



# Séminaire GPG

Théo « bleizi » LE MOIGNE encadré par ds-ac

31 janvier 2022



Séminaire GPG

Introduction à la  
cryptographie

GPG

Conclusion

## Introduction à la cryptographie

Chiffrement symétrique

Chiffrement asymétrique (RSA)

Utilité

## GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de documents

Mail (Thunderbird et Evolution)

## Conclusion

Pour aller plus loin

Références



# Introduction à la cryptographie

## Chiffrement symétrique

Séminaire GPG

Introduction à la cryptographie

Chiffrement symétrique

Chiffrement asymétrique (RSA)

Utilité

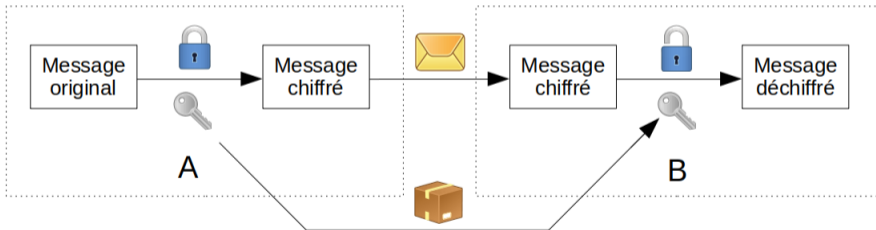
GPG

Conclusion

### ► Une clé

► Chiffrer et déchiffrer

► Partagée entre l'expéditeur et le destinataire





# Introduction à la cryptographie

## Chiffrement asymétrique (RSA)

Séminaire GPG

Introduction à la  
cryptographie

Chiffrement symétrique

**Chiffrement asymétrique  
(RSA)**

Utilité

GPG

Conclusion

▶ Un couple de clés par personne



# Introduction à la cryptographie

## Chiffrement asymétrique (RSA)

Séminaire GPG

Introduction à la cryptographie

Chiffrement symétrique

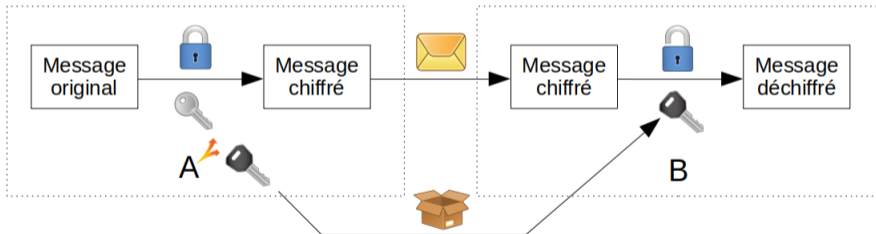
Chiffrement asymétrique (RSA)

Utilité

GPG

Conclusion

- ▶ Un couple de clés par personne
  - ▶ Une clé publique (connue de tous)
  - ▶ Une clé privée (connue de seulement le propriétaire)





# Introduction à la cryptographie

Utilité

Séminaire GPG

Introduction à la  
cryptographie

Chiffrement symétrique

Chiffrement asymétrique  
(RSA)

**Utilité**

GPG

Conclusion

▶ Chiffrer



# Introduction à la cryptographie

Utilité

Séminaire GPG

Introduction à la  
cryptographie

Chiffrement symétrique

Chiffrement asymétrique  
(RSA)

Utilité

GPG

Conclusion

- ▶ Chiffrer
  - ▶ Chiffrer avec la clé publique



# Introduction à la cryptographie

## Utilité

### Séminaire GPG

#### Introduction à la cryptographie

Chiffrement symétrique

Chiffrement asymétrique (RSA)

Utilité

GPG

Conclusion

### ▶ Chiffrer

- ▶ Chiffrer avec la clé publique
- ▶ Transmettre des données secrètes
- ▶ Protéger un disque





# Introduction à la cryptographie

## Utilité

### Séminaire GPG

#### Introduction à la cryptographie

Chiffrement symétrique

Chiffrement asymétrique  
(RSA)

Utilité

#### GPG

#### Conclusion

- ▶ Chiffrer
  - ▶ Chiffrer avec la clé publique
  - ▶ Transmettre des données secrètes
  - ▶ Protéger un disque
- ▶ Signer



# Introduction à la cryptographie

## Utilité

### Séminaire GPG

#### Introduction à la cryptographie

Chiffrement symétrique

Chiffrement asymétrique  
(RSA)

Utilité

GPG

Conclusion

- ▶ Chiffrer
  - ▶ Chiffrer avec la clé publique
  - ▶ Transmettre des données secrètes
  - ▶ Protéger un disque
- ▶ Signer
  - ▶ Chiffrer avec la clé privée



# Introduction à la cryptographie

## Utilité

### Séminaire GPG

#### Introduction à la cryptographie

Chiffrement symétrique

Chiffrement asymétrique  
(RSA)

Utilité

GPG

Conclusion

### ▶ Chiffrer

- ▶ Chiffrer avec la clé publique
- ▶ Transmettre des données secrètes
- ▶ Protéger un disque

### ▶ Signer

- ▶ Chiffrer avec la clé privée
- ▶ Authentifier l'expéditeur



# GPG

## Présentation

Séminaire GPG

▶ GNU Privacy Guard

Introduction à la  
cryptographie

GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion



# GPG

## Présentation

Séminaire GPG

- ▶ GNU Privacy Guard
- ▶ Clone de PGP (Pretty Good Privacy)
- ▶ Libre et gratuit

Introduction à la  
cryptographie

GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion



# GPG

## Présentation

### Séminaire GPG

Introduction à la  
cryptographie

### GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ GNU Privacy Guard
- ▶ Clone de PGP (Pretty Good Privacy)
- ▶ Libre et gratuit
- ▶ Chiffrement asymétrique (RSA ou ElGamal)



# GPG

## Présentation

### Séminaire GPG

Introduction à la  
cryptographie

### GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ GNU Privacy Guard
- ▶ Clone de PGP (Pretty Good Privacy)
- ▶ Libre et gratuit
- ▶ Chiffrement asymétrique (RSA ou ElGamal)
- ▶ Une clé :
  - ▶ Clé cryptographique publique



# GPG

## Présentation

### Séminaire GPG

Introduction à la  
cryptographie

### GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ GNU Privacy Guard
- ▶ Clone de PGP (Pretty Good Privacy)
- ▶ Libre et gratuit
- ▶ Chiffrement asymétrique (RSA ou ElGamal)
- ▶ Une clé :
  - ▶ Clé cryptographique publique
  - ▶ Date de fin de validité





# GPG

## Présentation

### Séminaire GPG

Introduction à la  
cryptographie

### GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ GNU Privacy Guard
- ▶ Clone de PGP (Pretty Good Privacy)
- ▶ Libre et gratuit
- ▶ Chiffrement asymétrique (RSA ou ElGamal)
- ▶ Une clé :
  - ▶ Clé cryptographique publique
  - ▶ Date de fin de validité
  - ▶ Identités (nom, mail, commentaire)



# GPG

## Présentation

### Séminaire GPG

Introduction à la  
cryptographie

### GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ GNU Privacy Guard
- ▶ Clone de PGP (Pretty Good Privacy)
- ▶ Libre et gratuit
- ▶ Chiffrement asymétrique (RSA ou ElGamal)
- ▶ Une clé :
  - ▶ Clé cryptographique publique
  - ▶ Date de fin de validité
  - ▶ Identités (nom, mail, commentaire)
  - ▶ Sous-clés (chiffrement, signature ...)



# GPG

## Présentation

### Séminaire GPG

Introduction à la  
cryptographie

### GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ GNU Privacy Guard
- ▶ Clone de PGP (Pretty Good Privacy)
- ▶ Libre et gratuit
- ▶ Chiffrement asymétrique (RSA ou ElGamal)
- ▶ Une clé :
  - ▶ Clé cryptographique publique
  - ▶ Date de fin de validité
  - ▶ Identités (nom, mail, commentaire)
  - ▶ Sous-clés (chiffrement, signature ...)
  - ▶ Signatures



# GPG

## Présentation

### Séminaire GPG

Introduction à la  
cryptographie

### GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ GNU Privacy Guard
- ▶ Clone de PGP (Pretty Good Privacy)
- ▶ Libre et gratuit
- ▶ Chiffrement asymétrique (RSA ou ElGamal)
- ▶ Une clé :
  - ▶ Clé cryptographique publique
  - ▶ Date de fin de validité
  - ▶ Identités (nom, mail, commentaire)
  - ▶ Sous-clés (chiffrement, signature ...)
  - ▶ Signatures
  - ▶ Et pour votre clé : une clé privée



# GPG

## Création de clés

Séminaire GPG

Introduction à la  
cryptographie

GPG

Présentation

**Création de clés**

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

▶ Installation : `apt install gnupg`



# GPG

## Création de clés

### Séminaire GPG

Introduction à la  
cryptographie

GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Installation : `apt install gnupg`
- ▶ Création : `gpg --full-gen-key`
  - ▶ Type de clés : (1) RSA et RSA



# GPG

## Création de clés

### Séminaire GPG

Introduction à la  
cryptographie

GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Installation : `apt install gnupg`
- ▶ Création : `gpg --full-gen-key`
  - ▶ Type de clés : (1) RSA et RSA
  - ▶ Longueur : 4096



# GPG

## Création de clés

Séminaire GPG

Introduction à la  
cryptographie

GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Installation : `apt install gnupg`
- ▶ Création : `gpg --full-gen-key`
  - ▶ Type de clés : (1) RSA et RSA
  - ▶ Longueur : 4096
  - ▶ Durée : 0 (infinie) ou 1m (un mois)...





# GPG

## Création de clés

### Séminaire GPG

Introduction à la  
cryptographie

GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Installation : `apt install gnupg`
- ▶ Création : `gpg --full-gen-key`
  - ▶ Type de clés : (1) RSA et RSA
  - ▶ Longueur : 4096
  - ▶ Durée : 0 (infinie) ou 1m (un mois)...
  - ▶ Informations personnelles : Nom, mail, commentaire



# GPG

## Création de clés

Séminaire GPG

Introduction à la  
cryptographie

GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Installation : `apt install gnupg`
- ▶ Création : `gpg --full-gen-key`
  - ▶ Type de clés : (1) RSA et RSA
  - ▶ Longueur : 4096
  - ▶ Durée : 0 (infinie) ou 1m (un mois)...
  - ▶ Informations personnelles : Nom, mail, commentaire
  - ▶ Phrase clef → compliquée et secrète



# GPG

## Création de clés

### Séminaire GPG

Introduction à la  
cryptographie

### GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Installation : `apt install gnupg`
- ▶ Création : `gpg --full-gen-key`
  - ▶ Type de clés : (1) RSA et RSA
  - ▶ Longueur : 4096
  - ▶ Durée : 0 (infinie) ou 1m (un mois)...
  - ▶ Informations personnelles : Nom, mail, commentaire
  - ▶ Phrase clef → compliquée et secrète
- ▶ Visualisation : `gpg --list-keys` ou `gpg --fingerprint`



# GPG

## Partage de clés

Séminaire GPG

Introduction à la  
cryptographie

GPG

Présentation

Création de clés

**Partage de clés**

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

▶ Être sûr d'une clé → rencontre physique



# GPG

## Partage de clés

Séminaire GPG

Introduction à la  
cryptographie

GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Être sûr d'une clé → rencontre physique
- ▶ Trouver la clé :
  - ▶ Échange physique ou numérique (USB, mail, IRC ...)
  - ▶ En ligne (`gitlab.crans.org` ou site perso)



# GPG

## Partage de clés

### Séminaire GPG

Introduction à la  
cryptographie

### GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Être sûr d'une clé → rencontre physique
- ▶ Trouver la clé :
  - ▶ Échange physique ou numérique (USB, mail, IRC ...)
  - ▶ En ligne (`gitlab.crans.org` ou site perso)
  - ▶ Serveur de clés
    - ▶ `hkps://keyserver.ubuntu.com`
    - ▶ `hkps://pgp.mit.edu`



# GPG

## Partage de clés

### Séminaire GPG

Introduction à la  
cryptographie

### GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Être sûr d'une clé → rencontre physique
- ▶ Trouver la clé :
  - ▶ Échange physique ou numérique (USB, mail, IRC ...)
  - ▶ En ligne (`gitlab.crans.org` ou site perso)
  - ▶ Serveur de clés
    - ▶ `hkps://keyserver.ubuntu.com`
    - ▶ `hkps://pgp.mit.edu`
- ▶ Exporter : `gpg --export --armor [ID]`



# GPG

## Partage de clés

### Séminaire GPG

Introduction à la  
cryptographie

### GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Être sûr d'une clé → rencontre physique
- ▶ Trouver la clé :
  - ▶ Échange physique ou numérique (USB, mail, IRC ...)
  - ▶ En ligne ([gitlab.crans.org](https://gitlab.crans.org) ou site perso)
  - ▶ Serveur de clés
    - ▶ `hkps://keyserver.ubuntu.com`
    - ▶ `hkps://pgp.mit.edu`
- ▶ Exporter : `gpg --export --armor [ID]`
- ▶ Importer : `gpg --import [fichier]`





# GPG

## Partage de clés

### Séminaire GPG

Introduction à la  
cryptographie

### GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Être sûr d'une clé → rencontre physique
- ▶ Trouver la clé :
  - ▶ Échange physique ou numérique (USB, mail, IRC ...)
  - ▶ En ligne ([gitlab.crans.org](https://gitlab.crans.org) ou site perso)
  - ▶ Serveur de clés
    - ▶ `hkps://keyserver.ubuntu.com`
    - ▶ `hkps://pgp.mit.edu`
- ▶ Exporter : `gpg --export --armor [ID]`
- ▶ Importer : `gpg --import [fichier]`
- ▶ Éditer : `gpg --edit-key [info]`



# GPG

## Serveur de clé

Séminaire GPG

Introduction à la  
cryptographie

GPG

Présentation

Création de clés

Partage de clés

**Serveur de clé**

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Base de donnée : clé, nom, mail, signature
- ▶ Partage entre les différents serveurs



# GPG

## Serveur de clé

Séminaire GPG

Introduction à la  
cryptographie

GPG

Présentation

Création de clés

Partage de clés

**Serveur de clé**

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Base de donnée : clé, nom, mail, signature
- ▶ Partage entre les différents serveurs
  
- ▶ Exporter : `gpg [--keyserver [serveur]] --send-keys`



# GPG

## Serveur de clé

Séminaire GPG

Introduction à la  
cryptographie

GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Base de donnée : clé, nom, mail, signature
- ▶ Partage entre les différents serveurs
  
- ▶ Exporter : `gpg [--keyserver [serveur]] --send-keys`
- ▶ Chercher : `gpg --search-keys [info]`



# GPG

## Serveur de clé

Séminaire GPG

Introduction à la  
cryptographie

GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Base de donnée : clé, nom, mail, signature
- ▶ Partage entre les différents serveurs
  
- ▶ Exporter : `gpg [--keyserver [serveur]] --send-keys`
- ▶ Chercher : `gpg --search-keys [info]`
- ▶ Importer : `gpg --recv-keys [info]`



# GPG

## Serveur de clé

### Séminaire GPG

Introduction à la  
cryptographie

GPG

Présentation

Création de clés

Partage de clés

**Serveur de clé**

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Base de donnée : clé, nom, mail, signature
- ▶ Partage entre les différents serveurs
  
- ▶ Exporter : `gpg [--keyserver [serveur]] --send-keys`
- ▶ Chercher : `gpg --search-keys [info]`
- ▶ Importer : `gpg --recv-keys [info]`
- ▶ Mise à jour : `gpg --refresh-keys`



# GPG

## Serveur de clé

### Séminaire GPG

Introduction à la  
cryptographie

GPG

Présentation

Création de clés

Partage de clés

**Serveur de clé**

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Base de donnée : clé, nom, mail, signature
- ▶ Partage entre les différents serveurs
  
- ▶ Exporter : `gpg [--keyserver [serveur]] --send-keys`
- ▶ Chercher : `gpg --search-keys [info]`
- ▶ Importer : `gpg --recv-keys [info]`
- ▶ Mise à jour : `gpg --refresh-keys`



# GPG

## Serveur de clé

### Séminaire GPG

Introduction à la  
cryptographie

### GPG

Présentation

Création de clés

Partage de clés

**Serveur de clé**

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

### ▶ Serveur par défaut :

- ▶ `keyserver hkps://keyserver.ubuntu.com`
- ▶ dans `~/.gnupg/gpg.conf`





# GPG

## Serveur de clé

### Séminaire GPG

Introduction à la  
cryptographie

### GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Serveur par défaut :
  - ▶ `keyserver hkps://keyserver.ubuntu.com`
  - ▶ dans `~/.gnupg/gpg.conf`
  
- ▶ Certificat de révocation :
  - ▶ Pour dire à un serveur que la clé est obsolète



# GPG

## Serveur de clé

### Séminaire GPG

Introduction à la  
cryptographie

### GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Serveur par défaut :
  - ▶ `keyserver hkps://keyserver.ubuntu.com`
  - ▶ dans `~/.gnupg/gpg.conf`
  
- ▶ Certificat de révocation :
  - ▶ Pour dire à un serveur que la clé est obsolète
  - ▶ Générer : `gpg --generate-revocation`
  - ▶ Exporter : `gpg --send-keys`



# GPG

## Serveur de clé

### Séminaire GPG

Introduction à la  
cryptographie

### GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Serveur par défaut :
  - ▶ `keyserver hkps://keyserver.ubuntu.com`
  - ▶ dans `~/.gnupg/gpg.conf`
- ▶ Certificat de révocation :
  - ▶ Pour dire à un serveur que la clé est obsolète
  - ▶ Générer : `gpg --generate-revocation`
  - ▶ Exporter : `gpg --send-keys`
- ▶ Signer une clé : `gpg --sign-key`
- ▶ Réseaux de confiance



# GPG

## Chiffrement et signature de documents

### Séminaire GPG

Introduction à la  
cryptographie

GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

**Chiffrement et signature de  
documents**

Mail (Thunderbird et  
Evolution)

Conclusion

▶ Signer : `gpg --sign [fichier]`



# GPG

## Chiffrement et signature de documents

### Séminaire GPG

Introduction à la  
cryptographie

GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Signer : `gpg --sign [fichier]`
- ▶ Signature séparée : `gpg --detach-sign [fichier] (ou -b)`



# GPG

## Chiffrement et signature de documents

### Séminaire GPG

Introduction à la  
cryptographie

GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Signer : `gpg --sign [fichier]`
- ▶ Signature séparée : `gpg --detach-sign [fichier] (ou -b)`
- ▶ Vérifier : `gpg --verify`



# GPG

## Chiffrement et signature de documents

### Séminaire GPG

Introduction à la  
cryptographie

GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Signer : `gpg --sign [fichier]`
- ▶ Signature séparée : `gpg --detach-sign [fichier] (ou -b)`
- ▶ Vérifier : `gpg --verify`
  
- ▶ Chiffrer : `gpg --encrypt [fichier]`



# GPG

## Chiffrement et signature de documents

### Séminaire GPG

Introduction à la  
cryptographie

GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

- ▶ Signer : `gpg --sign [fichier]`
- ▶ Signature séparée : `gpg --detach-sign [fichier]` (ou `-b`)
- ▶ Vérifier : `gpg --verify`
  
- ▶ Chiffrer : `gpg --encrypt [fichier]`
- ▶ Déchiffrer : `gpg --decrypt [fichier]`
- ▶ `-a` pour du ASCII, `-o` pour la destination, `-r` pour le destinataire





# GPG

## Mail (Thunderbird et Evolution)

### Séminaire GPG

Introduction à la  
cryptographie

### GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

## ▶ Thunderbird

- ▶ Chiffre et signe les mails
- ▶ Trousseau de clé géré par Thunderbird
- ▶ Adresse mail → chiffrement de bout en bout → ajouter une clé



# GPG

## Mail (Thunderbird et Evolution)

### Séminaire GPG

Introduction à la  
cryptographie

### GPG

Présentation

Création de clés

Partage de clés

Serveur de clé

Chiffrement et signature de  
documents

Mail (Thunderbird et  
Evolution)

Conclusion

## ▶ Thunderbird

- ▶ Chiffre et signe les mails
- ▶ Trousseau de clé géré par Thunderbird
- ▶ Adresse mail → chiffrement de bout en bout → ajouter une clé

## ▶ Evolution

- ▶ Chiffre et signe les mails
- ▶ Utilise le trousseau de clé de GPG
- ▶ Adresse mail → propriétés → sécurité → ID de la clé



# Conclusion

Pour aller plus loin

Séminaire GPG

Introduction à la  
cryptographie

GPG

Conclusion

Pour aller plus loin

Références

- ▶ Gestion des sous-clés
- ▶ Stockage de clés sur une carte / clé USB
- ▶ Différentes gestions du réseau de confiance



# Conclusion

Séminaire GPG

Introduction à la  
cryptographie

GPG

Conclusion

Pour aller plus loin

Références

Des questions ?



# Conclusion

## Références

Séminaire GPG

Introduction à la  
cryptographie

GPG

Conclusion

Pour aller plus loin

Références

- ▶ <https://doc.ubuntu-fr.org/gnupg>
- ▶ <https://fr.wikibooks.org/wiki/GPG>
- ▶ <http://www.francoz.net/doc/gpg/gpg.html>