COURS

Sécurisation des communications

Tle

Programme de terminale générale, enseignement de spécialité — BO spécial n°8 du 25 juillet 2019

Relue le 14 novembre 2026

Quand tu te connectes à ta banque, tes données traversent Internet, où n'importe qui pourrait les intercepter. Le chiffrement rend ces messages illisibles pour un intrus. Le cadenas du navigateur repose sur une combinaison astucieuse de deux types de chiffrement.

1 Chiffrement symétrique

DÉFINITION

La **même clé** sert à chiffrer et à déchiffrer (César, XOR, AES). Rapide, mais il faut partager la clé secrètement.

RÈGLE

Exemple : chiffrement par XOR avec une clé ; appliquer deux fois la même clé redonne le message.

2 Chiffrement asymétrique

DÉFINITION

Chaque personne possède une **clé publique**, diffusée, et une **clé privée**, gardée secrète. Un message chiffré avec la clé publique ne se déchiffre qu'avec la clé privée (RSA).

RÈGLE

Il est plus lent, mais résout le problème du partage de clé. Il permet aussi la **signature** : chiffrer avec sa clé privée prouve l'identité de l'émetteur.

3 HTTPS

RÈGLE

HTTPS = HTTP + TLS. Le serveur présente un **certificat** signé par une autorité de certification, qui garantit son identité. Le chiffrement asymétrique sert à échanger une **clé de session** ; les échanges sont ensuite chiffrés en **symétrique**, plus rapide.

EXEMPLE

Alice veut envoyer un message secret à Bob avec RSA. Quelle clé utilise-t-elle ?

1. Bob a publié sa clé publique.
2. Alice chiffre avec la clé publique de Bob.
3. Seul Bob, avec sa clé privée, peut déchiffrer.

On chiffre avec la clé publique du destinataire ; lui seul déchiffre avec sa clé privée.

LE PIÈGE QUI COÛTE LE PLUS DE POINTS

Croire que la clé publique permet de déchiffrer. — La clé publique chiffre ; seule la clé privée correspondante déchiffre.

Le réflexe : Retenir : publique pour fermer, privée pour ouvrir.

ANALYSER UN PROTOCOLE SÉCURISÉ

1. Identifier les clés et qui les détient.
2. Repérer le type de chiffrement à chaque étape.
3. Vérifier comment l'identité est garantie (certificat, signature).
4. Expliquer pourquoi l'intrus ne peut pas lire.

À VÉRIFIER

- Ai-je défini le vocabulaire ?
- Mon code est-il testé sur un exemple ?
- Ai-je traité les cas limites ?
- Ai-je justifié la complexité ou le résultat ?

À RETENIR

- **Symétrique** : même clé, rapide (AES) ; problème du partage de clé.
- **Asymétrique** : clé publique / clé privée (RSA) ; signature.
- **HTTPS** (TLS) : certificat, clé de session échangée en asymétrique, échanges en symétrique.