# OpenPGP

# Réseau de confiance

Lundi 12 février — Prism

# OpenPGP et réseau de confiance

- Qu’est-ce que c’est ?
- À quoi ça sert ?
- Comment bien l’utiliser ?
- Pourquoi et comment signer les clefs d’autrui ?
- Qu’est-ce que le réseau de confiance et le « strong set » ?

# Clef OpenPGP

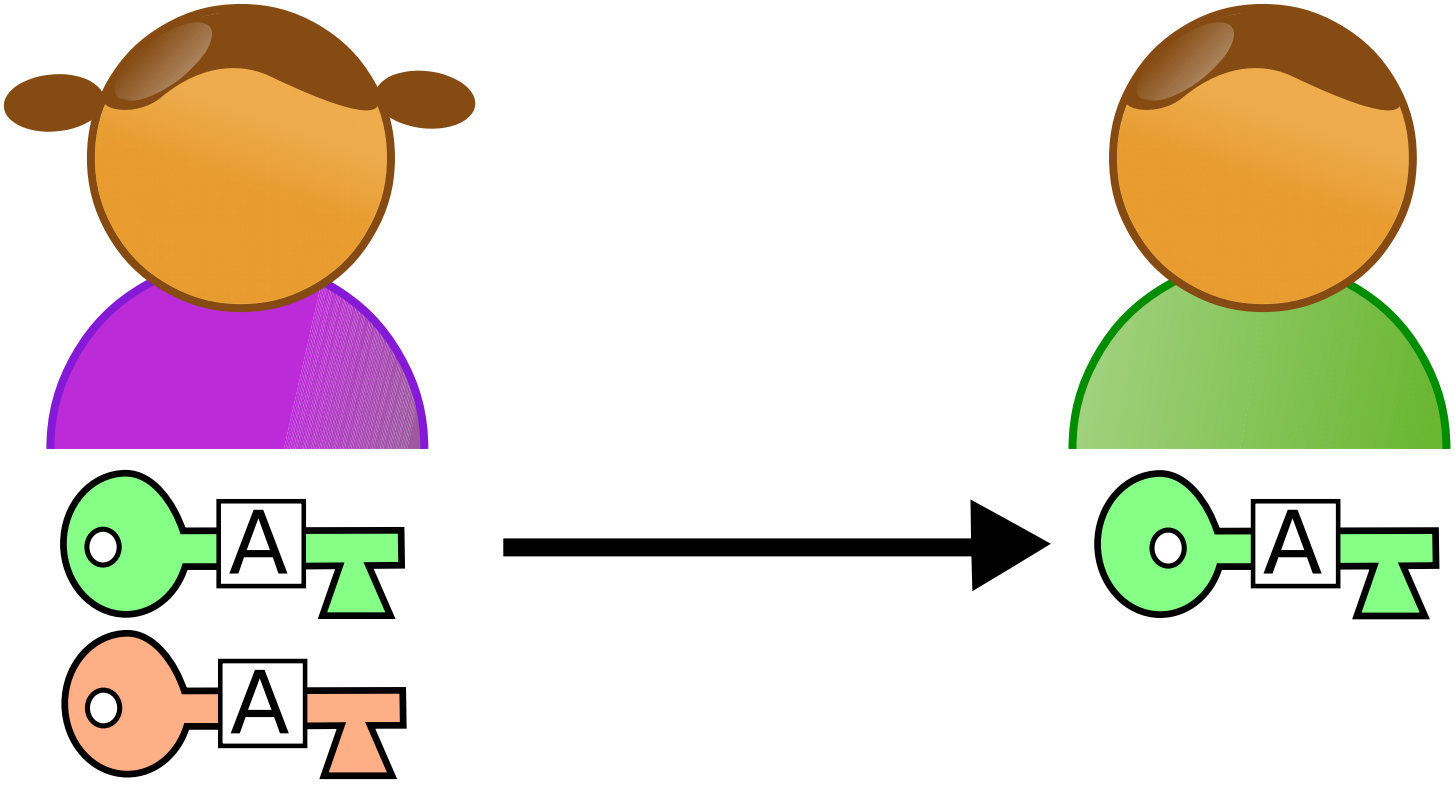
- Cryptographie asymétrique
  (une clef publique et une clef privée)
- Une clef primaire et des sous-clefs
  (des sous-clefs pour signer ou chiffrer)
- Des serveurs de clefs
- Des normes (RFC 4880 et RFC 5881)
- Des logiciels pour gérer les clefs

# Principe de fonctionnement


If you want to be extra safe, check that there's a big block of jumbled characters at the bottom.

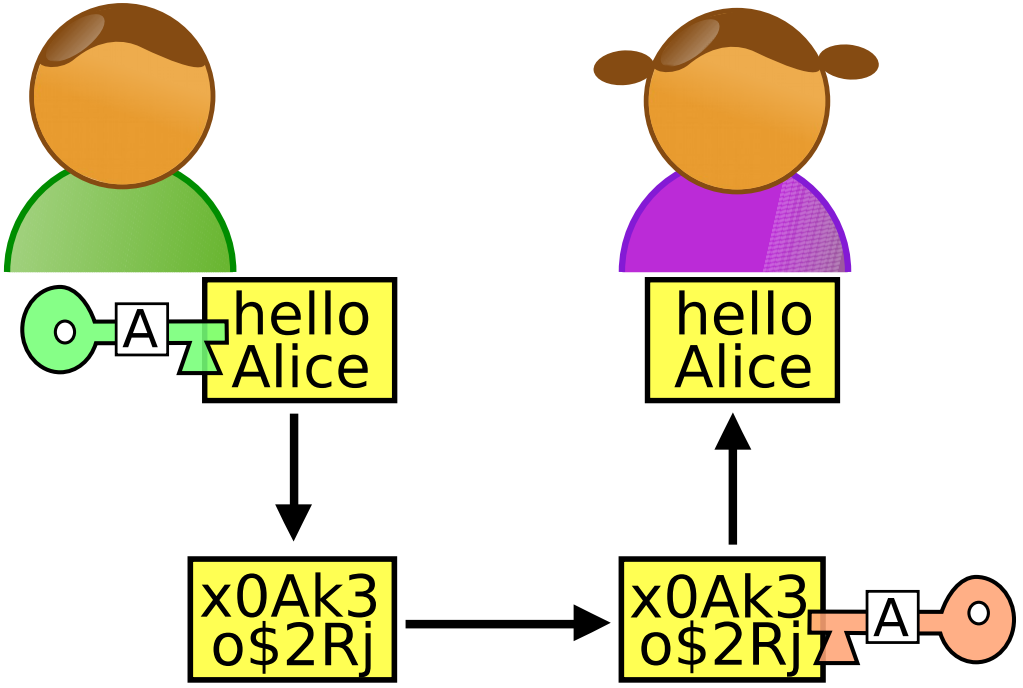
https://xkcd.com/1181/

# Chiffrement




https://fr.wikipedia.org/wiki/Cryptographie_asymétrique

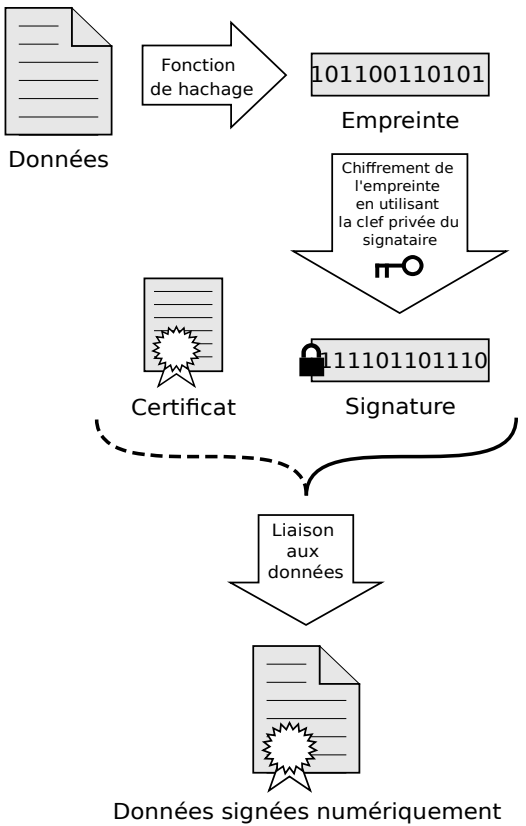
# Chiffrement



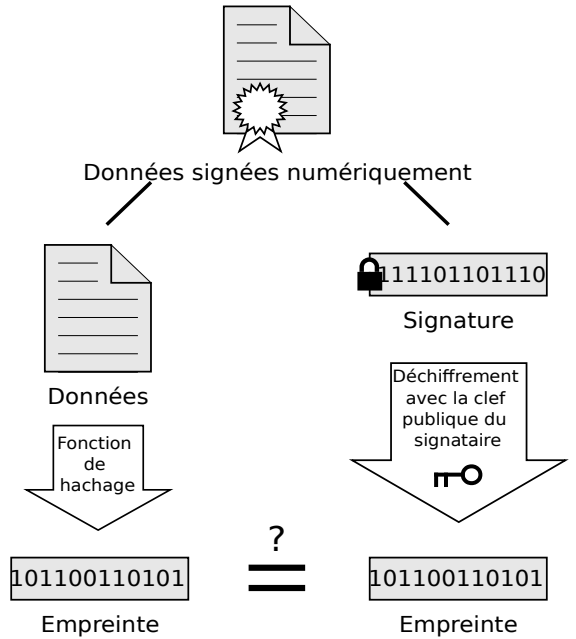

https://fr.wikipedia.org/wiki/Cryptographie_asymétrique

# Signature

## Signature




## Vérification




Si les empreintes sont identiques, la signature est valide

https://fr.wikipedia.org/wiki/Signature_numérique

# Créer une clef

- Utiliser un logiciel libre à jour
- Utiliser un algorithme RSA
- Utiliser une taille de clef de 4096 bits
- Utiliser un hachage SHA-512

https://riseup.net/fr/security/message-security/openpgp/gpg-keys

# Créer une clef

- Pas de commentaire pour les identités
- Déclarer une date d’expiration pour les clefs
- Envoyer sa clef publique sur les serveurs

https://riseup.net/fr/security/message-security/openpgp/gpg-keys

# Bonnes pratiques

- Utiliser des sous-clefs
- Conserver en lieu sûr la clef privée primaire
- Préparer un certificat de révocation
- Utiliser les empreintes complètes
- Mettre à jour son trousseau

https://riseup.net/fr/security/message-security/openpgp/best-practices

# Signer des clefs

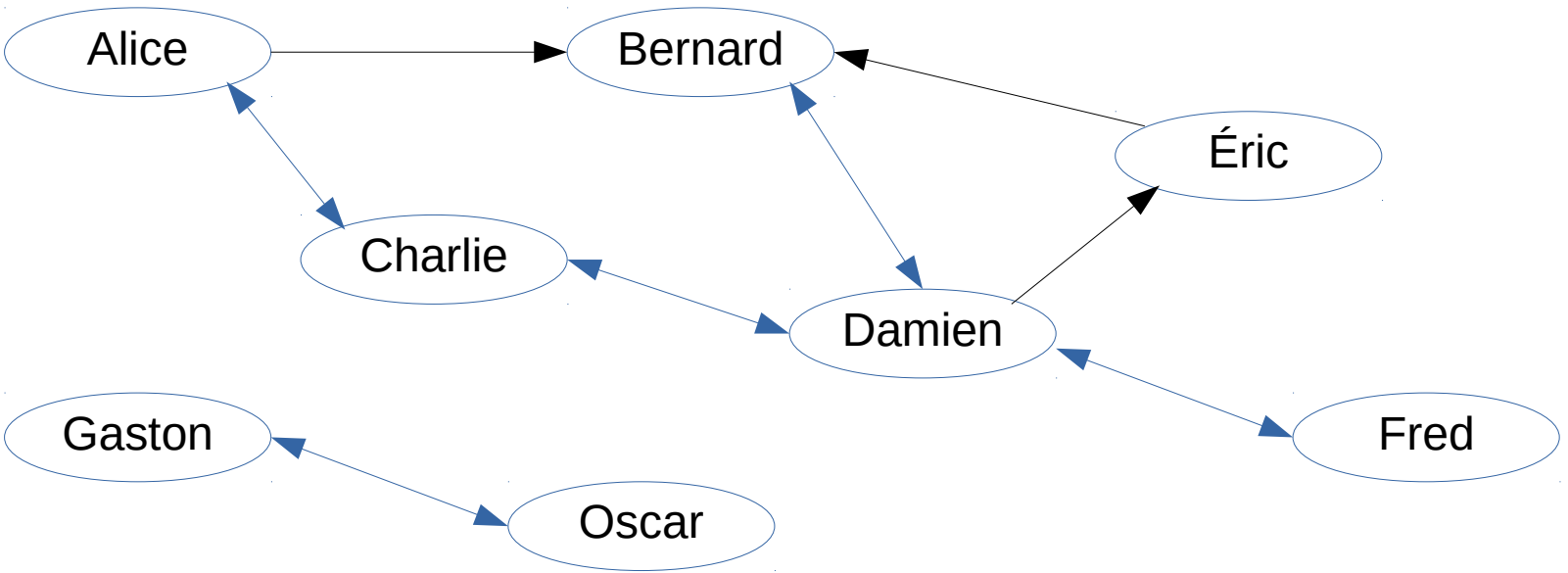
- Exiger l’empreinte complète en personne
- S’assurer de l’identité du porteur
- Envoyer directement la signature chiffrée

```
pub  rsa4096/FDFE09F2  1290555542
      Key fingerprint = AE14 AD01 426D 2BFB 82EF  7E1E B82A 217A FDFE 09F2
uid                                 David Prévot <david@tilapin.org>
uid                                 David Prévot <taffit@debian.org>
uid                                 David Prévot <davidp@altern.org>
uid                                 David Prévot <davidp@no-log.org>
```

https://wiki.debian.org/Keysigning

# Réseau de confiance

- Modèle décentralisé



# « Strong set »

- Plus grand ensemble de clefs tel que, quelque soit le couple de clefs de l’ensemble, il existe un chemin pour aller d’une clef à l’autre

- La plus courte distance moyenne (MSD) caractérise la distance moyenne vers une clef donnée

https://pgp.cs.uu.nl/plot/

# Utilisations

- Échange de courriers
- Git (commit et tag)
- Données ou logiciels
- Paquets de distribution
- Envoi de paquets et autres commandes

# Sources

- https://xkcd.com/1181/
- https://fr.wikipedia.org/wiki/Cryptographie_asymétrique
- https://fr.wikipedia.org/wiki/Signature_numérique
- https://riseup.net/fr/security/message-security/openpgp/gpg-keys
- https://riseup.net/fr/security/message-security/openpgp/best-practices
- https://evil32.com/
- https://wiki.debian.org/Keysigning
- https://pgp.cs.uu.nl/plot/
- https://gnupg.org/
- https://gaffer.ptitcanardnoir.org/intrigeri/code/parcimonie/