Sécuriser les communications

Astrolab Cours · astrolabcours.fr

L'image. Un cadenas ouvert envoyé par la poste : tout le monde peut le fermer, seul son propriétaire peut l'ouvrir.

01 L'essentiel

Chiffrement	Clés	Exemples	Atout
symétrique	une clé partagée	César, XOR, AES	rapide
asymétrique	publique + privée	RSA	pas de secret à échanger

> HTTPS : certificat avec la clé publique du serveur, échange d'une clé symétrique chiffrée en asymétrique, puis tout en AES.

Les pièges

- On chiffre avec la clé publique du destinataire.
- Le certificat protège de l'homme du milieu.

© Astrolab Cours · astrolabcours.fr/nsi/terminale/securiser-les-communications/ · Tous droits réservés : usage personnel uniquement, republication et usage commercial interdits