Sécurisation des communications

Table des matières

---

1. Introduction

La sécurité des communications numériques est essentielle pour protéger les échanges sur internet. Elle repose sur plusieurs objectifs :

- **Confidentialité** : seuls les destinataires autorisés peuvent lire le message.
- **Authenticité** : le message vient bien de la personne annoncée.
- **Intégrité** : le contenu du message n’a pas été modifié.

---

2. Chiffrement symétrique

Principe

Une **même clé secrète** est utilisée à la fois pour chiffrer et déchiffrer le message. Cette clé doit être connue à l’avance par les deux parties.

Exemple : Chiffrement de César

Chaque lettre est décalée d'un certain nombre de positions dans l'alphabet.
Ex. : avec un décalage de +3 → `ABCD` devient `DEFG`

- Avantage : rapide et simple
- Inconvénient : la clé doit être échangée **de manière sécurisée, très simple à casser** avec les moyens actuels

---

3. Chiffrement asymétrique

Principe

Chaque utilisateur possède **deux clés** :

- Une **clé publique** (diffusée librement),
- Une **clé privée** (gardée secrète).

Ce système repose sur le fait qu'un message chiffré avec la clé publique ne peut être déchiffré qu'avec la clé privée correspondante.

Exemple d'échange : Alice → Bob

1. Bob génère une paire de clés (publique / privée).
2. Il envoie sa **clé publique** à Alice.
3. Alice chiffre le message avec la **clé publique de Bob**.
4. Bob déchiffre le message avec sa **clé privée**.

=> Ainsi, **seul Bob** peut lire le message, même si quelqu'un intercepte le message chiffré.

---

4. Hachage et intégrité

Fonction de hachage

Une **fonction de hachage** est un algorithme qui transforme un message de taille quelconque en une **empreinte numérique unique** de taille fixe appelée **haché** ou **digest**.

Exemples de fonctions : SHA-256, SHA-1, MD5 (obsolète)

Propriétés importantes :

- Deux messages différents doivent produire des empreintes différentes (propriété de collision).
- Il est **impossible de retrouver** le message original à partir de son haché.
- Une **petite modification** du message entraîne un haché **totalement différent**.

Intégrité

Le haché permet de vérifier que le message n'a **pas été modifié** :

- L'expéditeur calcule le haché du message et l'envoie avec celui-ci.
- Le destinataire recalcule le haché à partir du message reçu.
- S'ils sont identiques : le message est intact.

---

5. Signature numérique

Principe

Une **signature numérique** permet de :

- **vérifier l'identité de l'expéditeur** (authenticité),
- **garantir l'intégrité** du message.

Étapes du processus

1. **Hachage** du message (ex : SHA-256).
2. L'expéditeur **chiffre le haché** avec **sa propre clé privée** : c'est la signature.
3. Il envoie **le message en clair + la signature**.
4. Le destinataire :
    - **Recalcule le haché** du message reçu.
    - **Déchiffre la signature** avec la **clé publique de l'expéditeur**.
    - Compare les deux hachés :
        - S'ils sont identiques → message authentique et non modifié.
        - Sinon → message modifié ou signature fausse.

=> La signature permet donc de **certifier l'émetteur** et de **garantir que le message n'a pas été altéré**.

---

6. Certificats numériques

Un **certificat numérique** associe une identité à une clé publique. Il est délivré et signé par une **autorité de certification (CA)**.

Il contient :

- Le nom du propriétaire (ex : un site web),
- Sa clé publique,
- La signature de l'autorité.

=> Utilisé pour prouver qu'une **clé publique appartient bien à un serveur légitime**

---

7. Protocoles sécurisés : HTTPS et TLS

- **HTTP** : pas de sécurité (données en clair).
- **HTTPS** = HTTP + **TLS** (Transport Layer Security)

TLS assure :

- La **confidentialité** : les messages sont chiffrés.
- L'**authentification** : via les certificats numériques.
- L'**intégrité** : grâce au hachage et à la signature.

=> Utilisé dans tous les sites web sérieux (banques, messagerie, achats…).

Si vous désirez une explication en vidéo, consultez :

https://youtu.be/7W7WPMX7arI?si=ERZxK1VZK0VbucVM