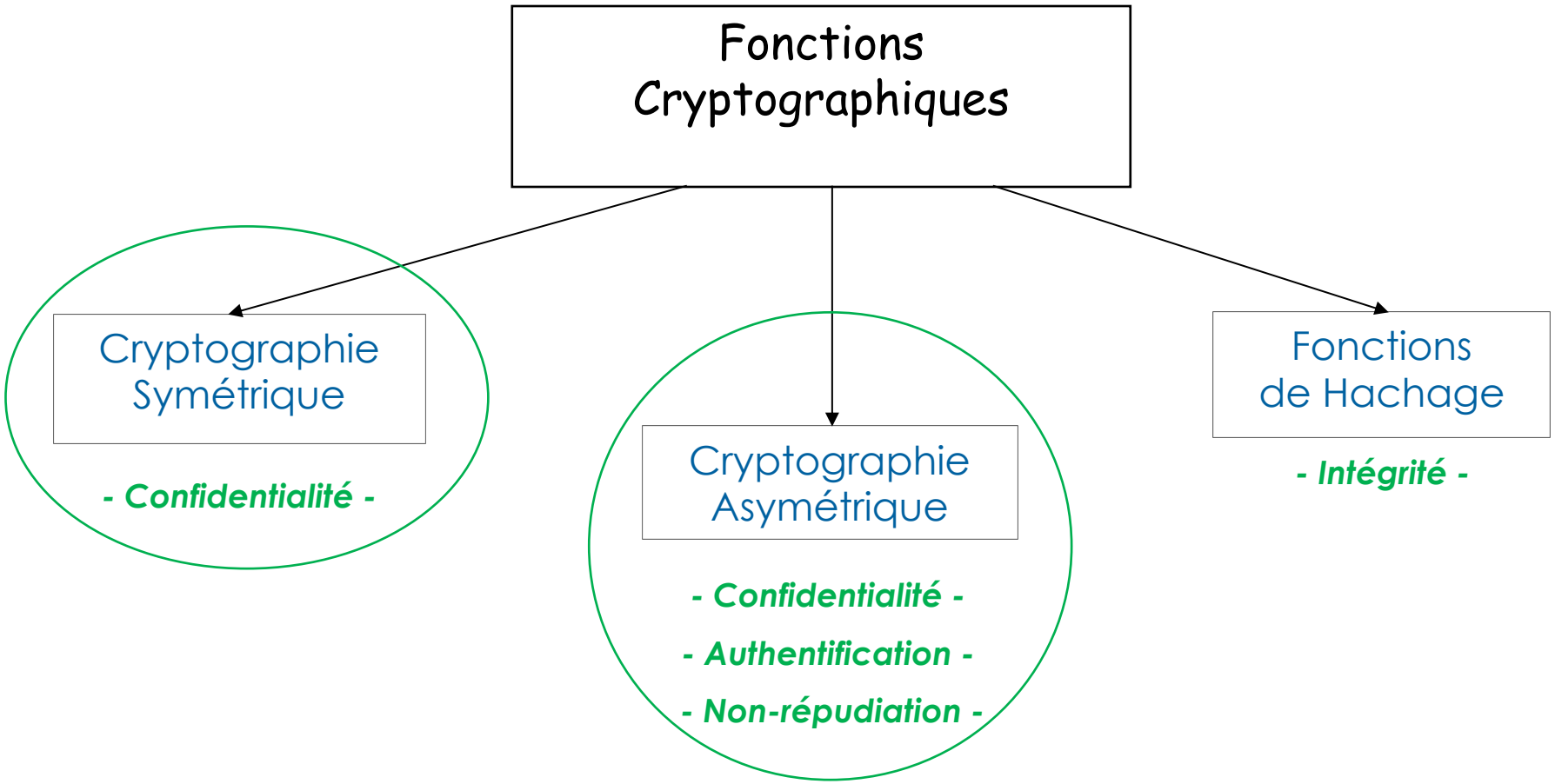


Comment les propriétés de sécurité:

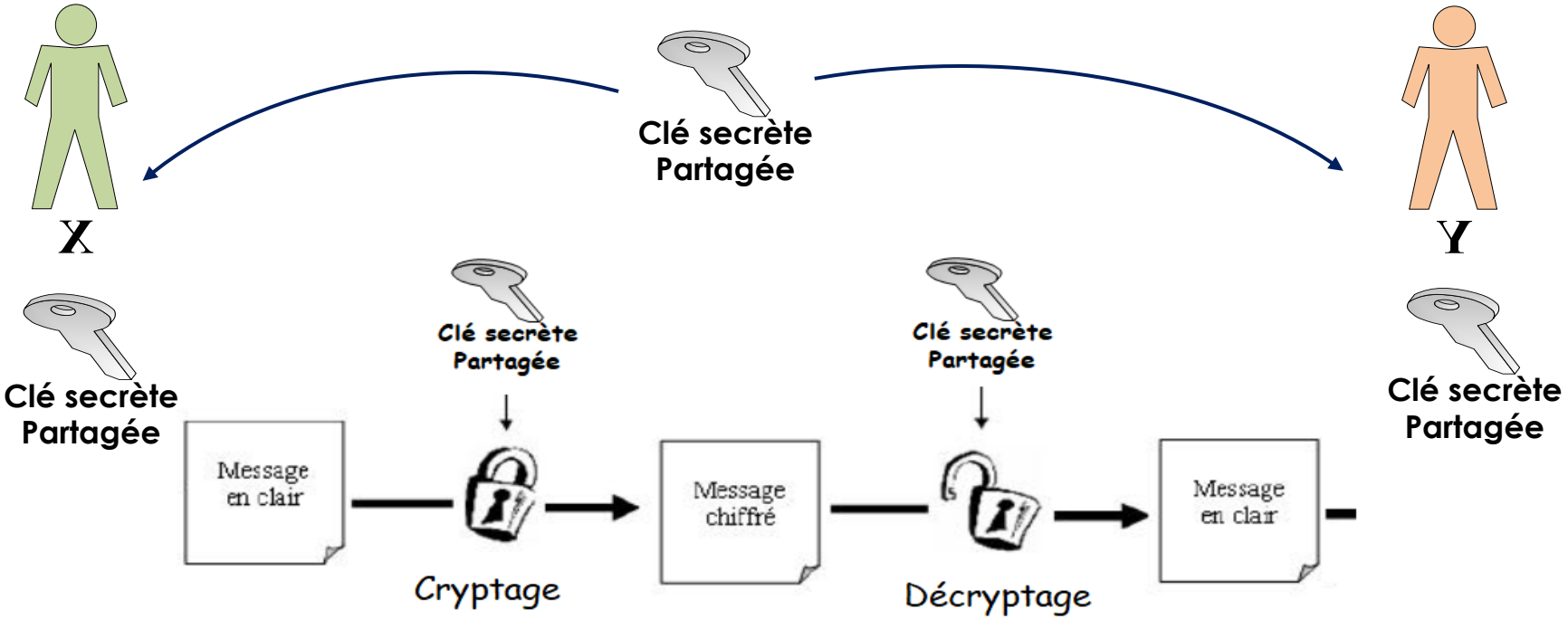
« Confidentialité, **Intégrité**, Authentification, Non-Répudiation»

sont assurées lors d'une communication entre **X** et **Y** ?

Fonctions cryptographiques



Cryptographie symétrique



- Confidentialité du message -

Cryptographie symétrique

- Définition:

  - Une seule clé partagée entre l'émetteur et le récepteur

  - La même clé est utilisée par l'émetteur (pour crypter) et par le récepteur (pour décrypter)

  - Elle est utilisée pour assurer la confidentialité des échanges

Cryptographie symétrique

- Avantages:

  - Une cryptographie très simple

  - Une cryptographie très rapide

Cryptographie symétrique

- Inconvénients :

  - L'échange de la clé doit être sécurisé: comment ?

  - Si la clé est échangée d'une manière non sécurisée --> Il est facile pour un pirate informatique d'obtenir cette clé

Cryptographie symétrique

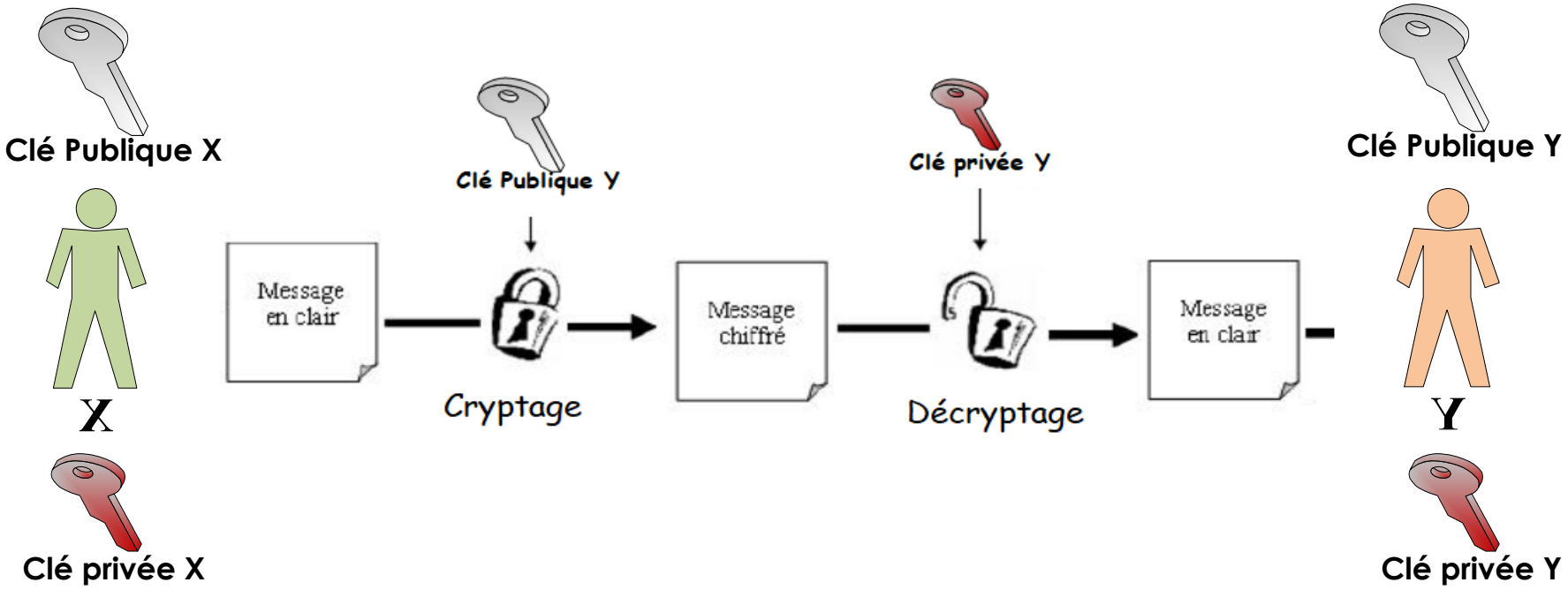
Problème de la cryptographie symétrique:

Comment partager la clé secrète entre X et Y d'une manière sécurisée ?

Solution

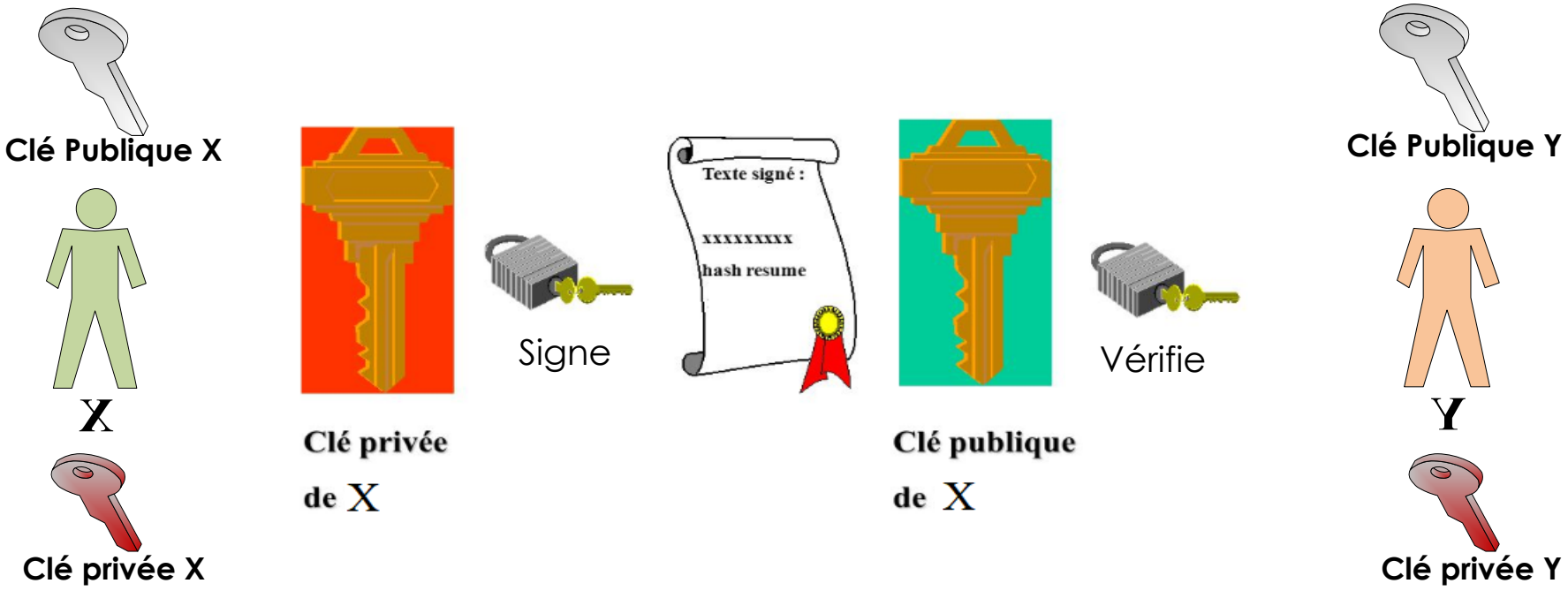
« Utiliser la cryptographie asymétrique »

Cryptographie asymétrique



- Confidentialité du message -

Cryptographie asymétrique



- Authentification et non-répudiation pour X -

Cryptographie asymétrique

- Définition:

  - Le cryptage asymétrique utilise deux clés qui sont générées ensemble

  - Ces deux clés sont liées mathématiquement mais on ne peut pas calculer l'une de l'autre

  - La clé publique est distribuée librement entre l'expéditeur et le destinataire

  - La clé privée reste cachée et elle ne sera pas partagée

Cryptographie asymétrique

- Définition:

  - Pour assurer la confidentialité:

    Clé publique: pour chiffrer les données

    Clé privée: pour déchiffrer les données

  - Pour assurer l'authentification et la non-répudiation:

    Clé privée: pour signer les données

    Clé publique: pour vérifier la signature

Cryptographie asymétrique

- Avantages:

  - Cette cryptographie est plus sécurisée que la cryptographie symétrique

  - Elle permet de garantir la confidentialité, l'authentification et non-répudiation

  - Elle résout le problème de la cryptographie symétrique: le partage de la clé secrète d'une manière sécurisée entre l'expéditeur et le destinataire

Cryptographie asymétrique

- Inconvénients

  - Une cryptographie qui est relativement complexe

  - Une cryptographie beaucoup plus lente que la cryptographie symétrique

Communication sécurisée

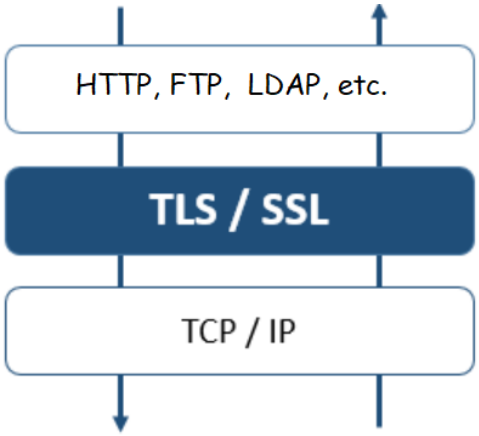
Les deux cryptographies ont des avantages et des inconvénients

« Comment donc profiter des avantages des deux cryptographies pour sécuriser une communication ? »

Communication sécurisée

Protocole TLS/SSL

Exemple: *communication sécurisée entre un navigateur et un serveur web*



- TLS: Transport Layer Security
- TLS: Version 3 du protocole SSL
- SSL: Secure Socket Layer
- Permet de sécuriser les applications

Communication sécurisée

Protocole TLS/SSL

Exemple: *communication sécurisée entre un navigateur et un serveur web*

Client (Navigateur)

TLS/SSL fonctionne en mode client-serveur

Il permet d'assurer les propriétés de sécurité:

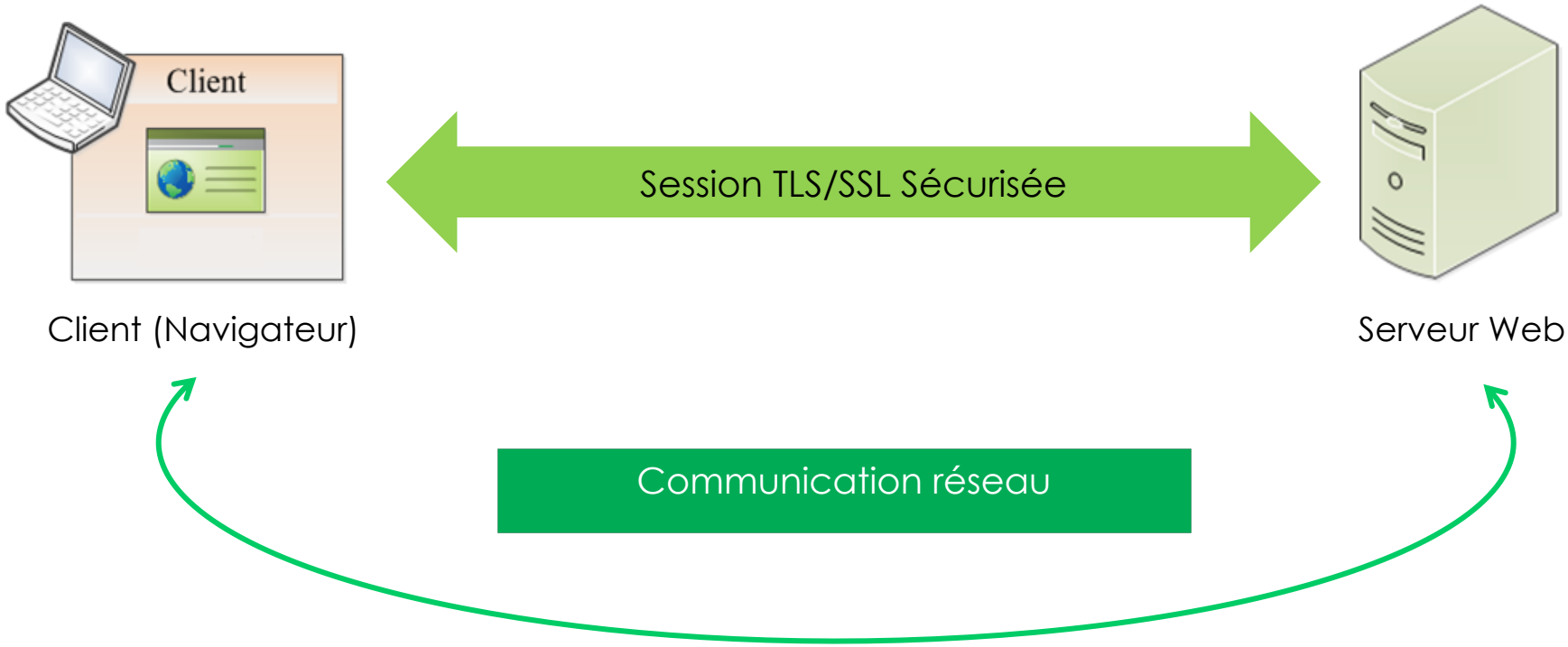
* Authentification du serveur
* Non répudiation de serveur
* Confidentialité des données échangées

Serveur Web

Communication sécurisée

Protocole TLS/SSL

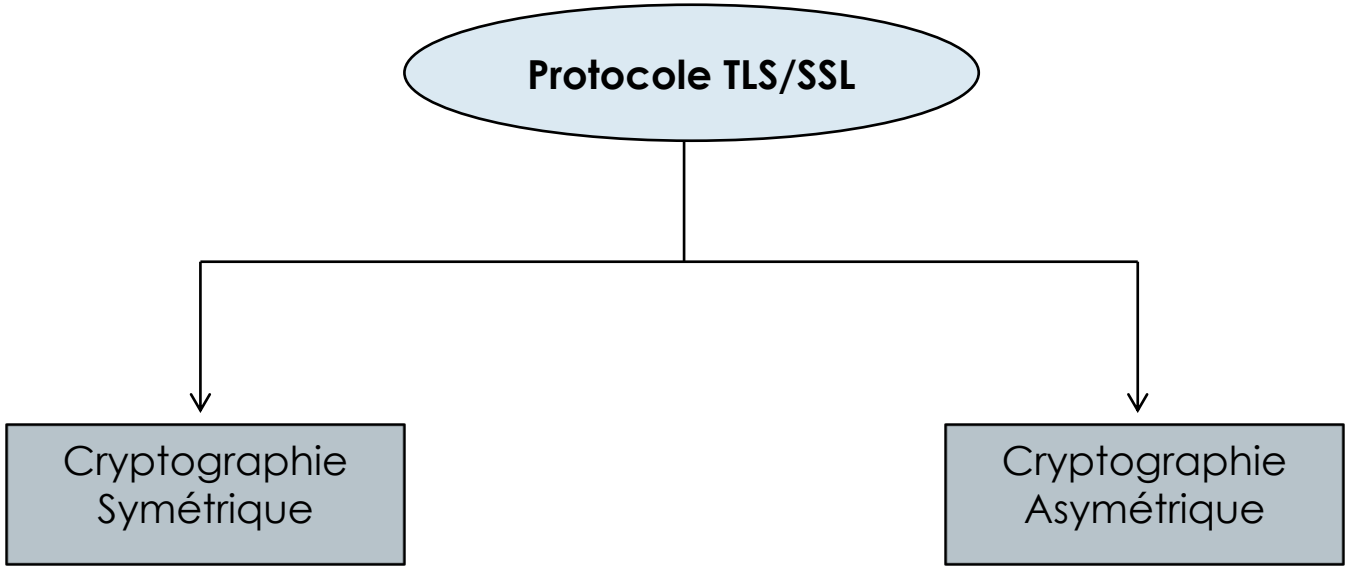
Exemple: *communication sécurisée entre un navigateur et un serveur web*



Communication sécurisée

Protocole TLS/SSL

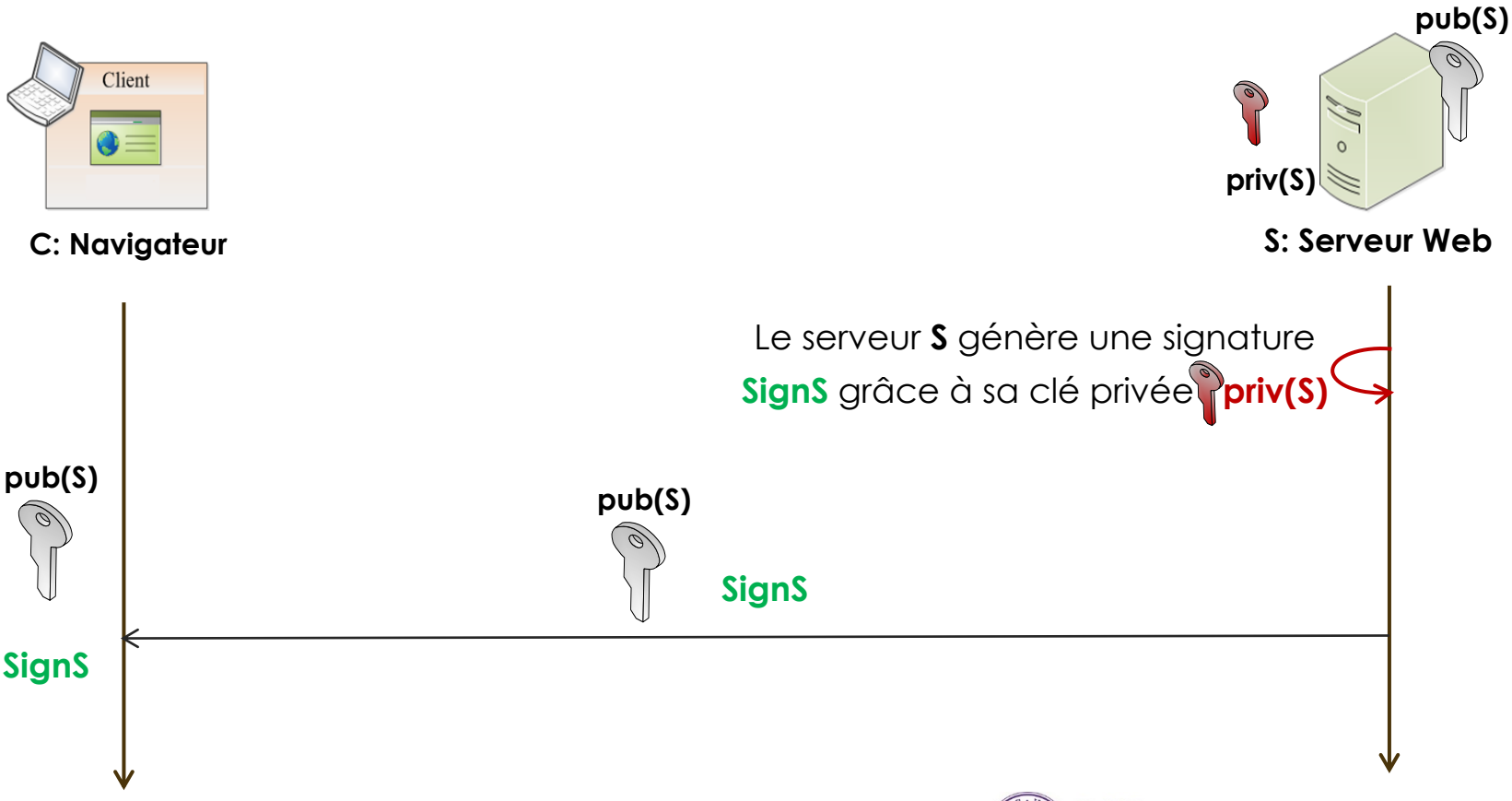
Exemple: *communication sécurisée entre un navigateur et un serveur web*



Communication sécurisée

Protocole TLS/SSL

Exemple: *communication sécurisée entre un navigateur et un serveur web*

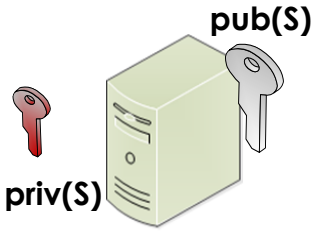


Communication sécurisée

Protocole TLS/SSL

Exemple: *communication sécurisée entre un navigateur et un serveur web*

C: Navigateur



S: Serveur Web

pub(S)

SignS

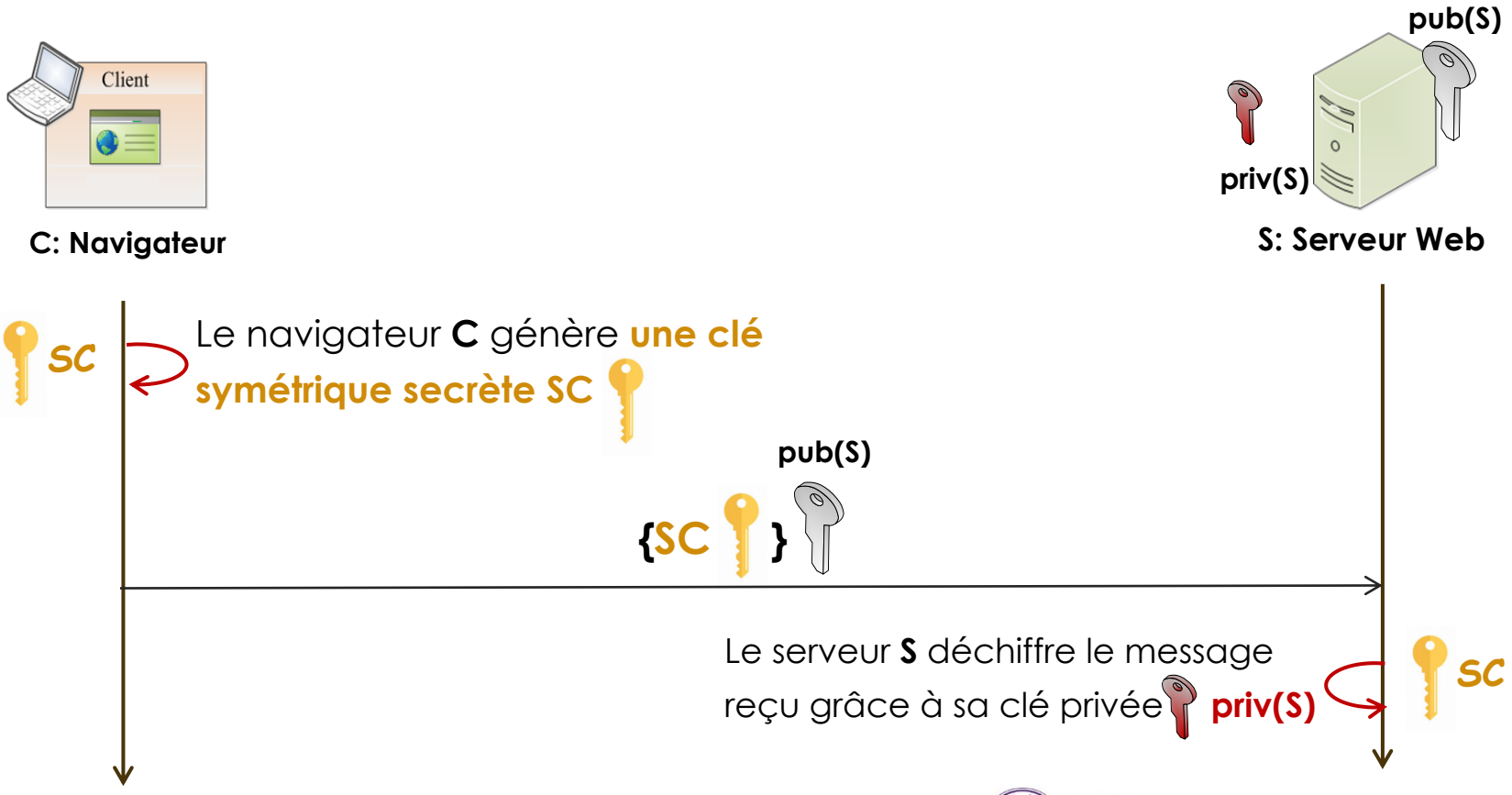
Le navigateur **C** vérifie **SignS** avec **pub(S)**

Le serveur est bien authentifié

Communication sécurisée

Protocole TLS/SSL

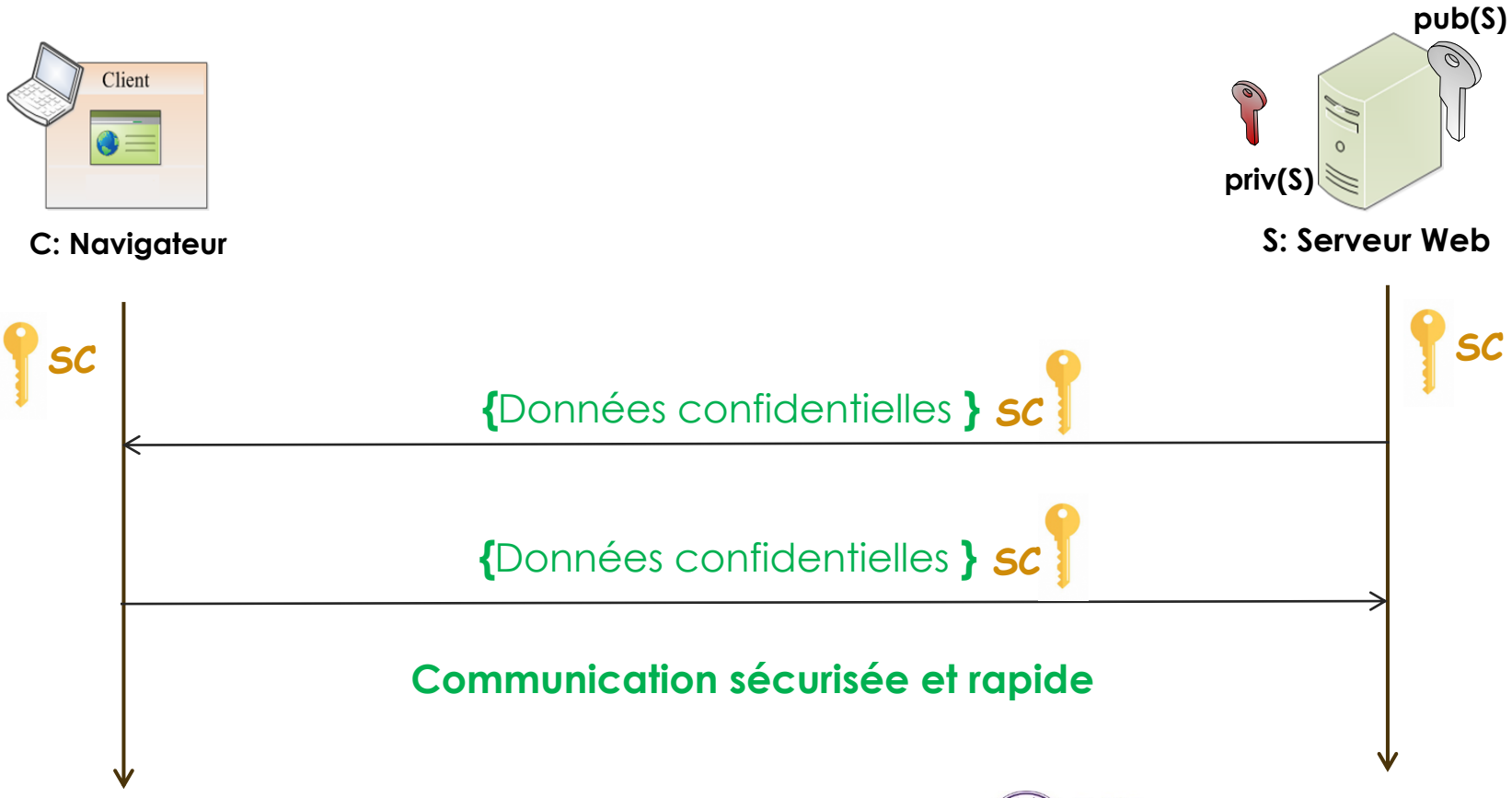
Exemple: *communication sécurisée entre un navigateur et un serveur web*



Communication sécurisée

Protocole TLS/SSL

Exemple: *communication sécurisée entre un navigateur et un serveur web*



Merci

Nour EL MADHOUN

Enseignante – Chercheuse à l'ISEP

nour.el-madhoun@isep.fr

isep
École d'ingénieurs du numérique

isep
Formation continue

ICP
ISP - FACULTÉ D'ÉDUCATION
L'esprit grand ouvert sur le monde