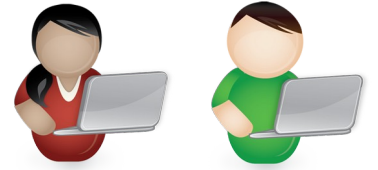


Sécurisation TLS

David ROUMANET

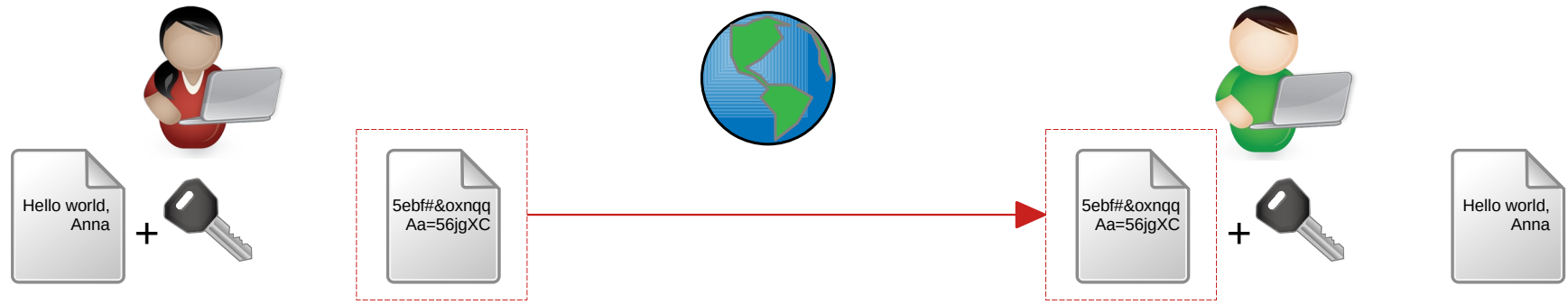
Échanges



Situation initiale

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

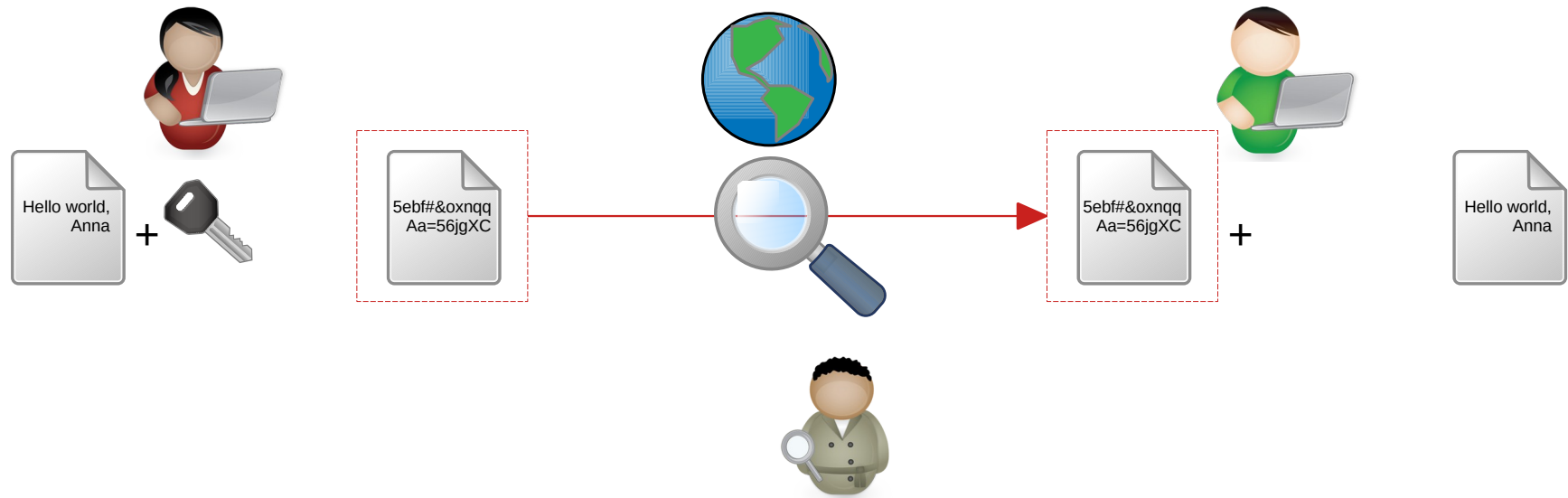
Échanges symétriques



Chiffrement symétrique

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

Échanges symétriques



Échanges symétriques

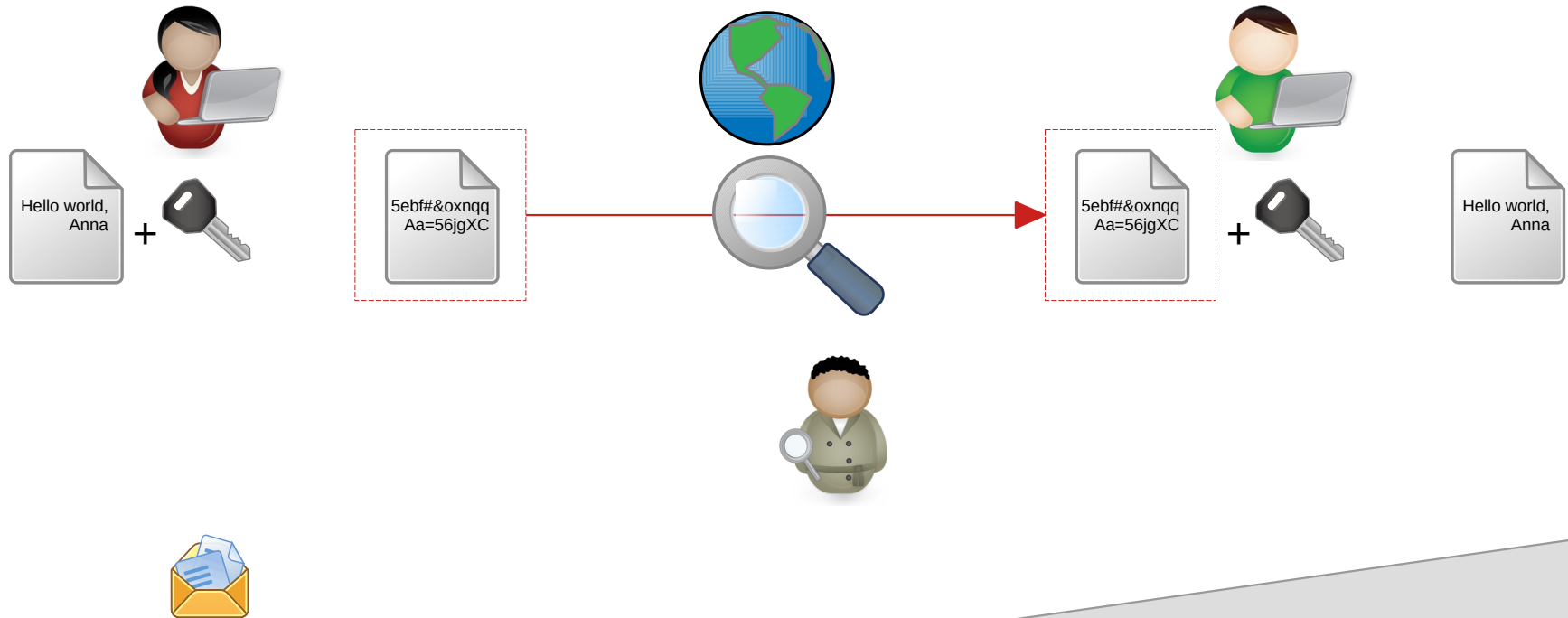
Problème réglé

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

Nouveau problème

- Comment échanger une clé de chiffrement ?

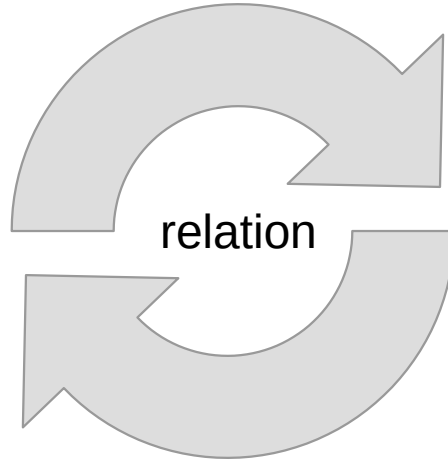
Échanges symétriques



Échanges **a**symétriques



Clé privée

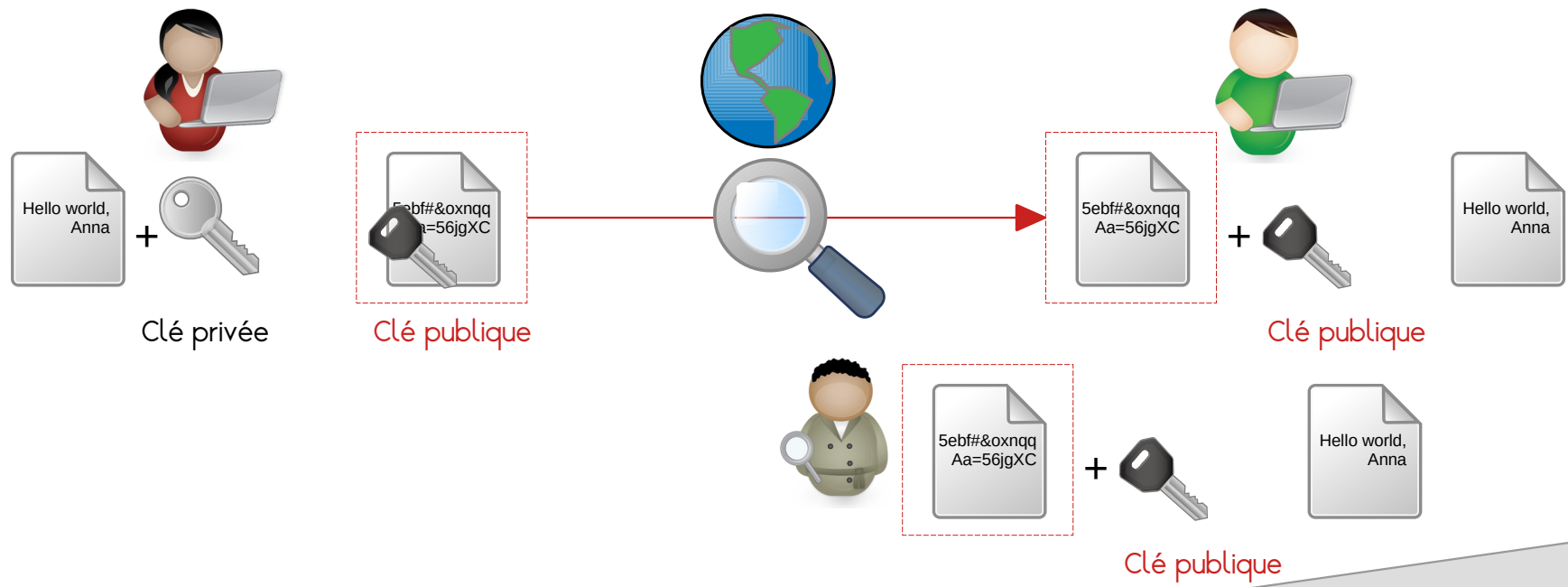


Clé publique

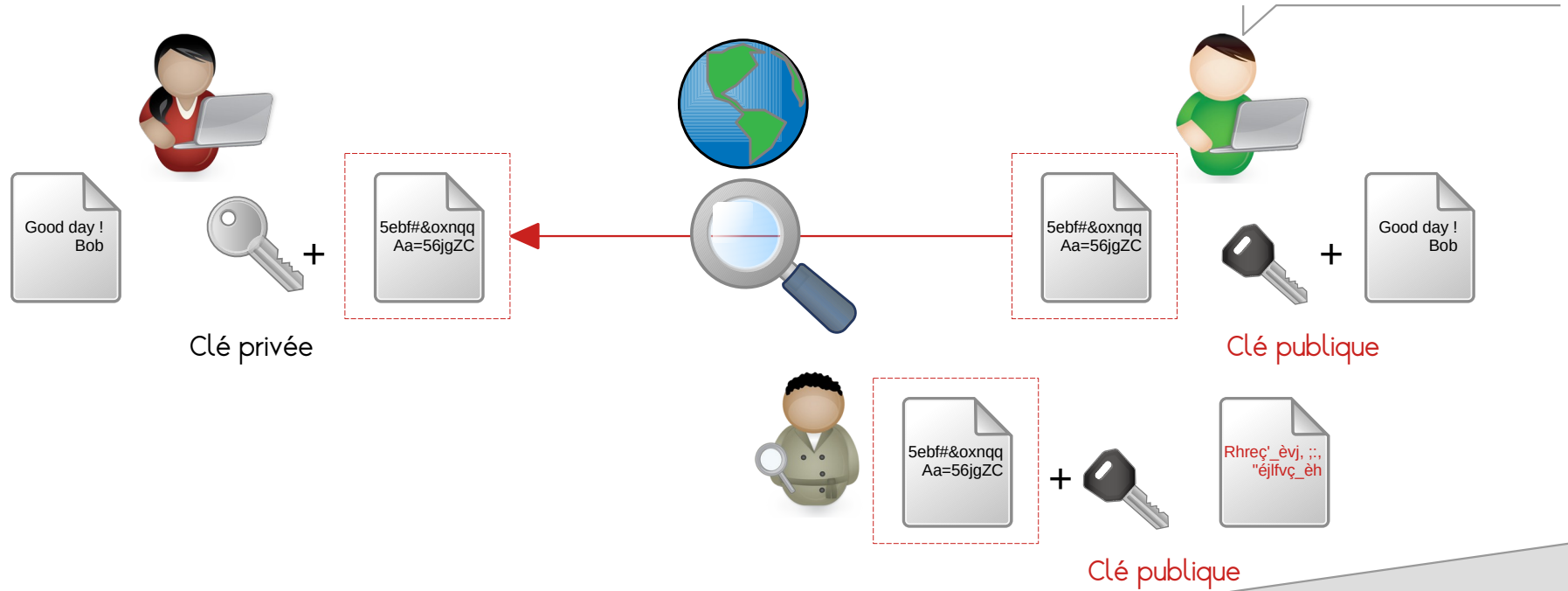
Basé sur :

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

Échanges asymétriques



Échanges asymétriques



Échanges **a**symétriques

Chiffrement asymétrique

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



Rivest, Shamir, Adleman



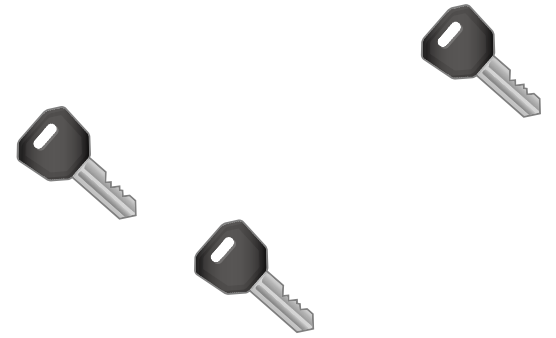
Clé privée

Les clés publiques peuvent
décoder ce que je code.



Clé publique

Seule la clé privée peut
décoder ce que je code.



Échanges **a**symétriques

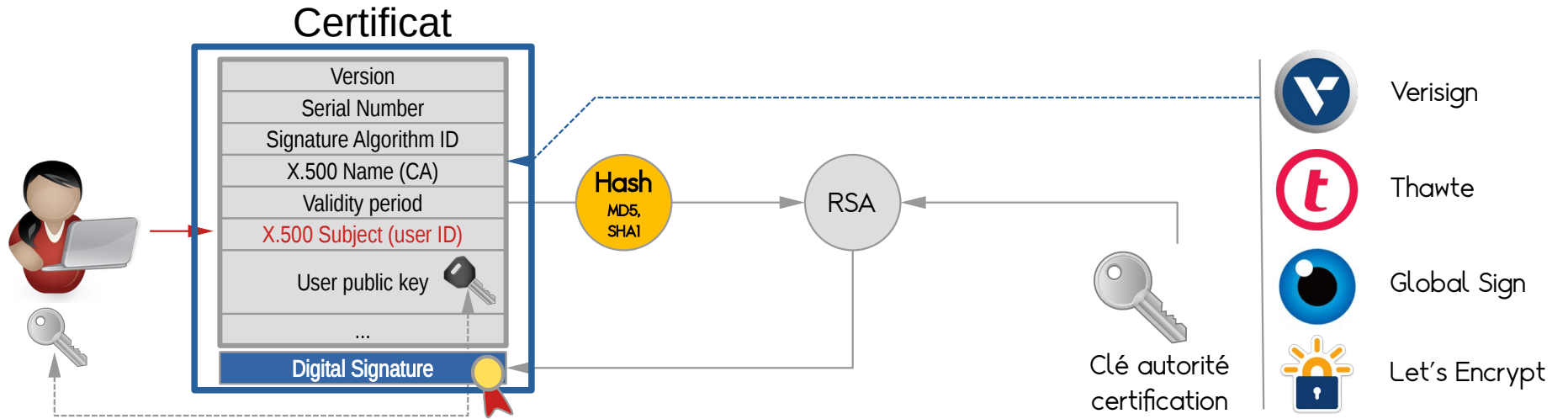
Problème réglé

- 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

Préférences SSL - Configuration du système

Configuration

- Serveur mandataire (proxy)
- Préférences de connexion
- Préférences SSL**
- Cookies
- Partages Windows

Préférences SSL

Signataires SSL

Organisation / Nom commun

- ✓ Certificats du système
 - ✓ ACCV
 - ✓ ACCVRAIZ1
 - ✓ Actalis S.p.A./03358520967
 - ✓ Actalis Authentication Root CA
 - ✓ AffirmTrust
 - ✓ AffirmTrust Commercial
 - ✓ AffirmTrust Networking
 - ✓ AffirmTrust Premium
 - ✓ AffirmTrust Premium ECC
 - ✓ Agence Nationale de Certification Electronique
 - ✓ TunTrust Root CA
 - ✓ Agencia Catalana de Certificacio (NIF Q-0801176-I)
 - ✓ EC-ACC
 - ✓ Amazon
 - ✓ Amazon Root CA 1
 - ✓ Amazon Root CA 2
 - ✓ Amazon Root CA 3
 - ✓ Amazon Root CA 4
 - ✓ ANF Autoridad de Certificacion

Affichage... Désactiver Activer Supprimer Ajouter...

Mettre en valeur les paramètres modifiés Aide Réglages par défaut Réinitialiser Appliquer

Configuration du système

Informations sur le sujet

Nom commun : Amazon Root CA 1
Organisation : Amazon
Unité organisationnelle :
Pays : US
État :
Ville :

Informations sur l'émetteur

Nom commun : Amazon Root CA 1
Organisation : Amazon
Unité organisationnelle :
Pays : US
État :
Ville :

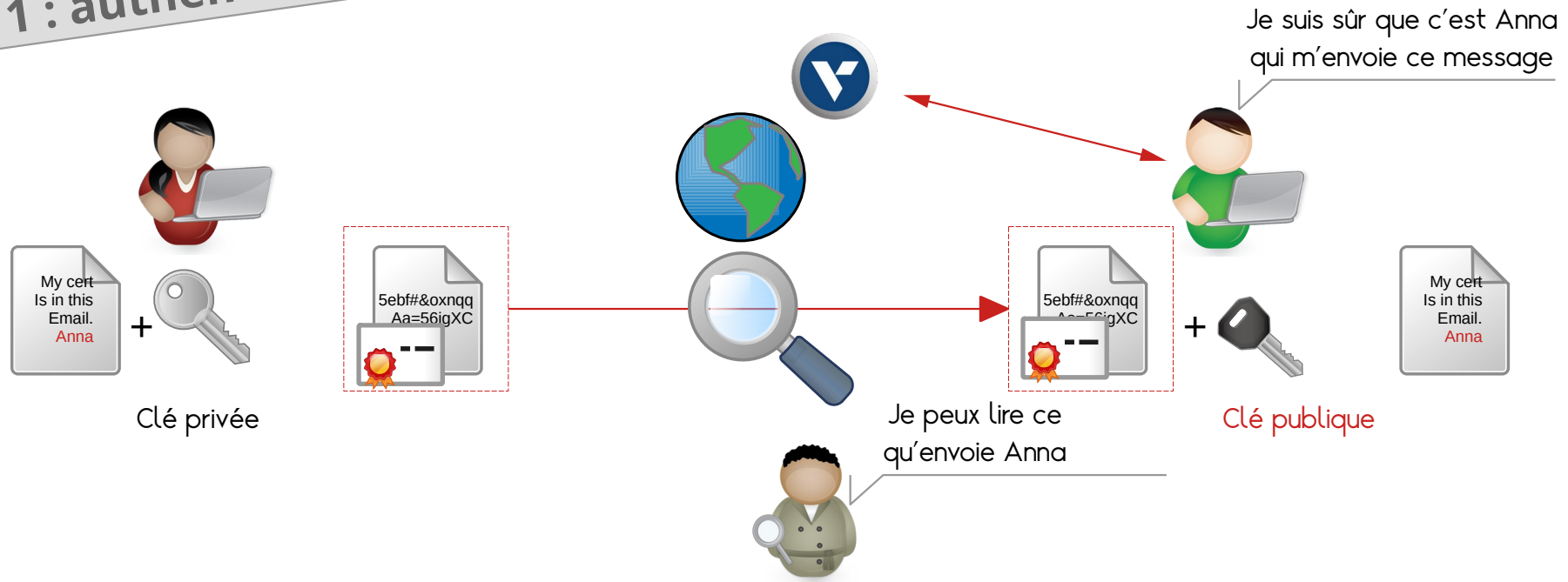
Autre

Période de validité mar. mai 26 00:00:00 2015 GMT à dim. janv. 17 00:00:00 2038 GMT
Numéro de série 06:6c:9f:cf:99:bf:8c:0a:39:e2:f0:78:8a:43:e6:96:36:5b:ca
Empreinte MD5 43c6bfaecfead2f18c6886830fcc8e6
Empreinte SHA1 8da7f965ec5efc37910f1c6e59fdc1cc6a6ede16

< Précédent > Suivant ✓ Ok

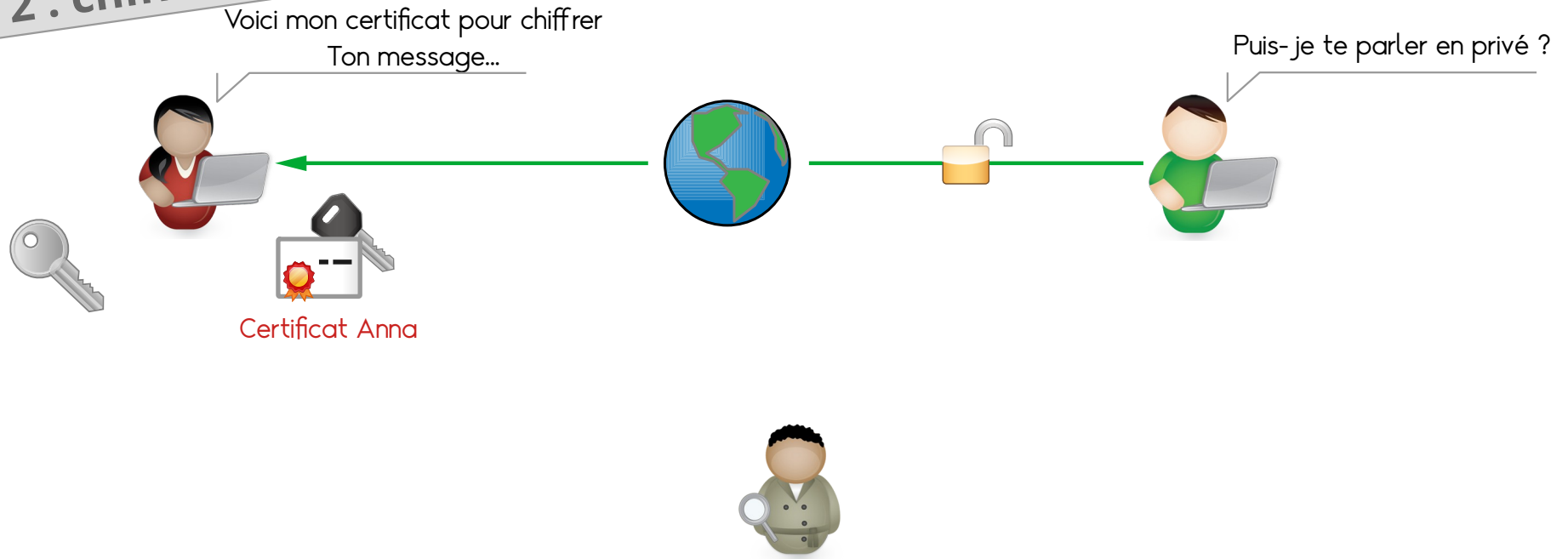
Certificats

Phase 1 : authentication



Certificats

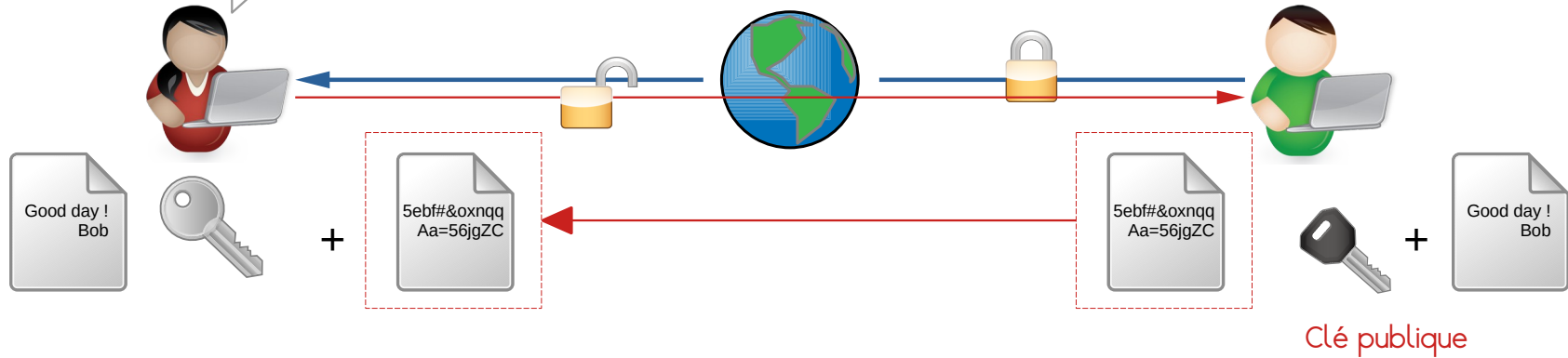
Phase 2 : chiffrement



Certificats

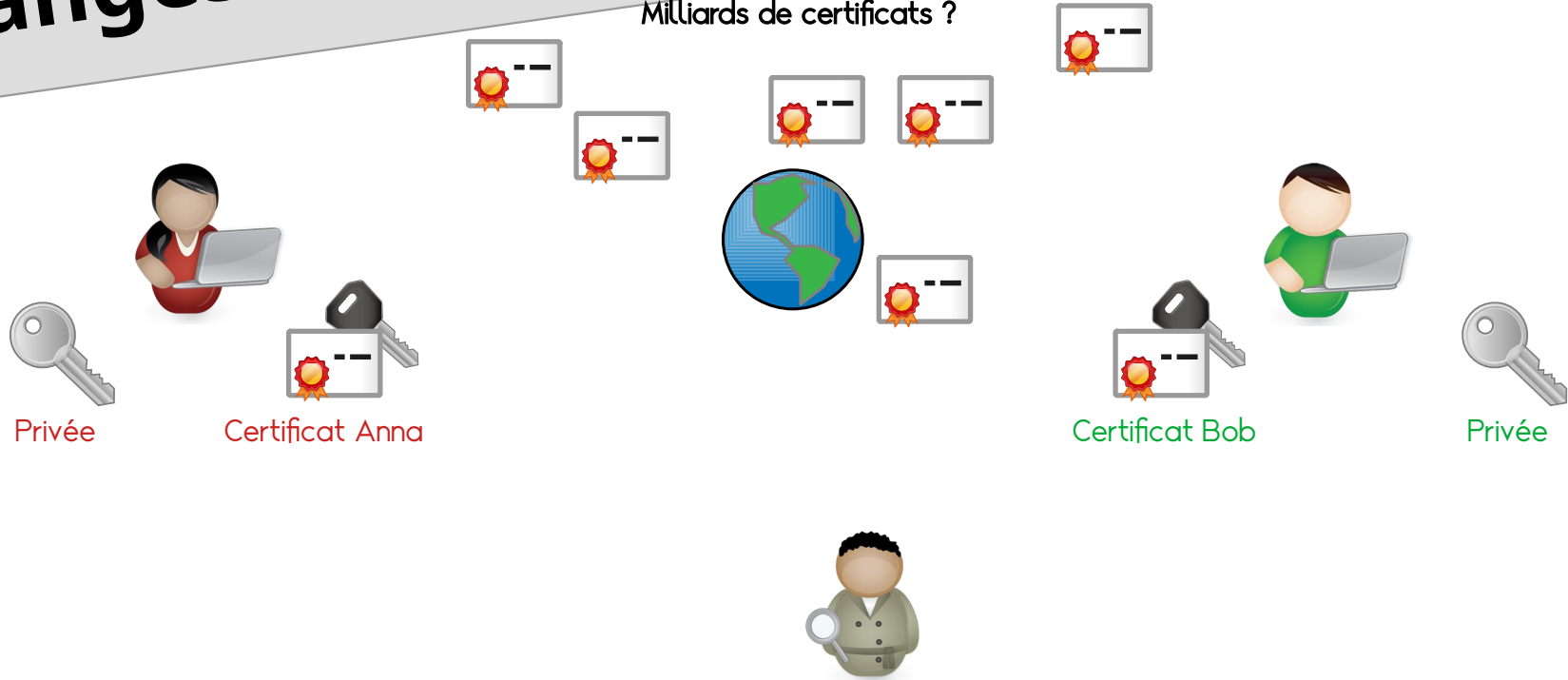
Phase 2 : chiffrement

À mon tour, je veux t'envoyer un message codé...



Échanges

Milliards de certificats ?



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)

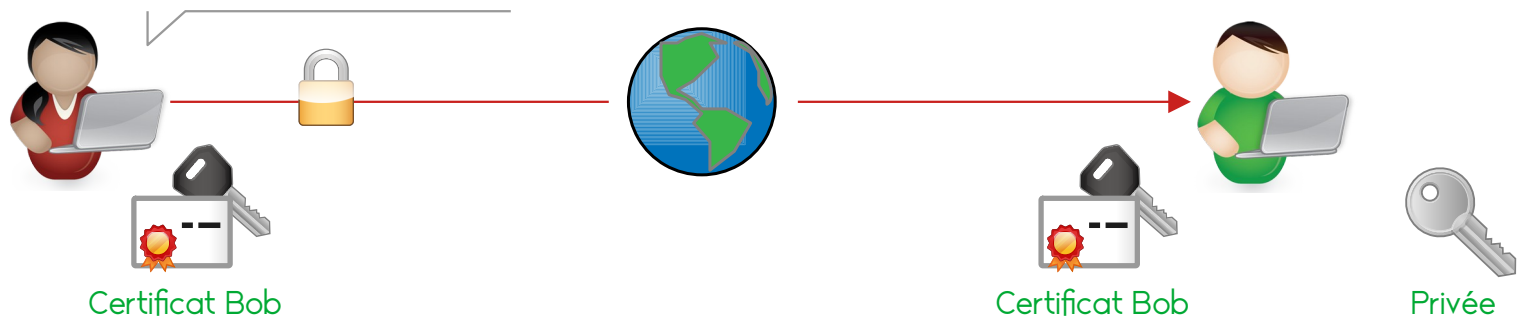
Nouveau problème

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

Échanges TLS (HTTPS)

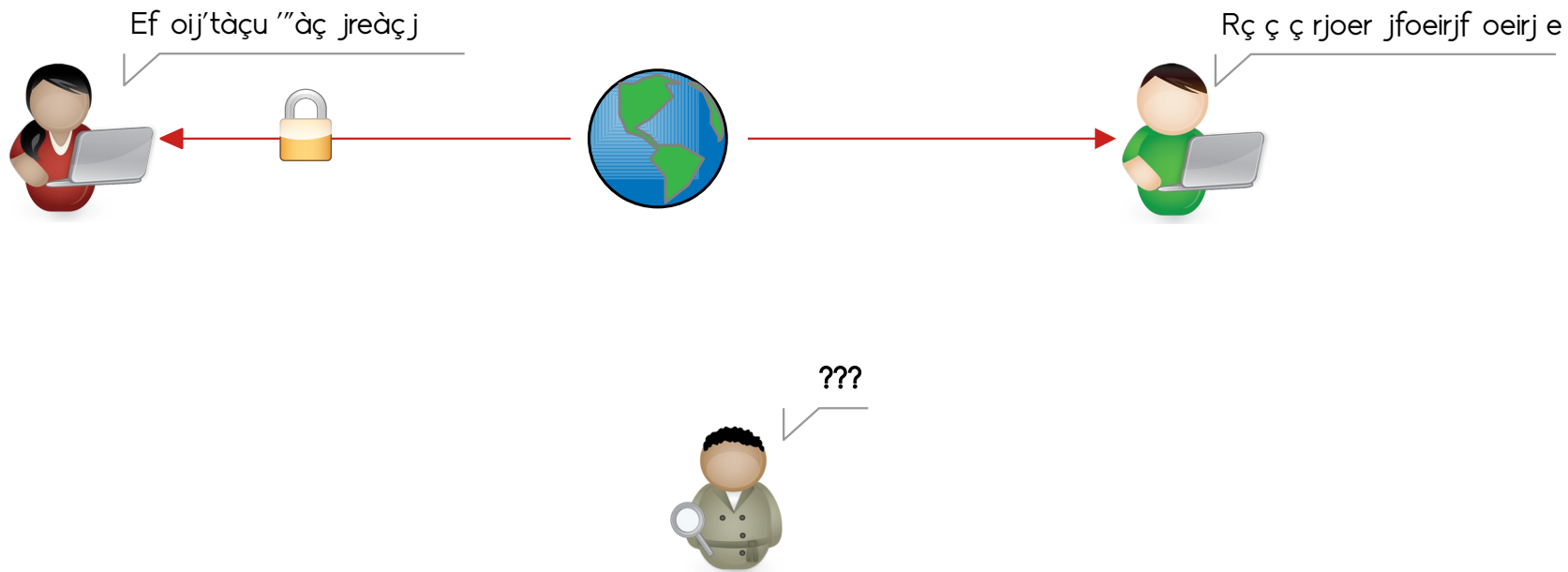
Phase 3 : choix d'une clé secrète symétrique

Voici une clé symétrique
De type AES !

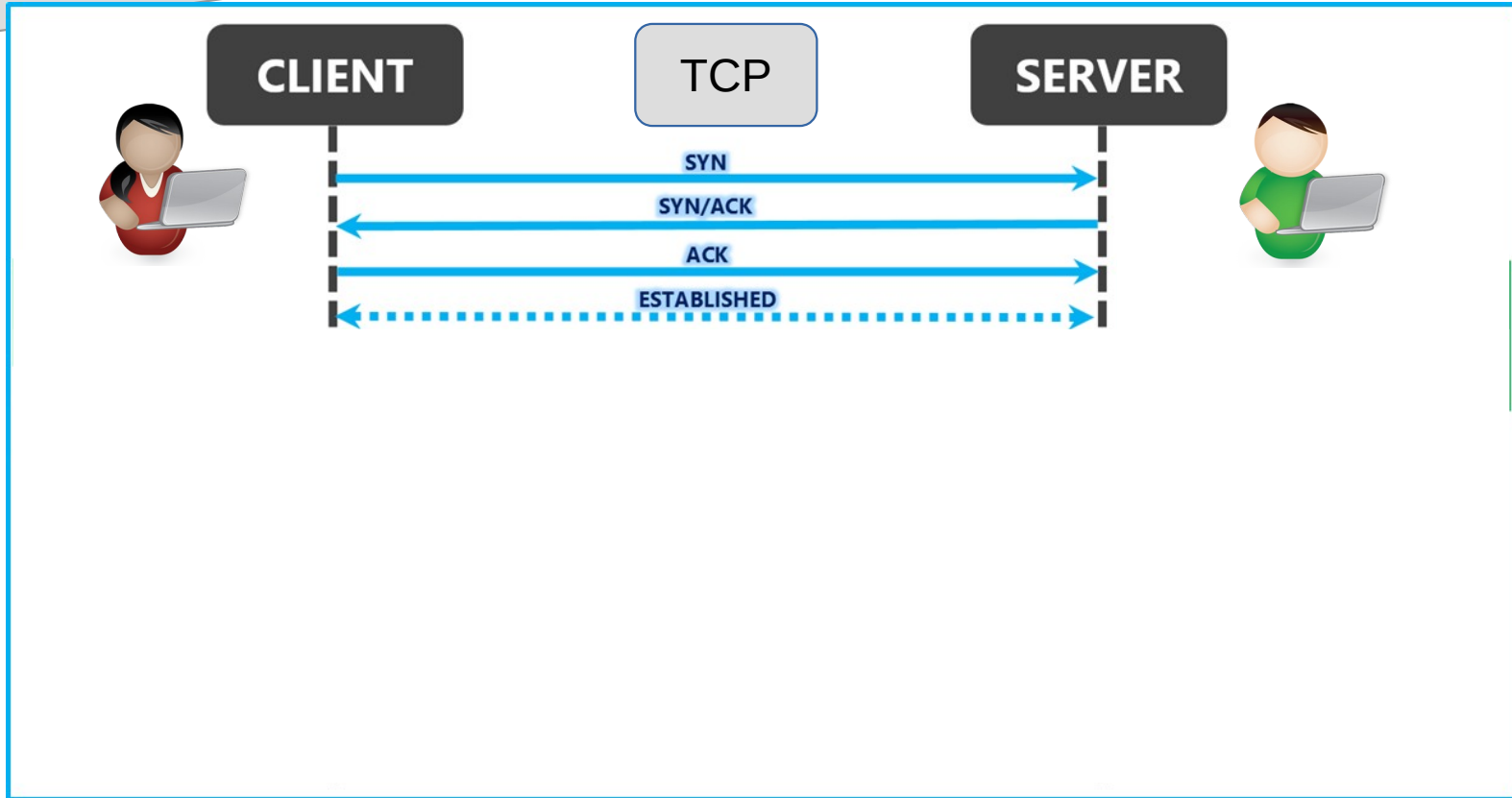


Échanges TLS (HTTPS)

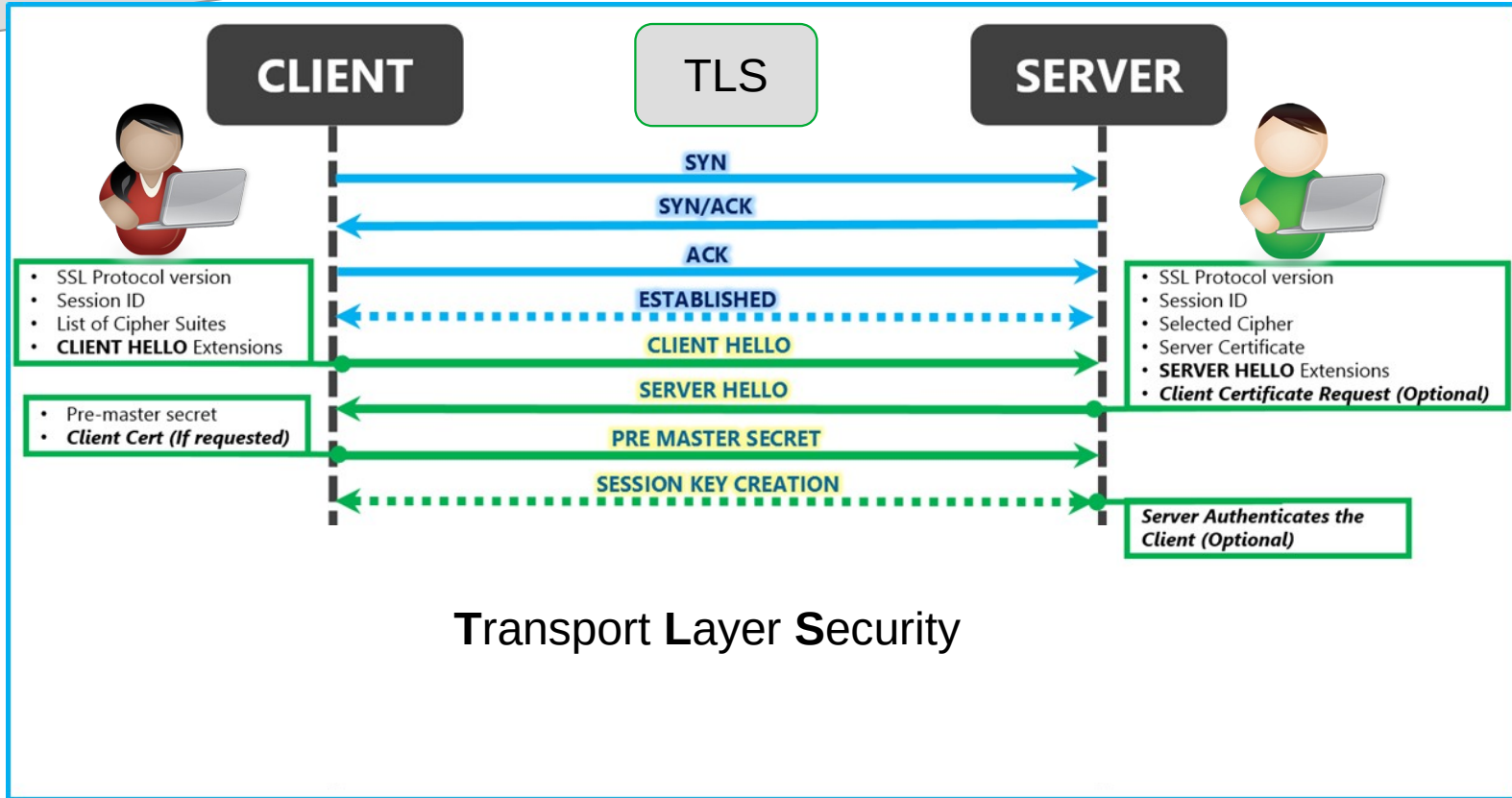
Phase 2 : chiffrement



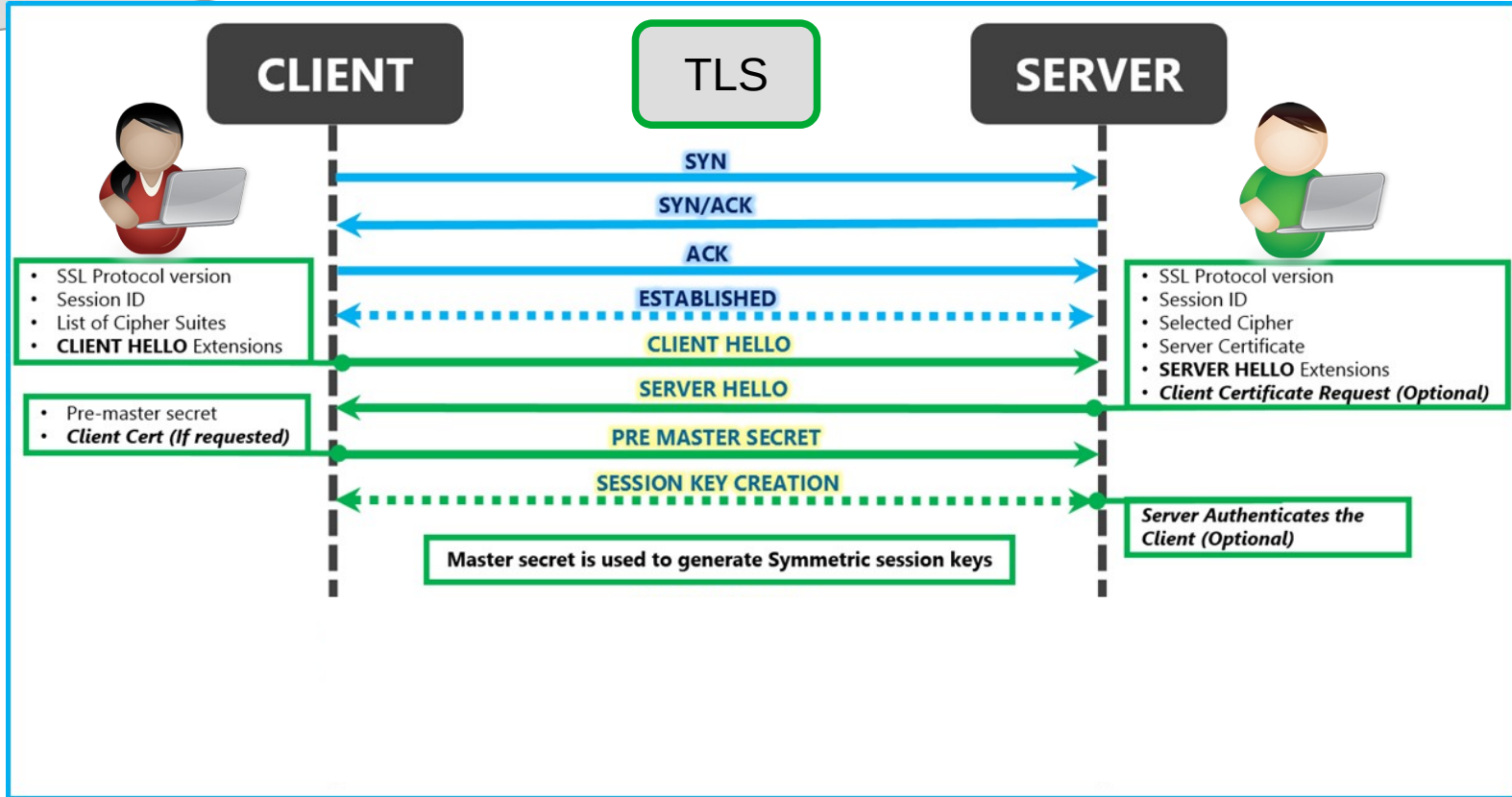
Échanges TLS (HTTPS)



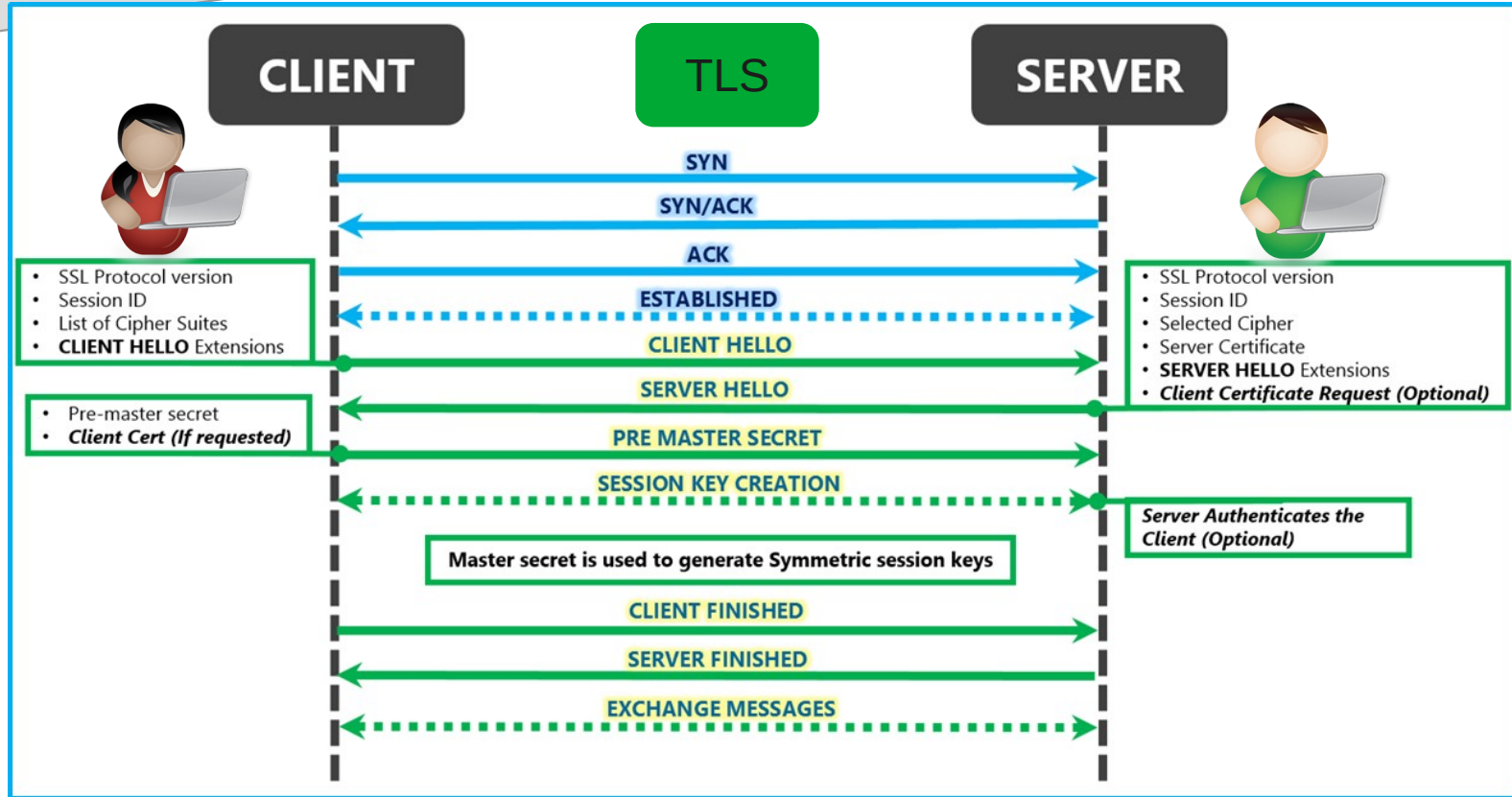
Échanges TLS (HTTPS)



Échanges TLS (HTTPS)



Échanges TLS (HTTPS)



Sauriez-vous reconstituer les échanges entre Bob et Anna ?

Exploration

300 Exploration sécurisation Node.JS

