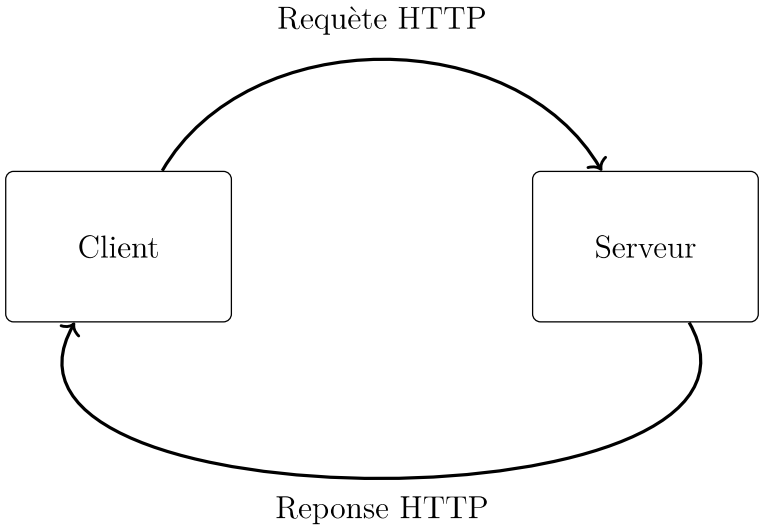
1.5 Le protocole HTTPS

NSI Tle - JB Duthoit

Ne pas hésiter à reprendre le cours de première sur ce sujet.

Rappel échanges client-serveur protocole HTTP



HTTPS est la version sécurisée de HTTP.
HTTPS s'appuie sur le protocole TSL (Transport Layer Security), connu aussi sous le nom de SSL (Secure Sockets Layer).

Principe :

Les communications vont être chiffrées grâce à une clé symétrique. Problème : comment échanger cette clé entre le client et le serveur ? Simplement en utilisant une paire clé publique / clé privée !

Voici le déroulement des opérations :

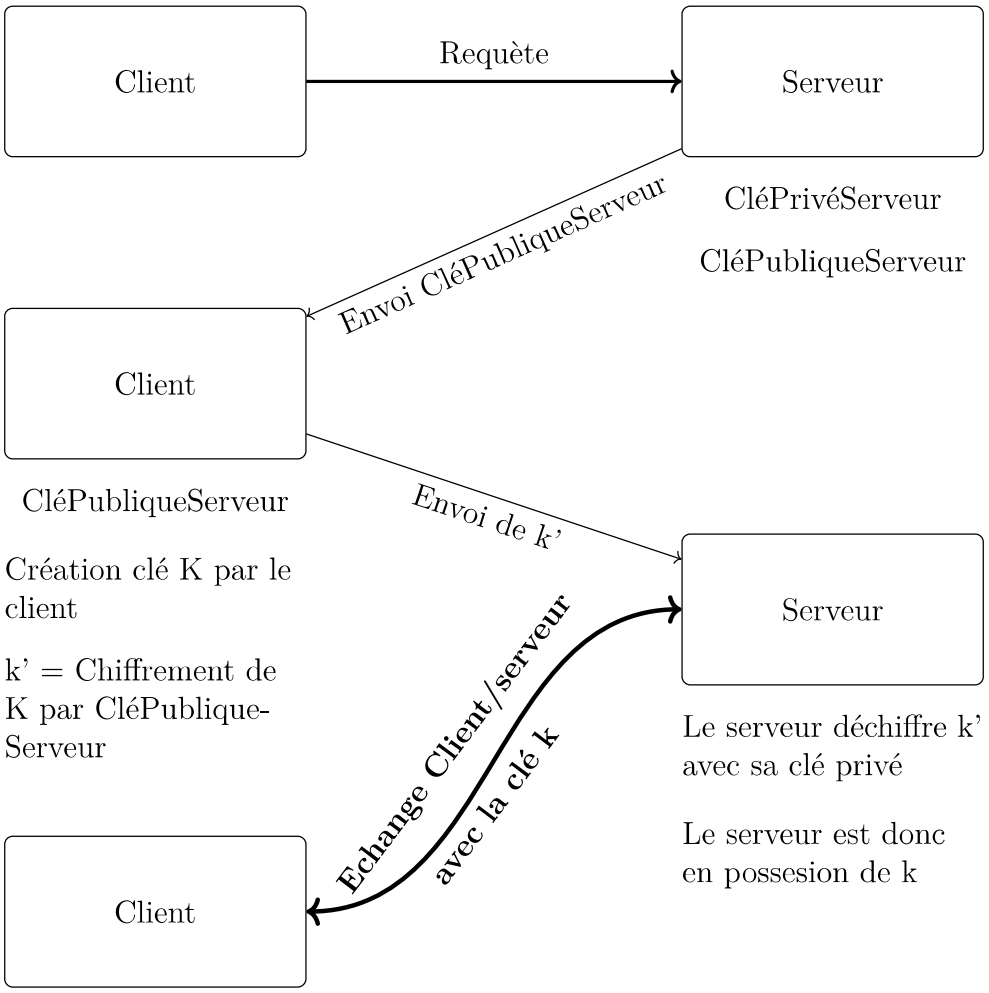
1. Le client effectue une requête HTTPS vers le serveur, en retour le serveur envoie sa clé publique (CléPubliqueServeur) au client

2. le client "fabrique" une clé k , chiffre cette clé k avec la clé publique CléPubliqueServeur et envoie la version k' chiffrée de la clé k au serveur

3. Le serveur reçoit la version chiffrée k' de la clé k et la déchiffre en utilisant sa clé privée (CléPrivéServeur).

4. À partir de ce moment-là, le client et le serveur sont tous les deux en possession de la clé k. Le client et le serveur peuvent échanger des données en les chiffrant et en les déchiffrant à l'aide de la clé K (chiffrement symétrique).

Principe du protocole TLS



À partir de ce moment-là, le client et le serveur sont en possession de la clé K le client et le serveur commencent à échanger des données en les chiffrant et en les déchiffrant à l'aide de la clé K (chiffrement symétrique).