# Sécurisation TLS

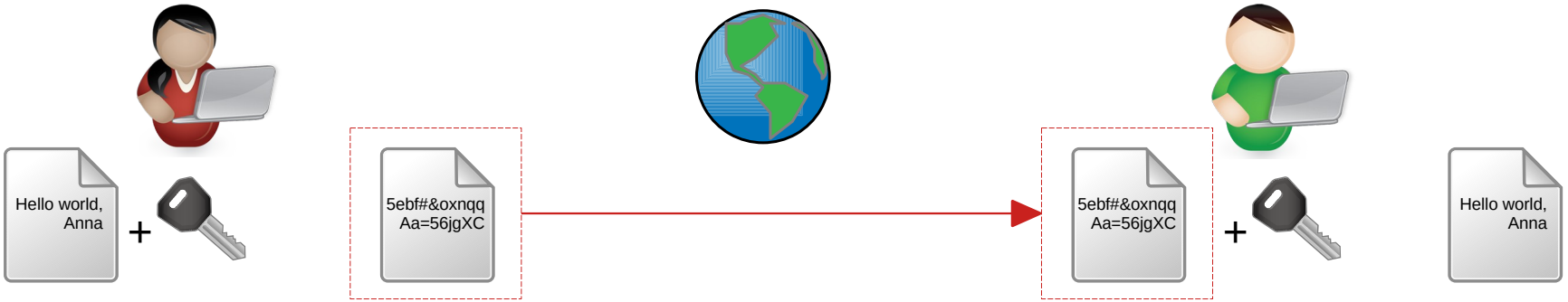
David ROUMANET

# Échanges

Situation initiale

- Deux amis veulent communiquer de manière sécurisée
  - Anna et Bob se connaissent
  - Travaillent à distance (Internet)
  - Respectent le secret industriel

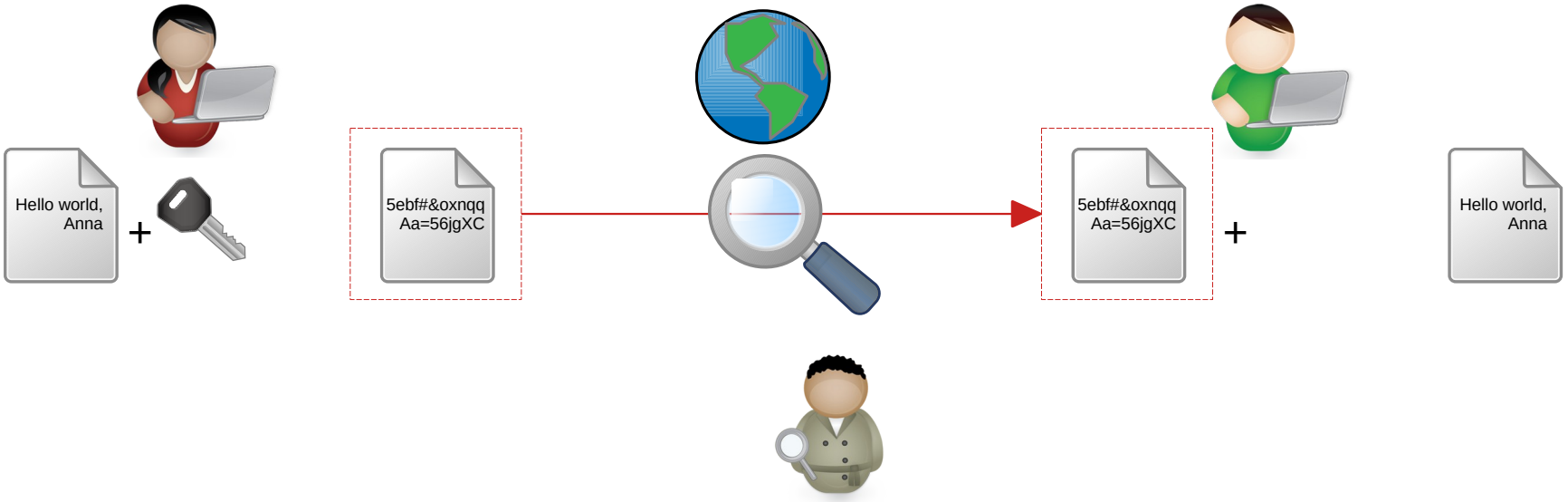
# Échanges symétriques




**Chiffrement symétrique**

* rapide, fiable, simple (processeur léger)
* AES, Blowfish, Twofish, DES/3DES...

# Échanges symétriques



# Échanges symétriques

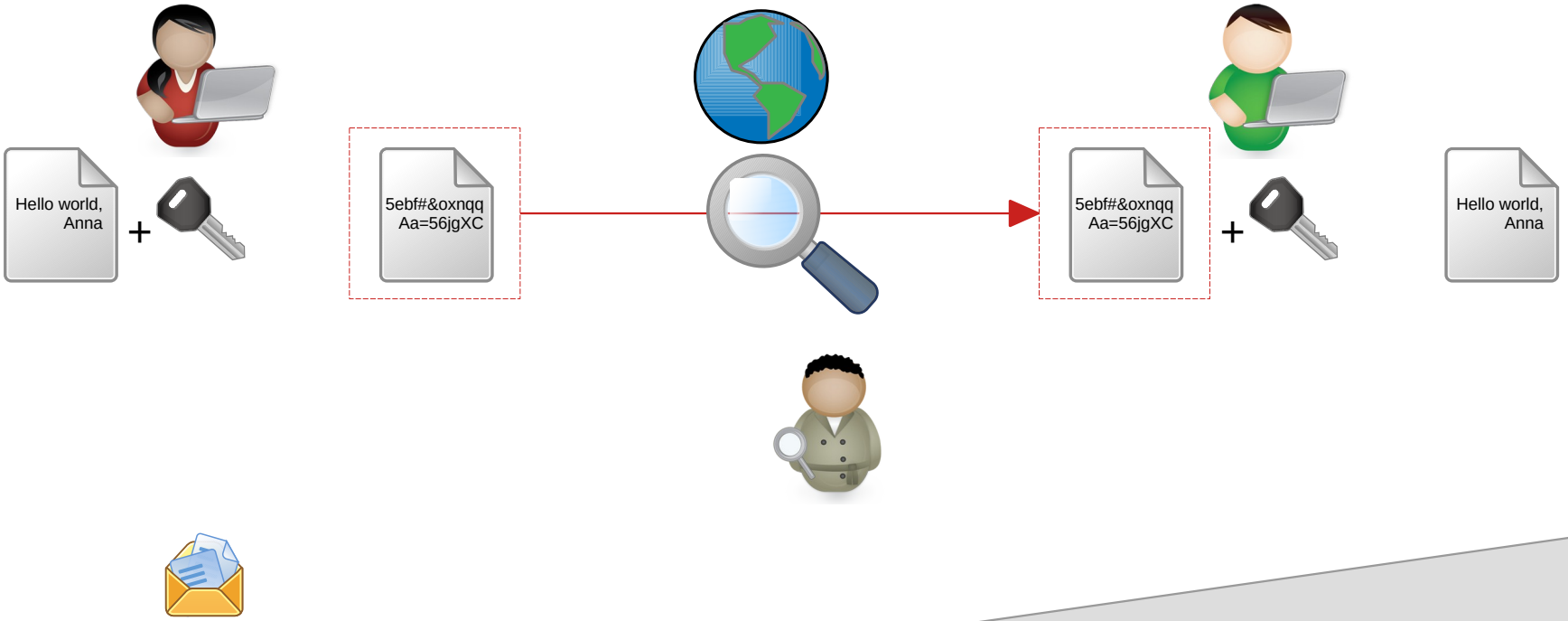
Problème réglé

- Le pirate ne peut plus lire les messages chiffrés avec la clé

Nouveau problème

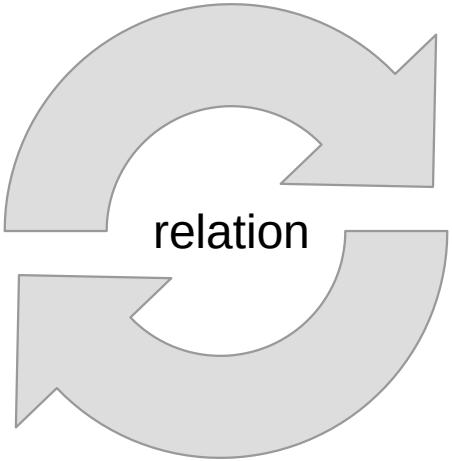
- Comment échanger une clé de chiffrement ?

# Échanges symétriques



# Échanges asymétriques

Clé privée

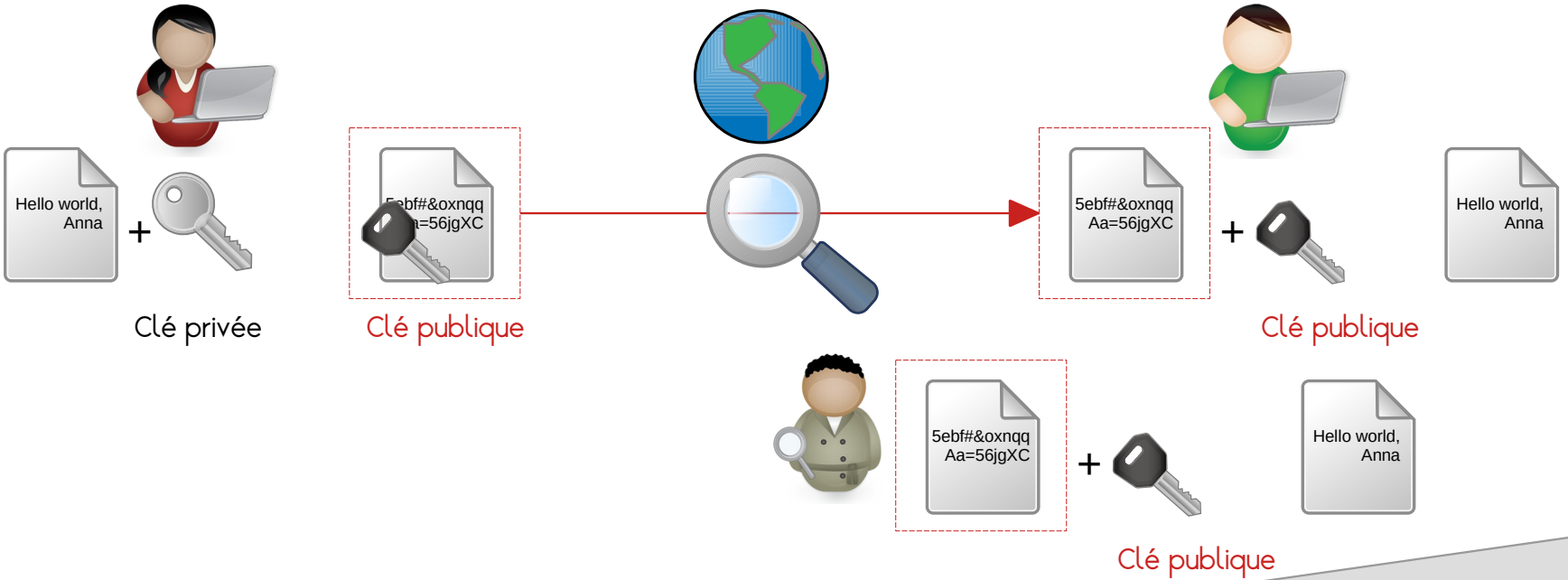



Clé publique

Basé sur :

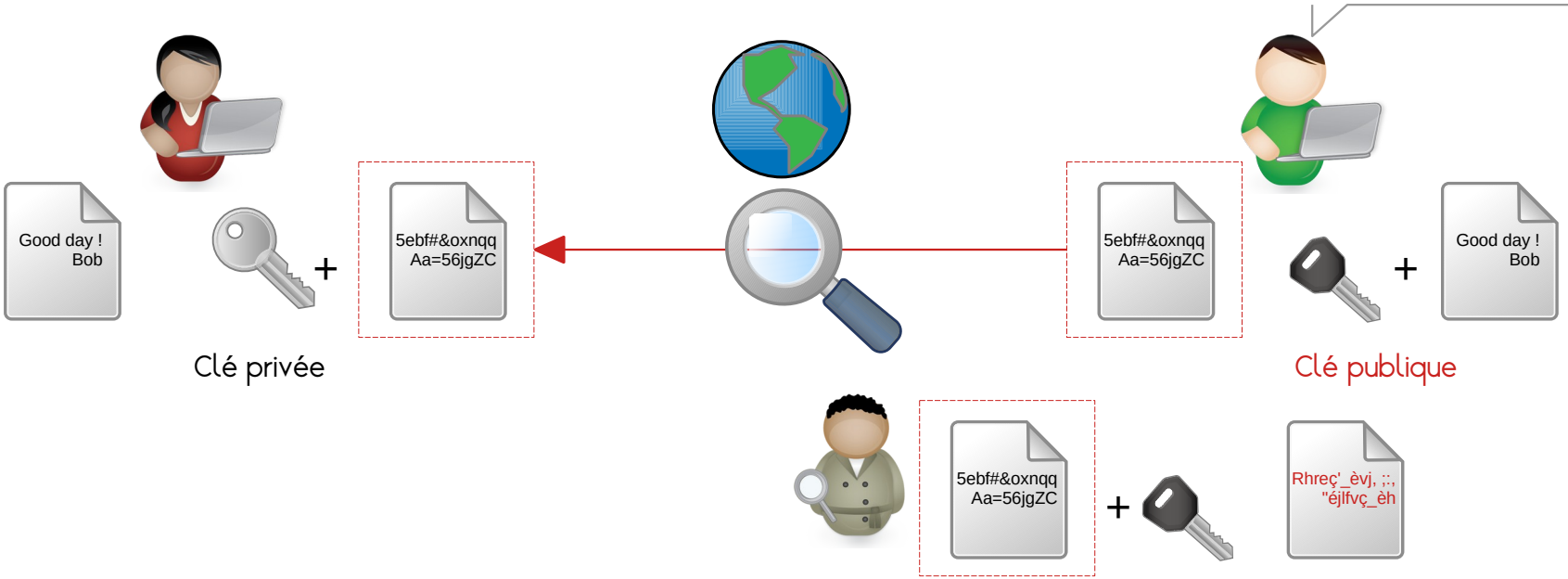
- les **congruences** (https://www.methodemaths.fr/les_congruences/)
- le **théorème de Fermat** (congruence et nombres premiers)

# Échanges asymétriques



# Échanges asymétriques

Seul, l'émetteur de la
Clé publique pourra relire
Mon message.



# Échanges asymétriques

**Chiffrement asymétrique**

* complexe (CPU), fiable, robuste
* RSA, DSA, ElGamal...

Rivest, Shamir, Adleman

Les clés publiques peuvent décoder ce que je code.

Clé privée

Seule la clé privée peut décoder ce que je code.

Clé publique

# Échanges asymétriques

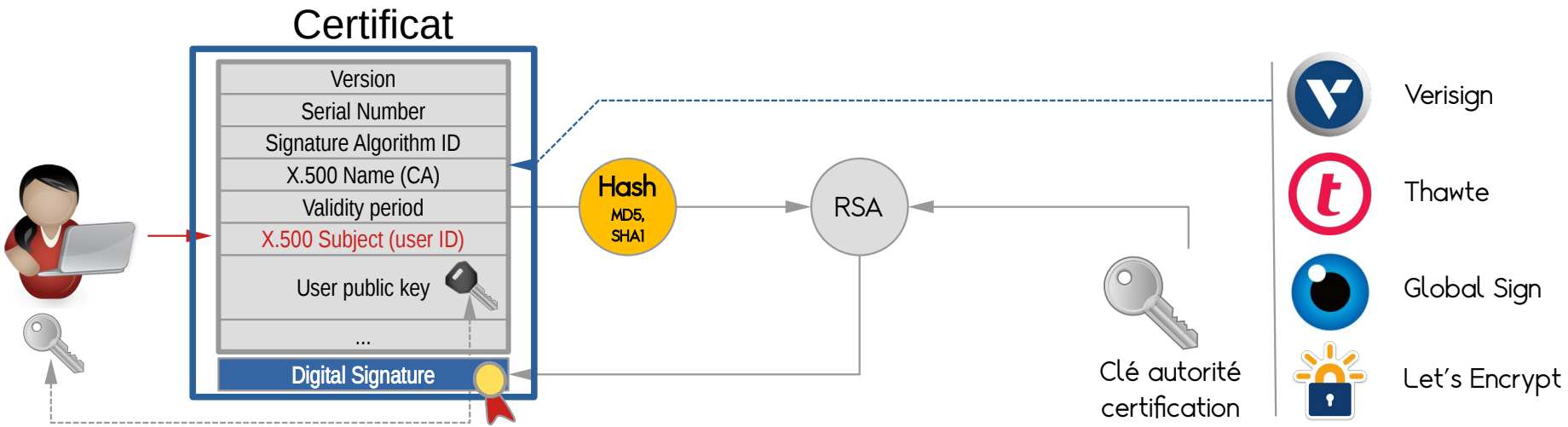
Problème réglé

- Le pirate ne peut plus lire les messages chiffrés avec la clé publique

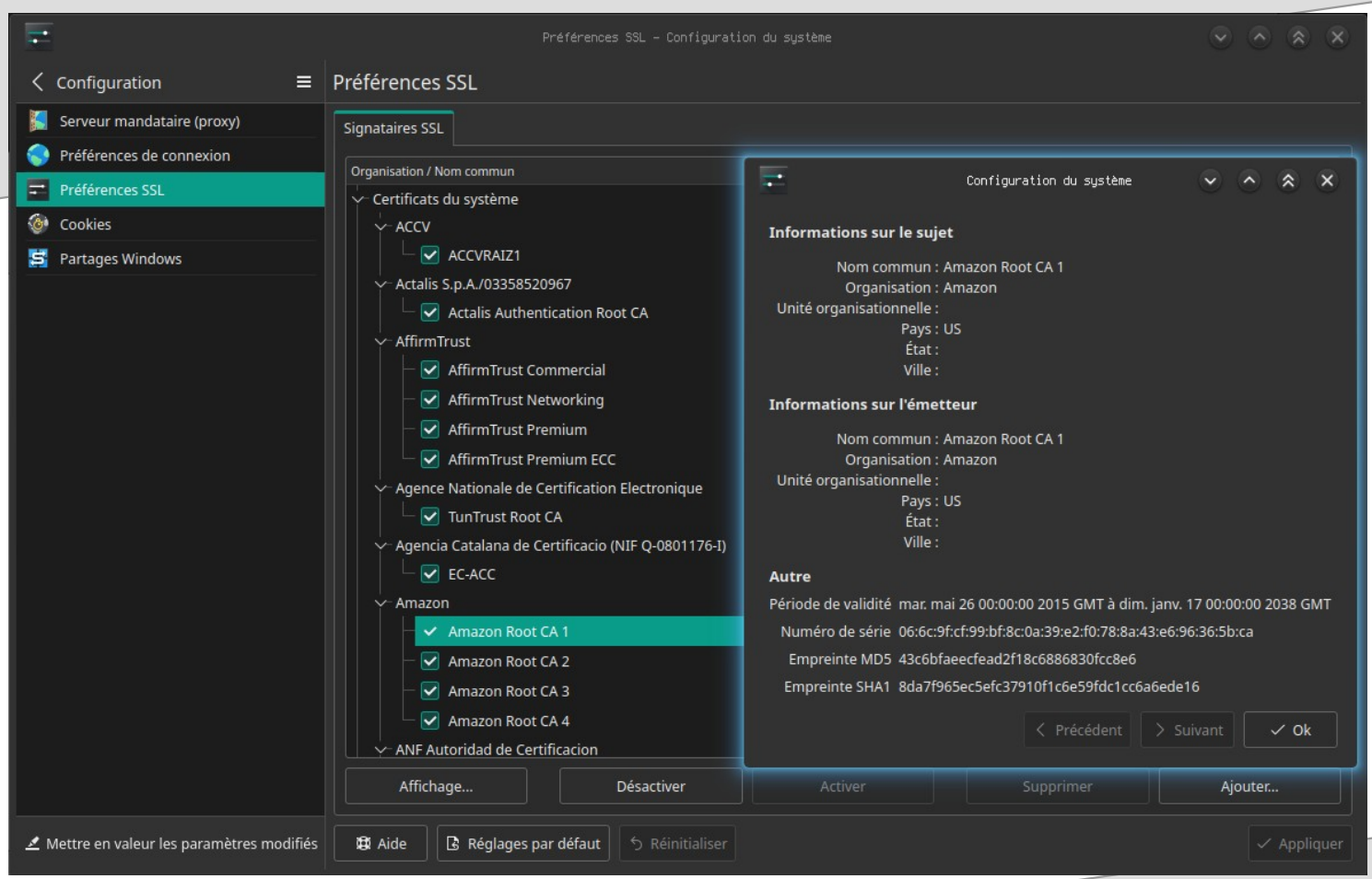
Nouveau problème

- Comment savoir si la clé publique est bien celle d'Anna ?
- Les chiffrements et déchiffrements ne sont pas performants (rapides).

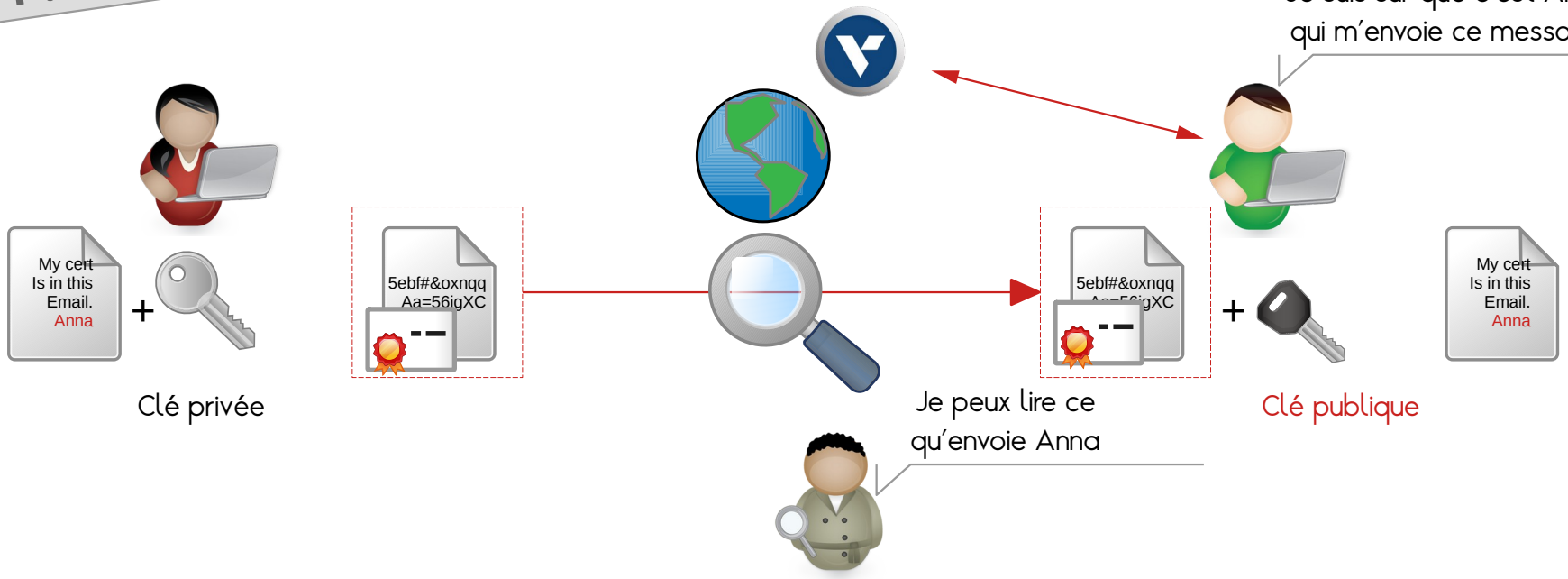
# Certificats



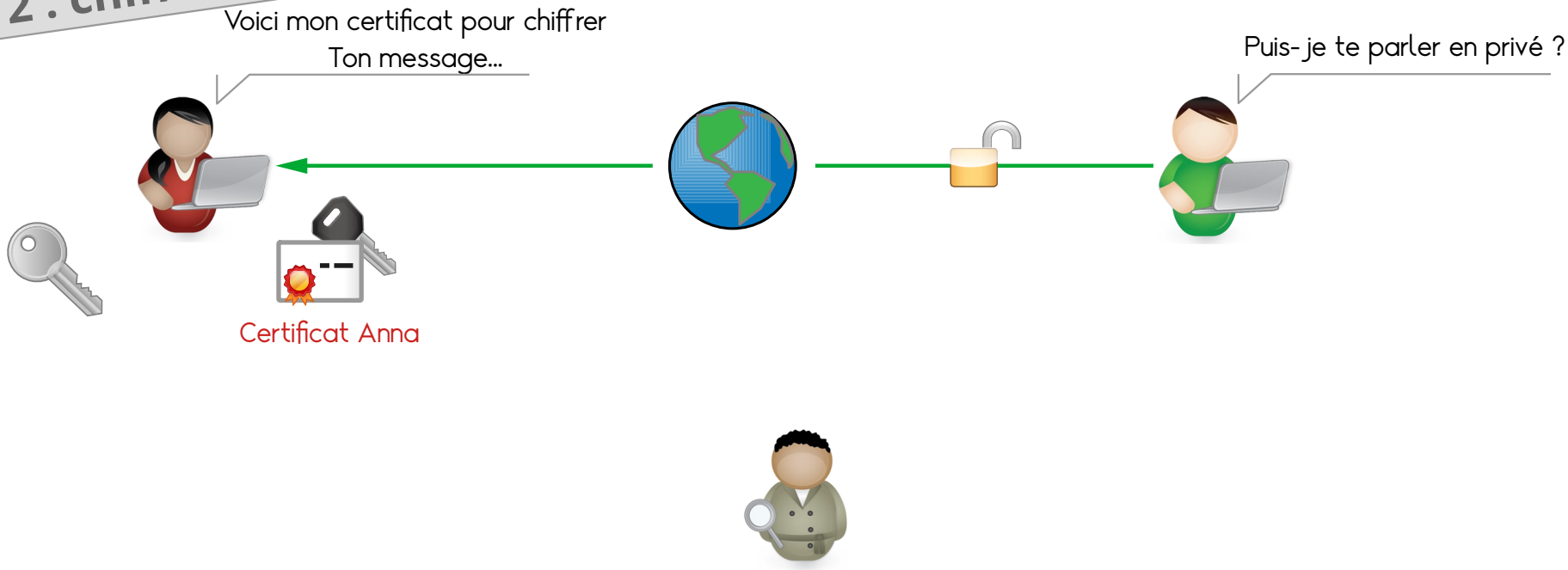
# Certificats



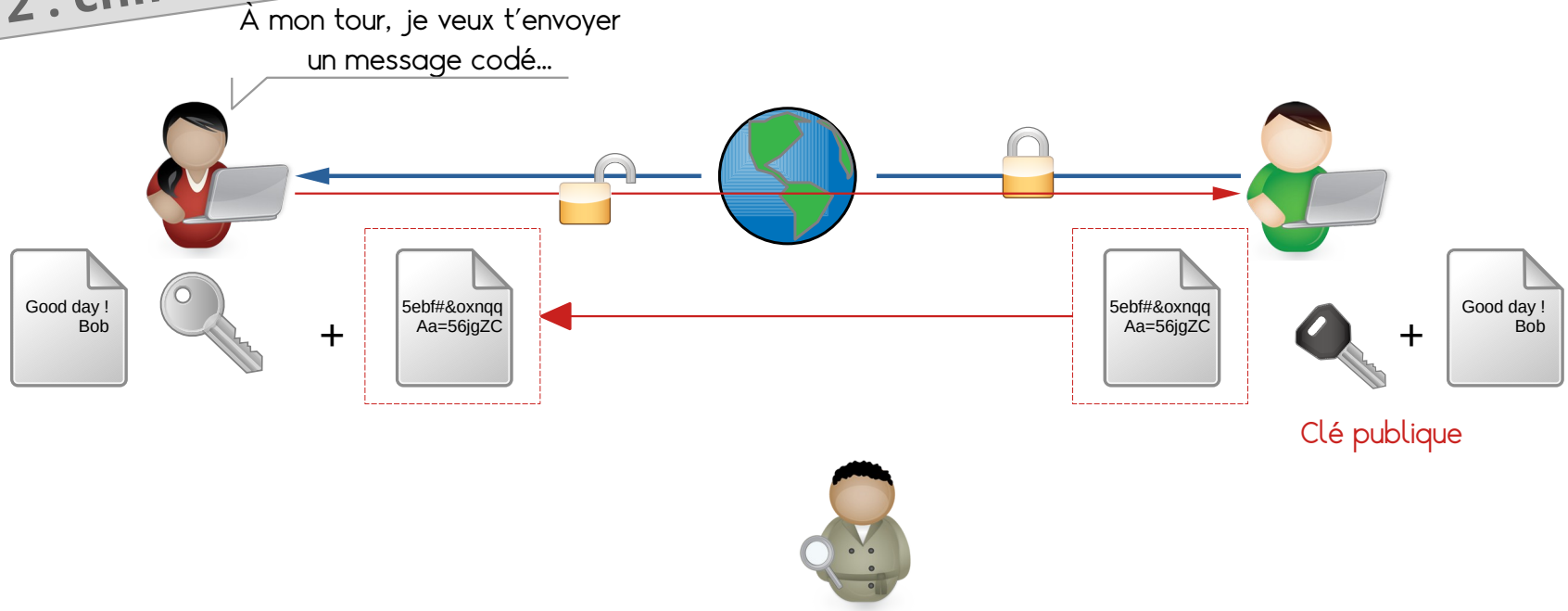
# Certificats
## Phase 1 : authentification



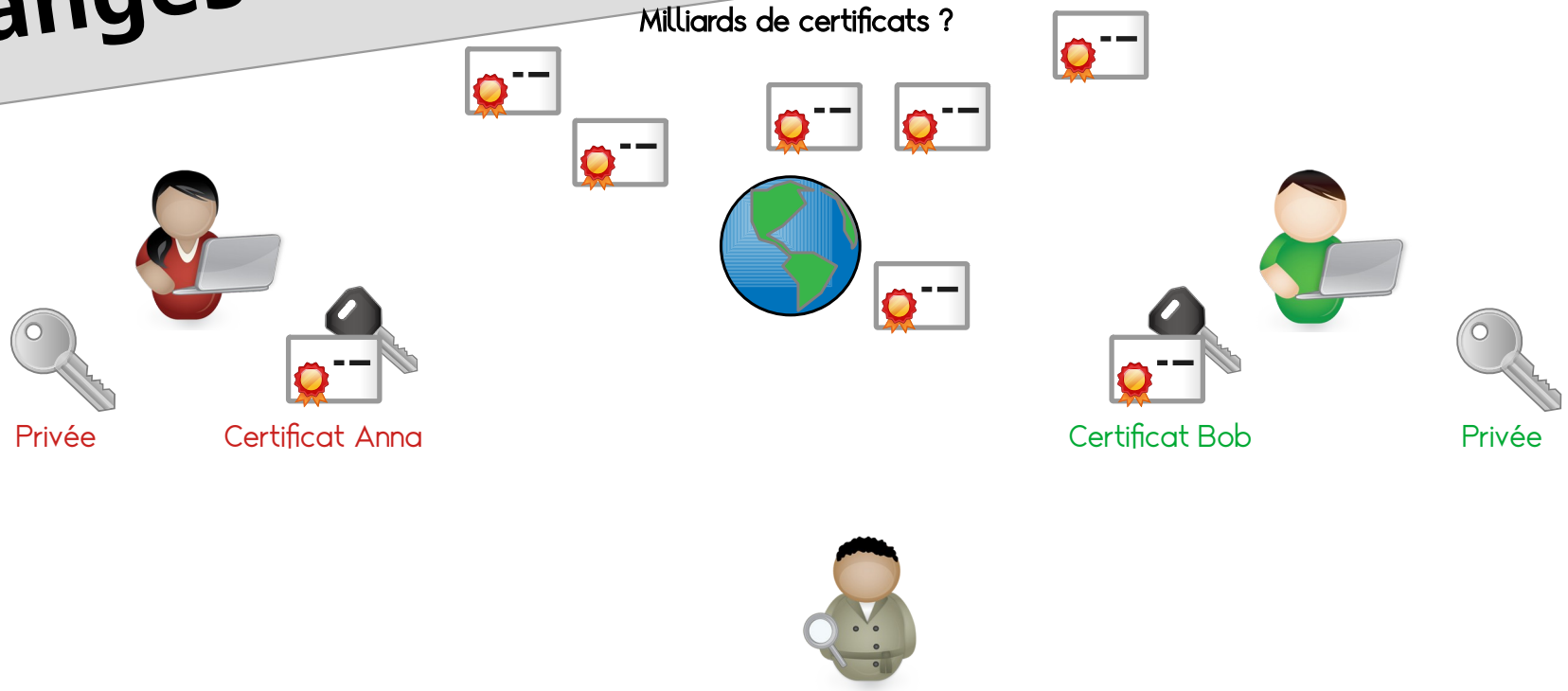
# Certificats
## Phase 2 : chiffrement



# Certificats
## Phase 2 : chiffrement



# Échanges


Milliards de certificats ?
Privée
Certificat Anna
Certificat Bob
Privée

# Certificats

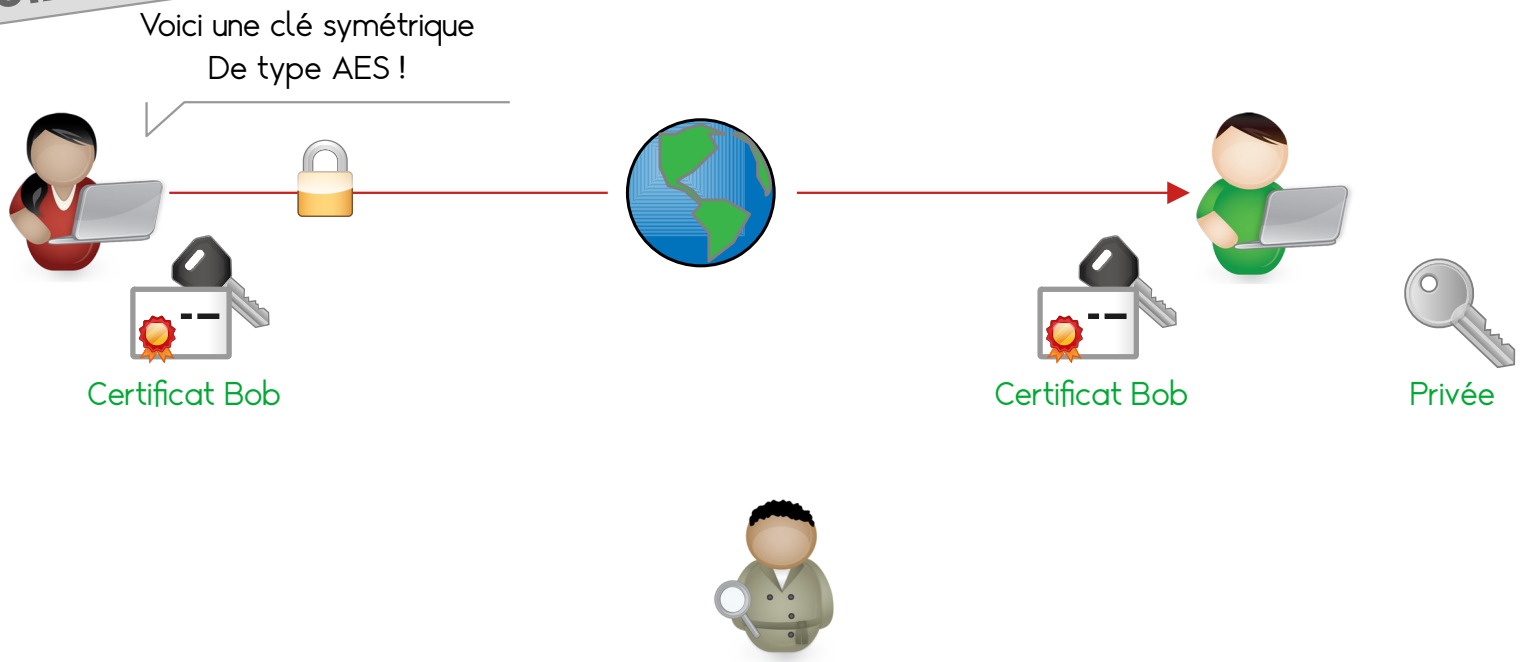
## Problème réglé

- Le pirate ne peut plus lire les messages chiffrés avec la clé publique
- Le destinataire a la garantie de l'émetteur du message (non répudiation)

## Nouveau problème

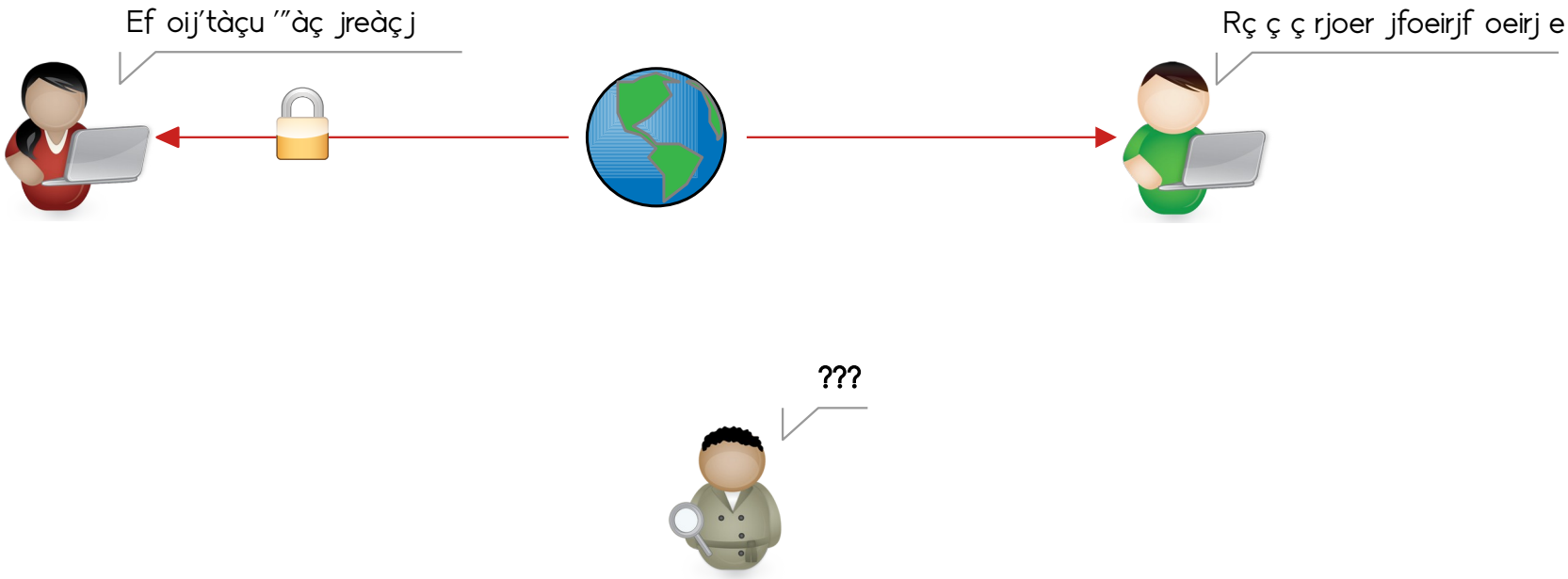
- Le chiffrement ne fonctionne que dans un sens (clé publique → clé privée)
- Tous les utilisateurs doivent avoir un certificat (coût) ?

# Échanges TLS (HTTPS)
## Phase 3 : choix d'une clé secrète symétrique

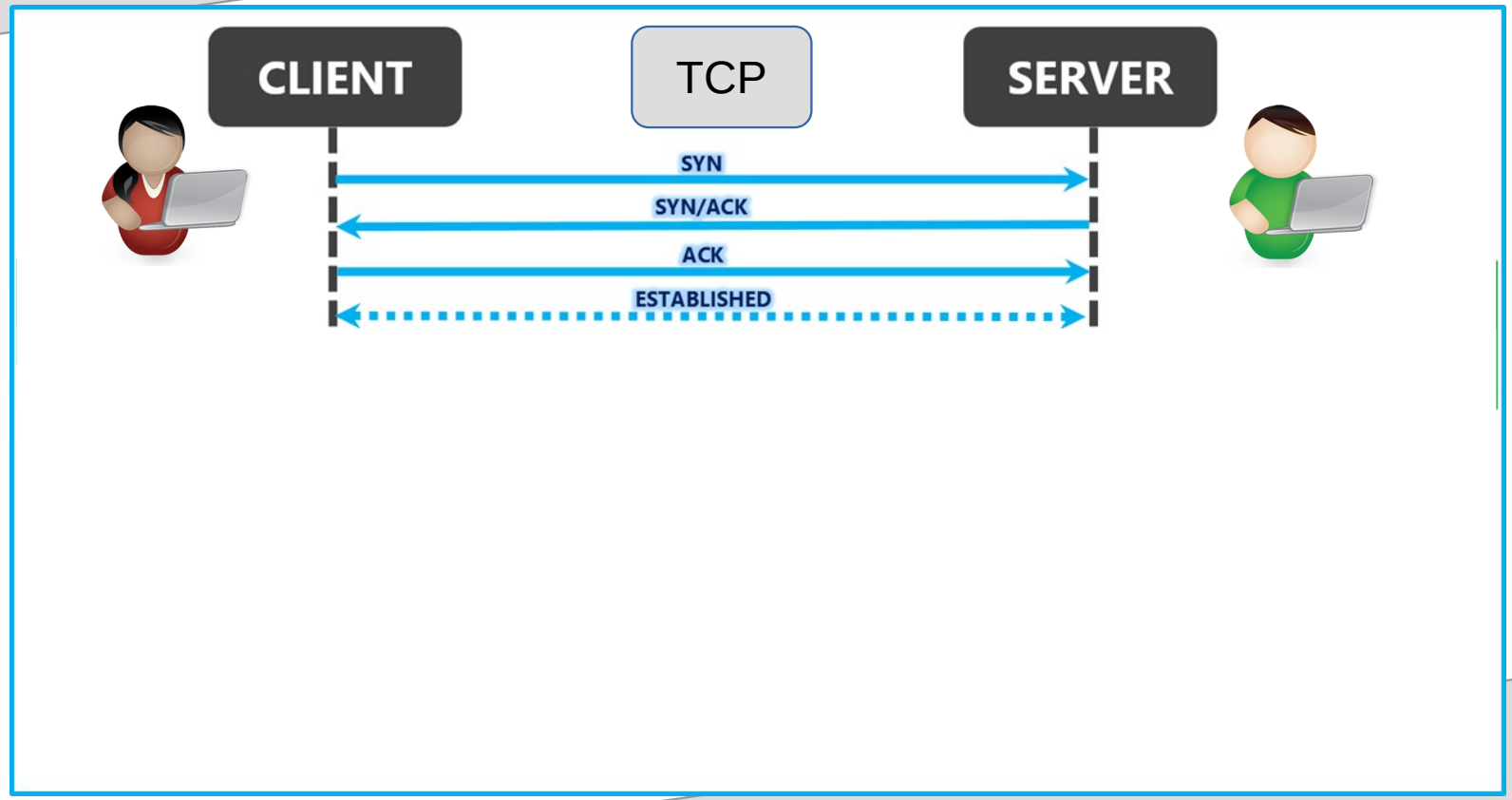


# Échanges TLS (HTTPS)

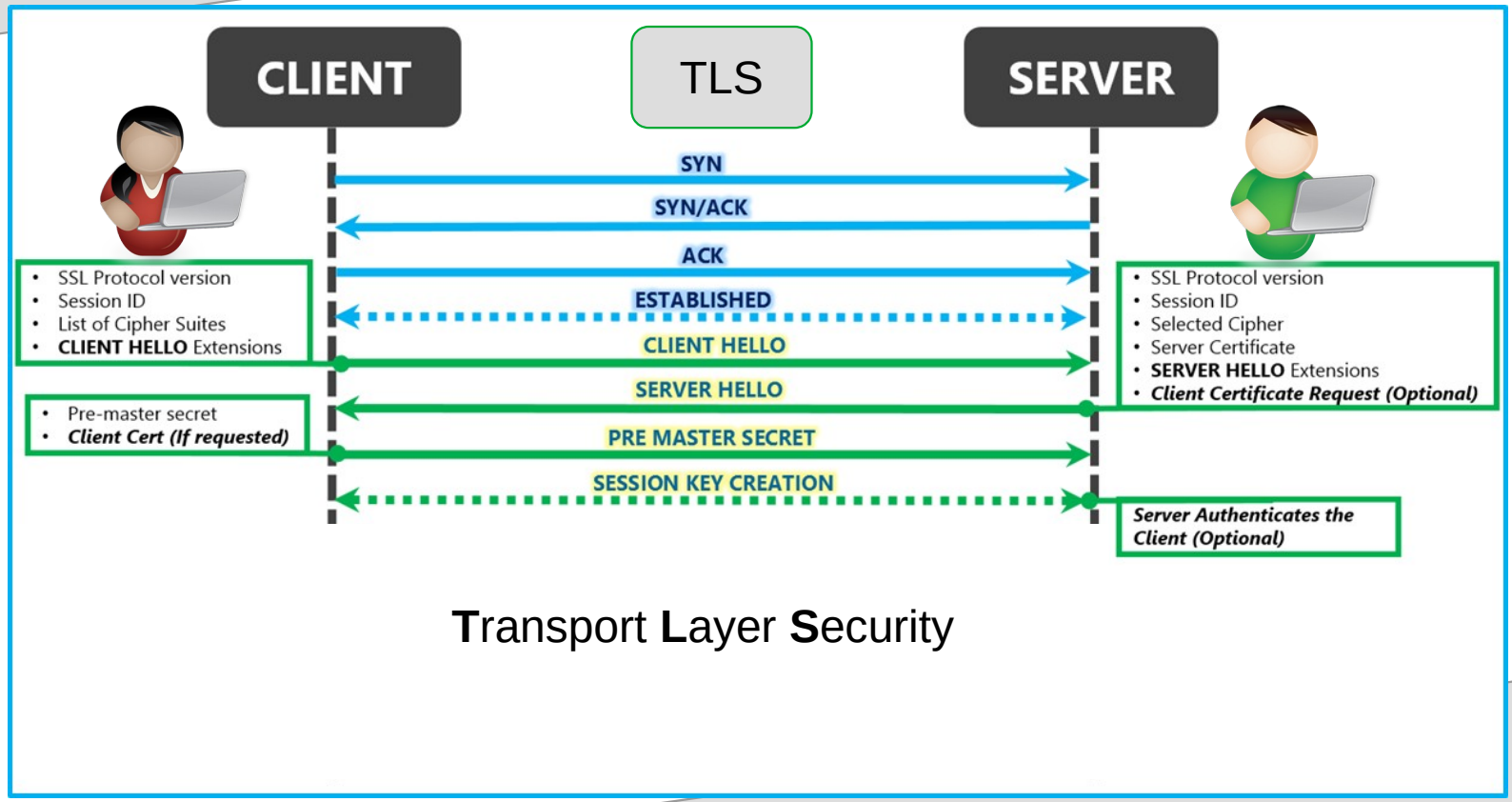
## Phase 2 : chiffrement



# Échanges TLS (HTTPS)

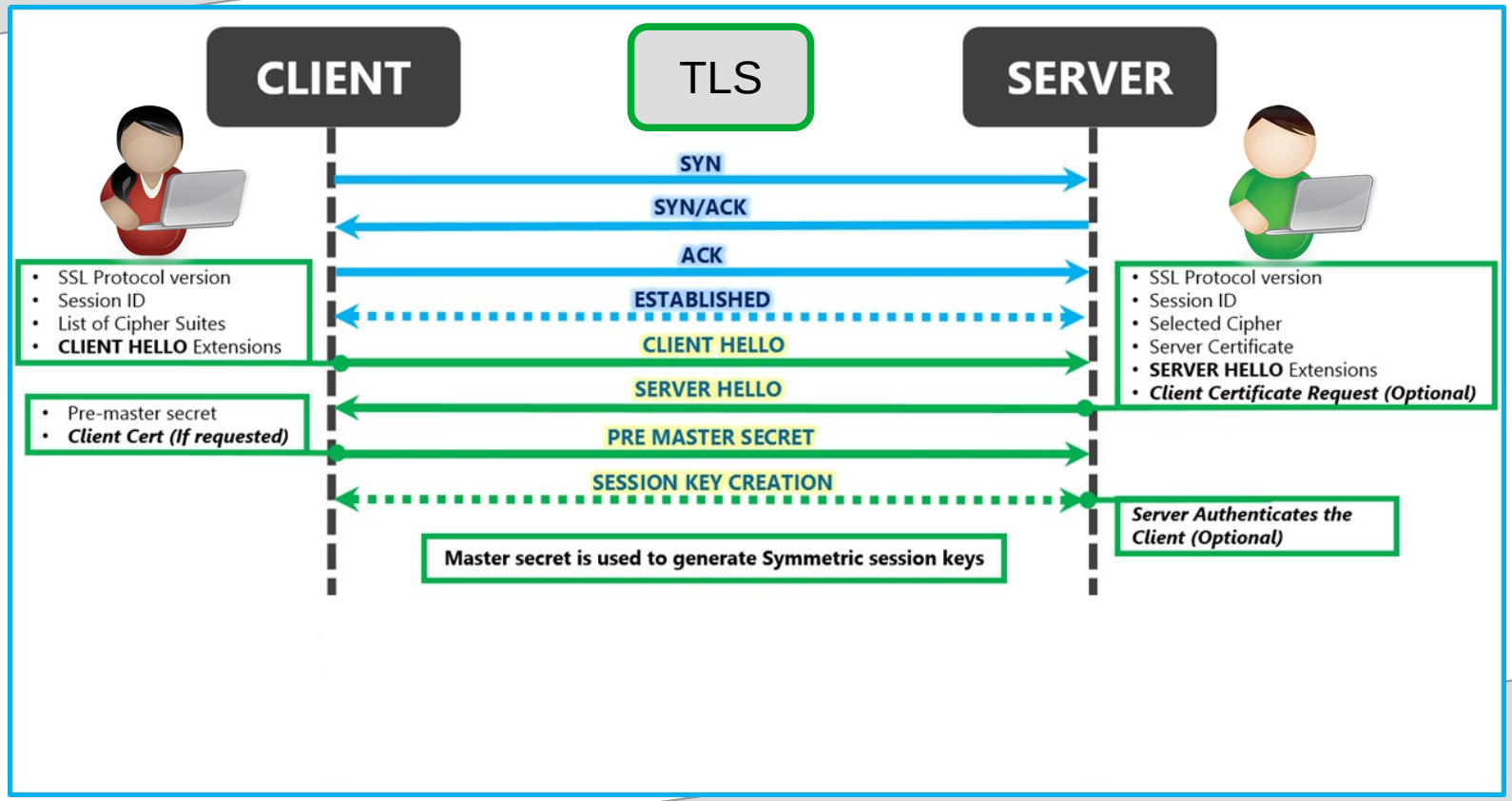


# Échanges TLS (HTTPS)

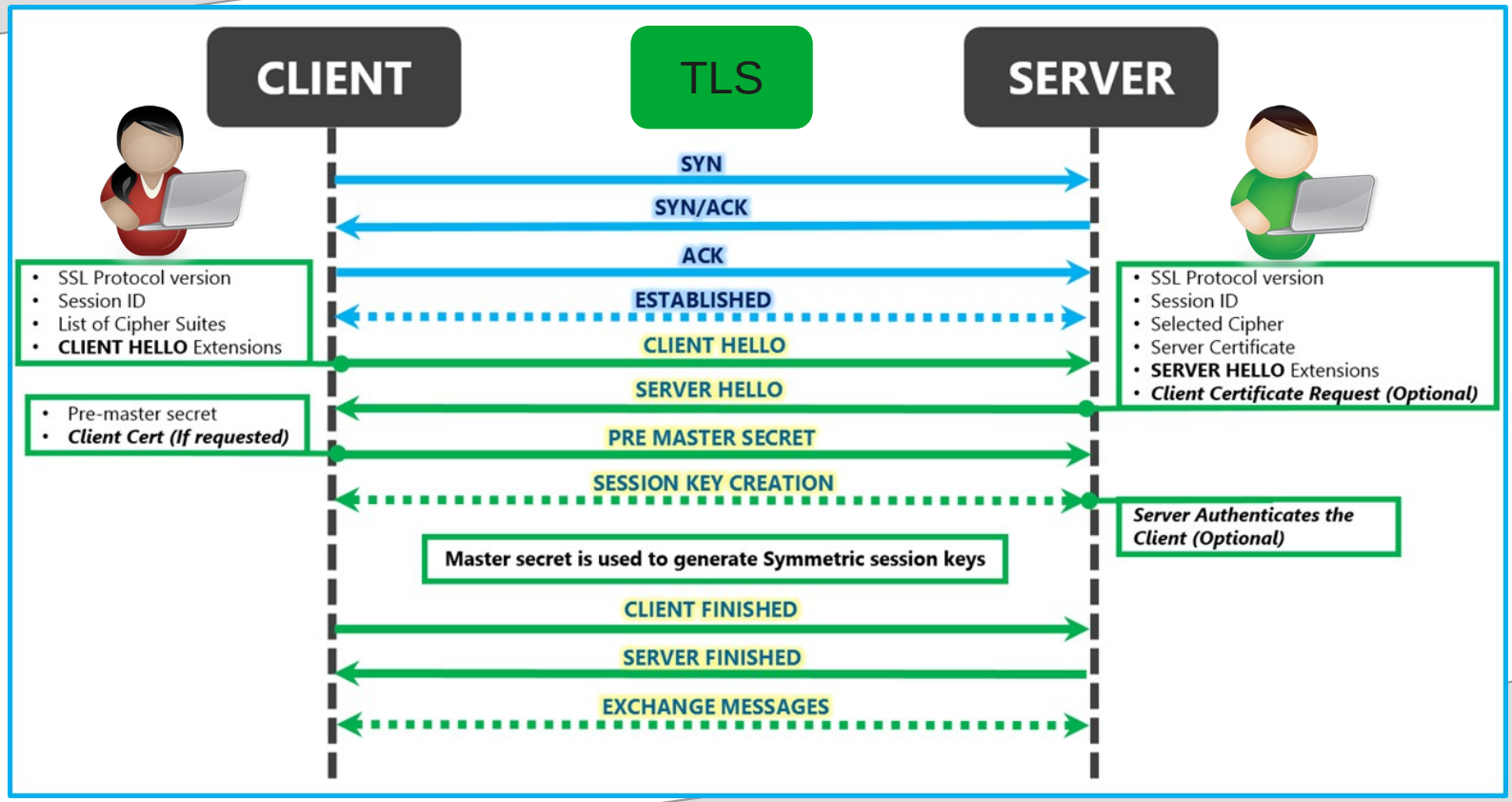



**T**ransport **L**ayer **S**ecurity

# Échanges TLS (HTTPS)



# Échanges TLS (HTTPS)



# QCM

Sauriez-vous reconstituer les échanges entre Bob et Anna ?

300 Exploration sécurisation Node.JS