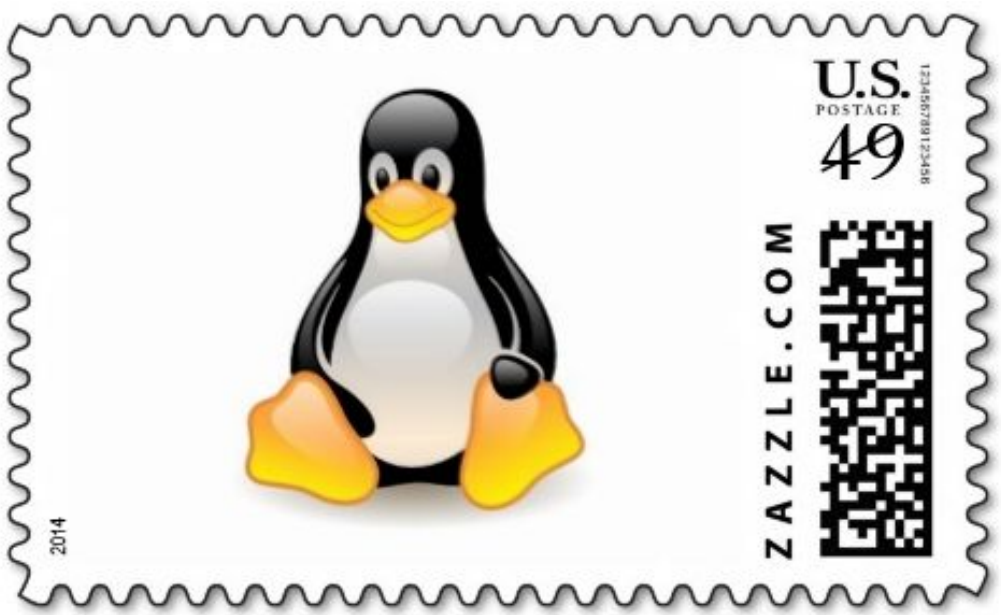
Sécurité des Courriels

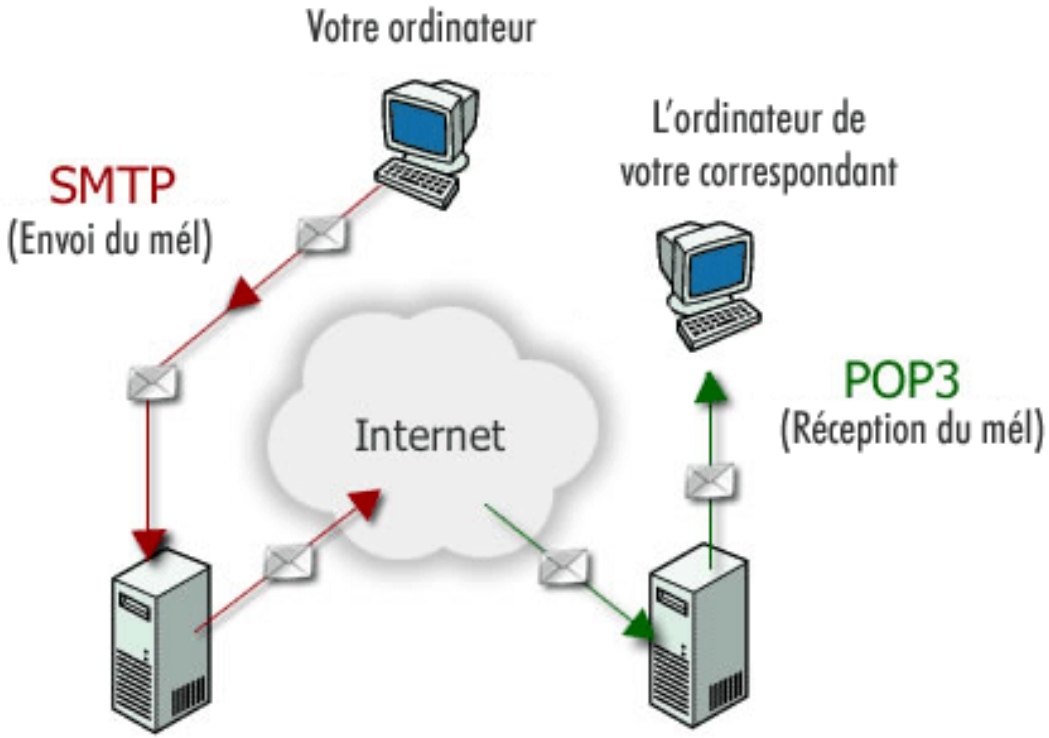
Éric BERTHOMIER
eric.berthomier@free.fr

March 16, 2022

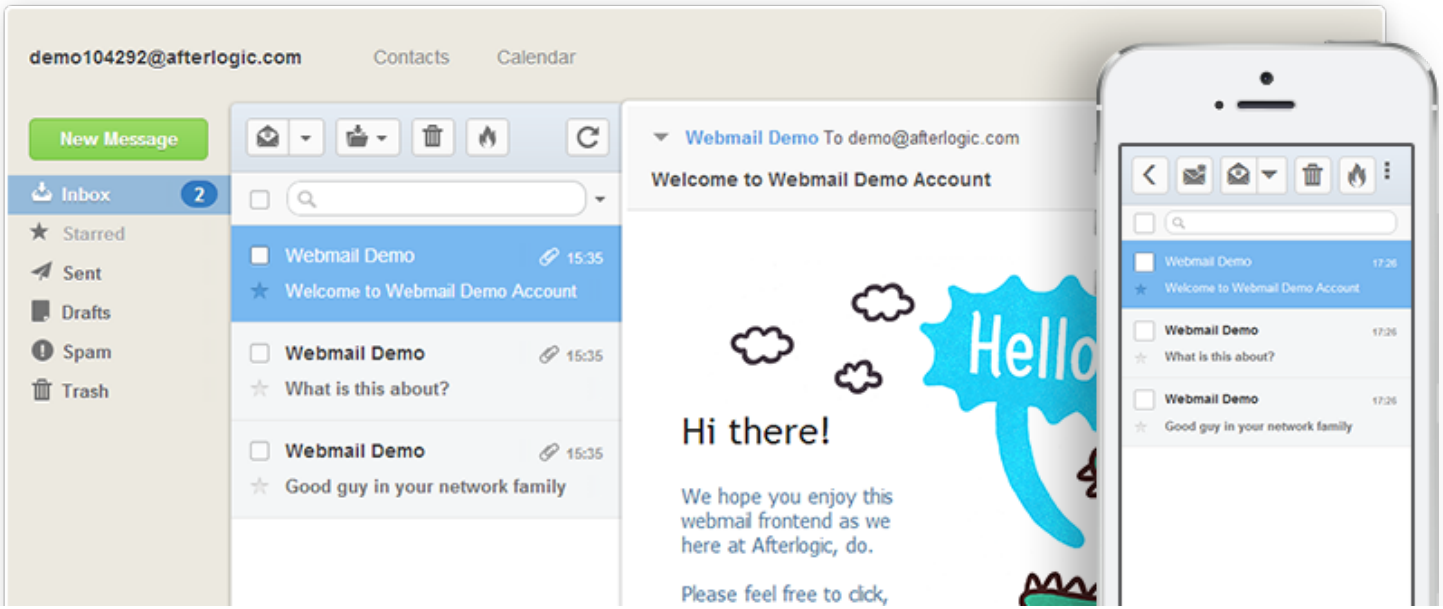


Version 1.0 - Version Stagiaire

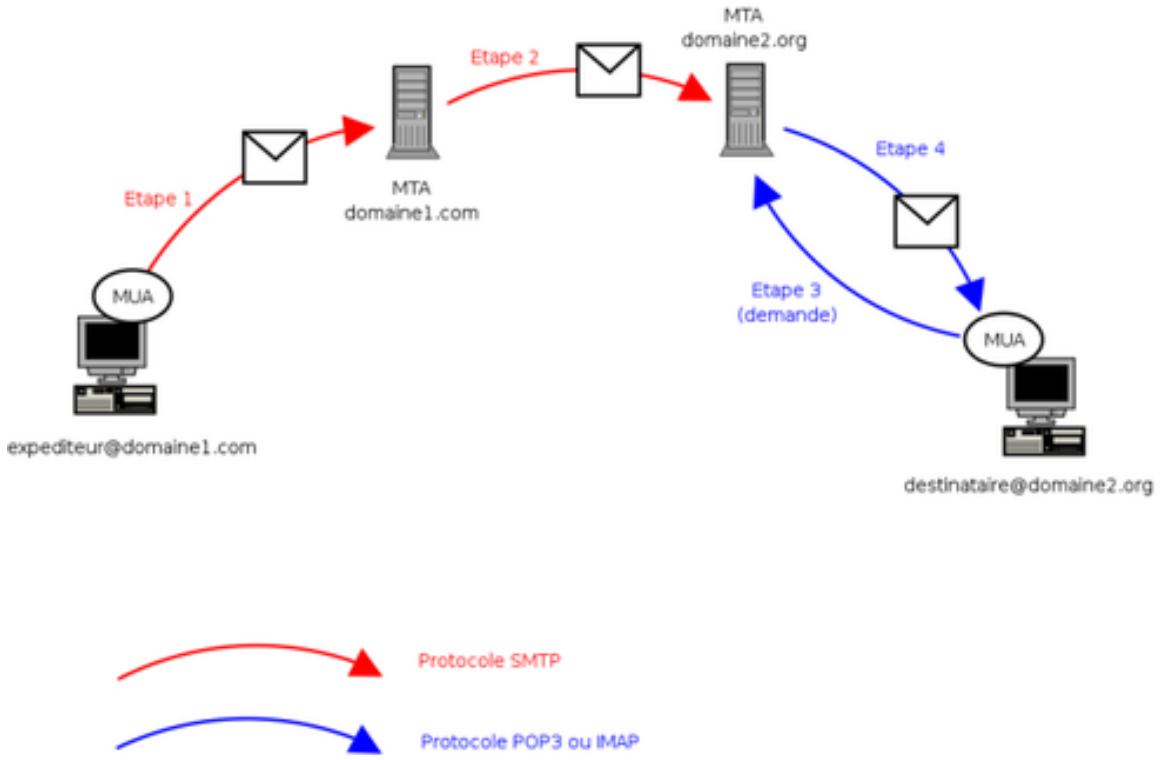
Utilisation du courriel à l'aide d'un logiciel de messagerie



Utilisation du courriel à l'aide d'un WebMail

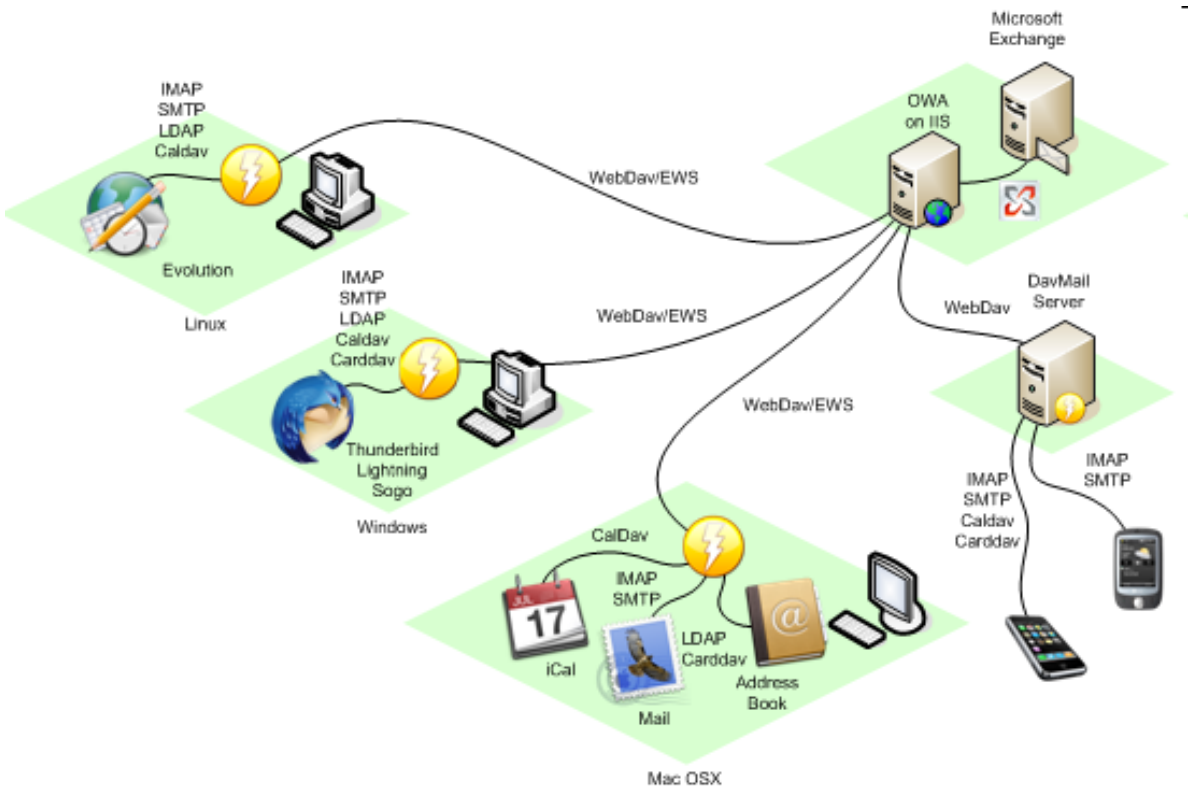


Acheminement d'un message



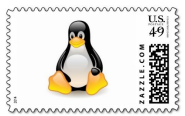
Conclusion sur la messagerie

On ne parle pas d'un courriel, on parle des courriels ...



Mail - Composants publiques

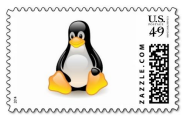
POP3 : *Post Office Protocol* permet d'aller récupérer ses courriels sur un serveur distant.



Mail - Composants publiques

POP3 : *Post Office Protocol* permet d'aller récupérer ses courriels sur un serveur distant.

SMTP : *Simple Mail Transfer Protocol* permet de transférer le courriel d'**un serveur à un autre**.



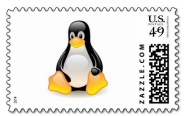
Mail - Composants publiques

POP3 : *Post Office Protocol* permet d'aller récupérer ses courriels sur un serveur distant.

SMTP : *Simple Mail Transfer Protocol* permet de transférer le courriel d'**un serveur à un autre**.

IMAP : *Internet Message Access Protocol* est un protocole alternatif au protocole POP3 mais offrant beaucoup plus de possibilités :

- permet de gérer plusieurs accès simultanés
- permet de gérer plusieurs boîtes aux lettres
- permet de trier le courrier selon plus de critères



Mail - Composants publiques

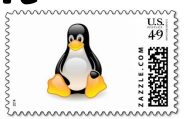
POP3 : *Post Office Protocol* permet d'aller récupérer ses courriels sur un serveur distant.

SMTP : *Simple Mail Transfer Protocol* permet de transférer le courriel d'**un serveur à un autre**.

IMAP : *Internet Message Access Protocol* est un protocole alternatif au protocole POP3 mais offrant beaucoup plus de possibilités :

- permet de gérer plusieurs accès simultanés
- permet de gérer plusieurs boîtes aux lettres
- permet de trier le courrier selon plus de critères

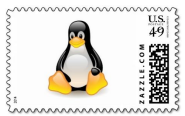
En général utilisé pour avoir un accès permanent sur ces courriels (donc gestion sur le serveur).



Mail - Composants privés

login : identifiant permettant d'associer un nom de compte à une personne ou une entité

mot de passe : suite de caractères visant à protéger un compte



Mail - Composants privés

login : identifiant permettant d'associer un nom de compte à une personne ou une entité

mot de passe : suite de caractères visant à protéger un compte

Mot de passe fort

Un mot de passe est considéré aujourd'hui comme fort si sa taille est **supérieure** à 12 caractères et si il comporte des caractères spéciaux et des chiffres, des minuscules et des MAJUSCULES.

Mail - Composants privés

login : identifiant permettant d'associer un nom de compte à une personne ou une entité

mot de passe : suite de caractères visant à protéger un compte

Mot de passe fort

Un mot de passe est considéré aujourd'hui comme fort si sa taille est **supérieure** à 12 caractères et si il comporte des caractères spéciaux et des chiffres, des minuscules et des MAJUSCULES.

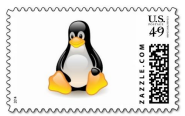
2]98yt!Ja}ZX

Conclusion - Sécurité du courriel côté utilisateur

Conclusion - Sécurité du courriel côté utilisateur

La messagerie d'un utilisateur n'est protégée que par un

MOT DE PASSE



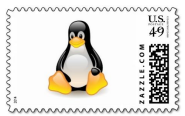
Conclusion - Sécurité du courriel côté utilisateur

Conclusion - Sécurité du courriel côté utilisateur

La messagerie d'un utilisateur n'est protégée que par un

MOT DE PASSE

Mot de passe stocké et personnalisable ! ...



Conclusion - Sécurité du courriel côté utilisateur

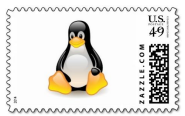
Conclusion - Sécurité du courriel côté utilisateur

La messagerie d'un utilisateur n'est protégée que par un

MOT DE PASSE

Mot de passe stocké et personnalisable ! ...

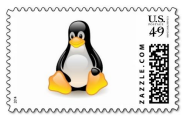
1. 123456
2. password
3. 12345
4. 12345678
5. qwerty
6. 123456789
7. 1234
8. baseball
9. dragon
10. football



Menaces et Risques

Perte d'un courriel

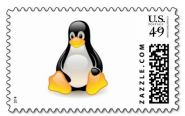
Deux cas sont à considérer :



Perte d'un courriel

Deux cas sont à considérer :

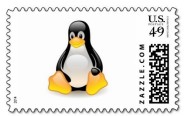
- La perte dun e-mail au cours de sa transmission,
  - problème sur un serveur de messagerie nécessitant sa restauration (les derniers messages reçus peuvent être perdus)
  - suppression à tort par un logiciel antispam



Perte d'un courriel

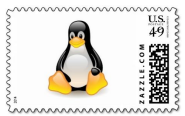
Deux cas sont à considérer :

- La perte dun e-mail au cours de sa transmission,
  - problème sur un serveur de messagerie nécessitant sa restauration (les derniers messages reçus peuvent être perdus)
  - suppression à tort par un logiciel antispam
- La disparition dun message reçu, voire de lensemble des messages reçus. Ce risque est particulièrement important lorsque lutilisateur stocke ses e-mails sur son propre ordinateur (rarement sauvegardé).



Perte de confidentialité

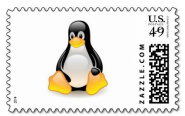
La messagerie représente un facteur important de perte de confidentialité.
Cette perte de confidentialité peut être provoquée par différents événements :



Perte de confidentialité

La messagerie représente un facteur important de perte de confidentialité.
Cette perte de confidentialité peut être provoquée par différents événements :

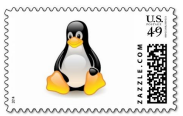
- une divulgation accidentelle : le message a été envoyé trop rapidement;



Perte de confidentialité

La messagerie représente un facteur important de perte de confidentialité.
Cette perte de confidentialité peut être provoquée par différents événements :

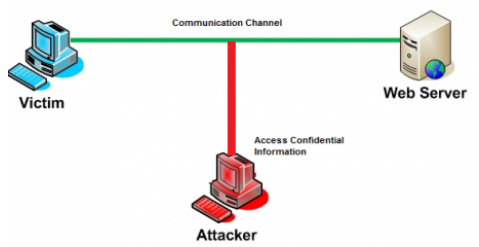
- une divulgation accidentelle : le message a été envoyé trop rapidement;
- une divulgation par négligence ou par méconnaissance des règles;

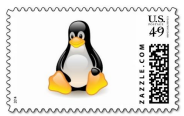


Perte de confidentialité

La messagerie représente un facteur important de perte de confidentialité.
Cette perte de confidentialité peut être provoquée par différents événements :

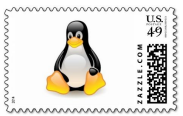
- une divulgation accidentelle : le message a été envoyé trop rapidement;
- une divulgation par négligence ou par méconnaissance des règles;
- un espionnage des messages lors de la transmission sur le réseau à laide dun logiciel spécialisé (sniffer) ou d'un malware.





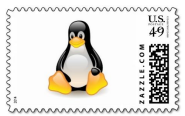
Perte d'intégrité

- Un message peut être altéré, accidentellement (dysfonctionnement déquipement, modification de format entraînant une perte dinformation, . . .) ou par malveillance pendant sa transmission ou son stockage, sur un serveur de messagerie ou sur le poste destinataire.



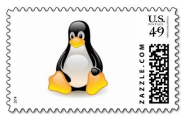
Perte d'intégrité

- Un message peut être altéré, accidentellement (dysfonctionnement déquipement, modification de format entraînant une perte dinformation, . . .) ou par malveillance pendant sa transmission ou son stockage, sur un serveur de messagerie ou sur le poste destinataire.
- La perte dintégrité peut également provenir de modifications ou ajouts volontaires effectués au niveau du serveur de messagerie.



Usurpation d'identité de l'émetteur

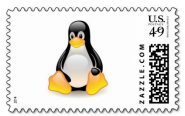
Lorsquune adresse e-mail est connue, elle peut aisément être utilisée par nimporte qui dans lintention de nuire.



Usurpation d'identité de l'émetteur

Lorsquune adresse e-mail est connue, elle peut aisément être utilisée par nimporte qui dans lintention de nuire.

Il nexiste pas de mécanisme dauthentification dans le protocole SMTP, on peut donc envoyer un message au nom de n'importe quelle personne.

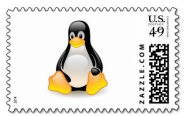


Usurpation d'identité de l'émetteur

Lorsquune adresse e-mail est connue, elle peut aisément être utilisée par nimporte qui dans lintention de nuire.

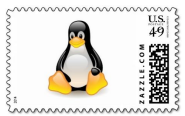
Il nexiste pas de mécanisme dauthentification dans le protocole SMTP, on peut donc envoyer un message au nom de n'importe quelle personne.

Seul, le protocole SMTPs permet de qualifier l'expéditeur.



Répudiation

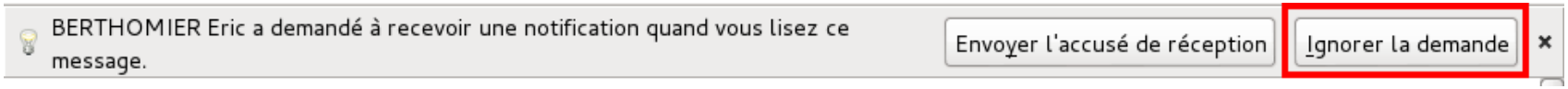
La répudiation est le risque de reniement de lenvoi ou de la réception dun message.

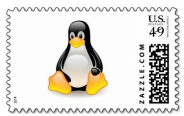


Répudiation

La répudiation est le risque de reniement de lenvoi ou de la réception dun message.

En labsence de dispositif de sécurité spécifique, il est difficile de garantir le fait quun message ait été émis ou reçu.



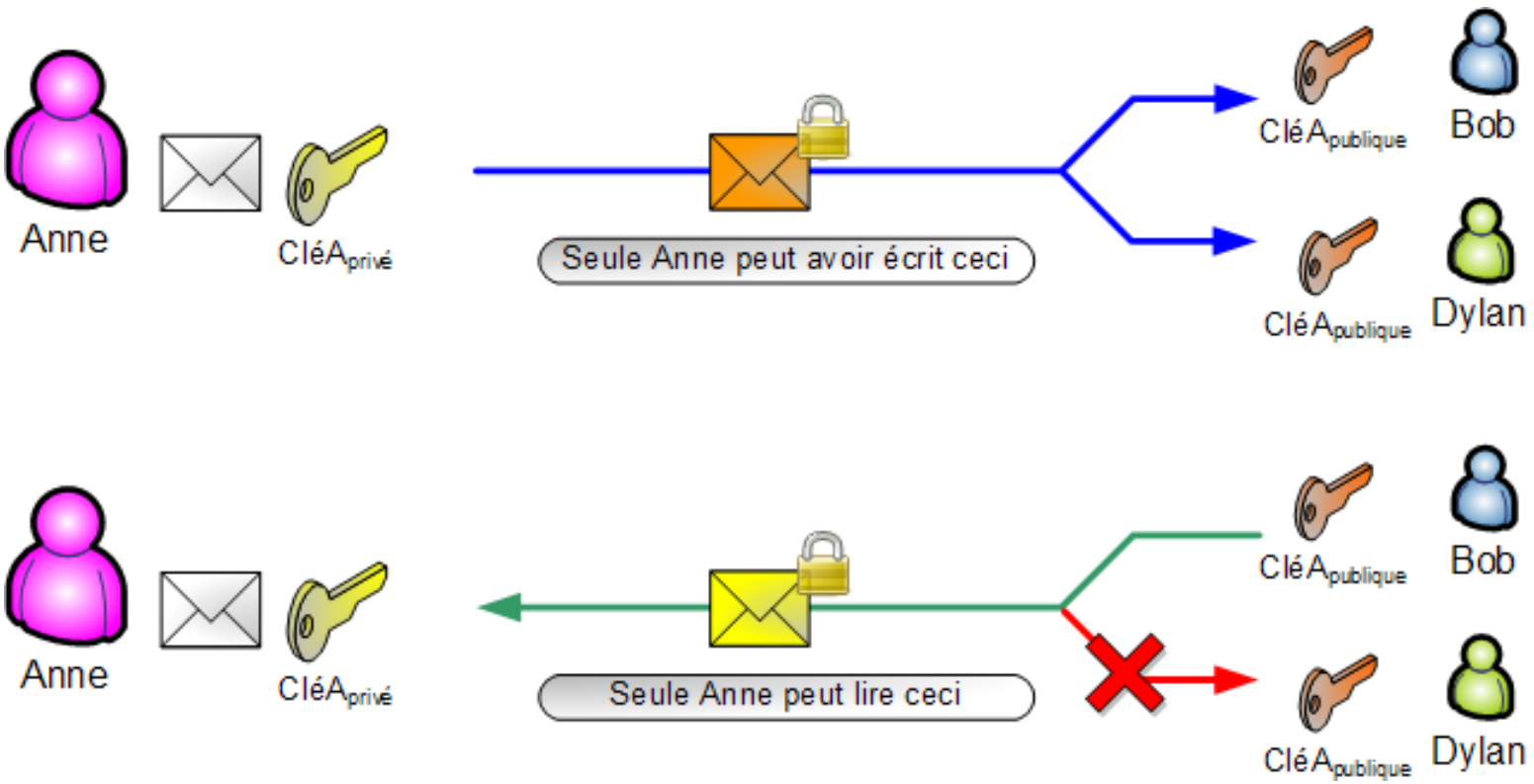


Vidéo

ARTE : XENIUS - La Cryptologie

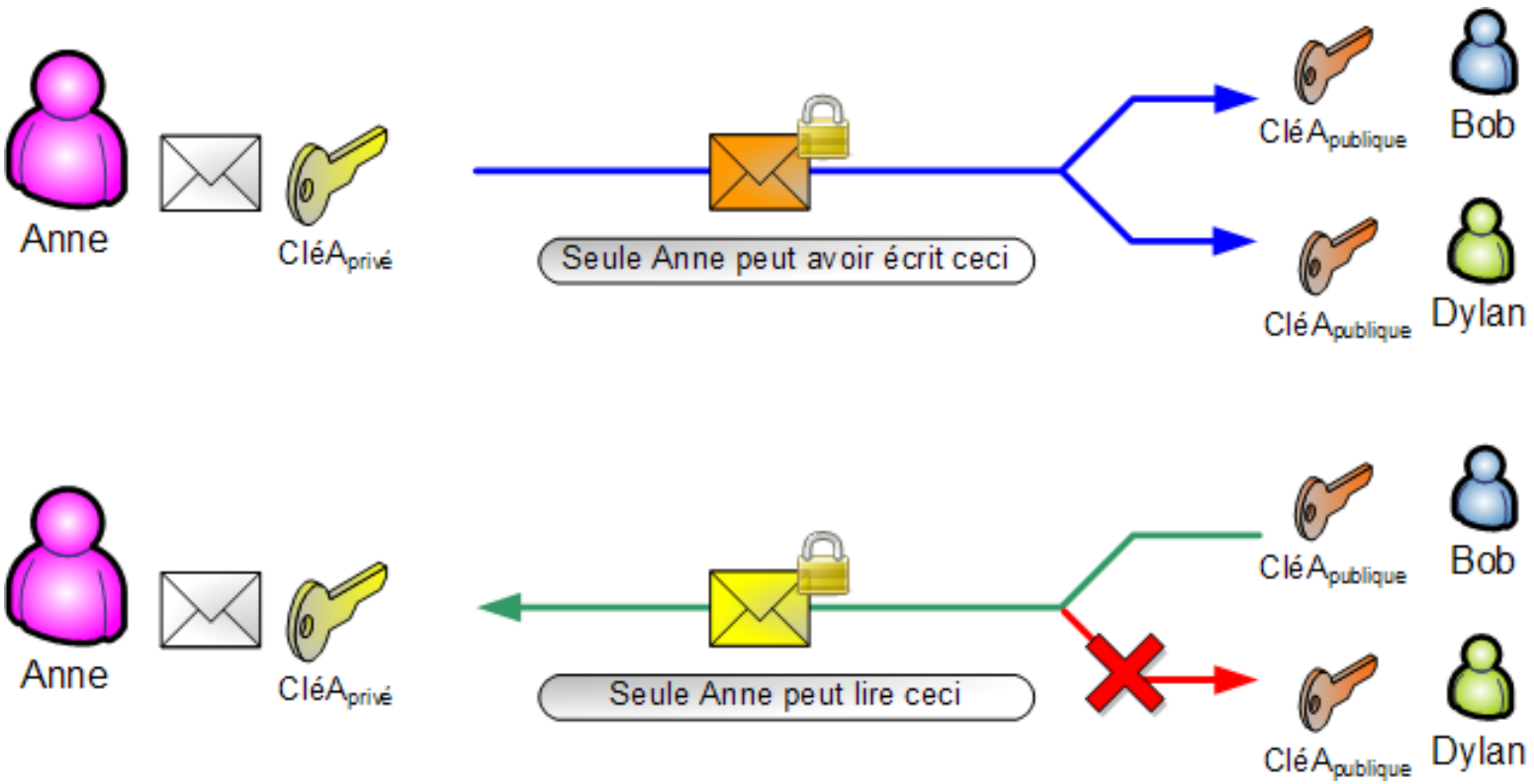
Quelques solutions envisageables

Signature électronique des messages



Signature Numérique

Signature électronique des messages



Signature Numérique

Difficile à mettre en œuvre sans un certain coût ...