Se réapproprier sa vie privée
En sécurisant ses e-mails

Philippe Wambeke

LoliGrUB

18 juin 2016

1. Vie privée
   - Tous sous surveillance
   - Je ne suis pas concerné
2. Sécuriser ses e-mails
   - Un peu de théorie
   - Comment y parvenir
   - Le réseau de confiance
3. GnuPG
   - Présentation
   - Utilisation
4. Conclusion
   - Pour aller plus loin
   - Questions

Nous sommes tous sur écoute !

- Prism
- StellarWind
- XKeyScore
- Turmoil
- ...

Ou est le problème ?

Réactions courantes face au phénomène de la surveillance massive :

- *«Ils ne pourront rien faire des informations récoltées»*
- *«Je n'ai rien à cacher»*
- *«Je n'ai rien à me reprocher»*
- ...

Ou est le problème ?

Réactions courantes face au phénomène de la surveillance massive :

- *«Ils ne pourront rien faire des informations récoltées»*
- *«Je n'ai rien à cacher»*
- *«Je n'ai rien à me reprocher»*
- ...

Maintenant, on n'a plus le choix... Chiffrons !

Sécuriser ses e-mails

La sécurisation des échanges de mails passe obligatoirement par :

Sécuriser ses e-mails

La sécurisation des échanges de mails passe obligatoirement par :

- La confidentialité : seuls l'émetteur et le destinataire du message peuvent le lire

Sécuriser ses e-mails

La sécurisation des échanges de mails passe obligatoirement par :

- La confidentialité : seuls l'émetteur et le destinataire du message peuvent le lire
- L'intégrité : le message ne peut pas être altéré entre l'émission et la réception

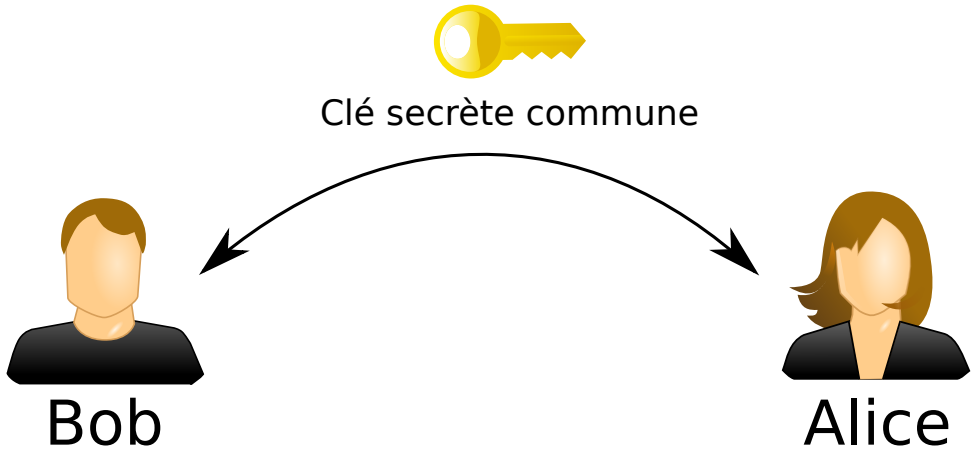
Sécuriser ses e-mails

La sécurisation des échanges de mails passe obligatoirement par :

- La confidentialité : seuls l'émetteur et le destinataire du message peuvent le lire
- L'intégrité : le message ne peut pas être altéré entre l'émission et la réception
- La non-répudiation : le destinataire est certain de l'identité de l'émetteur

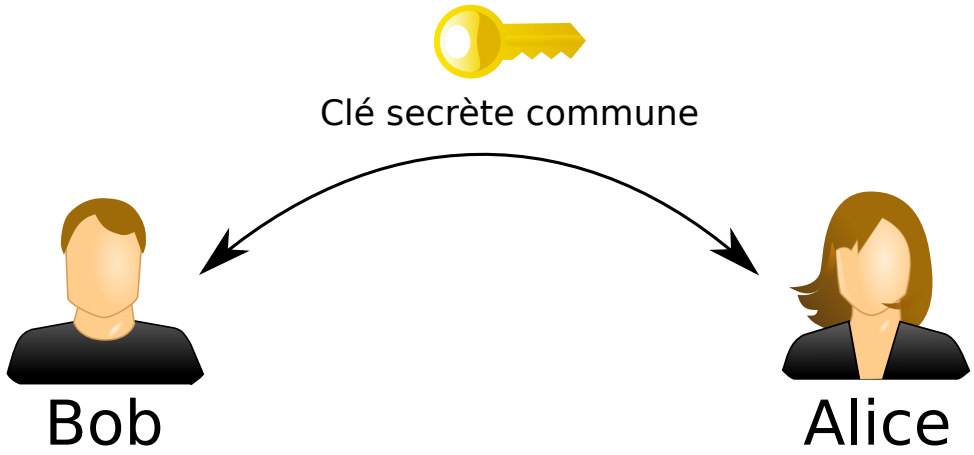
Le partage d'un secret commun

Les deux parties utilisent un secret commun pour s'échanger des messages.



Le partage d'un secret commun

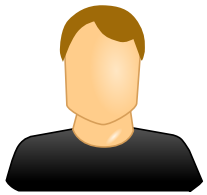
Les deux parties utilisent un secret commun pour s'échanger des messages.



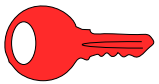
Simple, mais présente des inconvénients majeurs.

La cryptographie asymétrique

Etape 1 : la génération d'une paire de clés.



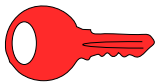
Bob



Clé privée

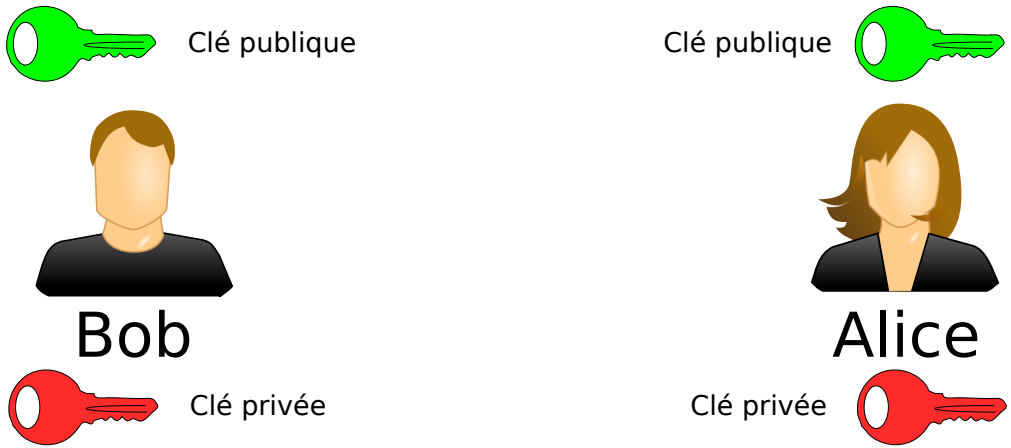
Alice

Clé privée



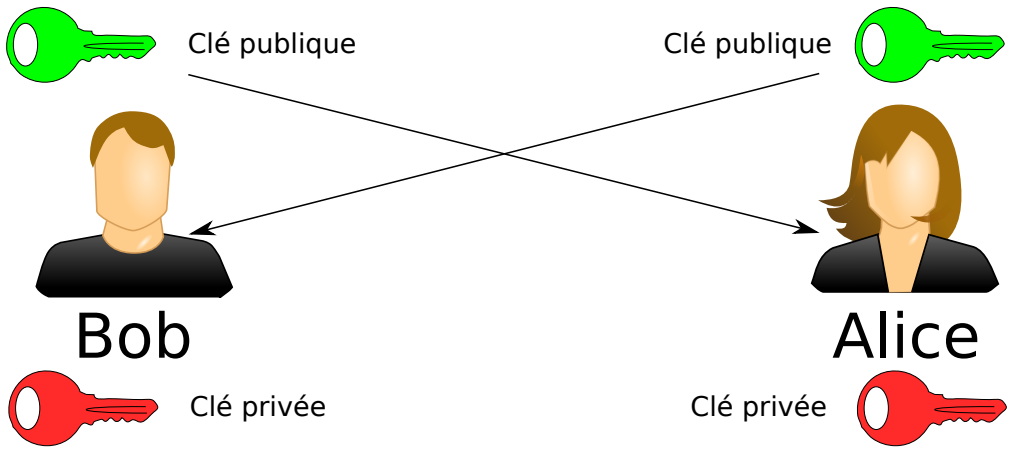
La cryptographie asymétrique

Etape 1 : la génération d'une paire de clés.



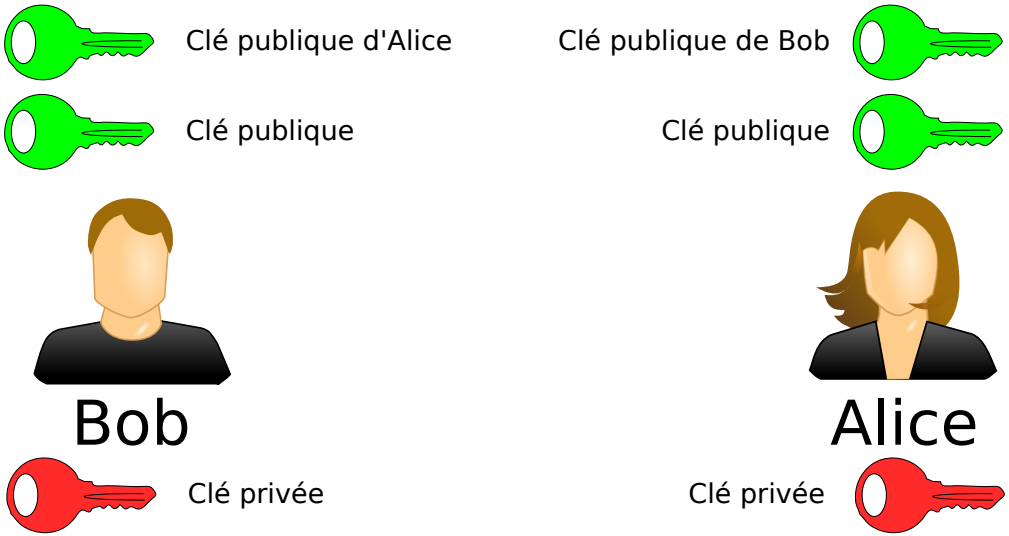
La cryptographie asymétrique

Etape 2 : l'échange des clés publiques.

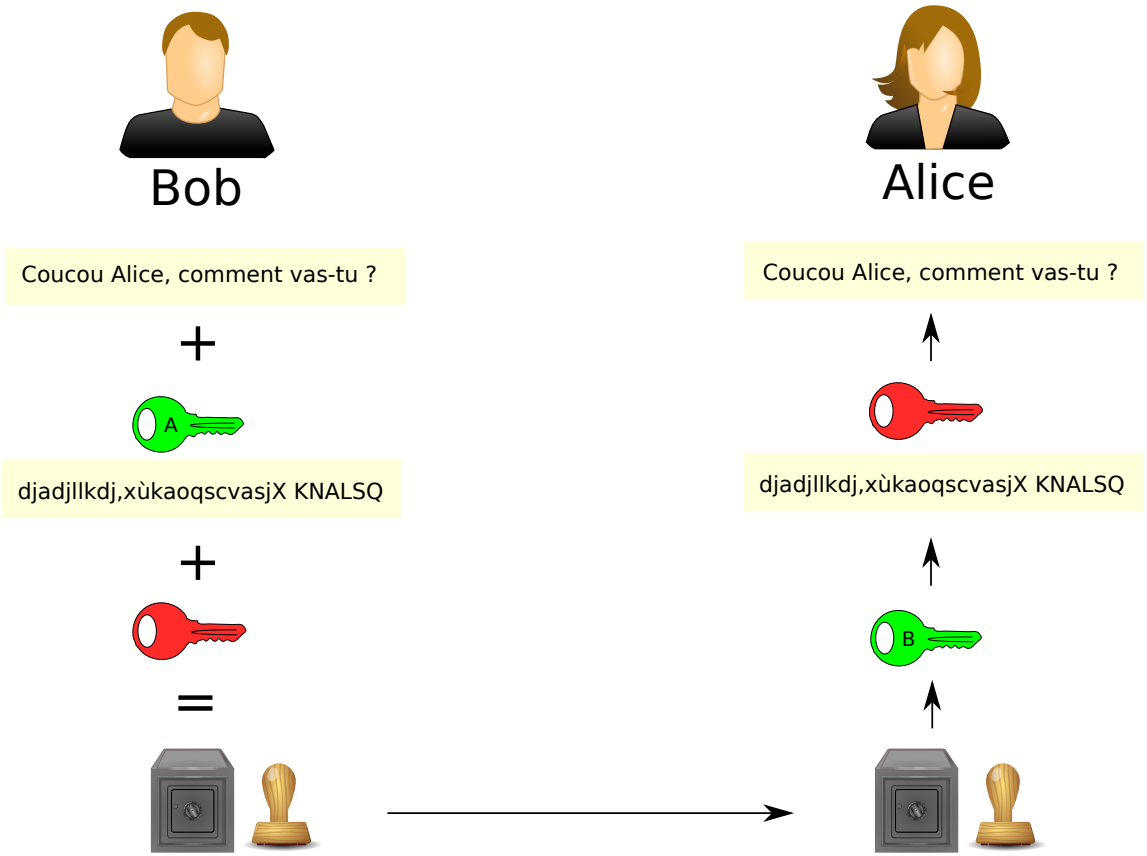


La cryptographie asymétrique

Etape 2 : l'échange des clés publiques.



Le flux complet

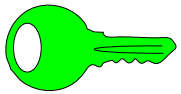


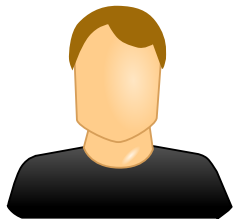
Il reste un problème...

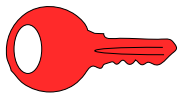
Que pourrait faire quelqu'un voulant écouter Bob et Alice ?

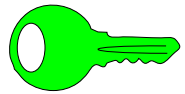
Il reste un problème...

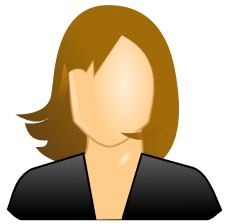
Que pourrait faire quelqu'un voulant écouter Bob et Alice ?

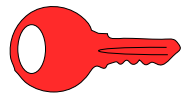

Clé publique

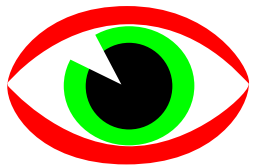

Bob




Clé publique

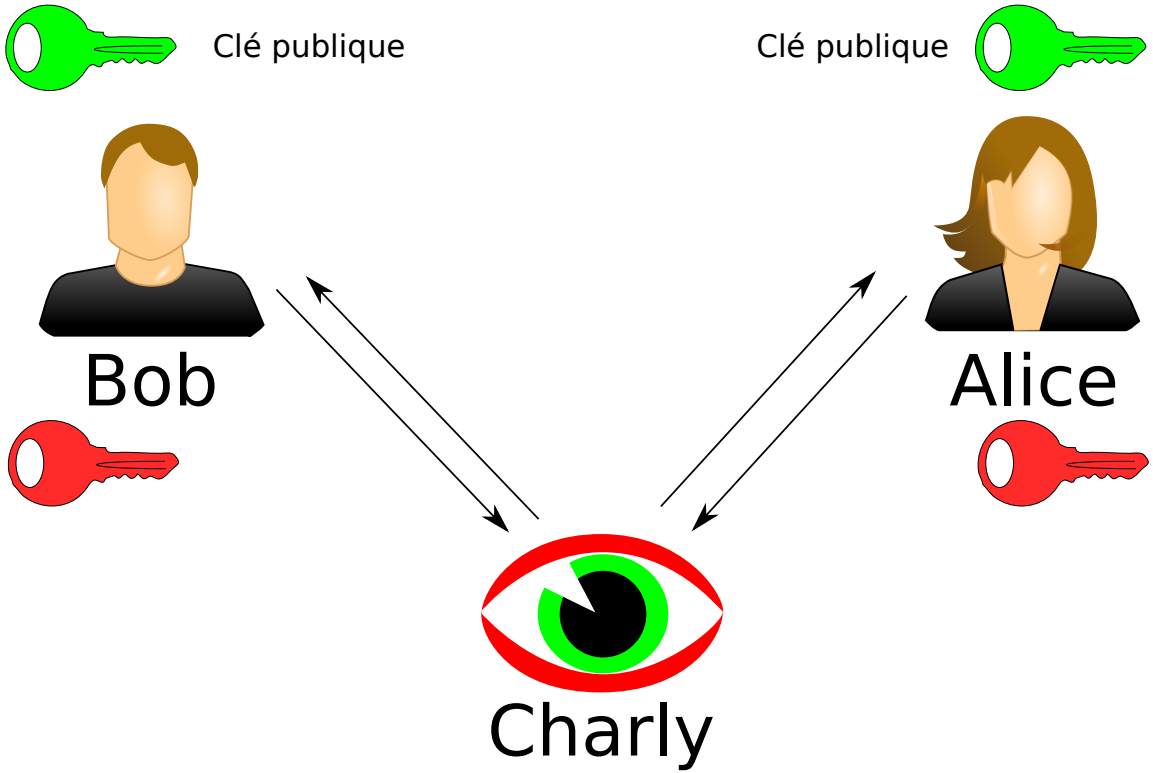

Alice




Charly

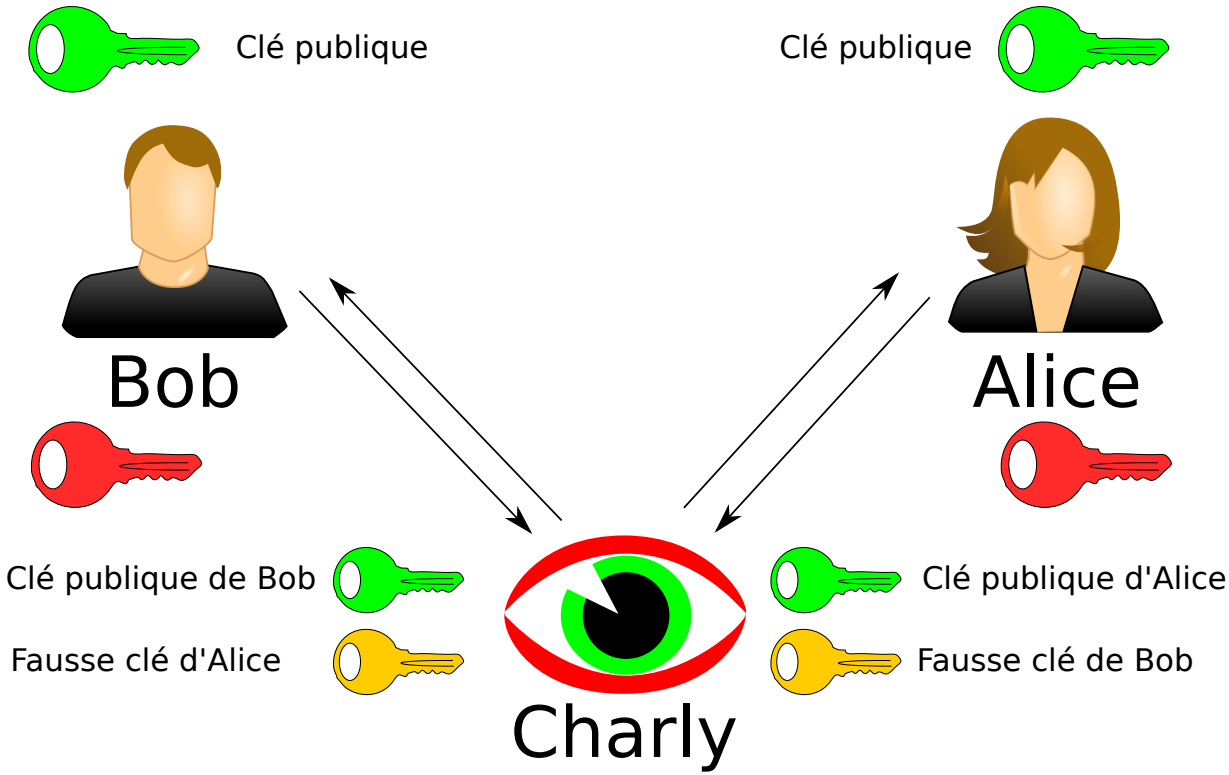
Il reste un problème...

Il suffit qu'il se fasse passer pour Alice et Bob !



Il reste un problème...

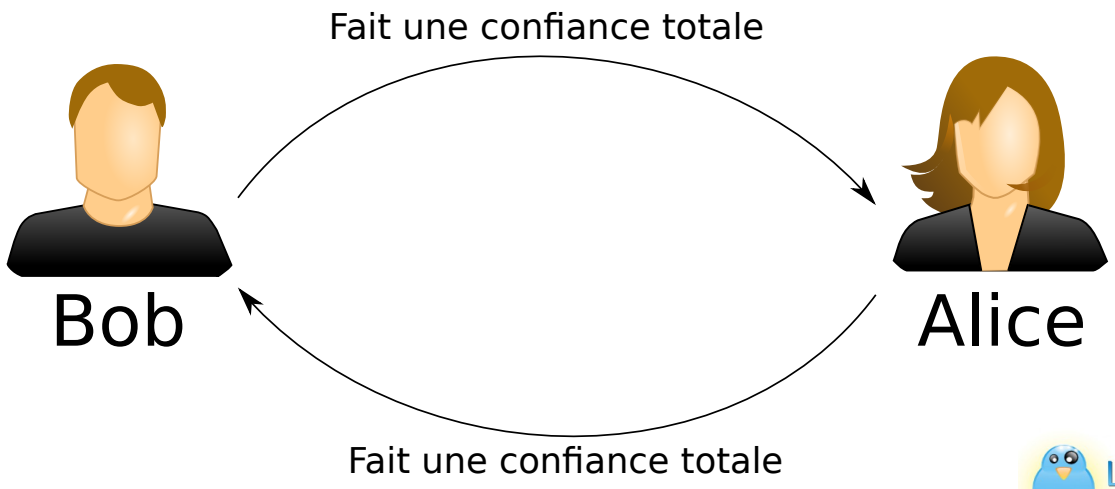
C'est ce qu'on appelle l'attaque de "l'homme du milieu"



On résout ce problème par la signature des clés.

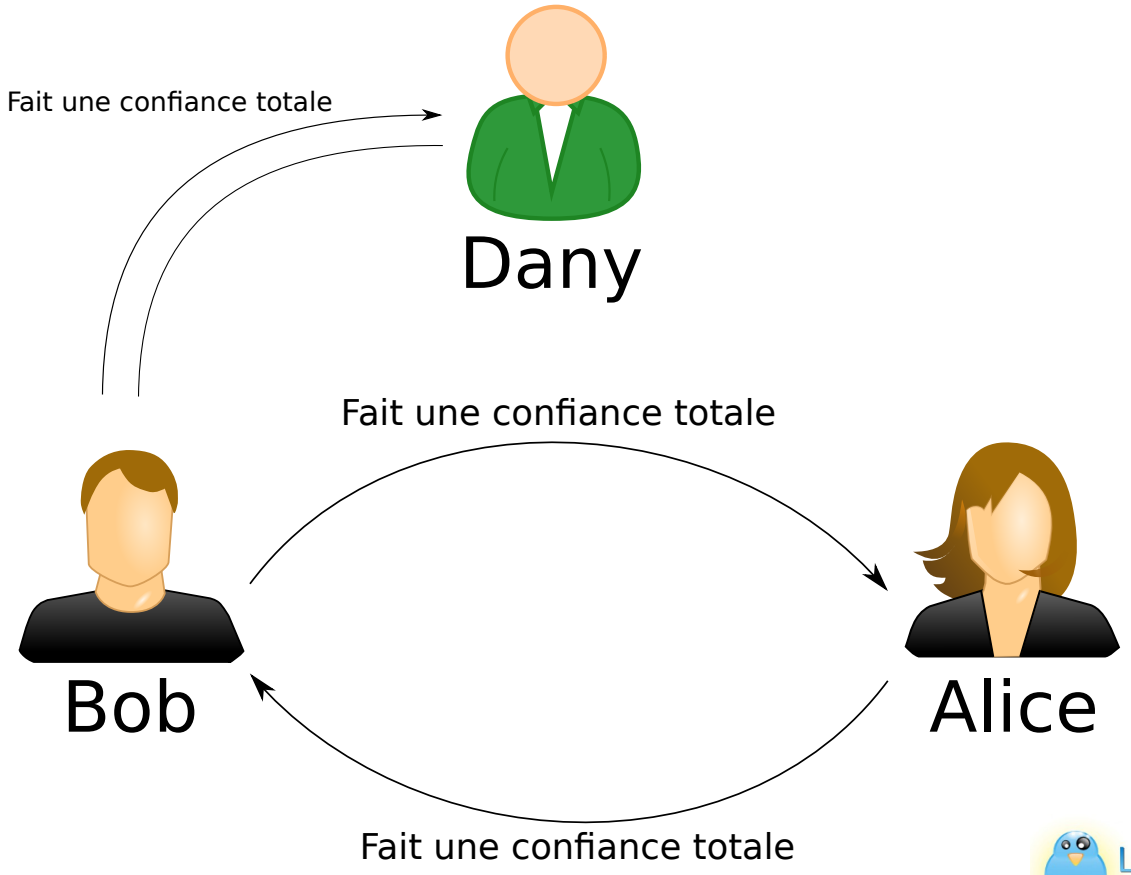
Signer les clés

Signer une clé publique revient à lui attribuer un niveau de confiance :



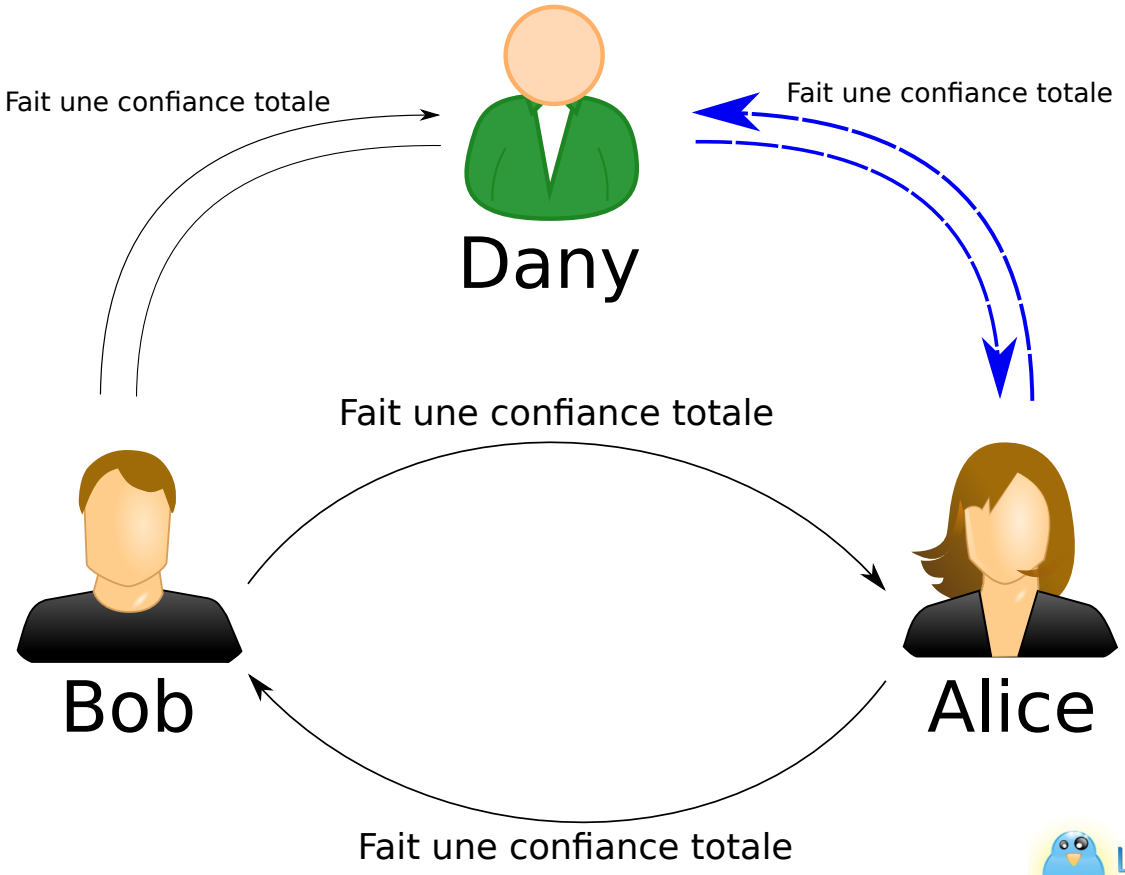
Signer les clés

Signer une clé publique revient à lui attribuer un niveau de confiance :



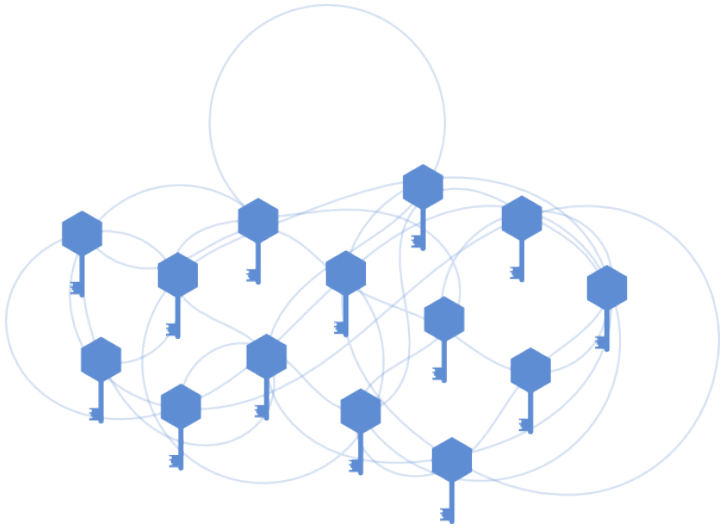
Signer les clés

Signer une clé publique revient à lui attribuer un niveau de confiance :



Le réseau de confiance

De proche en proche, on établit un réseau de confiance.



GNU Privacy Guard

- Jeu de mot avec le logiciel dont il s'inspire : PGP (Pretty Good Privacy)
- Installable très facilement sur toutes les distributions. Existe aussi pour un autre OS
- Outil en ligne de commande mais interactif
- Intégrable à différents clients mails :
  - Kmail (natif)
  - Thunderbird grâce à l'extension Enigmail,
  - ...

La génération des clés

Générer la paire de clés maîtresse

```
gpg --full-gen-key
gpg --list-keys
gpg --list-secret-keys
```

La génération des clés

Générer la paire de clés maîtresse

```
gpg --full-gen-key
gpg --list-keys
gpg --list-secret-keys
```

La clé maîtresse ne peut pas servir à chiffrer. On génère donc une sous-clé pour le chiffrement. Et donc, la clé maîtresse ne sert qu'à signer les sous-clés.

La signature des clés

Exporter la clé publique :

```
gpg --armor --export <id> > clepub.asc
```

Importer une clé publique :

```
gpg --import clepub.asc
```

Editer une clé :

```
gpg --edit-key <id>
```

Signer la sous-clé et lui attribuer un niveau de confiance :

```
sign
trust
```

Chiffrer et signer un message

```
gpg --encrypt --sign --armor --recipient bob message.txt
```

Génère un fichier `message.txt.asc` contenant le message chiffré et signé.

Vérifier et déchiffrer un message

```
gpg --decrypt message.txt.asc
```

Si le message est signé, l'option `--decrypt` déchiffre ET vérifie la signature.

Quelques bonnes pratiques

- Chiffrez **tous** vos mails : aucun n'est insignifiant
- N'indiquez rien dans l'objet du message : il n'est pas chiffré !
- N'utilisez la clé maîtresse que pour signer les sous-clés
- Ne signez pas n'importe quoi !
- Protégez votre clé privée maîtresse (phrase de passe, support chiffré, certificat de révocation, ...)
- Recyclez vos sous-clés régulièrement (tous les 6 mois par exemple)

Quelques liens utiles

- Documentaire sur les révélations d'Edwrad Snowden : "Citizen Four"
- "Lettre ouverte à ceux qui n'ont rien à cacher"
- La Quadrature Du Net (vidéo): "Reclaim our Privacy"
- La Quadrature Du Net (article): "De l'intimité et de sa nécessité"
- Free Software Foundation (tutoriel): "Auto-défense courriel"

Questions

Merci... Des questions ?

A vous de jouer !