Sécurisation des communications

1. Objectifs
   - authentification
   - intégrité
   - confidentialité
2. Chiffrement symétrique
   - une clé partagée
   - rapide
   - difficulté : échanger la clé
   - exemple : César
3. Chiffrement asymétrique
   - clé publique : chiffrer
   - clé privée : déchiffrer
   - plus lent
   - résout l'échange de clés
4. Signature électronique
   - hachage du message
   - chiffré avec la clé privée
   - intégrité et authentification
5. Certificat
   - signé par une autorité de certification
   - lie une clé publique à une identité
6. TLS (HTTPS)
   - protocole hybride
   - symétrique : les données
   - asymétrique : échange de la clé