Sécurité des messages

Cryptographie asymétrique avec PGP

07/02/2023

Sécurité des messages

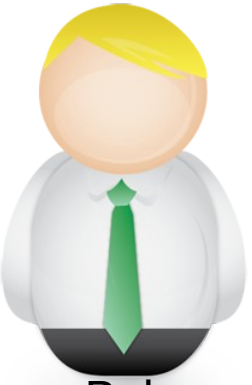
06/02/2023

Sommaire

Sommaire

Cas pratique, acteurs, problématique

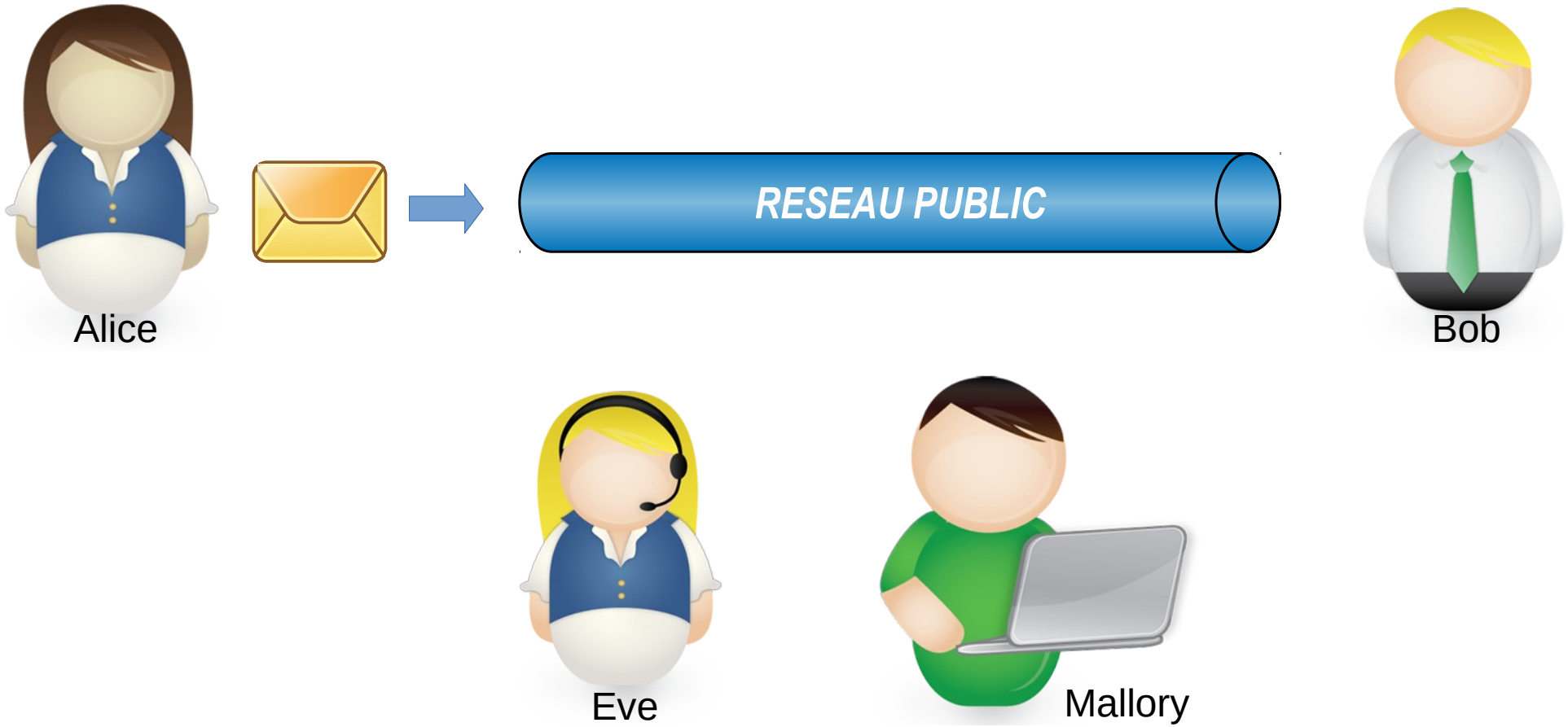
Alice



Bob

Cas pratique, acteurs, problématique

Cas pratique, acteurs, problématique



Cas pratique, acteurs, problématique

Problématique générale

- Que signifie

  « Alice a transmis un message à Bob de manière sécurisée » ?

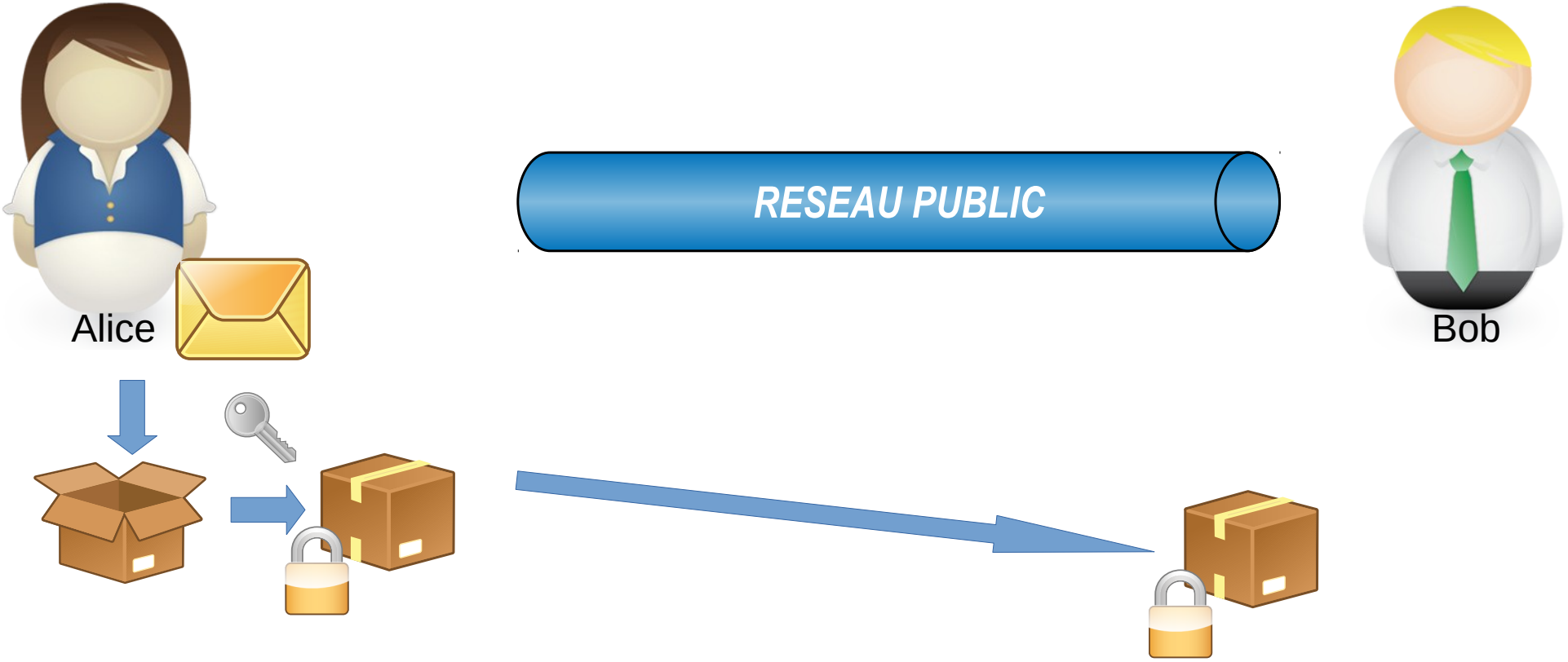
Cas pratique, acteurs, problématique

Problématique générale

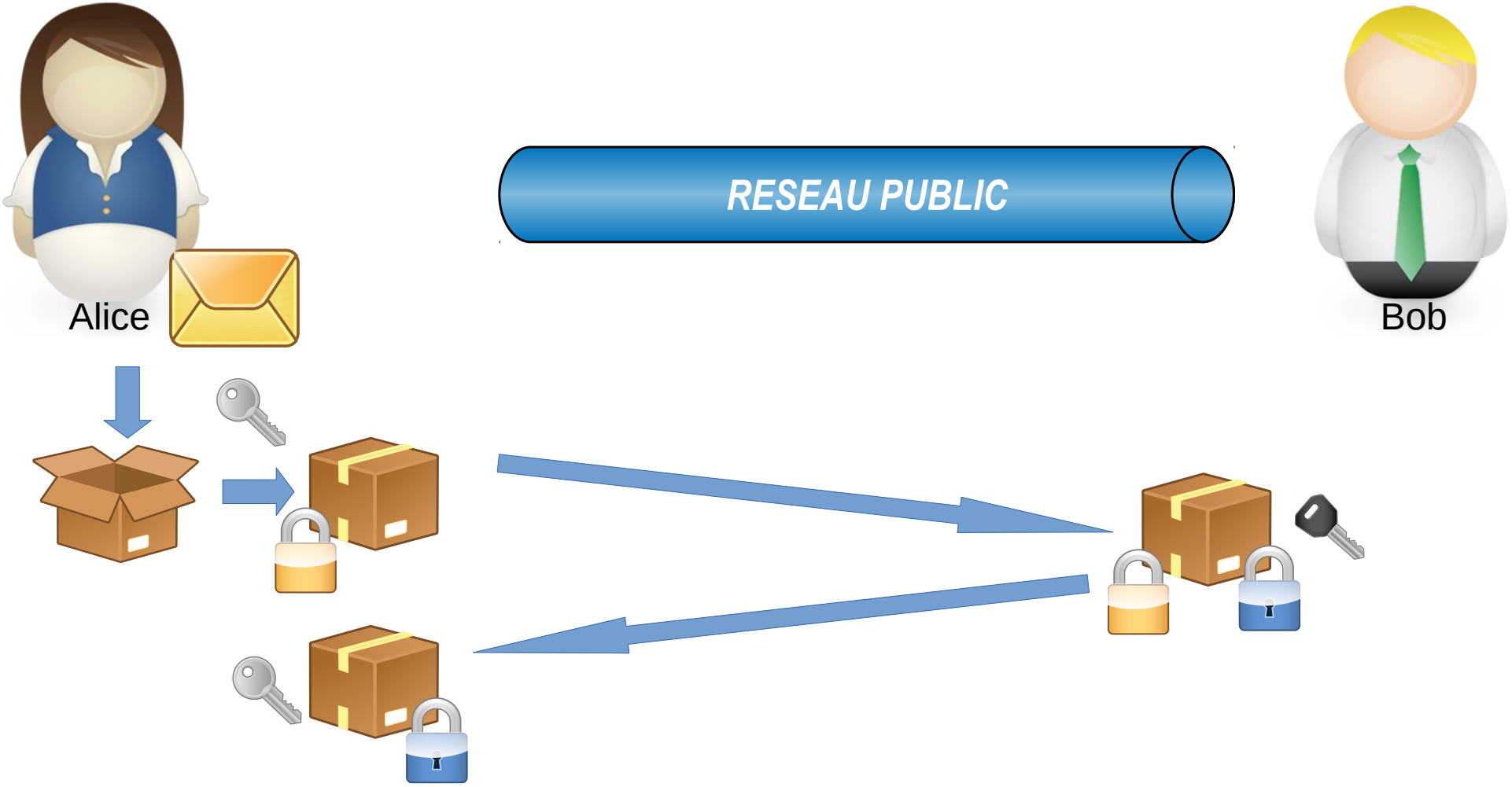
- Comment garantir la sécurité du message transmis par Alice à Bob ?

Sommaire

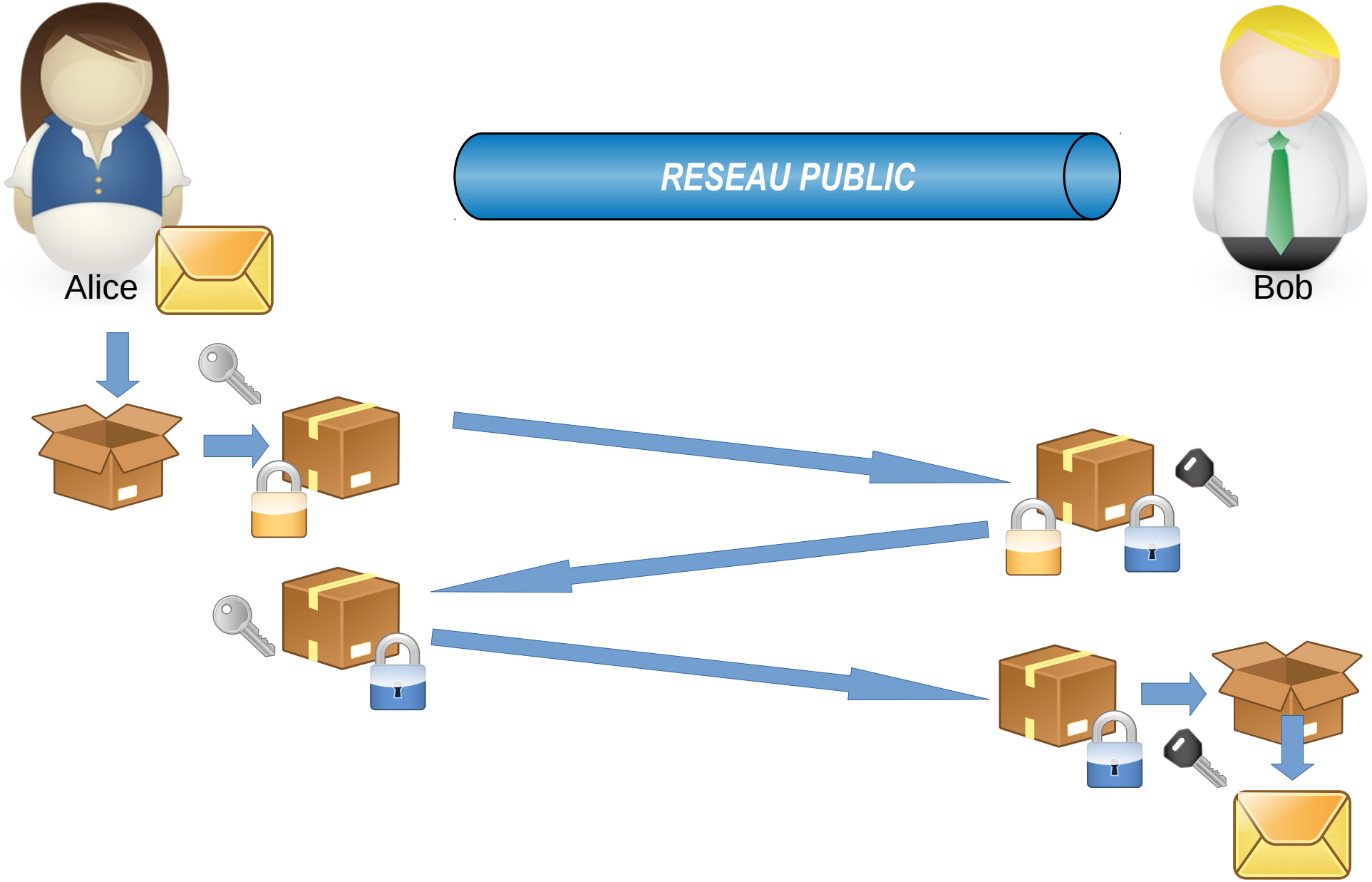
1- Le double cadenas



1- Le double cadenas



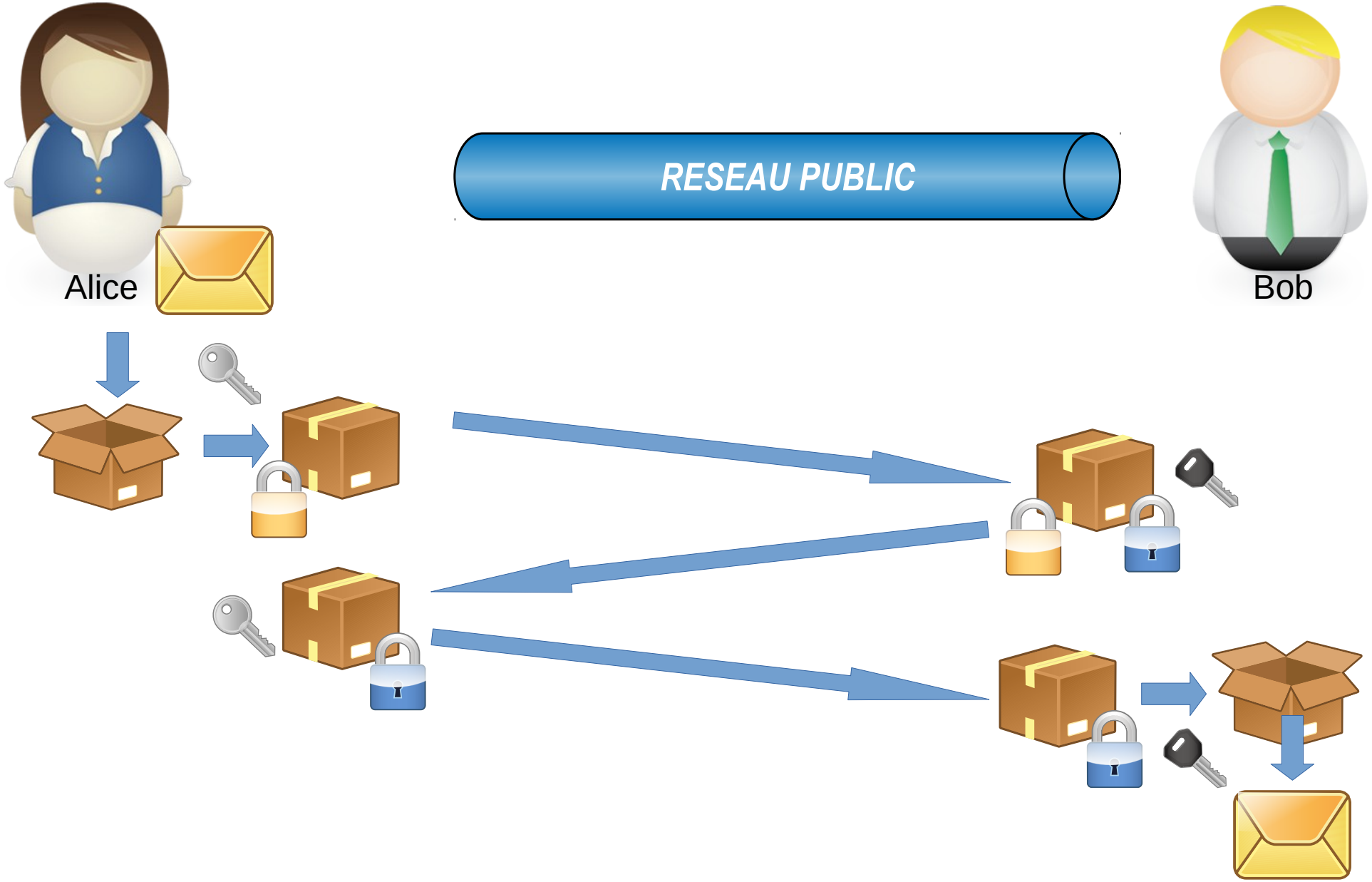
1- Le double cadenas



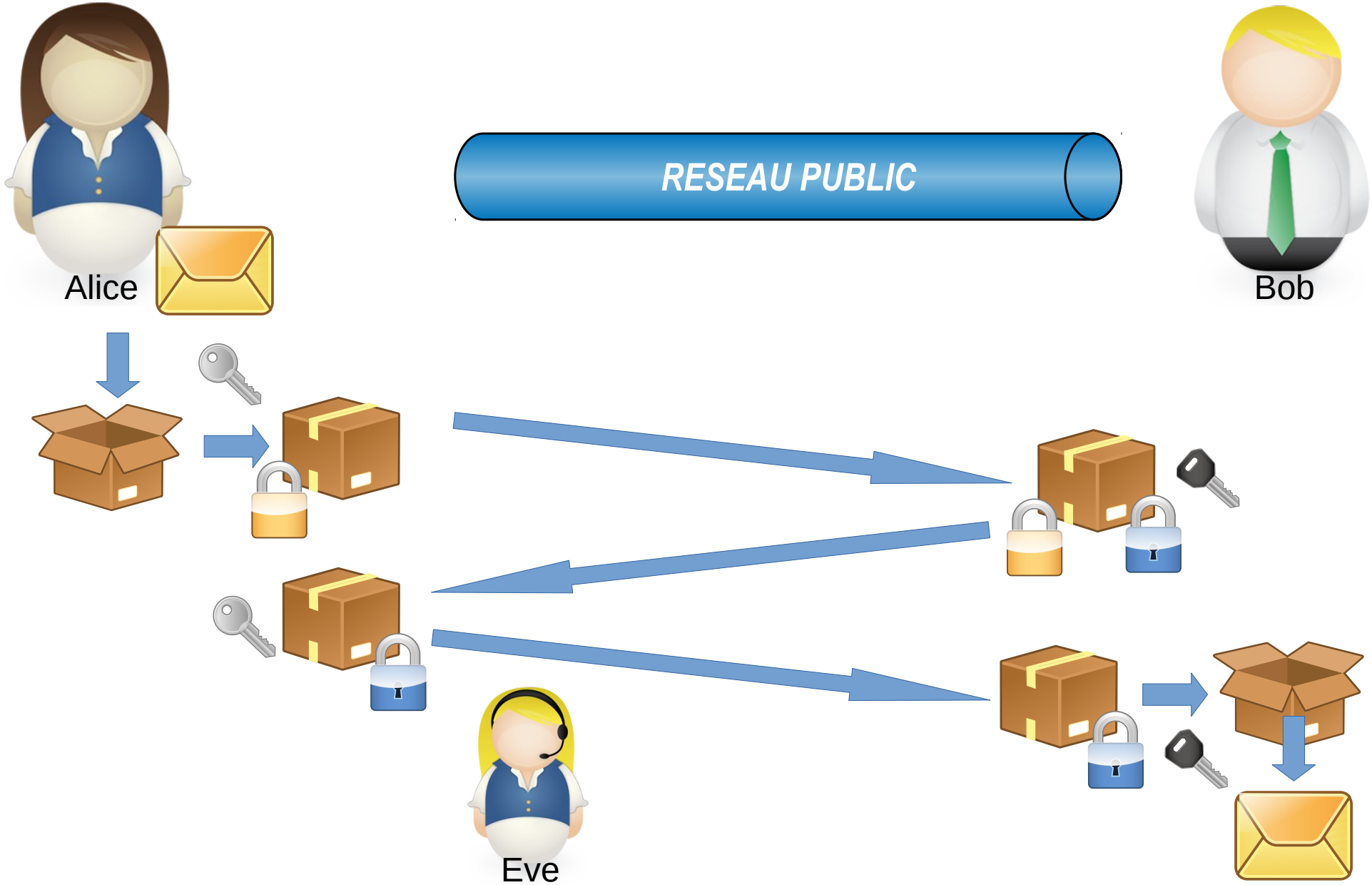
1- Le double cadenas

https://www.youtube.com/watch?v=U62S8SchxX4

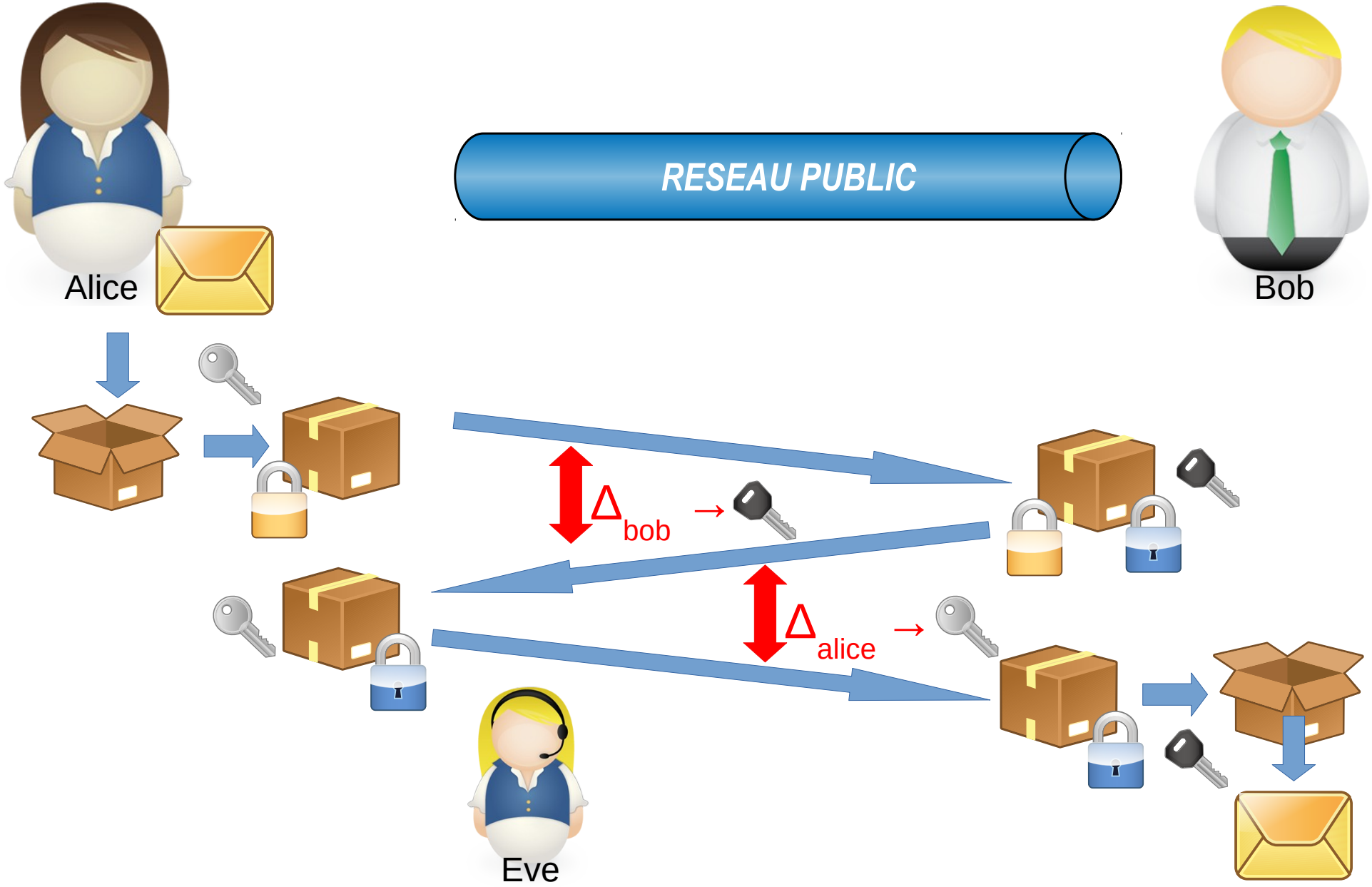
1- Le double cadenas



1- Le double cadenas

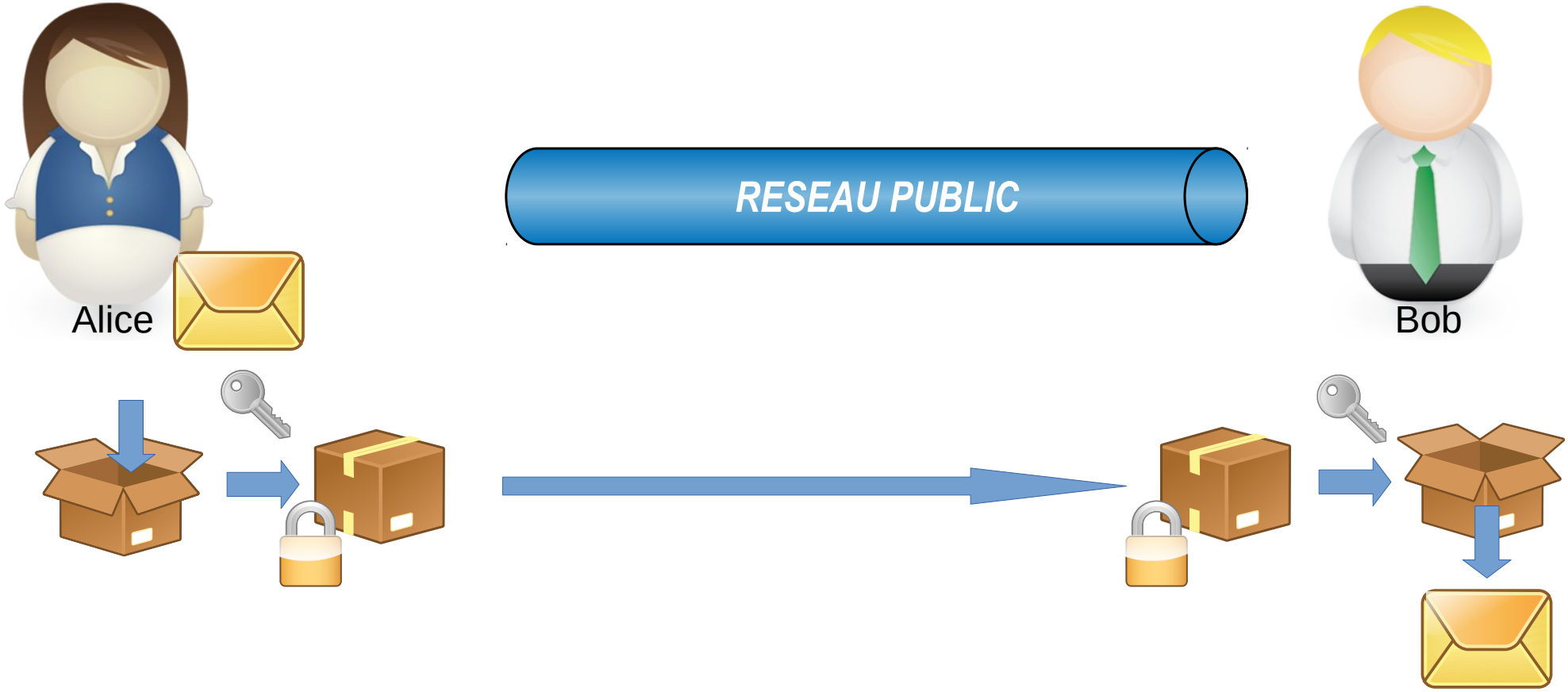


1- Le double cadenas



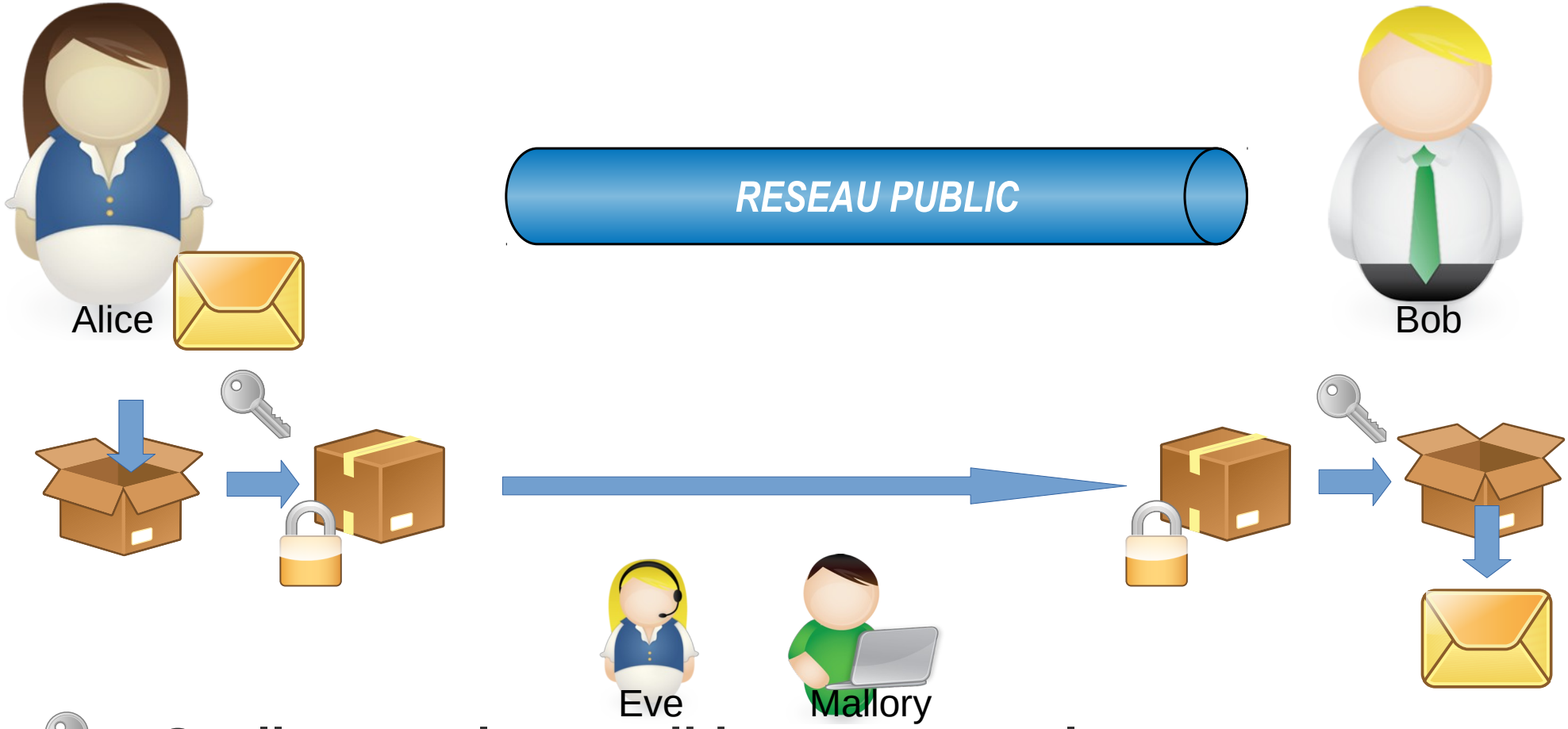
Sommaire

2- Le masque jetable



Alice et Bob se mettent d'accord sur une clé aléatoire.

2- Le masque jetable



Quelles sont les conditions pour que le message soit transmis de manière sécurisée ?

2- Le masque jetable

Conditions nécessaires pour assurer la confidentialité du message

- La clé n’est pas prévisible.
- La clé n’est pas réutilisée.
- Seuls Alice et Bob ont la clé.

2- Le masque jetable

Conditions nécessaires pour assurer la confidentialité du message

- Le masque est vraiment aléatoire.
- La longueur du masque est supérieure à la longueur du message.
- Alice et Bob se sont échangés la clé
  - avant la transmission,
  - sans que la clé ne soit compromise.

2- Le masque jetable

- C ?
- I ?
- D ?
- T/P/NR ?

2- Le masque jetable

Exemple d'algorithme

AES Advanced Encryption Standard (2001)
Accéléré par le jeu d'instructions AES-NI (2008)

Classe générale

Chiffrement symétrique
il y a une seule clé, utilisable aussi bien pour

- **chiffrer le message**
- **déchiffrer le message**

2- Le masque jetable

Exemple d’usage

Mot de passe sur une archive

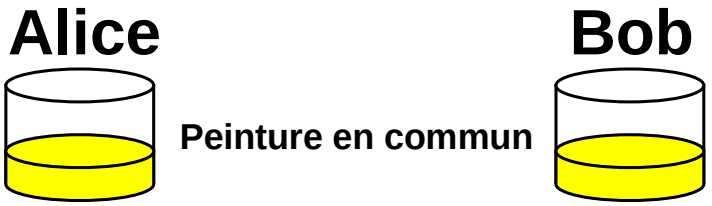
2- Le masque jetable

Nouvel enjeu

Comment Alice et Bob peuvent-ils se mettre d’accord sur une clé secrète partagée, sans se rencontrer ?

Sommaire

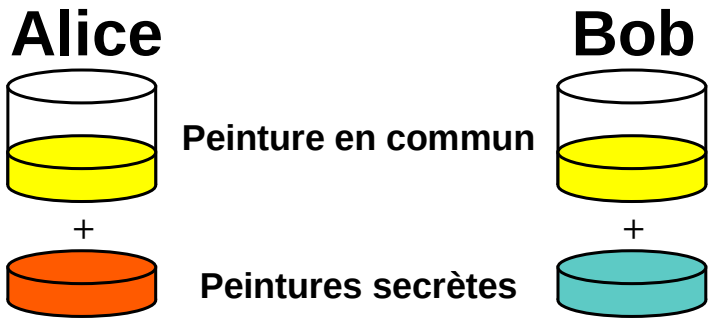
Principe d’échange de clés Diffie-Hellman (1976)



Eve peut connaître la peinture en commun...

https://fr.wikipedia.org/wiki/%C3%89change_de_cl%C3%A9s_Diffie-Hellman

Principe d'échange de clés Diffie-Hellman (1976)



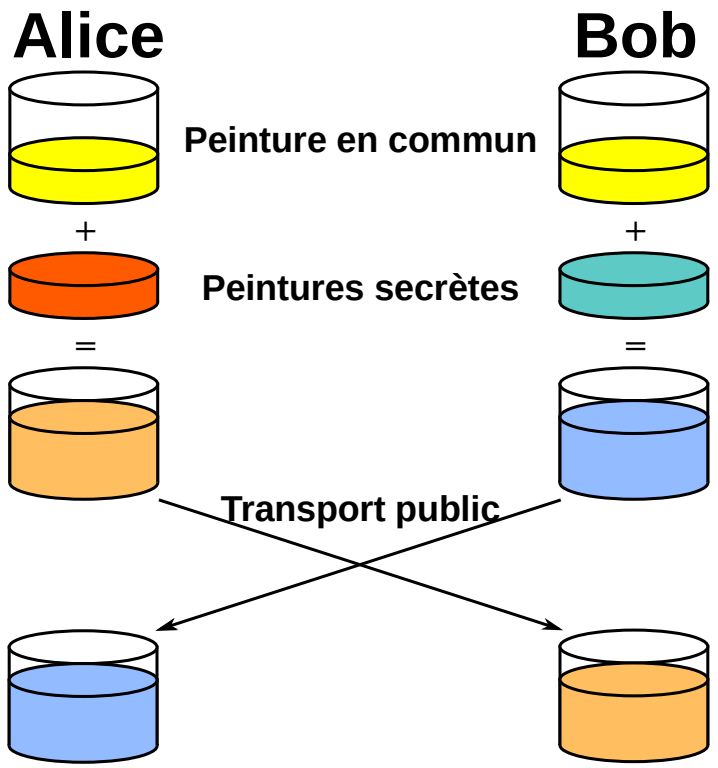
Les peintures secrètes ne sont jamais transmises

Eve peut connaître la peinture en commun...

… mais sans accès, **Eve** ne connaît pas les peintures secrètes.

https://fr.wikipedia.org/wiki/%C3%89change_de_cl%C3%A9s_Diffie-Hellman

Principe d'échange de clés Diffie-Hellman (1976)



Les peintures secrètes ne sont jamais transmises (sans être mélangées à une autre peinture).

Eve regarde et voit les mélanges...

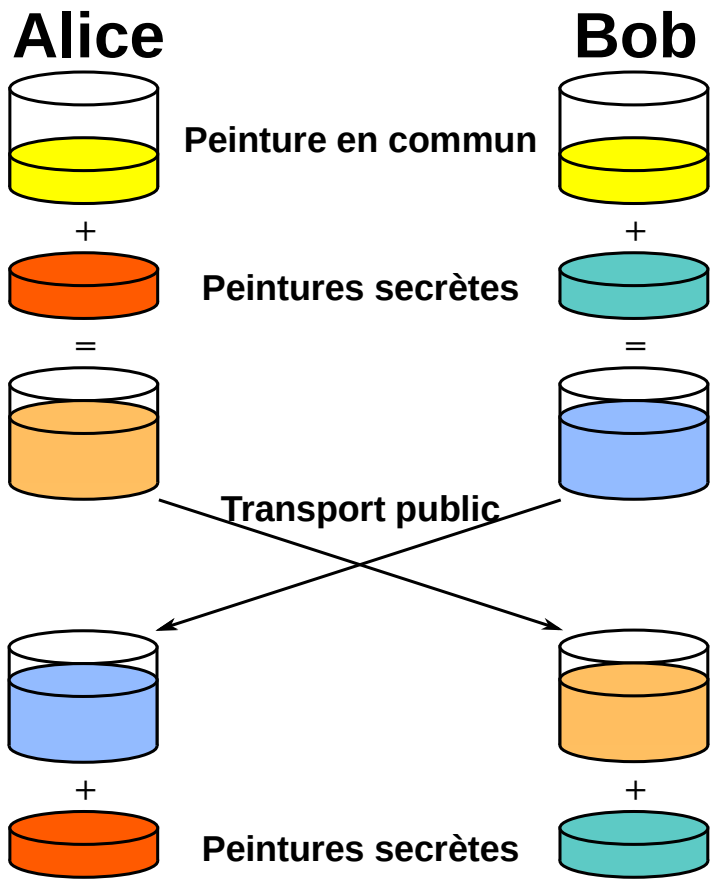
Eve peut connaître la peinture en commun...

… mais sans accès, **Eve** ne connaît pas les peintures secrètes.

On suppose que l'opération de séparation des composants du mélange est très longue.

https://fr.wikipedia.org/wiki/%C3%89change_de_cl%C3%A9s_Diffie-Hellman

Principe d'échange de clés Diffie-Hellman (1976)



Les peintures secrètes ne sont jamais transmises (sans être mélangées à une autre peinture).

Eve regarde et voit les mélanges...

et malgré cela...

Eve peut connaître la peinture en commun...

… mais sans accès, **Eve** ne connaît pas les peintures secrètes.

On suppose que l'opération de séparation des composants du mélange est très longue.

https://fr.wikipedia.org/wiki/%C3%89change_de_cl%C3%A9s_Diffie-Hellman

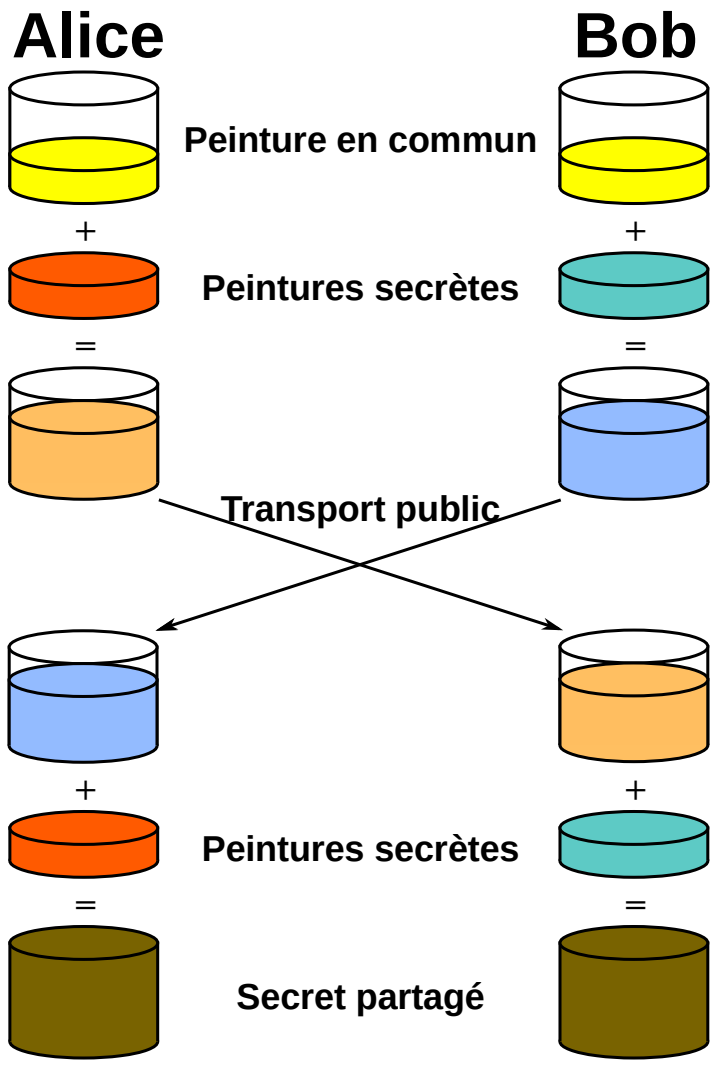
Principe d'échange de clés Diffie-Hellman (1976)

Les peintures secrètes ne sont jamais transmises (sans être mélangées à une autre peinture).

Eve regarde et voit les mélanges...

et malgré cela...

Eve ne connaît pas le secret partagé.



Eve peut connaître la peinture en commun...

… mais sans accès, **Eve** ne connaît pas les peintures secrètes.

On suppose que l'opération de séparation des composants du mélange est très longue.

Peu importe son contenu du mélange tant qu'il est **secret** et **partagé** !

https://fr.wikipedia.org/wiki/%C3%89change_de_cl%C3%A9s_Diffie-Hellman

Principe d’échange de clés Diffie-Hellman (1976)

https://youtu.be/YEBfamv-_do?t=138

Principe d’échange de clés Diffie-Hellman (1976)

- **Mallory peut interférer**
- en modifiant le contenu des échanges
- pour connaître lui aussi la clé

→ Attaque de l’homme du milieu (MITM)

Sommaire

Rivest-Shamir-Adleman (1977)

	Clé publique de Bob	Clé privée de Bob
Chiffrement	Permet à Alice de chiffrer un message destiné à Bob.	Permet à Bob de déchiffrer le message qui lui est destiné.

Rivest-Shamir-Adleman (1977)

	Clé publique de Bob	Clé privée de Bob
Chiffrement	Permet à Alice de chiffrer un message destiné à Bob.	Permet à Bob de déchiffrer le message qui lui est destiné.

	Clé publique d'Alice	Clé privée d'Alice
Signature	Permet à Bob de s'assurer que le message d'Alice n'a pas été modifié. Permet à Bob de prouver que le message a été envoyé par Alice.	Permet à Alice de signer le message.

Rivest-Shamir-Adleman (1977)

Utilité des signatures

Clé publique : Chiffrer, vérifier l'intégrité / prouver

Clé privée : Déchiffrer, signer

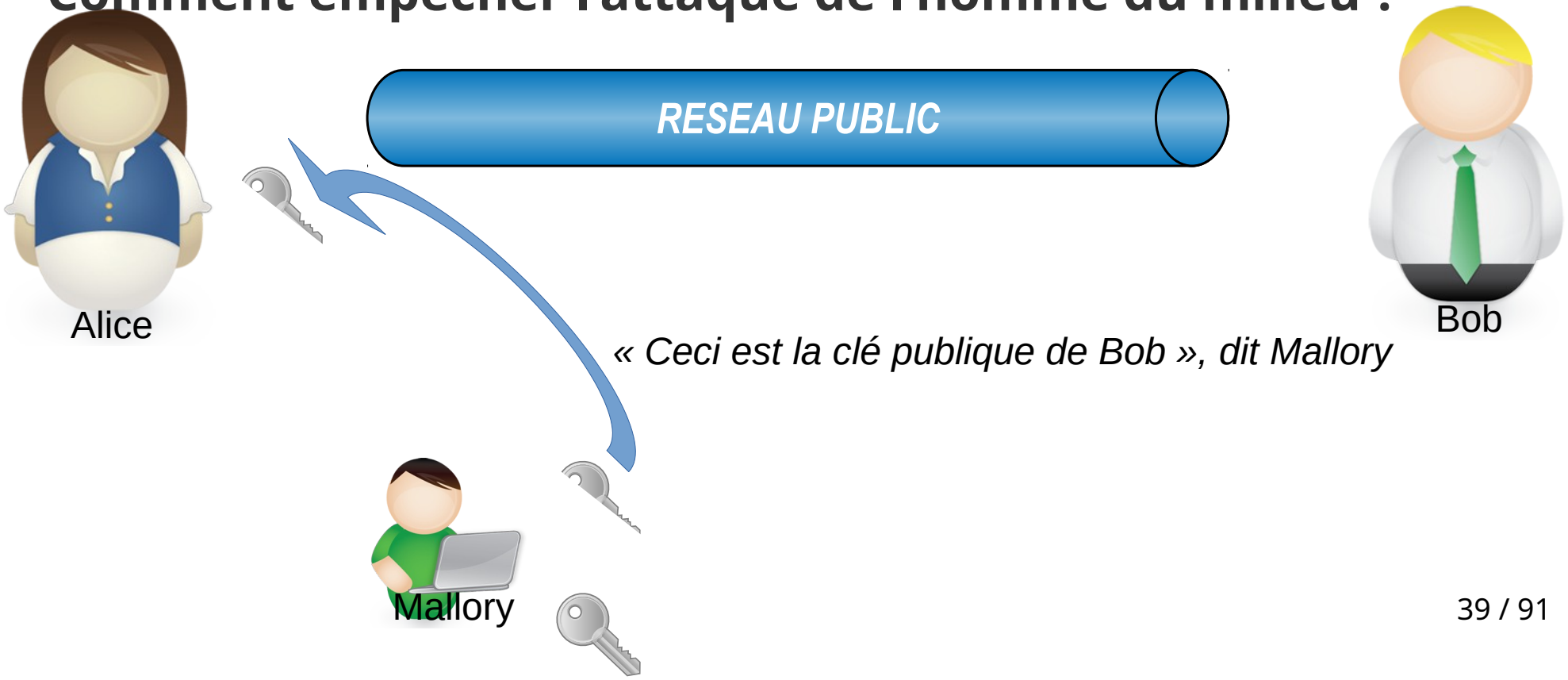
Principe fondamental d'utilisation

La clé privée n'est jamais transmise.

Rivest-Shamir-Adleman (1977)

Nouvel enjeu

Comment empêcher l'attaque de l'homme du milieu ?



Sommaire

Empreinte numérique

Empreinte numérique

Un algorithme d'empreinte numérique est une fonction arithmétique.

Tout fichier peut s'exprimer sous la forme d'un entier

- **(très) grand**
- **représenté sous forme binaire**

On définit une fonction *h(m)* **pour tout entier naturel** *m*

h(m) **est dans un intervalle donné** *[0 ; n]*

Empreinte numérique

Un algorithme d'empreinte numérique est une fonction arithmétique.

Tout message *m* (fichier…)
a une image *h(m)* « facilement » calculable.

Toute valeur dans l'intervalle *[0 ; n]*
a un nombre indéfini (potentiellement infini)
d'antécédents par cette fonction *h*

Ces antécédents s'appellent aussi « préimages ».

Empreinte numérique

Exemple : fonction « Taille du fichier »

Chaque fichier a une taille, facilement calculable.

Toute valeur de taille *t(m)* peut correspondre à un grand nombre de fichiers.

Pour une taille donnée, tout fichier ayant cette taille peut être désigné comme une préimage.

Empreinte numérique « de qualité »

Qualités attendues

+ Forte résistance à l'attaque de première préimage

Difficulté à déterminer *m* ***à partir de*** *h(m)*

+ Forte résistance à l'attaque de seconde préimage

Difficulté de créer <u>volontairement</u> *m'* **tq** *h(m') = h(m)*

+ Faible probabilité de collision

Improbabilité de « tomber <u>fortuitement</u> »

sur *m1* ***et*** *m2* ***tels que*** *m1 ≠ m2* ***et*** *h(m1) = h(m2)*

Empreinte cryptographique

Qualité supplémentaire requise

+ « Strict Avalanche Criterion »

Le plus petit changement dans un fichier
doit entraîner un changement dans son empreinte
avec une probabilité de 0,5 à chaque bit.

Empreinte cryptographique

Qualité supplémentaire requise

+ « Strict Avalanche Criterion »

Le changement de n’importe quel bit dans un fichier doit entraîner un changement dans son empreinte avec une probabilité de 0,5 à chaque bit.

Empreinte cryptographique

Qualité supplémentaire requise

+ « Strict Avalanche Criterion »

Le changement de n’importe quel bit dans un fichier doit totalement bouleverser l’empreinte du fichier, sur toute sa longueur.

Empreinte cryptographique

Qualités strictement requises

+ Forte résistance à l'attaque de première préimage

+ Forte résistance à l'attaque de seconde préimage

+ Improbabilité de collision

+ « Strict Avalanche Criterion »

Empreinte cryptographique

Exemples d'algorithmes d'empreinte

- Non-cryptographique
  - CRC32

- Obsolète en cryptographie
  - MD5 (Rivest, 1991)

- Considérés comme sûrs en 2023
  - Secure Hash Algorithm 2 (SHA-2)
  - d'une longueur suffisante (*SHA-256 et plus)*

Empreinte cryptographique

Synonymes

Empreinte cryptographique

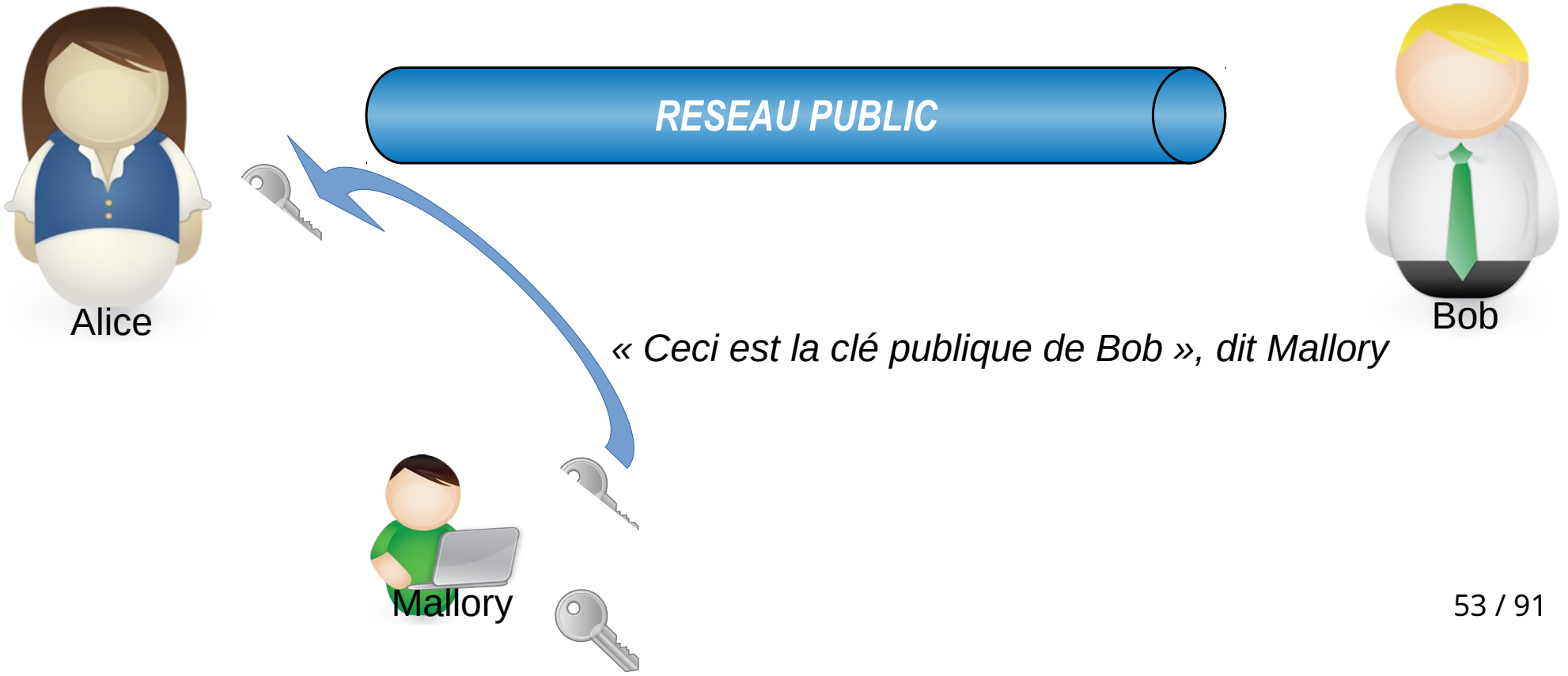
= *hash*, *message digest*, *digest*

= *condensat*

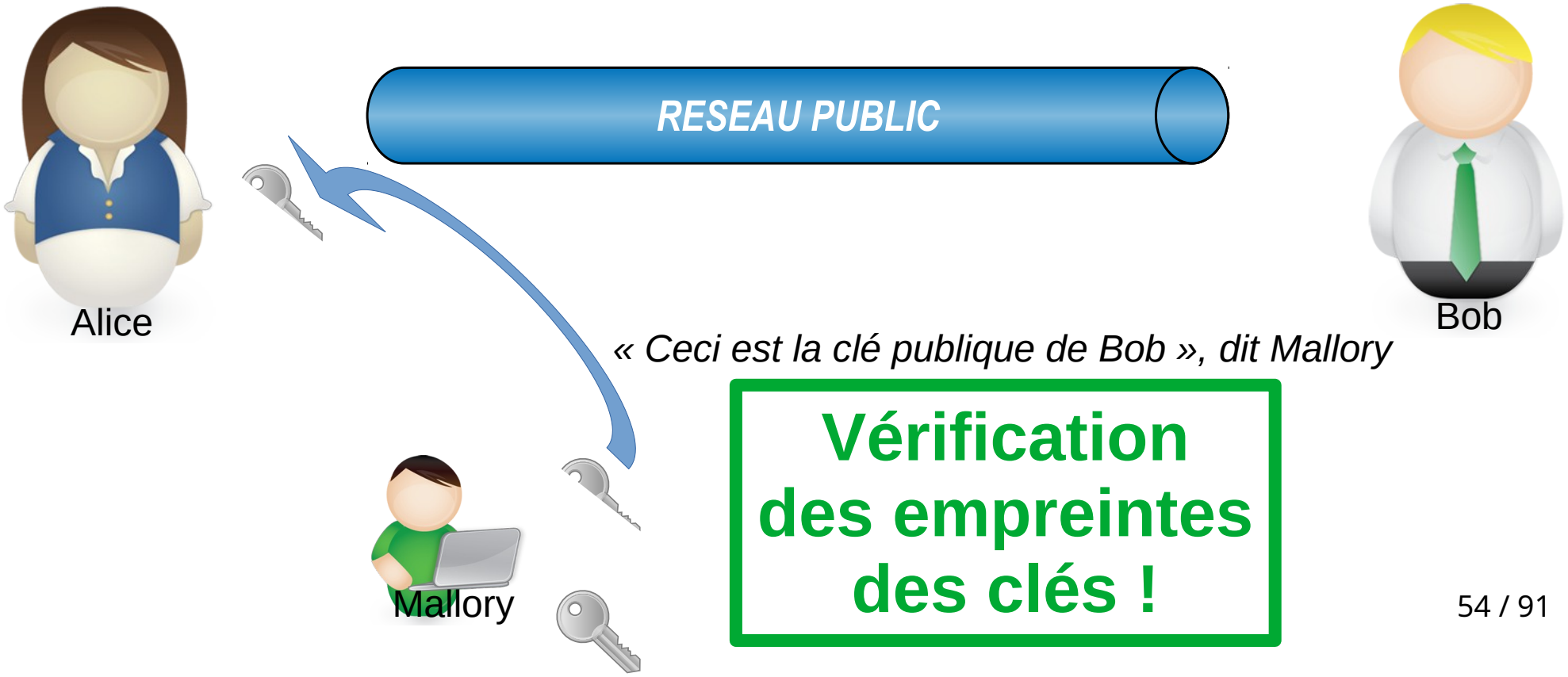
≠signature

Sommaire

Enjeu : éviter l'attaque de l'homme du milieu



Enjeu : éviter l'attaque de l'homme du milieu



Vérification des empreintes des clés !

Enjeu : éviter l'attaque de l'homme du milieu

Clé publique d'Alice
Informations
- **adresse mail d'Alice**
- **date de création du certificat**

Enjeu : éviter l'attaque de l'homme du milieu

Clé publique d'Alice
Informations
- **adresse mail d'Alice**
- **date de création du certificat**

→ **Condensat**

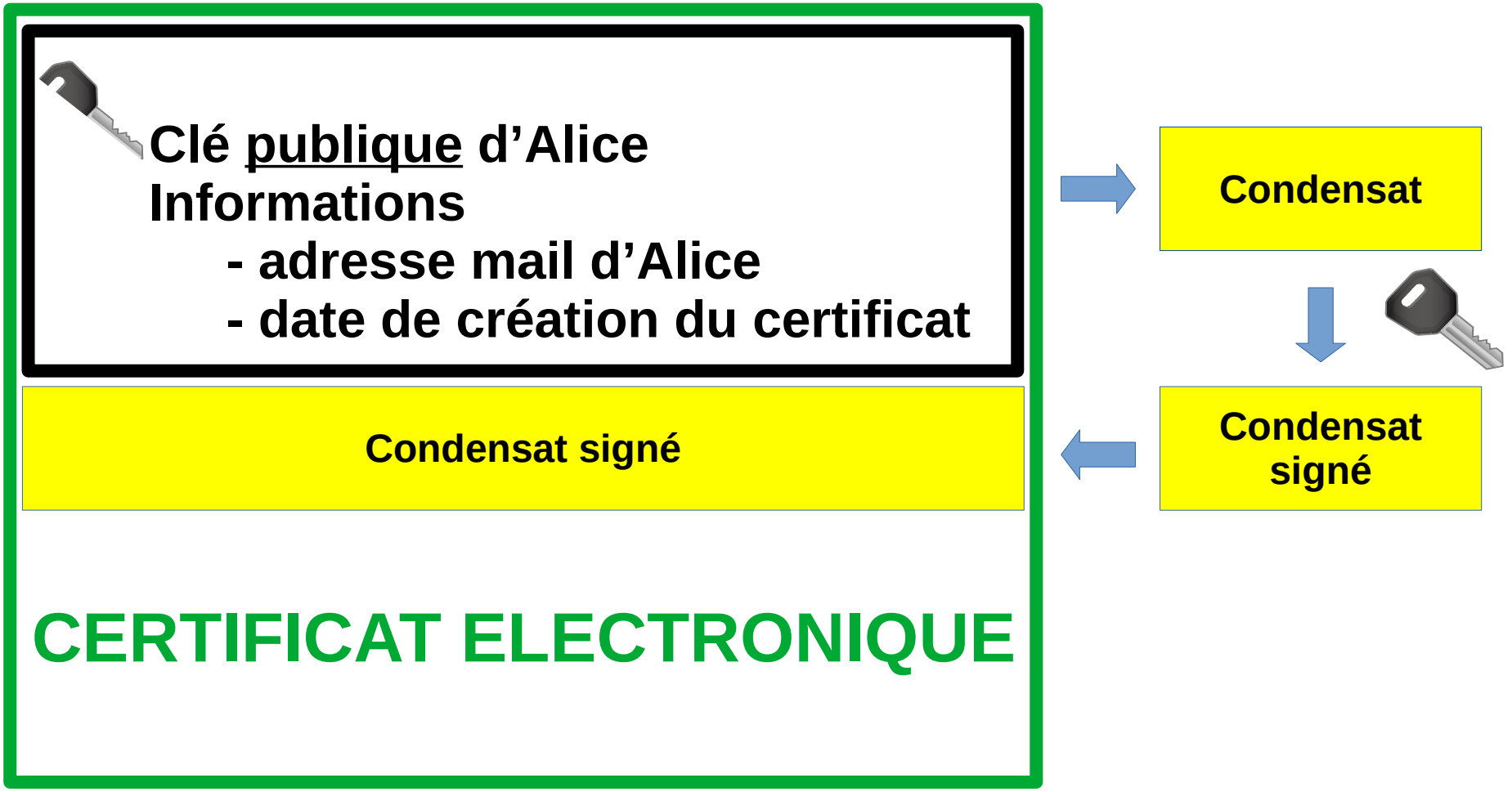
Enjeu : éviter l'attaque de l'homme du milieu

Clé publique d'Alice
Informations
- **adresse mail d'Alice**
- **date de création du certificat**

Condensat

Condensat signé

Enjeu : éviter l'attaque de l'homme du milieu



Enjeu : éviter l'attaque de l'homme du milieu

Clé <u>publique</u> d'Alice
Informations
- **adresse mail d'Alice**
- **date de création du certificat**

Condensat signé

CERTIFICAT ELECTRONIQUE AUTOSIGNE

Condensat

Condensat signé

Le certificat électronique

Contenu

- une clé publique

- des informations en rapport (*date et propriétaire*)

- une signature de l'empreinte de [la clé + les informations]

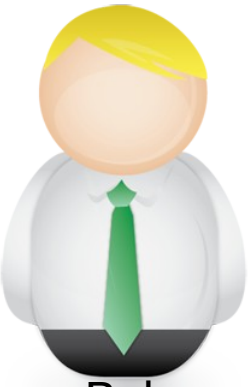
Un certificat électronique autosigné n'a pas plus de valeur qu'une clé publique !

Une contrainte courante

Alice

ne connaît pas

(ou ne l’a pas vu depuis un moment déjà)



Bob

Une opportunité courante


Alice

connaissent tous les deux


Charlie


Bob

Une opportunité courante


Alice

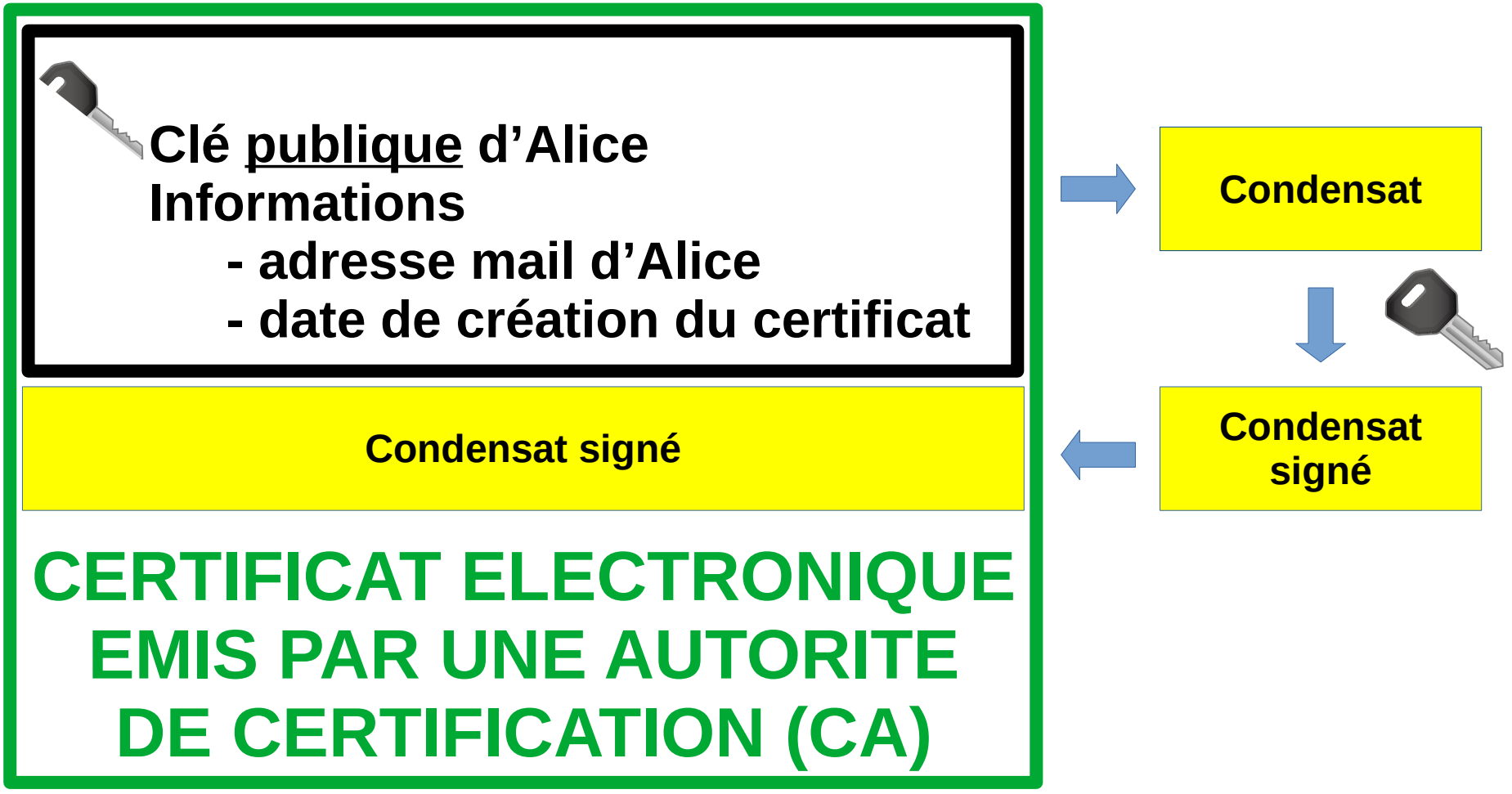
demandent tous les deux à


Bob

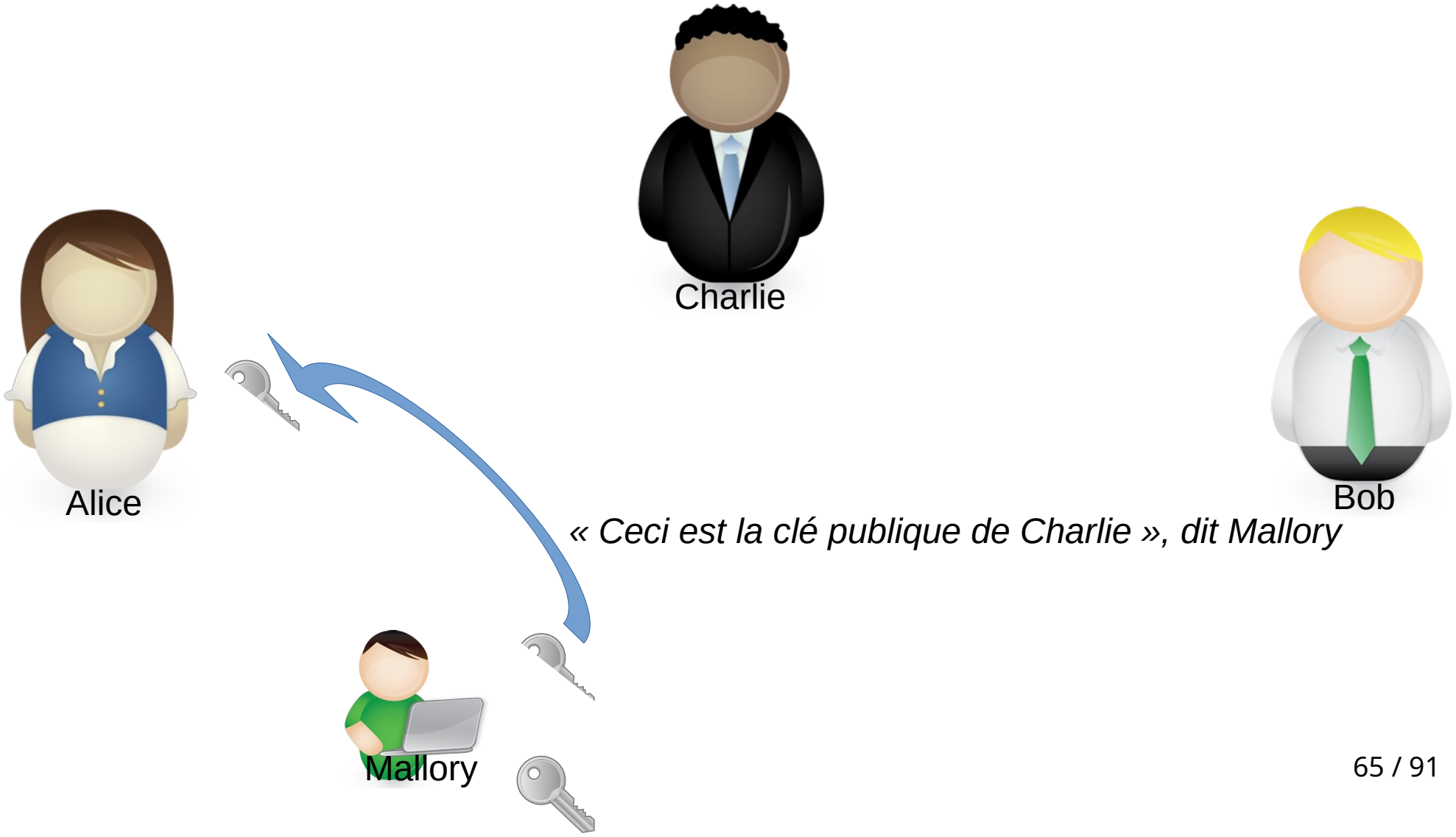

Charlie

de signer leurs certificats respectifs

Le certificat électronique



Enjeu : éviter l'attaque de l'homme du milieu



Une opportunité courante


Charlie


Alice


Bob

Tout le monde connaît

Enjeu : éviter l'attaque de l'homme du milieu

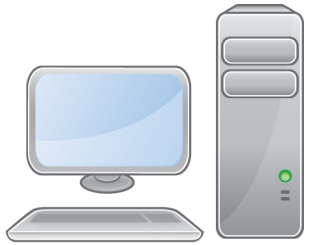
Chaîne de confiance

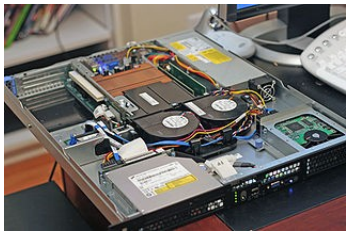
Dave signe le certificat électronique
de Charlie qui signe le certificat électronique
de Bob qui contient sa clé publique

qu'Alice peut donc vérifier avant de
chiffrer son message à destination de Bob
de même qu'elle vérifie le certificat émis par Charlie
de même qu'elle vérifie le certificat émis par Dave.

Une chaîne de confiance

Alice





Bob

Charlie
(CA de niveau 2)

GoDaddy

Dave
(CA de niveau 1)

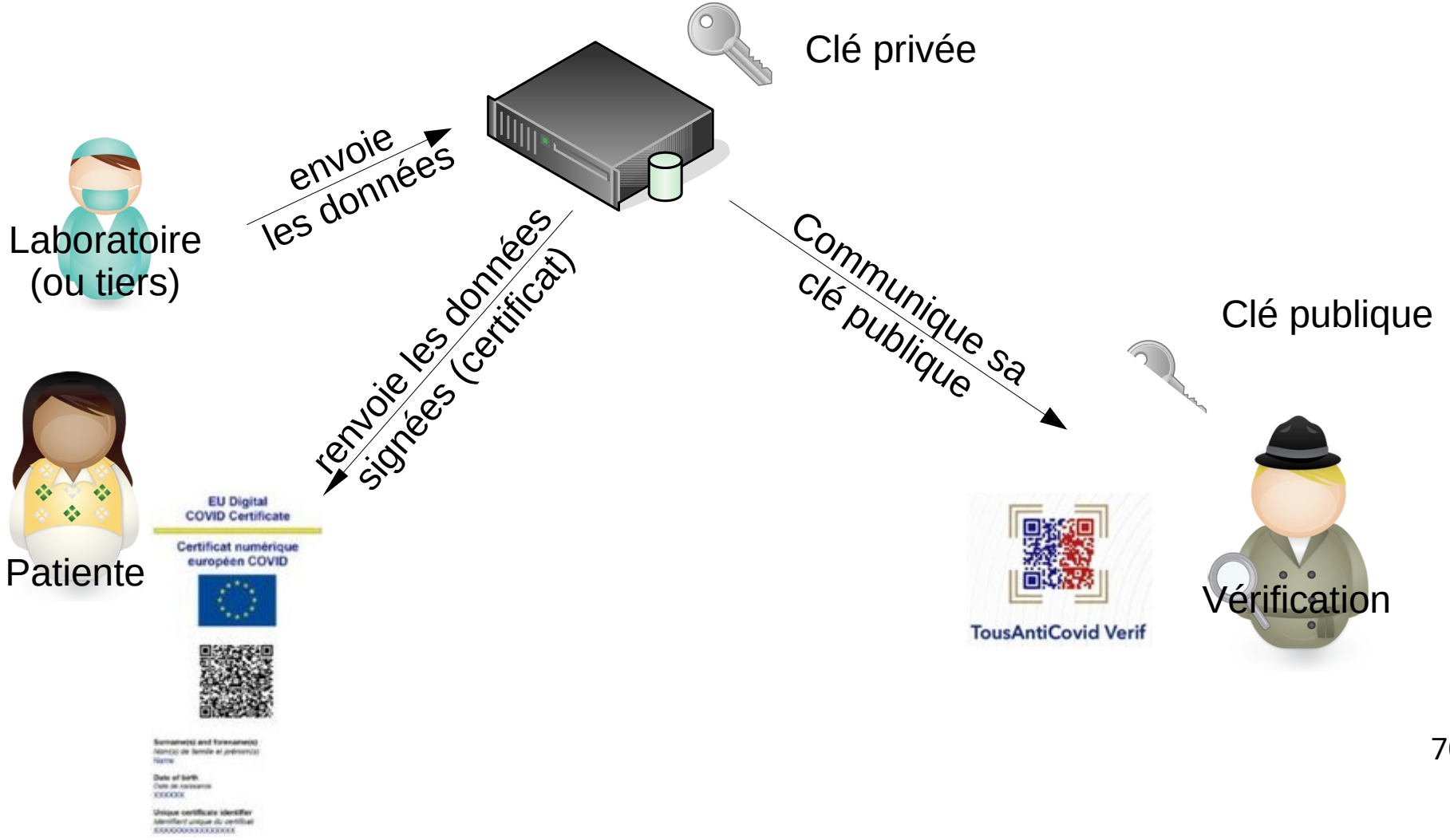
VERISIGN

Certificats racine

Une chaîne de confiance avec ses forces et faiblesses

https://cyberguerre.numerama.com/13609-des-dizaines-de-pass-sanitaires-frauduleux-generes-enquete-sur-une-gigantesque-faille-europeenne.html

Une chaîne de confiance avec ses forces et faiblesses



Une chaîne de confiance avec ses forces et faiblesses

Informations générales du certificat de signature	
Pays d'origine	(MK)
Organisation émettrice	Ministry of Health - Ministry of Health
Nom du certificat	zdravstvo.gov.mk
Certificat signé par	C=MK, ST=North Macedonia, L=Skopje, O=Ministry of Health, CN=zdravstvo.gov.mk, E=contact@zdravstvo.gov.mk
Date de début	15/09/2021

Sommaire

Tableau récapitulatif

Chiffrement	symétrique	asymétrique
Dimensions de la sécurité	C, I	C, I, T/P/NR
Nombre de clés	1	2 par acteur
Exemples d'algorithmes	AES	RSA
Temps de calcul nécessaire	x1	x1000
Logiciels	archiveurs « zip » applications bureautiques, KeePass TrueCrypt/VeraCrypt	PGP, GnuPG OpenSSL, LibreSSL OpenSSH Cartes de paiement Messagerie Olvid

Une solution optimale

Chiffrement hybride

Utiliser un chiffrement asymétrique pour transmettre une clé temporaire servant à un chiffrement symétrique.

Flexibilité, preuve et… vitesse !

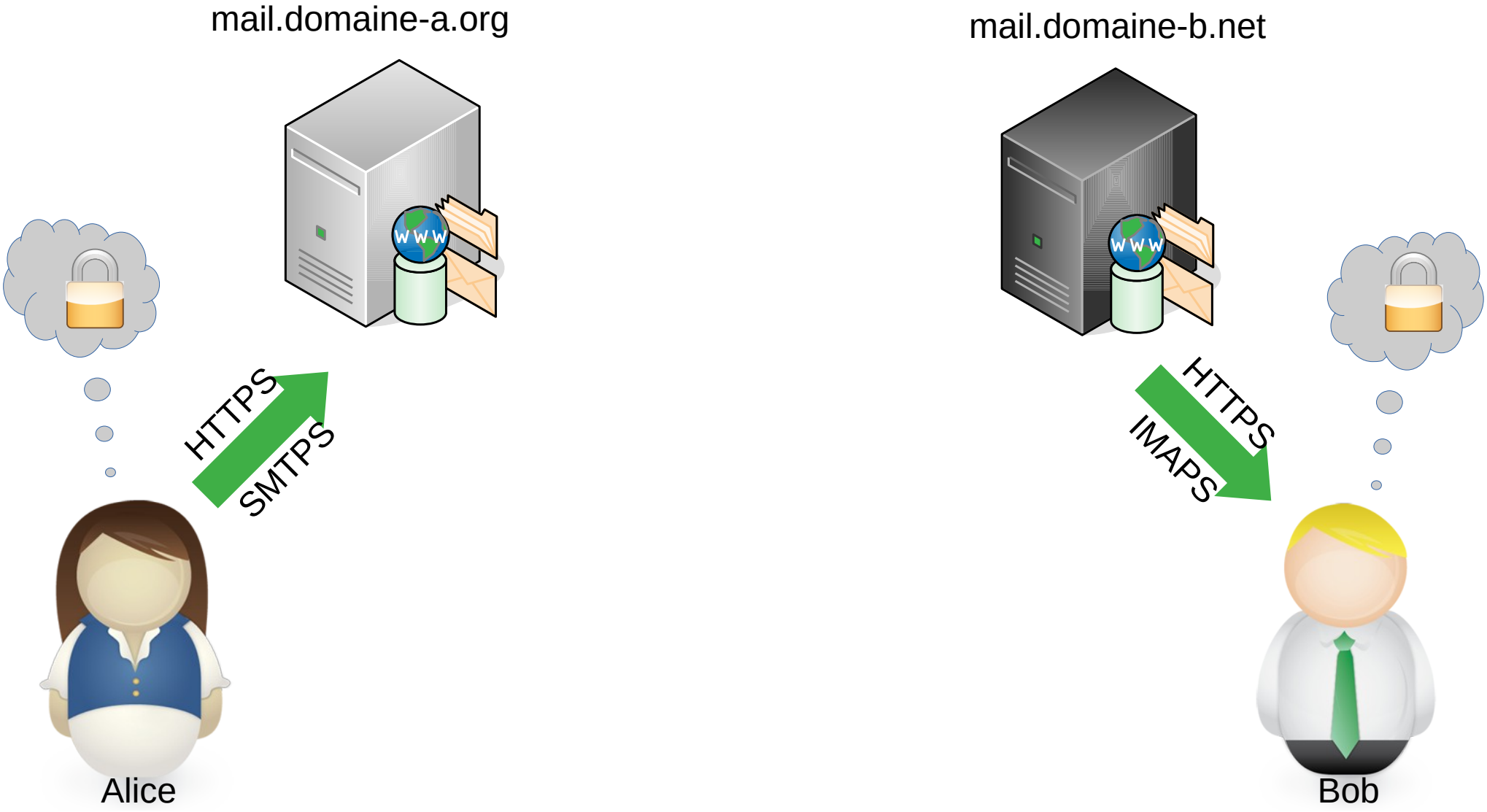
C’est la base du fonctionnement de la plupart des protocoles sur Internet.

Pause

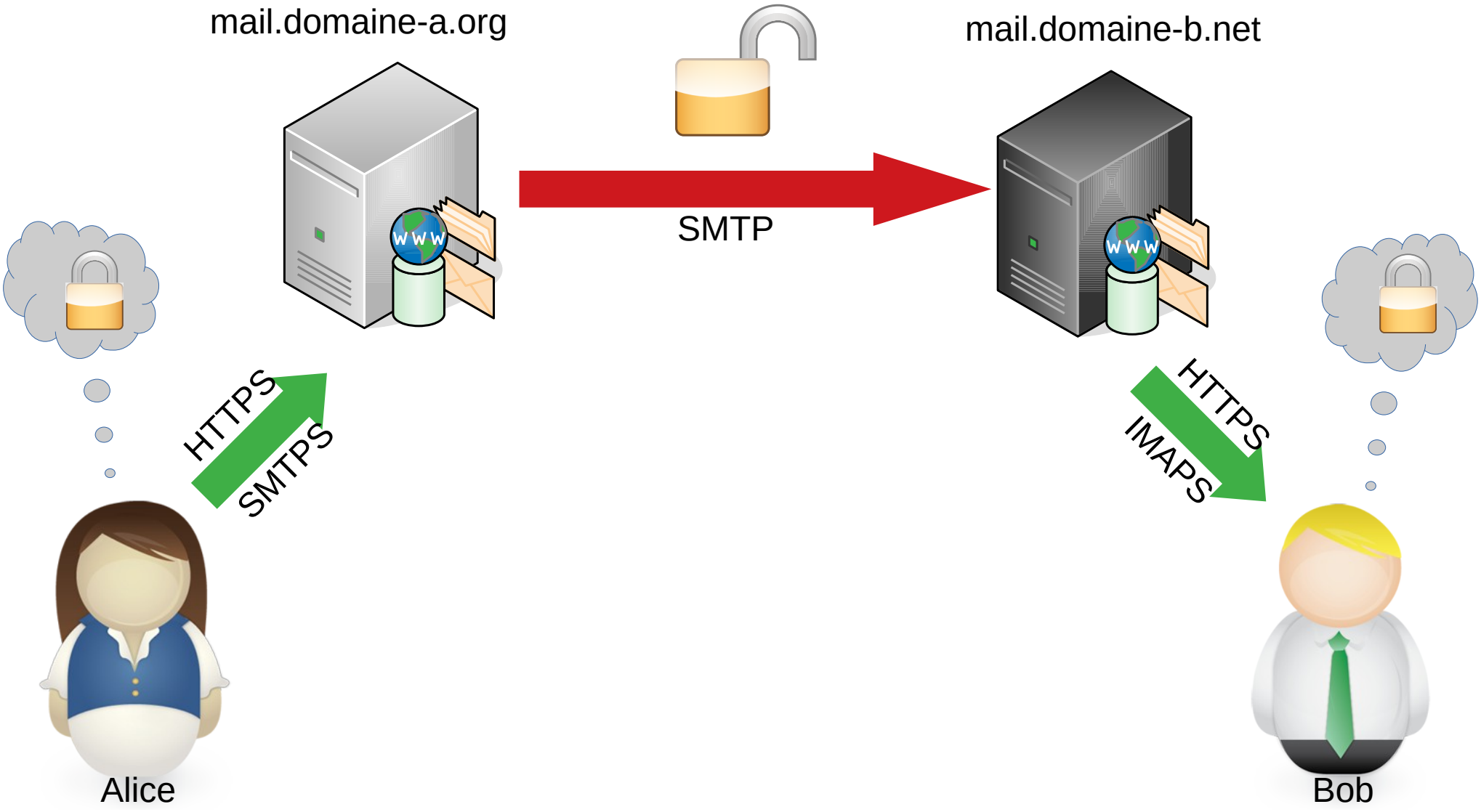
Cryptographie asymétrique avec PGP

06/02/2023

Contexte


mail.domaine-a.org
mail.domaine-b.net
HTTPS
SMTPS
HTTPS
IMAPS
Alice
Bob

Contexte


mail.domaine-a.org
mail.domaine-b.net
SMTP
HTTPS
SMTPS
HTTPS
IMAPS
Alice
Bob

Sommaire

- Contexte
- A propos de PGP
- Ressources utilisées pour la manipulation
- Gestion des clés
  - Création des clés
  - Publication et vérification des clés
- Cryptographie
  - Envoi d'un message chiffré
  - Vérification d'un message signé

A propos de PGP

- **PGP : le logiciel original (1991)**
  - **Pretty Good Privacy**
  - **Philip Zimmermann**

- **GNU Privacy Guard (GPG) :**

  une implémentation libre (1998)

- **OpenPGP : le format normalisé**

Ressources (publiques)

- Pad collaboratif **https://s.42l.fr/paf**

- Logiciel compatible OpenPGP

  `man gpg # ou sinon`

  https://aliceandbob.io > Online PGP tool

- Calcul d'empreinte cryptographique

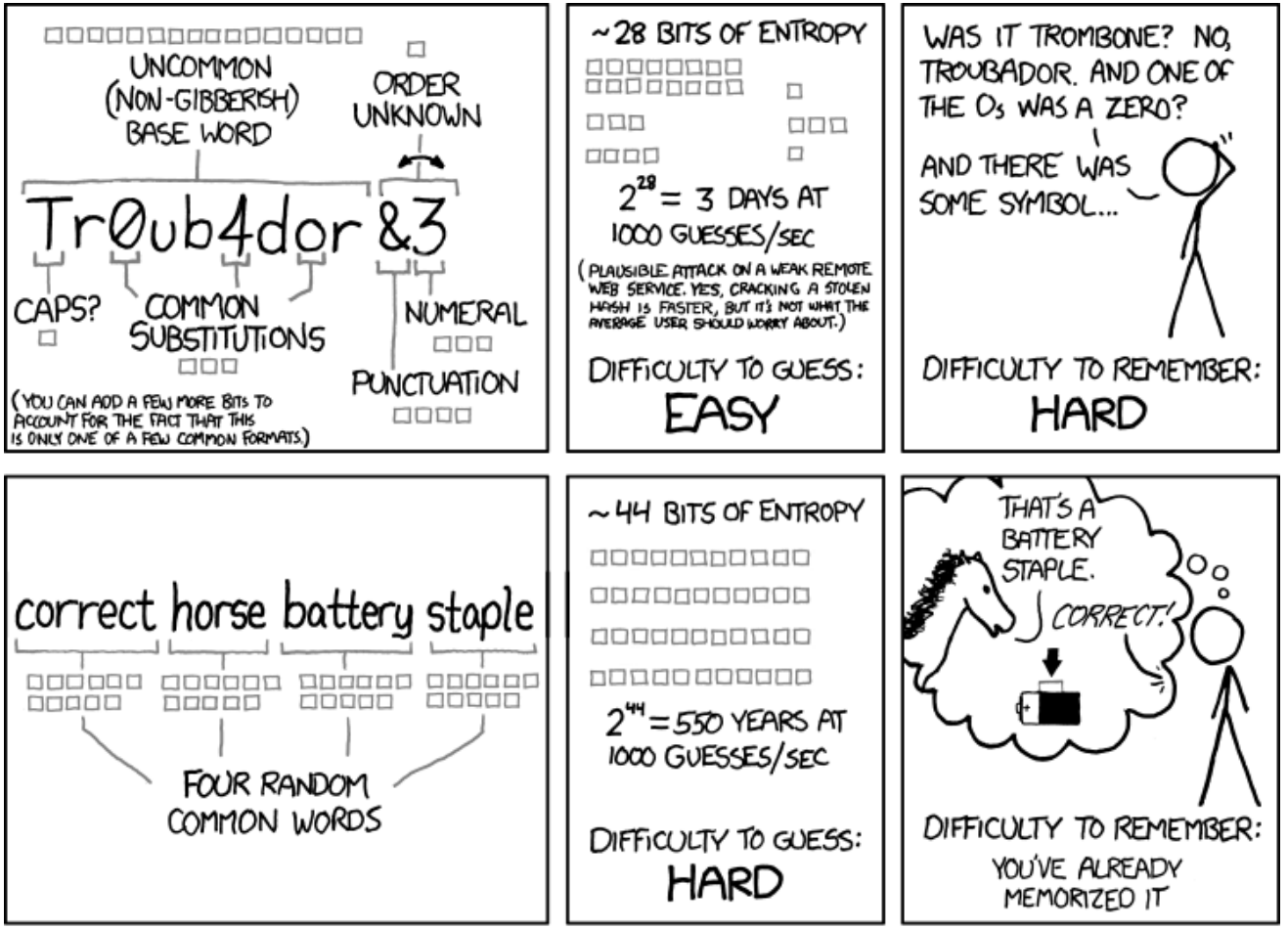
  `man sha256sum # ou` **https://www.sha256.fr/**

Gestion des clés
Création des clés

- `gpg --full-gen-key # ou`
  https://aliceandbob.io/online-pgp-tool

- **A faire** **Générer une paire de clés**
  - **Email : NN@pgp.test**
  - **Phrase de passe (robuste)**
  - **Algorithme utilisé : curve25519**

Gestion des clés
Création des clés



https://xkcd.com/936/

Gestion des clés
Publication des clés

- Pad collaboratif **https://s.42l.fr/paf**

  section A- Publication des clés

- **A faire** Poster un message

  « Je suis **NN@pgp.test** . Ma clé publique est »

- Copier-coller la clé (la bonne !)

```
gpg --export --armor NN@pgp.test > NN.pgp.test.pub
```

Gestion des clés
Vérification des clés

- **Comment vérifier l'authenticité des clés publiques postées ?**

- **A faire** **Vérifier les clés publiques de**
  - **(NN-1)@pgp.test**
  - **(NN+1)@pgp.test**

  [modulo « Nombre de participants »]

Cryptographie asymétrique
Chiffrement

- Pad collaboratif https://s.42l.fr/paf
- **A faire** Importer les clés de
  - (NN-1)@pgp.test
  - (NN+1)@pgp.test

Section B- Publication des messages

- Leur envoyer un message chiffré

  « Message de NN pour NN+1 : »

  « Message de NN pour NN+2 : »

Cryptographie asymétrique
Déchiffrement

- **Pad collaboratif** **https://s.42l.fr/paf**

- **A faire** **Déchiffrer les messages reçus**
  - ***« Message de NN-1 pour NN : »***
  - ***« Message de NN+1 pour NN : »***

Cryptographie asymétrique
Vérification

- Vérification de la signature d'un message

- Fonctionnalité non-disponible sur

  https://aliceandbob.io/online-pgp-tool

- Fonctionnalité disponible sur GnuPG

  `gpg --verify`

Cryptographie asymétrique Vérification

- Vérification des fichiers ISO

  https://www.debian.org/CD/verify

- Principe
  - Calcul d'une empreinte
  - Signature de cette empreinte

  https://cdimage.debian.org/debian-cd/current/amd64/iso-dvd/

Cryptographie asymétrique
Vérification d'une ISO

- **Il s'agit d'une mesure de réduction de risque.**
- **A faire Rédiger un scénario d'incident qui pourrait correspondre à cette mesure**

- **A faire Identifier des mesures alternatives de réduction du risque**

En ouverture

Le mystère Satoshi : enquête sur l'inventeur du bitcoin | ARTE

525 k vues • il y a 5 jours

ARTE

À l'ère d'Internet, un groupe d'informaticiens, les Cypherpunks, cherche à coder une monnaie électronique anonyme et autonome ...

Nouveau

https://www.youtube.com/watch?v=0ETcLj5jBy4