La Cryptographie : le chiffrement asymétrique

[sommaire]

1. ## Objectifs

- Connaitre la Cryptographie le chiffrement asymétrique

- ## Le chiffrement asymétrique ou à "clé publique"

  - Le chiffrement asymétrique suppose que le (futur) destinataire est muni d'une paire de clés (clé privée, clé publique) et qu'il a fait en sorte que les émetteurs potentiels aient accès à sa clé publique.
  - Dans ce cas, l'émetteur utilise la clé publique du destinataire pour chiffrer le message tandis que le destinataire utilise sa clé privée pour le déchiffrer.

- ## Avantages et inconvénients du chiffrement asymétrique

  - L'**avantage du chiffrement asymétrique** est qu'il ne force pas l'utilisateur à communiquer des clés (secrètes) comme le fait le chiffrement symétrique, ce qui élimine la nécessité de distribuer des clés. Le chiffrement asymétrique prend en charge la signature numérique qui authentifie l'identité du destinataire. De même, il garantit que le message n'est pas altéré pendant son transit.
  - L'**inconvénient du chiffrement asymétrique** est qu'il prend beaucoup de temps et qu'il nécessite beaucoup plus d'efforts. En outre, vous ne pouvez envoyer des emails chiffrés que si l'autre personne a créé des paires de clés.
  - Pour ainsi dire, que l'autre personne doit être bien informée. Enfin, si vous perdez votre clé privée, vous la perdrez à jamais. La clé privée est irrécupérable.

Sommaire du cours Administration et sécurité des sites web

Source : https://apcpedagogie.com/la-cryptographie-le-chiffrement-asymetrique · téléchargé le 04/11/2026 · © APC Pédagogie · apcpedagogie.com