Atelier pratique
Pourquoi et comment chiffrer ses mails

Introduction

- **Objectifs de la soirée**
  - Faire comprendre (un peu) le fonctionnement du mail et ses enjeux
  - permettre aux personnes d'améliorer leur confidentialité
  - rendre les personnes autonomes sur les outils sur lesquels on les formes
  - apprendre aux gens à chiffrer leurs mails
  - aborder la question des fournisseurs de mail
  - donner envie d'un autre atelier (sur un autre sujet)

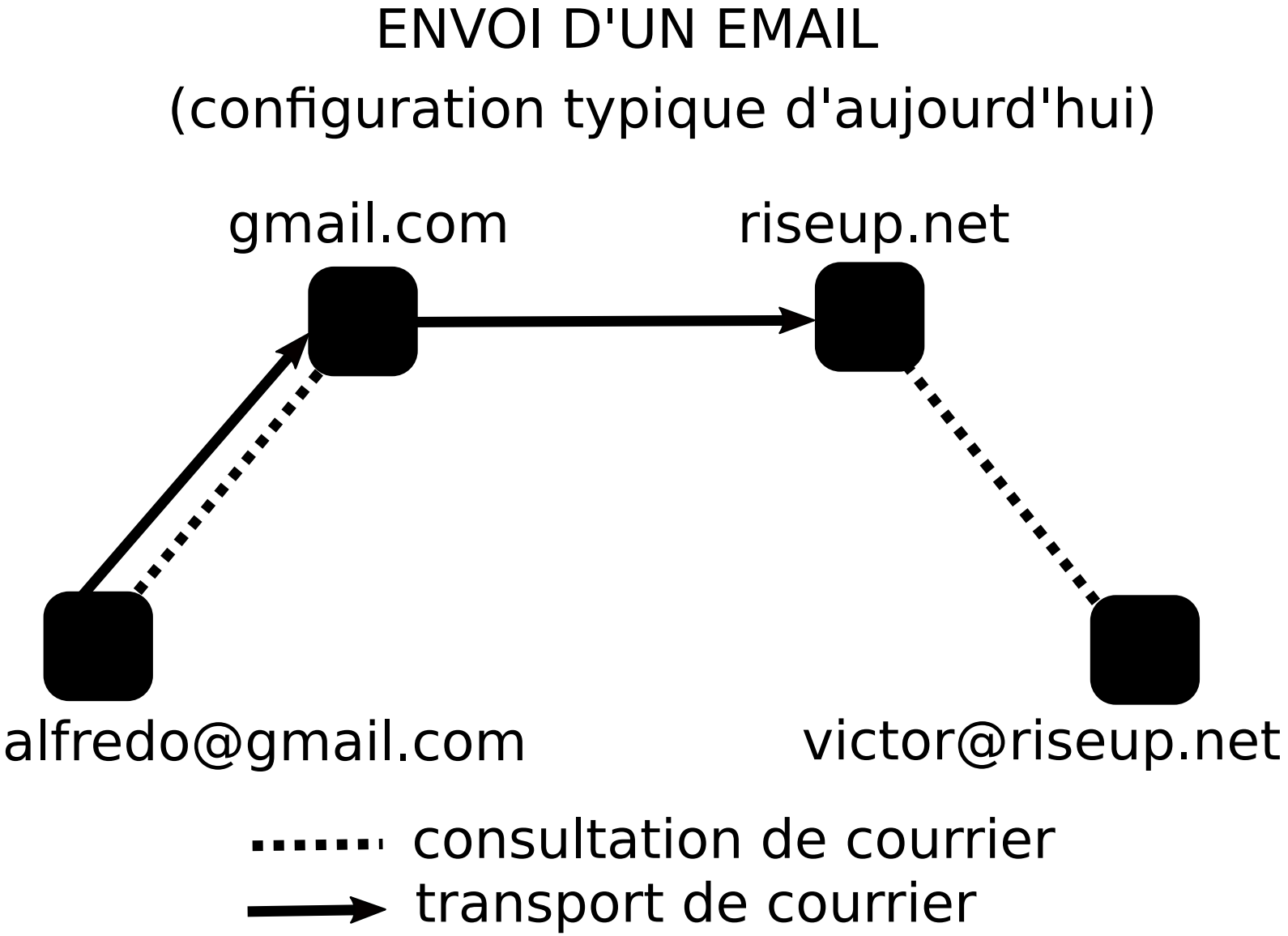
Introduction

Mycélium est une association loi 1901, autogérée, rattachée à la fédération FFDN (fédération de fournisseurs d’accès à Internet associatifs). Nous visons à nous (ré)approprier ensemble et autant que possible l’accès à Internet, mais aussi son fonctionnement et ses usages.

Mycelium à pour objet de :

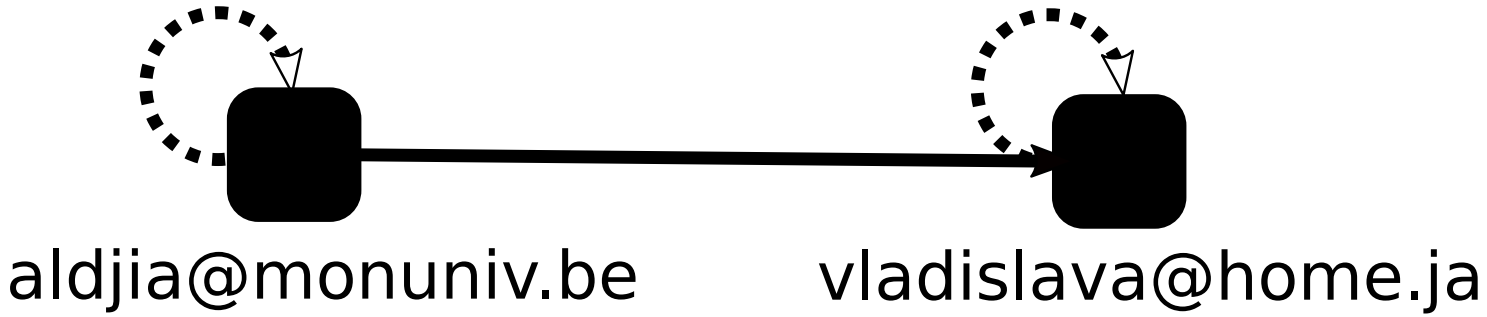
- Proposer à ses adhérent(e)s un accès non-marchand et solidaire à internet ;
- Encourager l'autonomie des internautes et leur prise de contrôle de leurs données et des services les concernant ;
- Permettre la compréhension du réseau internet et le développement d'un regard critique sur ses acteurs et ses usages ;
- Défendre la neutralité du net.

Partie 1 : C'est quoi un mail ?



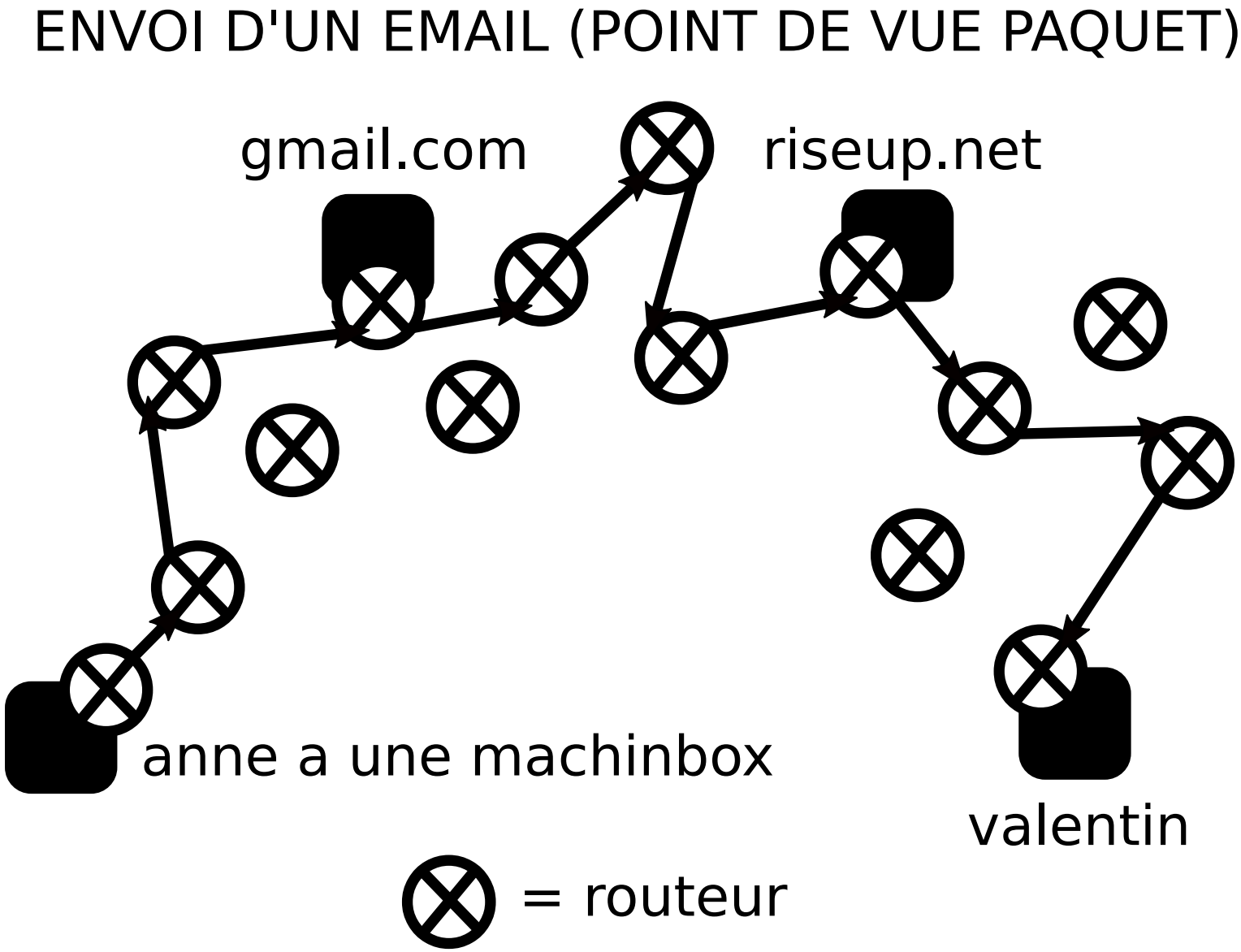
Partie 1 : C'est quoi un mail ?

ENVOI D'UN EMAIL
(configuration typique dans les 80's)



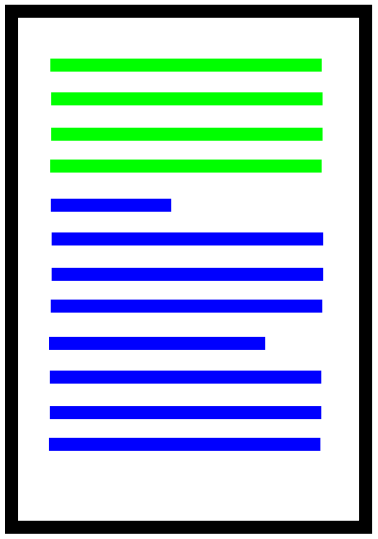
consultation de courrier
transport de courrier

Partie 1 : C'est quoi un mail ?



Partie 1 : C'est quoi un mail ?

STRUCTURE D'UN EMAIL



```
Date: Mon, 3 Jun 2019 09:44:05 +0800
From: Paul Wise <pabs@debian.org>
To: debian-www <debian-www@lists.debian.org>
Cc: _List Debian Publicity <debian-publicity@lists.debian.org>
Subject: Re: Small actions and large impacts
List-Id: <debian-publicity.lists.debian.org>

On Sun, Jun 2, 2019 at 11:30 PM Valessio Brito wrote:

> How difficult it would be to update the Debian logo in the
> 'KallesDesign' theme for the website and wiki for 1 week (maybe).

I think the easiest way would be to have the web server return the
diversity logo instead of the open logo when the referrer is not the
logos page. This way all uses of the logo switch to the diversity
logo, but if people are explicitly clicking on the Debian logo from
the logo page, then they get the Debian logo. The wiki uses the logo
from the website. Other Debian sites might also do this.

I noticed that the Debian diversity logo is not present on the Debian
logo pages:

https://www.debian.org/logos/
https://wiki.debian.org/DebianLogo

I think the first step should be to add it to the website Pics
directory and document it on the wiki so that it can be used by the
```

entêtes

corps

Partie 2 : Enjeux autour du mail

- **Quelle confiance avec nos postiers ? Et nos hébergeurs ?**
- **Risques de la centralisation des données**
- **Risques de la dépendance technique et de la dépossession des outils**
- **N’est-ce qu’un problème technique ?**

Partie 3 : les bons plans de Mycelium

Préambule : Les coûts d'être un hébergeur de mail et les problèmes auxquels il faut faire face.

Liste (non exhaustive) des fournisseurs :

- l'autre.net
- Autistici.org
- Riseup.net
- Disroot.org
- Sud-ouest.org
- … Et voir la carte des CHATONS

Beaucoup plus d'information sur le mail, son fonctionnement, ses enjeux ici :
https://linuxfr.org/news/se-passer-de-google-facebook-et-autres-big-brothers-2-0-2-le-courriel

Partie 4 : chiffrer ses mails

Exemple d’une clé de chiffrement :

mQENBFqlI94BCAC9qbSKJL1yP4H+knt1QhCH6sPo4dkpBBETn$VqNy/RWJlIkBRsF
m3G6zZ41jYLawtlevdQ+uc2PjlSFGGWwUXXhV1vtIH2yipTCL3KXWjD2XbVyGCnm
lBhY7yVzMPm6GR6sJ6KDb+pVeJsSujpkmMg2sfkfUsNp9CmYh+lgFWdGw+w9+Xrp
CsAVkOY/usZIDwsyoKUeWtjzjMgR7mlblGb3$u3TtOUSstc5Gr1WlIcw7E3wJ03HVA
Jblmp0tUlNMa6YNVD37Vo4xXniuh57MPuSnSRyy47Lt1EM3jobdDXGV8QbzkkInu
8jCQcdsIfZ7Fb8HCy01Klas0rOwlTazBissoQXkcaiUE,If2kkHqHEoDFMyyvXfnReO2P
FiEj8vPqXc736da9bAoL4HpLYge9J9J2DgNuga8sSGeUEI,yf3D7BSZ4YoGQbDKvKXb3
szNGhQfoA4HFEY98XbZOBvmX/KBFT0we3rxFgkt1KlWAlUMuSIgaTF31FeEJDLVs7Gl
bDXeEZp8EIzdSqOB47VqWF0TOsybrQMsSV9thT0BHmyIAoKc0urt1e/kj6Z6Da8hYl
fenKcHrC3eMLRbpPSkXVXHi1kOIntdNnu5eXQWqJ5ZYAJVAAbVxijYLD2aubHS8B6a
jsH0x+mOzWrl4ReQOSYb3pgqXhgL8qH1SpB865A74IU6slty/07oc/F0LI941g==
=PIe3FqlI94BCAC9qbSKJL1yP4H+knt1QhCH6sPo4dkpBBETn$VqNy/RWJlIkBRsF
m3G6zZ41jYLawtlevdQ+uc2PjlSFGGWwUXXhV1vtIH2yipA32TCL3KXWjD2XbVyGCn
lhY7yVzMPm6GR6sJ6KDb+pVeJsSujpkmMg2sfkfUsNp9CmYh+lgFWdGw+w9+Xrp
CsAVkY/usZIDwsyoKUeWtjzjMgR7mlblGb33TtOUSstc5Gr1Wll3AIcw7E3wJ03HVA
Jblmp0tUlNMa6YNVD37Vo4xXniuh57MPuSnSRyy47Lt1EM3jobdDXGV8QbzkkInu
8jCQcsIfZ7Fb8HCy01Klas0rOwlTazBissoQXkcIf2kkHqHEoDFMyyAE8vXfnReO2P
lhY7yVzMPm6GR6sJ6KDb+pVeJsSujpkmMg2sfkfUsNp9CmYh+lgFWdGw+w9+Xrp
CsAVkY/usZIDwsyoKUeWtjzjMgR7mlblGb33TtOUSstc5Gr1Wll3AIcw7E3wJ03HVA
Jblmp0tUlNMa6YNVD37Vo4xXniuh57MPuSnSRyy47Lt1EM3jobdDXGV8QbzkkInu
8jCQcsIfZ7Fb8HCy01Klas0rOwlTazBissoQXkcIf2kkHqHEoDFMyyAE8vXfnReO2P
FiEj8vPqXc736da9bAoL4HpLYge9J9J2DgNuga8sSGeyf3D7BSZ4YoGQbDKvKXb3
szNGhQfoA4HFEY98XbZOBvmX/KBFT0we3rxFgkt1KlWMuSIgaTF31FeEJDLVs7Gl
bDXeEZp8EIzdSqOB47VqWF0TOsybrQMsSV9thT0BHmyoKc0urt1e/kj6Z6Da8hYl
fenKcHrC3eMLRbpPSkXVXHi1kOIntdNnu5eXQWqJ5ZYAJVbVxijYLD2aubHS8B6a
jsH0x+mOzWrl4ReQOSYb3pgqXhgL8qH1SpB8slty/07oc/F0LI9ajeaLDIP3788EE=

Texte en clair

↓

f(texte en clair, clé)

↓

Texte chiffré

↓

f(texte chiffré, clé)

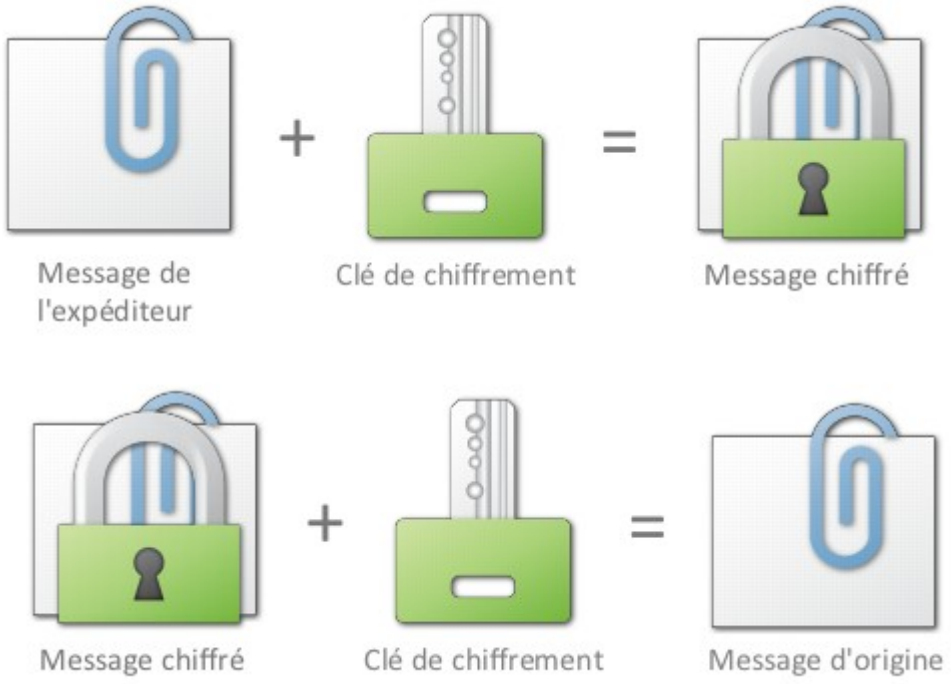
↓

Texte en clair

Partie 4 : Une solution pour plus de confidentialité : chiffrer ses mails

C’est quoi chiffrer ?

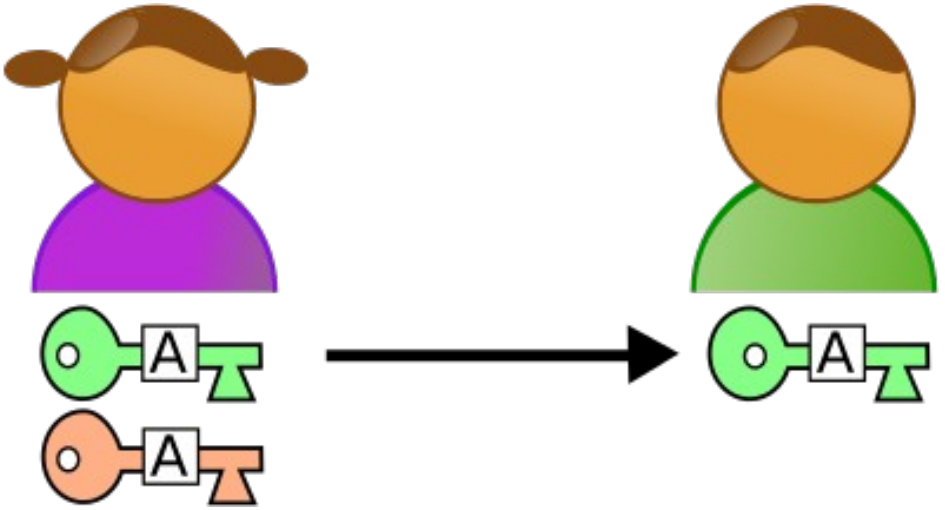
Chiffrement symétrique



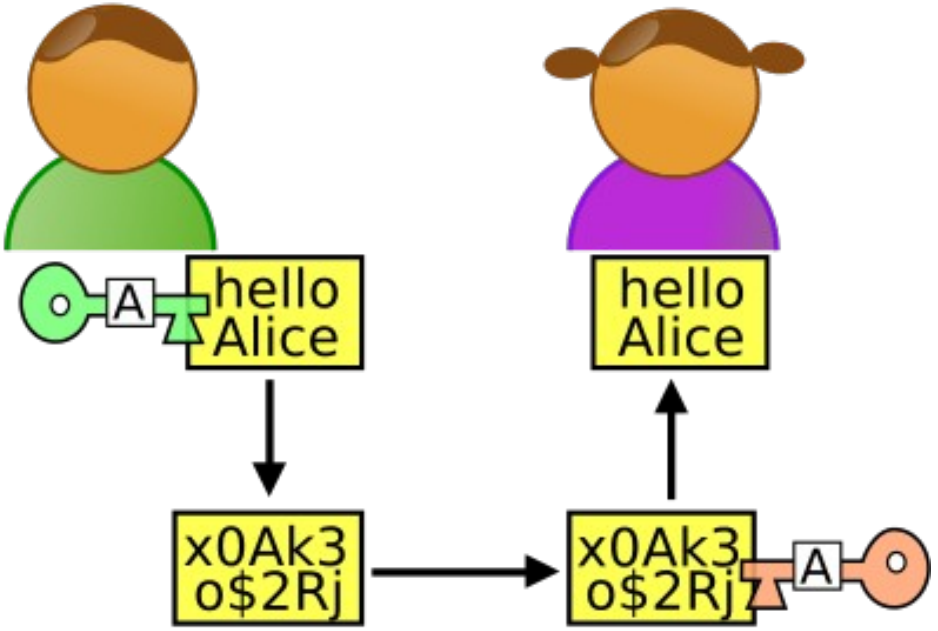
Le souci, c’est qu’il faut que l’expéditeur et le destinataire aient la même clé…

Partie 4 : chiffrer ses mails

Chiffrement asymétrique



1re étape : Alice génère deux clefs. La clef publique (verte) qu'elle envoie à Bob et la clef privée (rouge) qu'elle conserve précieusement sans la divulguer à quiconque.



2e et 3e étapes : Bob chiffre le message avec la clef publique d'Alice et envoie le texte chiffré. Alice déchiffre le message grâce à sa clef privée.

Partie 4 : chiffrer ses mails

Signature de message et confiance dans une clé publique

Comment faire confiance à une clé publique ? Comment savoir que celle-ci appartient bien à la personne à qui nous souhaitons parler ?

→ Possibilité de « noter » les clés publique que l'on a dans son trousseau (d'une confiance faible à une confiance ultime)

→ Regarder l'ID de la clé de la personne

→ Possibilité de signer le message.

- Signer un message c'est chiffrer le texte avec sa clé privée
- Une fois le message reçu, le destinataire utilise votre clé publique, il actionne alors l'algorithme qui se chargera de confirmer que c'est bien vous qui êtes à l'origine du message.

```
pub   rsa2048 2018-03-11 [SC]
      54D9F85E818D1BA5270E22AA496B0C1E4342EB30
uid   [ultimate] Valentin Auzanneau <v.auzanneau@vivaldi.net>
sub   rsa2048 2018-03-11 [E]
```

Partie 5 : Limites et risques

- **Des limites au chiffrement d'emails :**
  - Les entêtes sont visibles. Leur interception n'est pas aisée pour autant, mais on pourrait en déduire des graphes sociaux et des informations sur notre activité
  - Ajoute une petite contrainte à l'usage. Moins de mobilité (il faut avoir son jeu de clés sur soi).
  - On ne peut communiquer de façon chiffrée qu'avec des personnes dont on possède la clé publique.
  - L'intérêt pour la cryptographie d'auto-défense est relativement récent. Le chiffrement des emails par GPG est plus complexe qu'exposé. Ce sont des pratiques qu'on découvre aussi et nous n'en maitrisons pas chaque aspect.
  - Réservé aux expert(e)s ? Les moyens techniques de cryptographie sont encore largement débattus. Exemple : https://secushare.org/PGP
- **Comporte des risques :**
  - Tu perds ta clé = tu perds tes mails chiffrés
  - Utiliser sa clé privée sur un ordinateur vérolé/peu sûr
  - Ne pas s'être assuré de l'authenticité d'une clé publique

Partie 7 : Des outils pour chiffrer ses mails au quotidien

Mozilla Thunderbird

- **Un client de messagerie libre**
  - Lire et envoyer des courriels
  - Organiser sa boite mail (création de dossiers, système de filtre, …)
  - Gestionnaire de contact
  - Calendrier
  - ….

Énigmail

- **Un module de chiffrement et de signature de courriel pour Thunderbird**
  - C’est super pratique

https://support.mozilla.org/fr/kb/signature-numerique-et-chiffrement-des-messages

À vous de jouer !

- télécharger Thunderbird et Énigmail
- configurer Thunderbird pour qu'il receptionne correctement vos mails
- créer une paire de clé avec Énigmail
- configurer Thunderbird pour qu'il fonctionne bien avec la paire de clé
- apprendre à échanger/chercher des clés publiques
- écrire des messages aux autres dans la salle
- (Accéder au trousseau de clé dans le système de fichiers)

>> Pour les plus aguerri·e, nous pouvons vous montrer PASS, un logiciel de gestion de mots-de-passe qui chiffre vos mots de passe avec votre clé.