

# H4ck 1n TN

## GnuPG

Gabrielle TOULET MORLANNE  
Olivier DAUTRICOURT  
Benoît TALLANDIER

Ceten – TELECOM Nancy

October 22, 2016



# Plan

## Introduction

- Chiffrement asymétrique

- Signature

- PGP, OpenPGP, GPG ??

## Pratique

- Création paire de clefs

- Enigmail

- OpenKeyChain (Android)

- K9-Mail (Android)



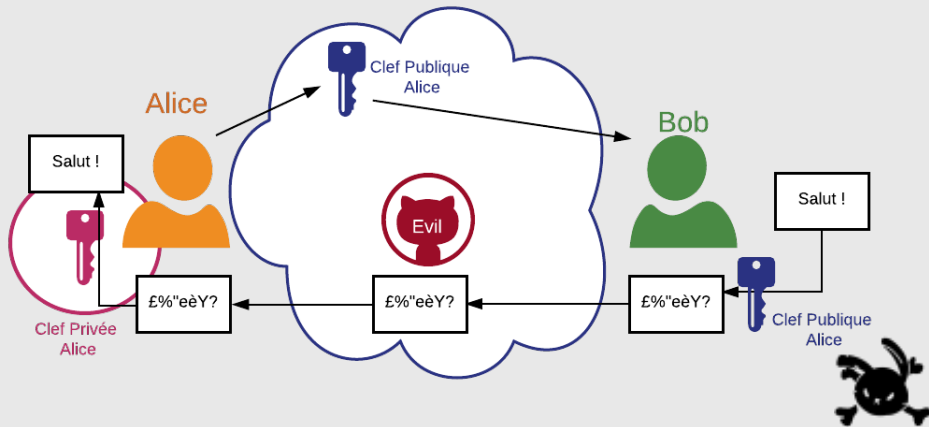
# Prérequis

- ▶ Paquets nécessaires : gnupg2, thunderbird, enigmail.
- ▶ Installation :  
**sudo apt-get install gnupg2 thunderbird enigmail** (debian, mint,  
| **yum** (Fedora) ubuntu, kali)  
| **pacman** (Arch)  
| etc.
- ▶ Attention, sous debian et kali, thunderbird s'appelle **icedove** !



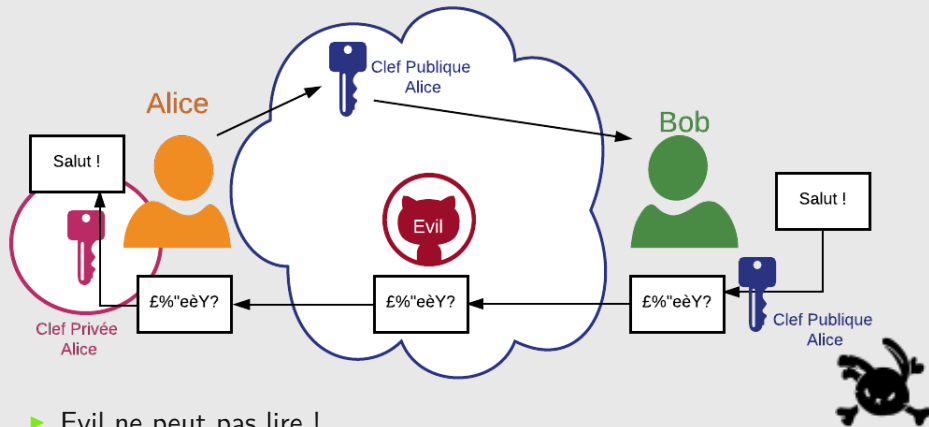
# Le chiffrement asymétrique

- ▶ 1 paire (Clef publique & clef privée)
- ▶ **Chiffrer** avec clef **publique** | **Déchiffrer** avec clef **privée**



# Le chiffrement asymétrique

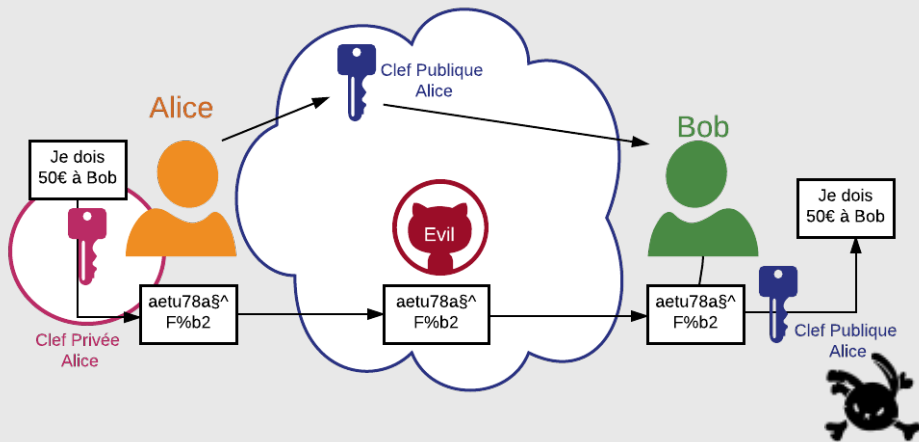
- ▶ 1 paire (Clef publique & clef privée)
- ▶ **Chiffrer** avec clef **publique** | **Déchiffrer** avec clef **privée**



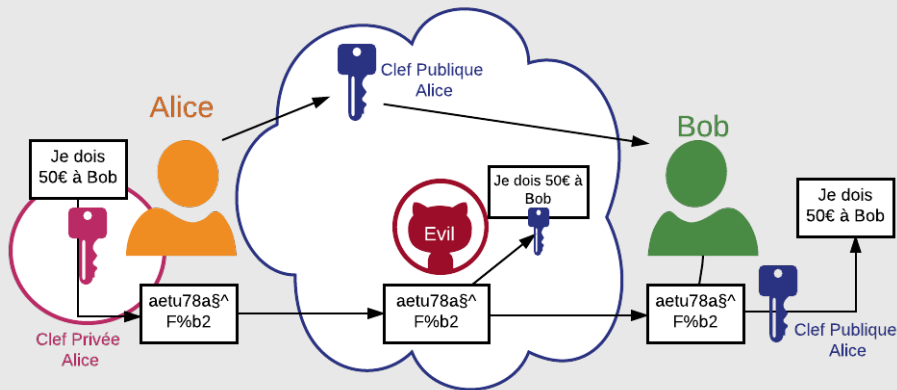
- ▶ Evil ne peut pas lire !

# La signature

## ► Signe avec clef **privée** | Vérifie clef **publique**



# La signature



- ▶ Tout le monde peut vérifier !
- ▶ Evil ne peut pas imiter la signature d'Alice !



# PGP, OpenPGP, GPG, ... ???

- ▶ PGP : Pretty Good Privacy
- ▶ OpenPGP : Equivalent libre de PGP  
Standard qui définit le format de clefs, de messages, etc.
- ▶ GPG (GnuPG) : Gnu Privacy Guard, implémentation logicielle
  
- ▶ et BGP ? : Border Gateway Protocol → Rien à voir





# Création paire de clefs

Outil GnuPG (**gpg2**)

(Interface graphique : seahorse)

**gpg2 - -gen-key**

- ▶ RSA
- ▶ 4096bits
- ▶ expiration
- ▶ infos persos
- ▶ passphrase



# Cheatsheet

Cheatsheet	
gpg2 - -list-keys	Liste toutes les clefs sur la machine
gpg2 - -keyserver <serveur> - -send-key <id>	Exporte une clef publique sur un serveur de clef
gpg2 - -keyserver <serveur> - -search-keys <id>	Cherche une clef publique sur le serveur
gpg2 - -keyserver <serveur> - -recv-keys <id>	Importe une clef publique depuis le serveur
gpg2 - -delete-keys <id>	Supprime une clef publique du trousseau
gpg2 - -gen-revoke <votre_email>	Révoque votre <b>propre clef publique</b>

Exemple de serveur : pgp.mit.edu :

```
gpg - -keyserver hkp://pgp.mit.edu
- -search-keys "Nom de quelqu'un"
```



# Enigmail

## Voir démo

- ▶ Suivre le Setup Wizard en mode avancé
- ▶ Choisir "j'ai déjà des clefs"
- ▶ Si les clefs ne sont pas repérés :
  - ▶ `cd ; cd .gnupg/`
  - ▶ `gpg2 - -export votre_mail > publickey.asc`
  - ▶ `gpg2 - -export-secret-key votre_mail > privatekey.asc`
  - ▶ Dans Thunderbird, choisir publickey.asc et privatekey.asc créés dans le dossier .gnupg
  - ▶ Une fois que le setup wizard est terminé : **rm privatekey.asc** (pour ne pas laisser trainer la clef dans le dossier...)
- ▶ Lors de l'écriture d'un mail, choisir "chiffrer" et/ou "signer" dans le menu Enigmail.

Aide : <http://enigmail.wiki/>

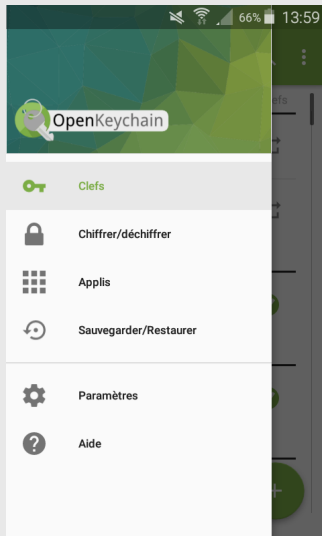


# OpenKeyChain (Android)

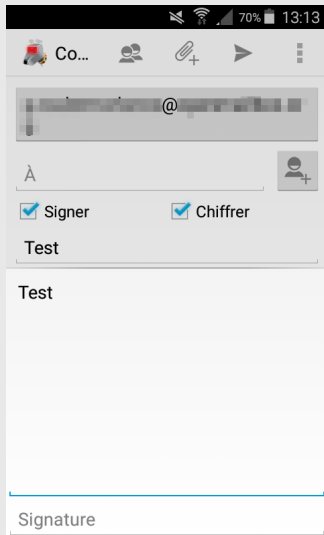
- ▶ Créer une paire de clefs personnelle
- ▶ Gérer les clefs publiques de vos amis
  - ▶ Ajout facile (QR code !, et depuis serveur)
- ▶ Chiffre/déchiffrer des documents
- ▶ Faire des sauvegardes/imports
- ▶ Compatible avec plein d'applis :  
K9-Mail, Conversations (chat), Password Store, etc. :-)



# OpenKeyChain



# K9-Mail



The screenshot shows the K9-Mail app's 'Compose' screen. At the top, the status bar displays signal strength, Wi-Fi, 70% battery, and the time 13:13. Below the status bar is a toolbar with icons for attachments, contacts, a plus sign, a send arrow, and a menu. The 'To' field contains a blurred email address ending in '@'. Below this is a 'From' field with the text 'À' and a contact selection icon. Two checkboxes, 'Signer' and 'Chiffrer', are both checked. The 'Subject' field contains the text 'Test'. The main body of the email is a large text area containing the word 'Test'. At the bottom, there is a signature line with the text 'Signature'.



# K9-Mail

