

Introduction à PGP





PGP

- « *Pretty Good Privacy* »
- Développé en 1991 par Paul Zimmerman
- Fournit toutes les caractéristiques d'un chiffrement asymétrique (échange de clés, chiffrement, signatures digitales)
- Notion de « clé PGP » : nom, but(s), algorithme de chiffrement...etc





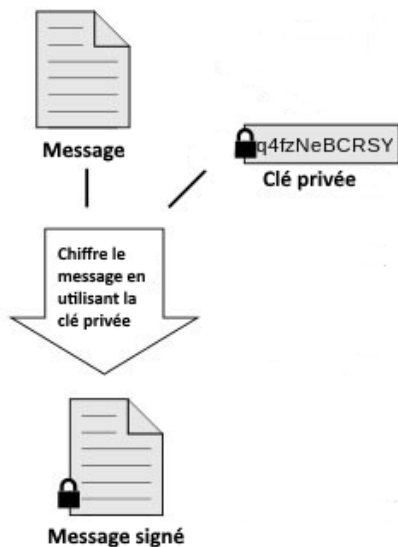
Fonctionnement de **PGP**

- ◉ Stockage de **plusieurs clés** :
- ◉ Sa propre clé privée (sécurisée par un mot de passe), et publique (clair)
- ◉ Stockage **des certificats** (copie des clés publiques signées par soi-même)
- ◉ Envoi d'un message signé : PGP chiffre un hash du message
- ◉ Envoi d'un message chiffré : utilisation de la clé publique du destinataire



Fonctionnement de PGP

Signature



Vérification

