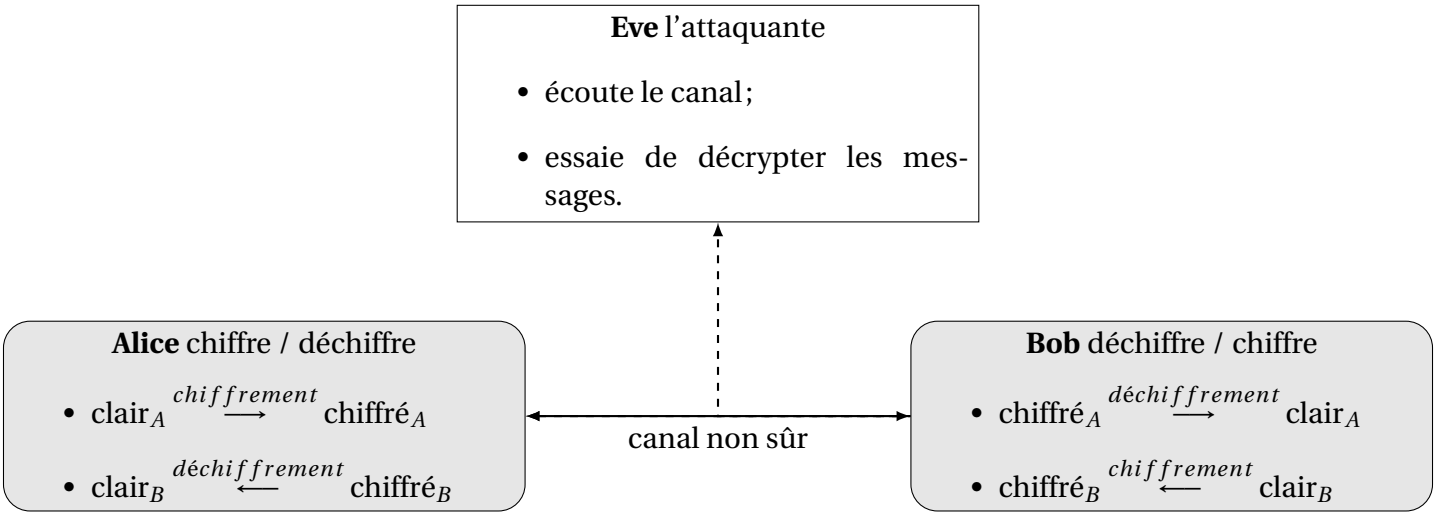
1 Problèmes

- **Problème 1 : confidentialité** Alice veut échanger avec Bob de façon **confidentielle** sur un canal non sûr.
- **Problème 2 : authentification** Alice veut une preuve que son interlocuteur est bien Bob.



Situation problème

2 Chiffrement symétrique

☞ **Principe :** Alice et Bob partage une **clef secrète** qui permet à la fois de chiffrer un message en clair et de déchiffrer un message chiffré.

☞ **Algorithmes :** Chiffres de César, de Vigenère, de Vernam (masque jetable inconditionnellement sûr), AES (clef de 256 bits).

☞ **Points forts :** AES est rapide et sûr (seules attaques connues par recherche exhaustive).

☞ **Points faibles :** Comment échanger la clef de chiffrement lors d'un échange sur le Web par exemple ?

3 Chiffrement asymétrique à clef publique

☞ **Principe :**

- Attribution d'une paire de clefs **(clef publique, clef privée)** à chaque utilisateur.
- La **clef publique** peut être publiée dans un annuaire, la **clef privée** doit rester secrète.
- Soit K^{pub}_{Alice} et K^{pub}_{Bob} les fonctions de chiffrement avec clef publique d'Alice et Bob et K^{priv}_{Alice} pour Alice et K^{priv}_{Bob}, leurs fonctions de déchiffrement avec clef privé.
- Pour transmettre un secret m à Alice :
  - Bob envoie le chiffré $K^{pub}_{\text{Alice}}(m)$ avec la clef publique d'Alice ;
  - Alice est la seule à pouvoir déchiffrer avec sa clef privée :

$$K^{priv}_{\text{Alice}}(K^{pub}_{\text{Alice}}(m)) = m$$

- Pour signer numériquement un message m :

- Bob chiffre m avec sa clef privé : $K_{\text{Bob}}^{priv}(m) = s$;
- Alice déchiffre la signature numérique s avec la clef publique de Bob et compare le résultat avec le message m. Si la clef publique a déchiffré la signature c'est que Bob a chiffré le message avec sa clef privée.

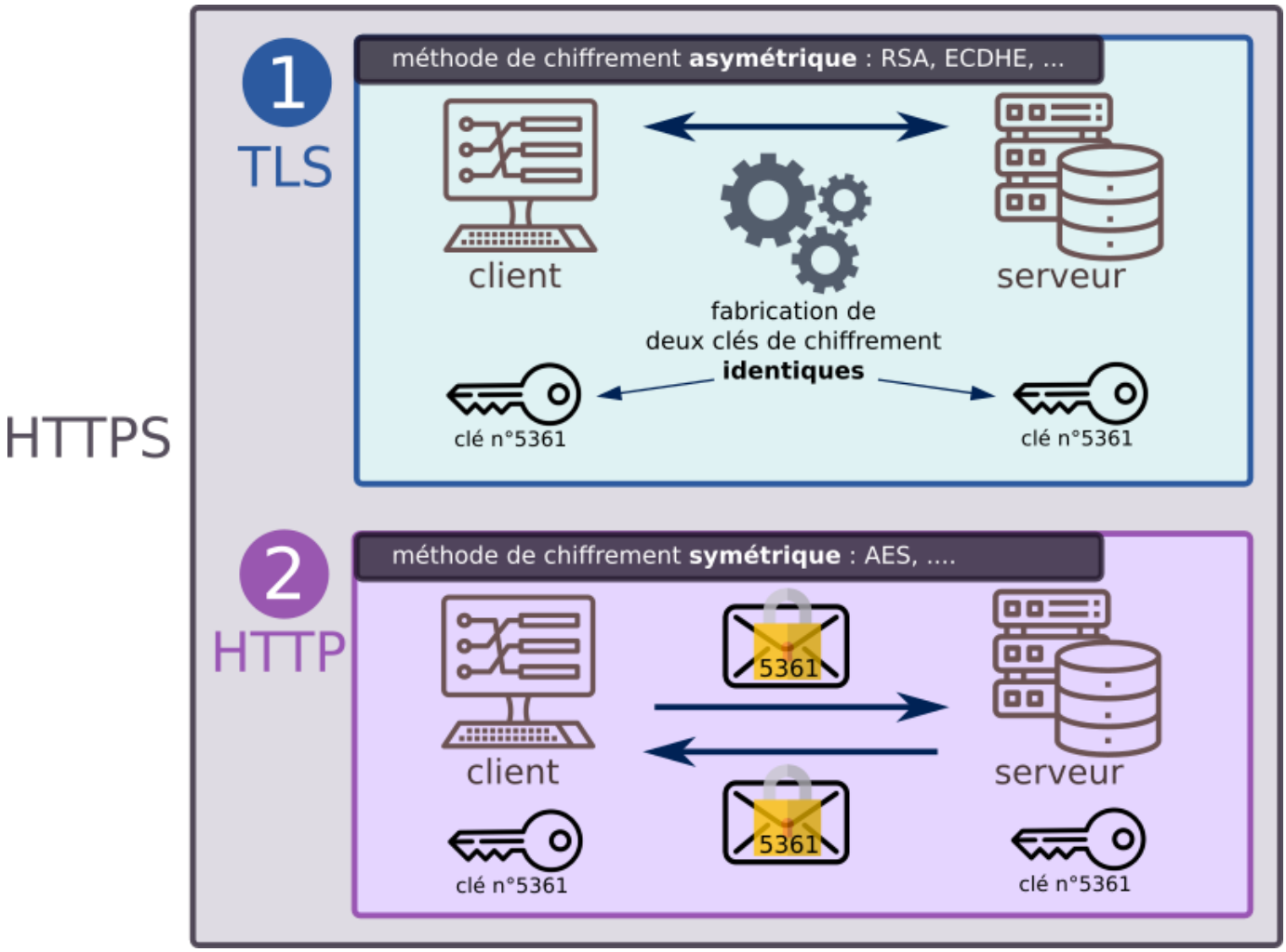
$$K_{\text{Bob}}^{pub}(s) = K_{\text{Bob}}^{pub}(K_{\text{Bob}}^{priv}(m)) = m$$

☞ **Algorithmes :** RSA.

☞ **Points forts :** RSA permet d'échanger un secret (comme une clef de chiffrement symétrique) à partir de seules données publiques, gestion des clefs (une paire de clefs par utilisateur au lieu d'une clef par paire d'utilisateurs avec une chiffrement symétrique)

☞ **Points faibles :** Coûts de calculs plus importants : opérations plus complexes et tailles de clefs sûtes plus grandes (2048 bits pour RSA contre 256 bits pour AES).

4 Protocole HTTPS



Source : Gilles Lassus https://glassus.github.io/terminale_nsi

Étapes d'une poignée de main TLS.

☞ **Étape 1 : présentation du client**

Le client envoie un message initial « Hello », ainsi que différentes informations : la version de TLS utilisée et les différents suites de chiffrement (asymétrique + symétrique) qu'il peut utiliser.

☞ **Étape 2 : présentation du serveur**

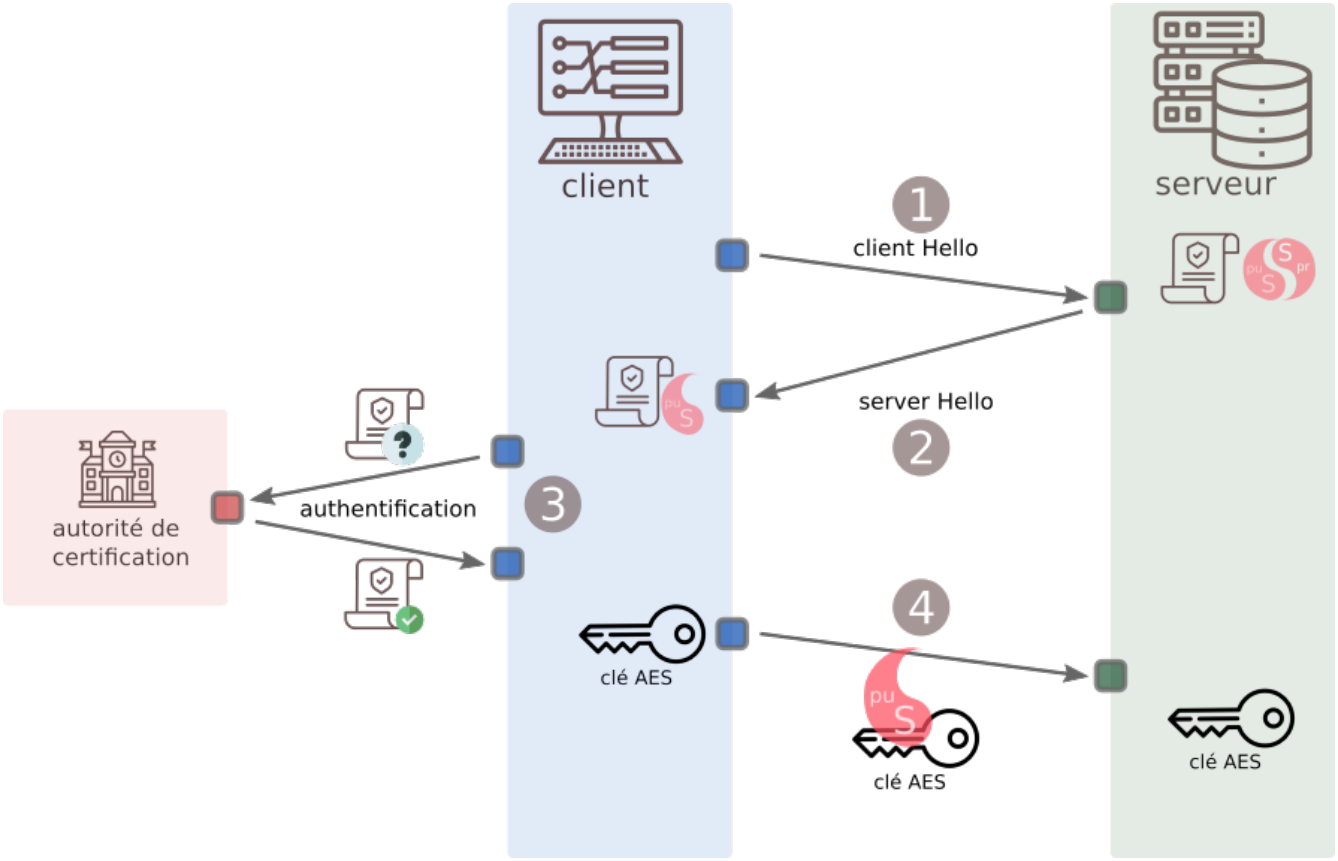
Le serveur répond en renvoyant son certificat contenant sa clé publique et signé par une autorité de certification (tiers de confiance) ainsi que la suite de chiffrement choisie.

☞ **Étape 3 : authentification du serveur par le client**

Le client vérifie avec un chiffrement asymétrique la validité du certificat avec la clef publique de l'autorité de certification qu'il possède en général dans son navigateur Web ou son système d'exploitation.

☞ **Étape 4 : choix de la clef de chiffrement**

Le client et le serveur conviennent d'une clef de chiffrement symétrique en utilisant un chiffrement asymétrique (RSA ou Diffie-Hellman).



Source : Gilles Lassus https://glassus.github.io/terminale_nsi