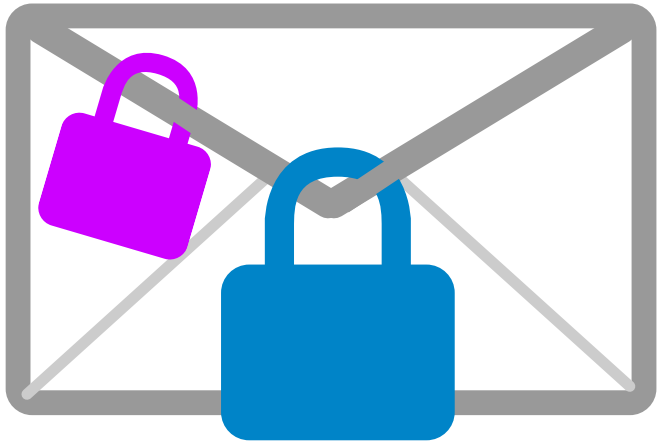
Enfin comprendre PGP !

-

Le chiffrement par clés publique et privée



D. Waiengnier – 23 / 04 / 2020
https://www.pragmasoft.be

Pragmasoft

Sécuriser ses courriels

Pourquoi sécuriser ses courriels ?

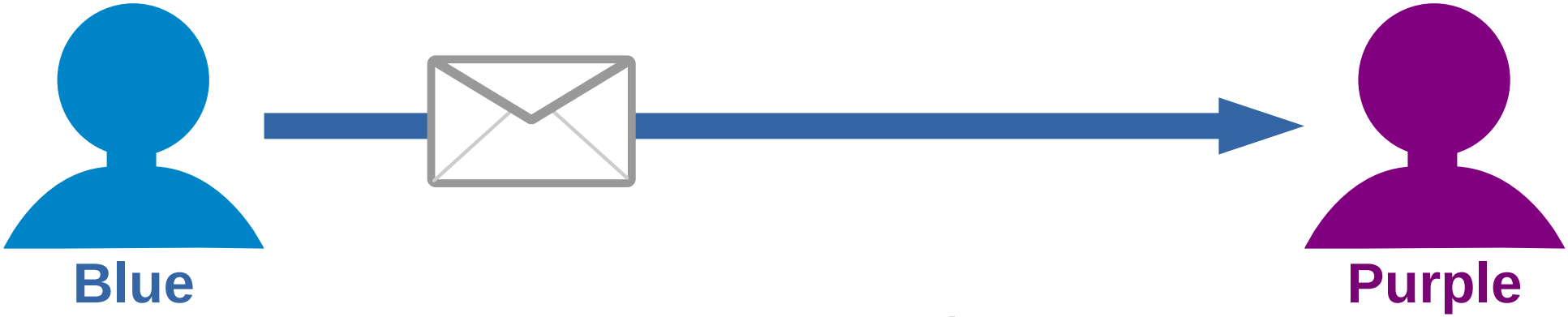
- Protéger sa **vie privée**
  - *courrier personnel, famille, amis…*

- Se protéger des **malversations**
  - *récupération commerciale, publicité, spamming...*
  - *escroqueries, abus de confiance…*
  - *pièces attachées : virus, malwares, ransomwares...*

- Se protéger du **fichage étatique**
  - *orientations philosophiques-politiques-sexuelles...*
  - *données médicales-fiscales-salariales-syndicales...*
  - *déplacements, fréquentations...*

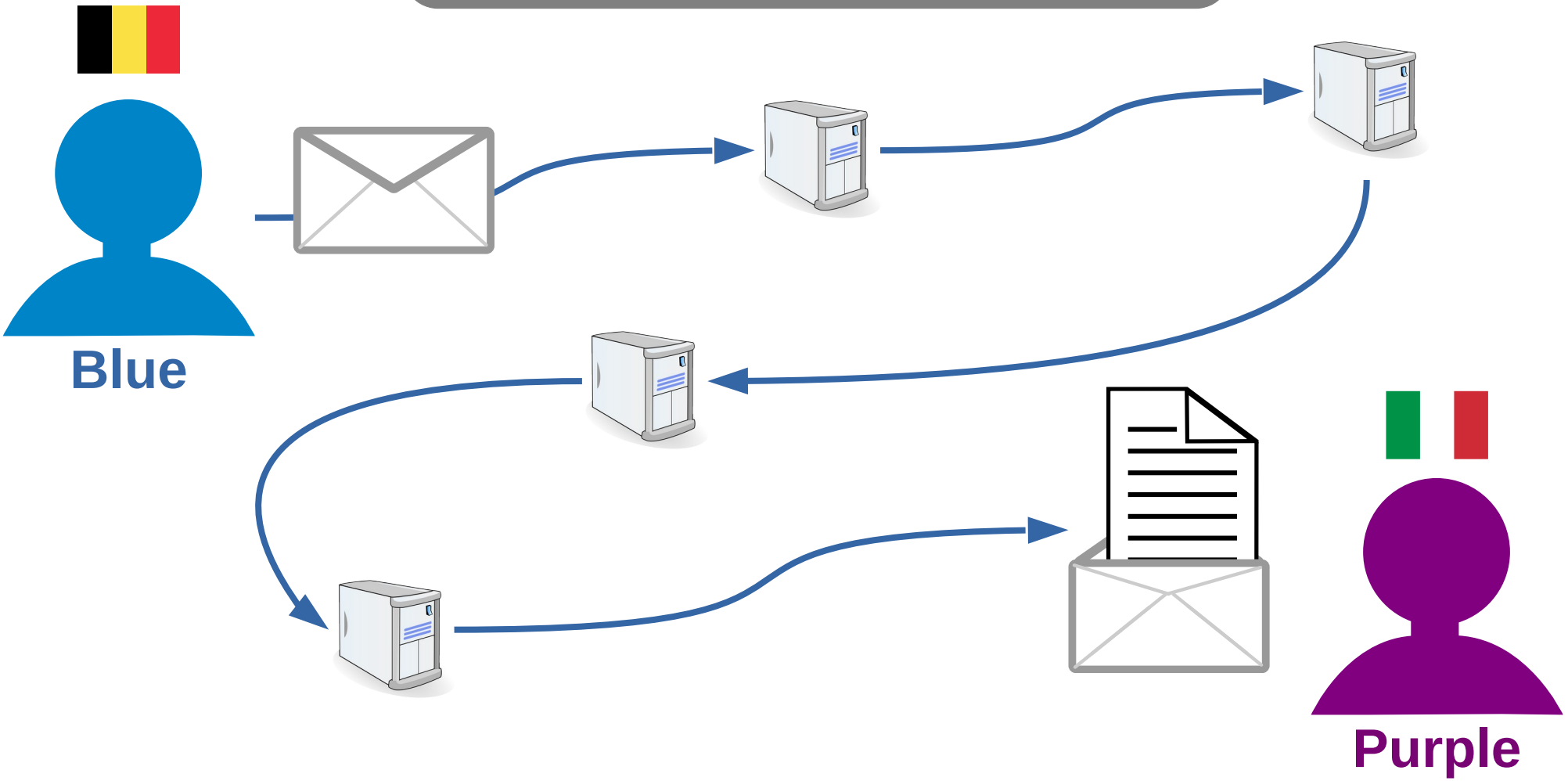
Envoi de courriel

Situation de base



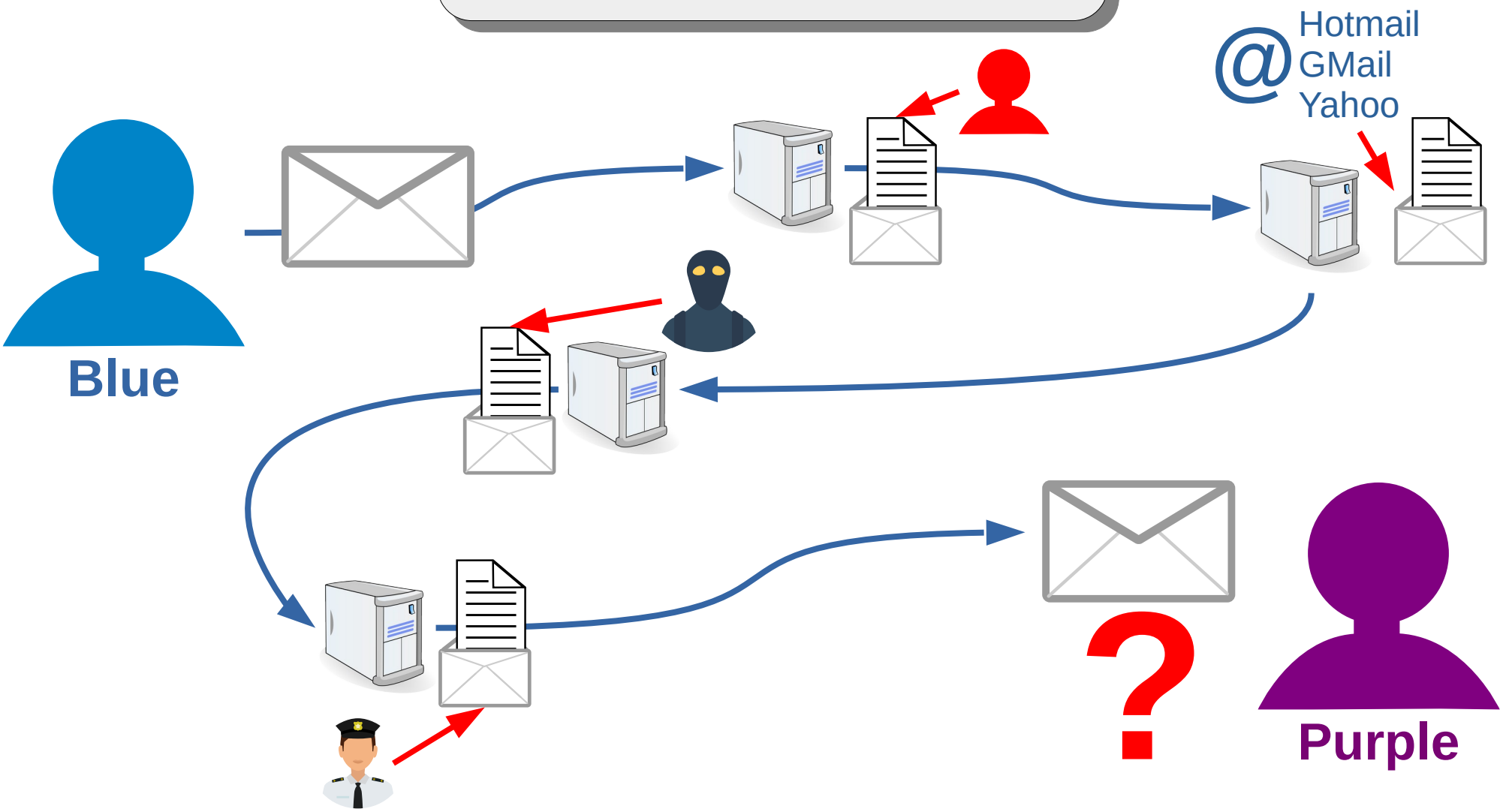
Blue envoie un **courriel** à **Purple**

Acheminement du courriel



Ce courriel va **transiter** autour du monde par
des ordinateurs particuliers : les « **serveurs de courrier** »,
destinés à acheminer les courriels à leurs destinataires.

Intégrité du courriel ?



A chaque passage d'un serveur, le courriel peut être **ouvert**, **lu**, **copié** et même **modifié par n'importe qui** !

Que faudrait-il faire pour sécuriser le courriel ?

Trois objectifs :

- [ ] **1.** Empêcher la **lecture-modification** du courriel par les intermédiaires.

- [ ] **2.** S'assurer de l'**identité** de l'émetteur du courriel.

- [ ] **3.** Solution à **distance**, sans nécessité de contact ou d'échange physique (*ex. clé USB*) entre les interlocuteurs.

Objectif 1 : empêcher la lecture du courriel

Le courriel ne peut être lu **que** par son destinataire !

La dictature parfaite serait une dictature qui aurait les apparences de la démocratie, une prison sans murs dont les prisonniers ne songeraient pas à s'évader. Un Système d'esclavage où, grâce à la consommation et au divertissement, les esclaves auraient l'amour de leur servitude ...

Aldous Huxley

Solution : rendre illisible au départ

Rendre lisible à l'arrivée

La dictature parfaite serait une dictature qui aurait les apparences de la démocratie, une prison sans murs dont les prisonniers ne songeraient pas à s'évader. Un Système d'esclavage où, grâce à la consommation et au divertissement, les esclaves auraient l'amour de leur servitude ...

Aldous Huxley

Acheminer au destinataire

Pragmasoft

L’outil ? « Pretty Good Privacy » (PGP)

PGP : logiciel de **chiffrement cryptographique**

- Ecrit et diffusé par Philip Zimmermann – 1991
- **Chiffrement – déchiffrement - signature** de données (*courriers, fichiers...*)
- **Cryptographie** asymétrique et symétrique
  - **Paire de clés** : publique - privée
  - Produit ouvert : **standard** OpenPGP (RFC 48803)

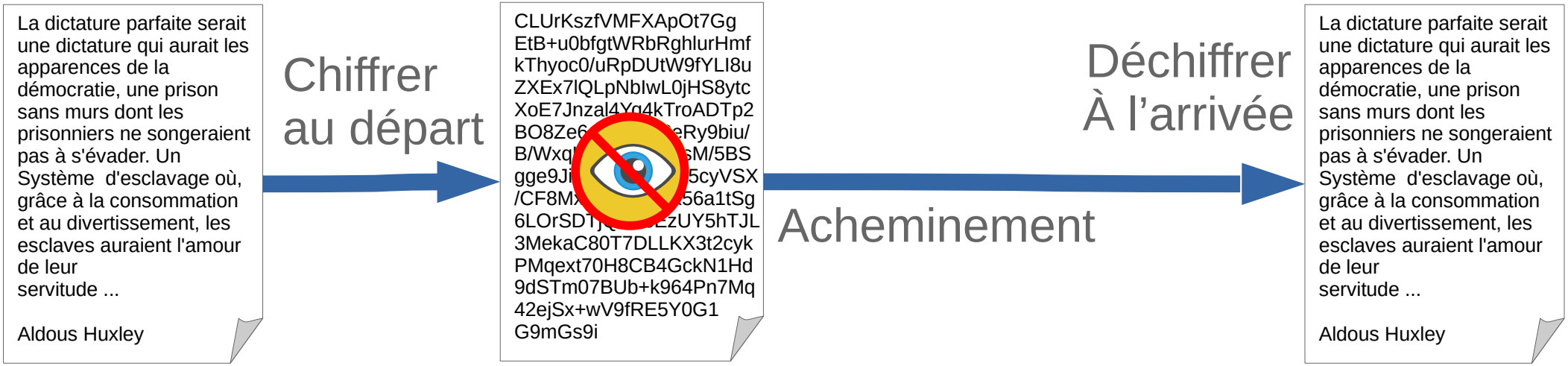
PGP®

GnuPG

Chiffrer...

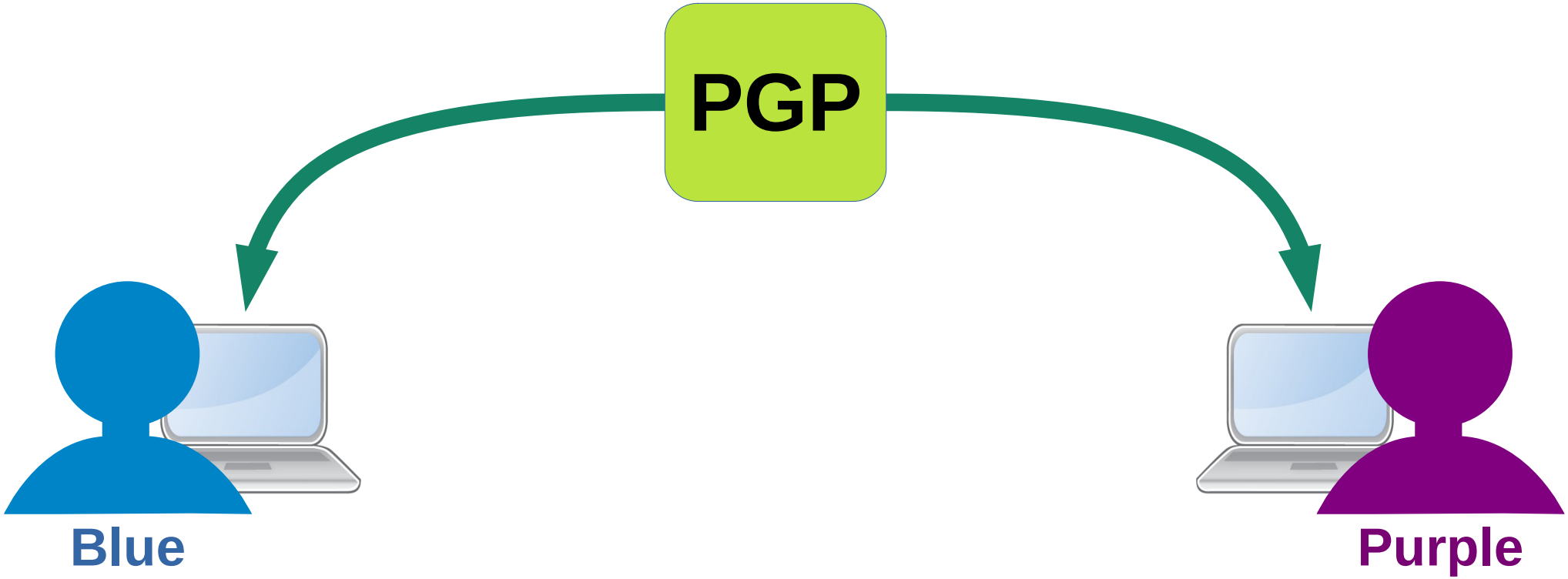
Rendre illisible s'appelle « **chiffrer** »

- Effectué par **PGP** avec des algorithmes mathématiques
- Avec des **clés** (= des morceaux d'algorithmes)



Mise en œuvre (1) : installer PGP

Blue et **Purple** installent tous deux **PGP** sur leur ordinateur



Mise en œuvre (2) : créer une paire de clés

Purple génère **2 clés personnelles** avec PGP

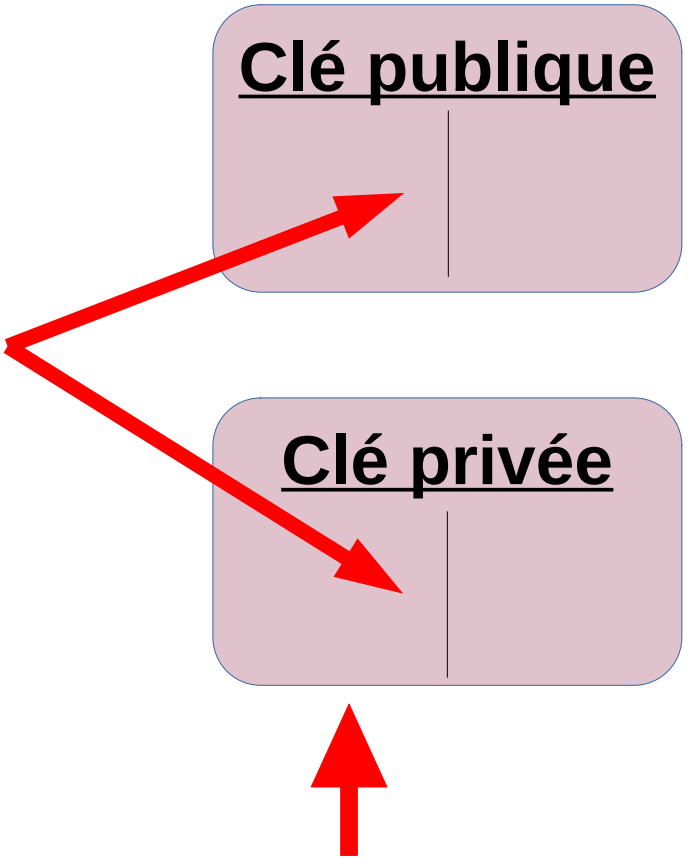
*Ces termes de « **clé publique** » et de « **clé privée** » prêtent à confusion pour bon nombre d'utilisateurs !*

*La page suivante va vous proposer une représentation **plus didactique**.*

Les clés : des « boîtiers »

On va considérer ces clés comme des « **boîtiers** »

*Chaque boîtier contient **2 compartiments** séparés ici par une **ligne verticale**.*



*Commençons par les compartiments de **gauche***

Contenu des 2 « boîtiers »

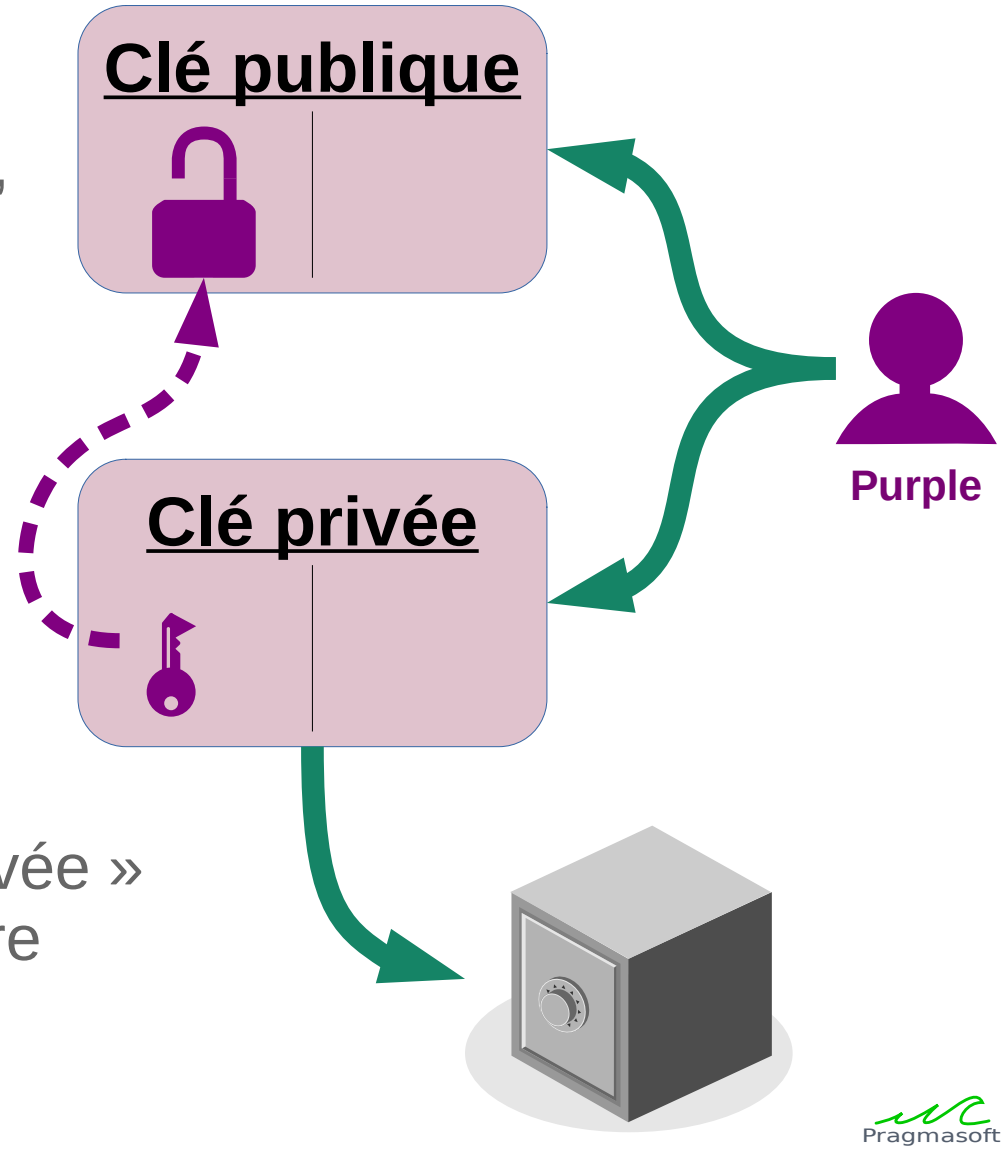
Le boîtier « **clé publique** »

- Il contient un « **cadenas ouvert** », prêt à être fermé.

Le boîtier « **clé privée** »

- Il contient la **clé du cadenas** contenu dans la « clé publique » !

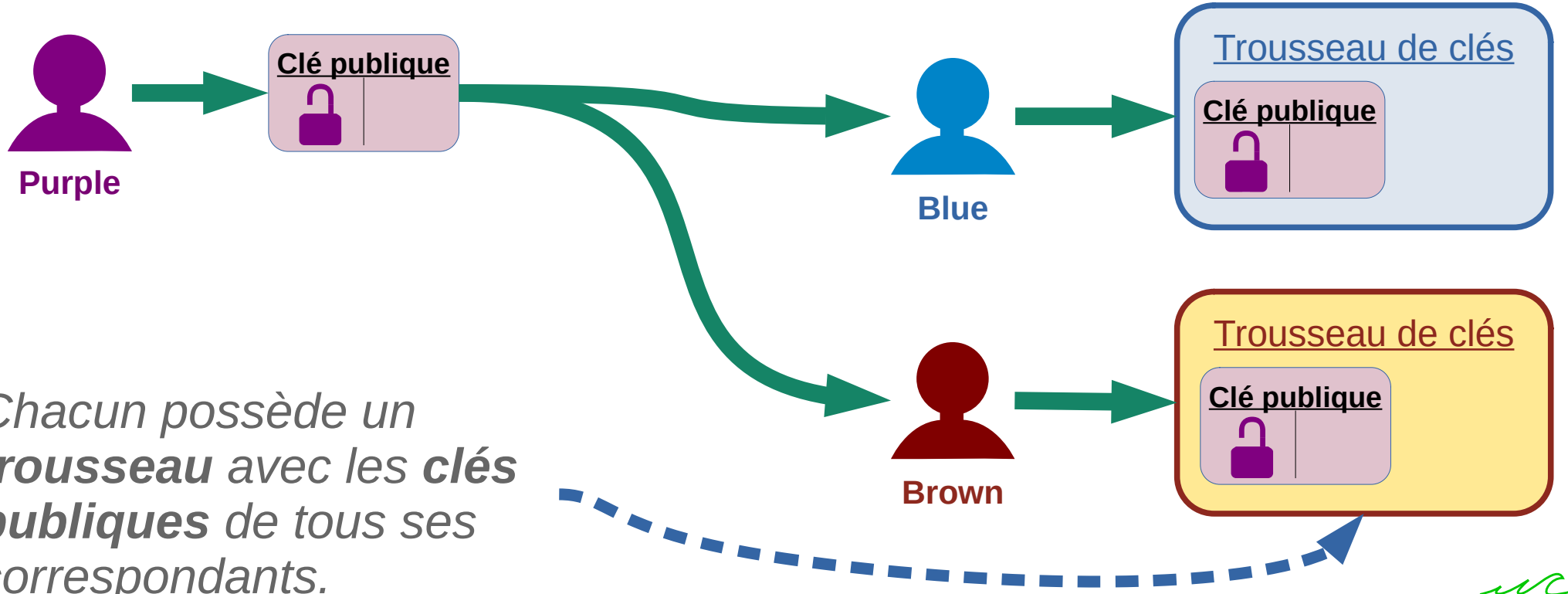
- **Purple** ne doit donner sa « clé privée » à absolument personne et la mettre en **sécurité absolue** !
  *(Et elle aura aussi un **mot de passe** !)*



Fonctionnement des 2 « boîtiers »

Purple envoie ensuite sa clé publique à ses correspondants.

Ces derniers ajoutent la clé de **Purple**, pour l'utiliser plus tard, dans leur **trousseau de clés publiques**.

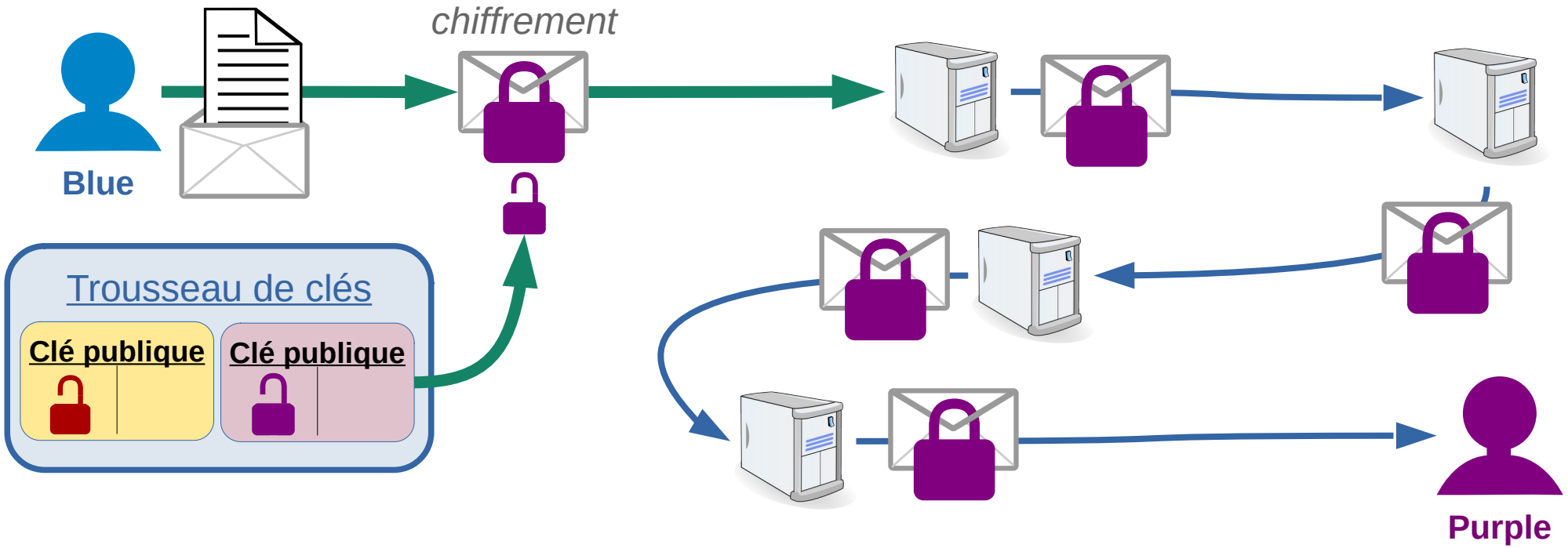


*Chacun possède un **trousseau** avec les **clés publiques** de tous ses correspondants.*

Fonctionnement des 2 « boîtiers »

Plus tard, **Blue** envoie un message chiffré à **Purple**

1. **Blue** rédige son message.
   Puis il utilise la clé publique de **Purple** (= son « cadenas ouvert »)
   et « **ferme** le cadenas » : il **chiffre** le message. Et enfin l'envoie**.**

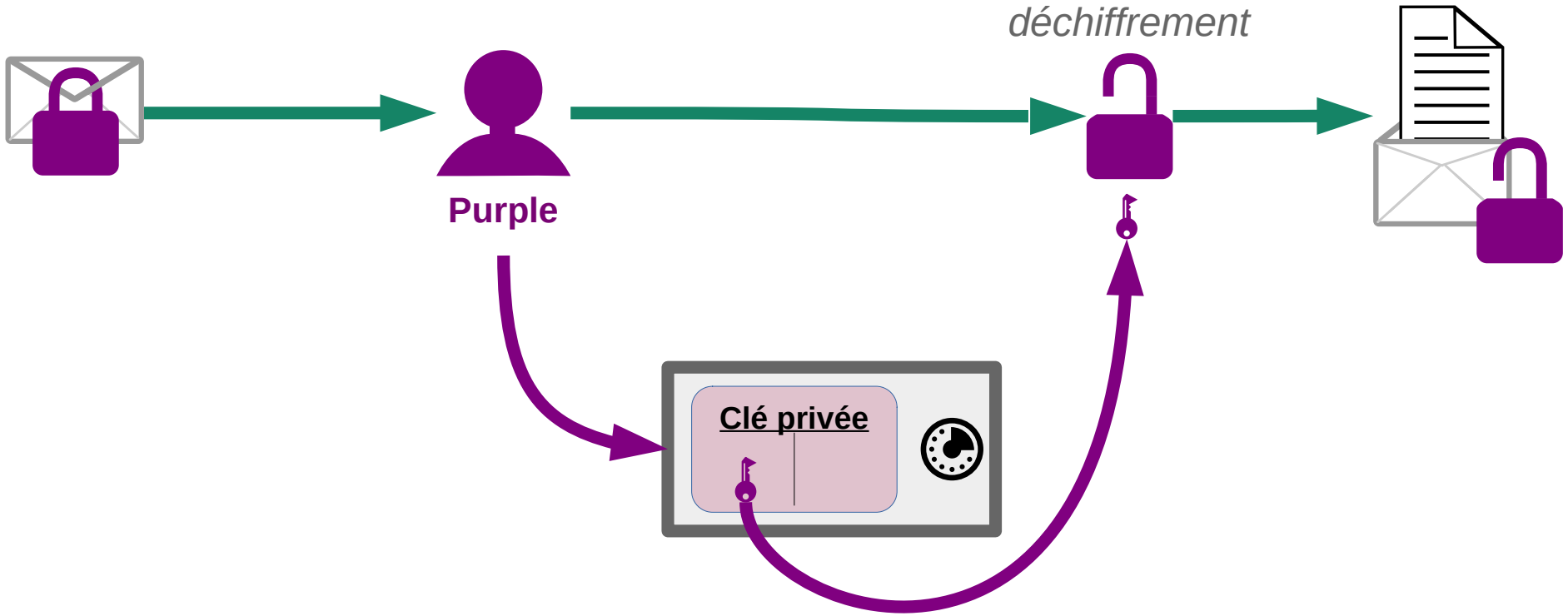


Personne ne peut lire le message car **seul Purple** en a la clé !

Fonctionnement des 2 « boîtiers »

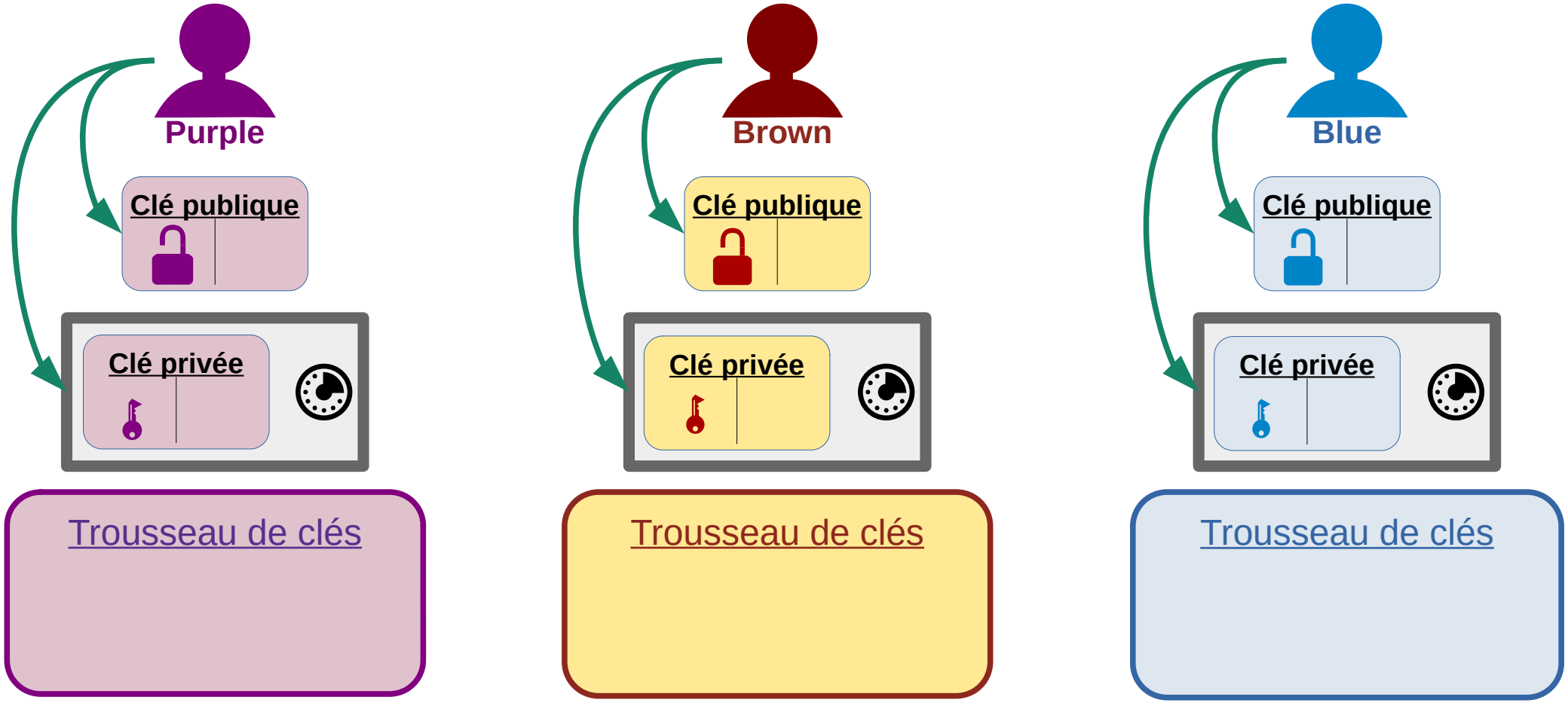
Purple reçoit ensuite le message chiffré

2. Purple utilise alors sa **clé privée** (qui contient la clé de son « cadenas public ») pour **déchiffrer** le message.



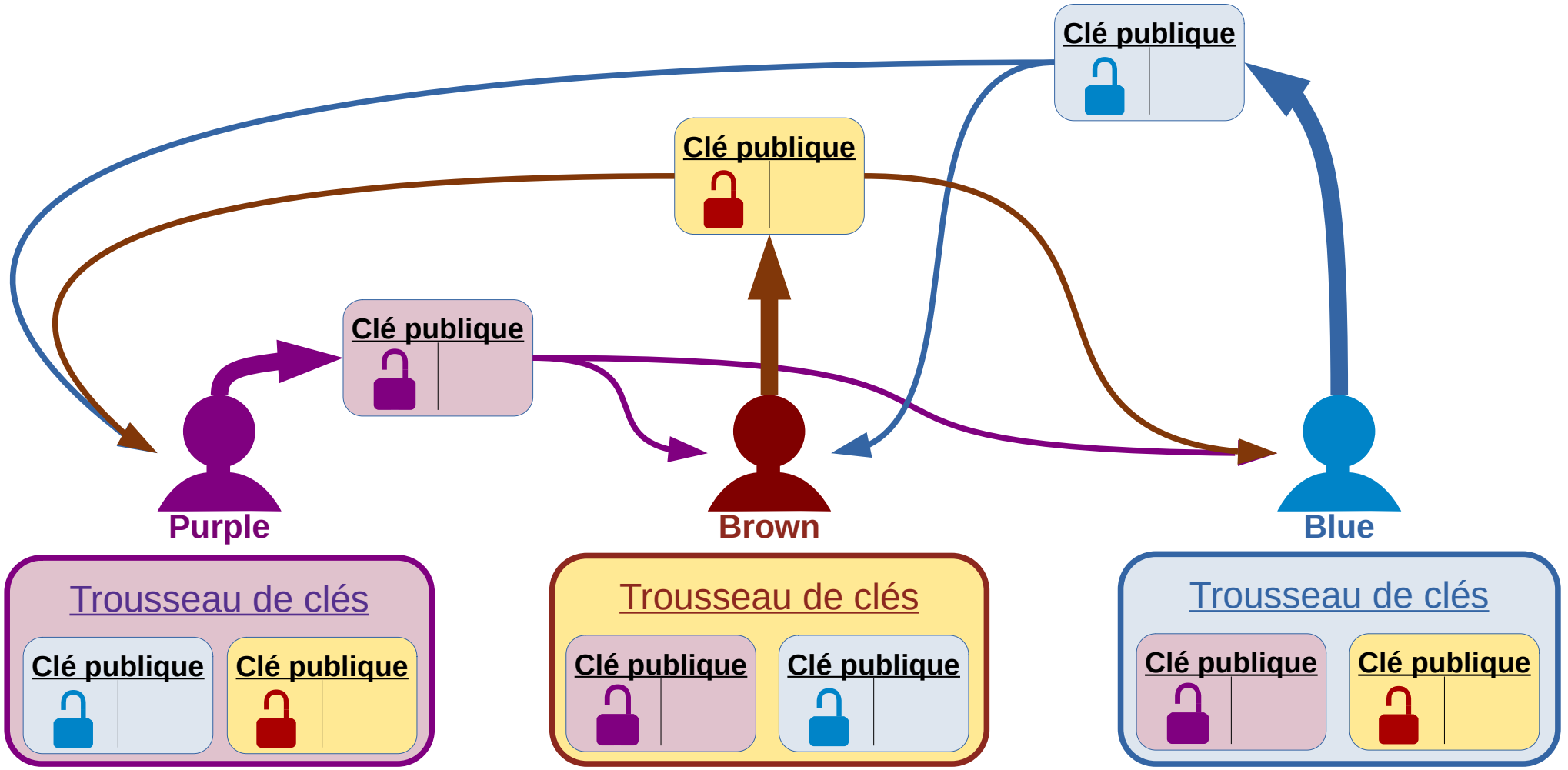
Récapitulatif : a) création des paires de clés

Chacun crée sa **paire** de clés, puis **sécurise** sa clé privée...



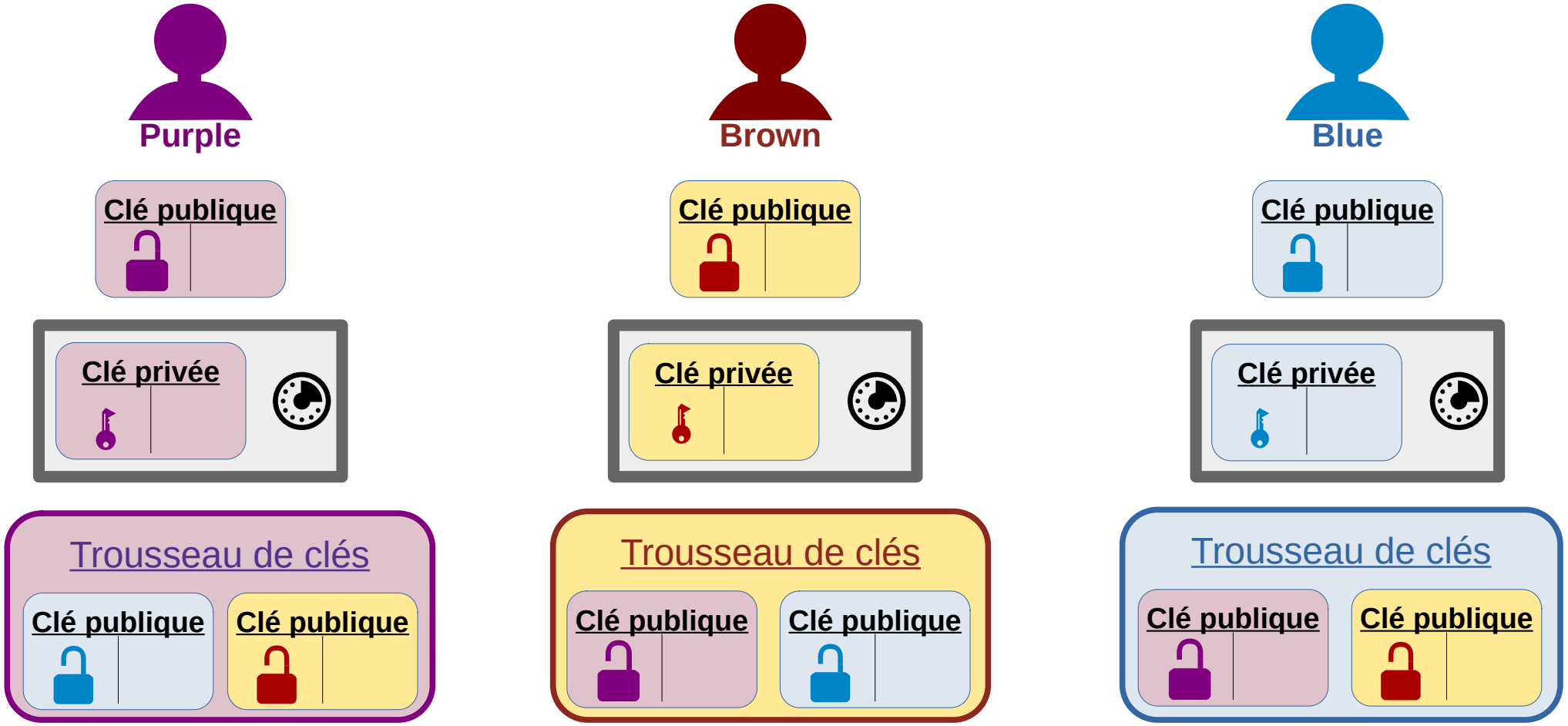
Récapitulatif : b) diffusion des clés publiques

...et envoie sa clé publique à tous ses correspondants...



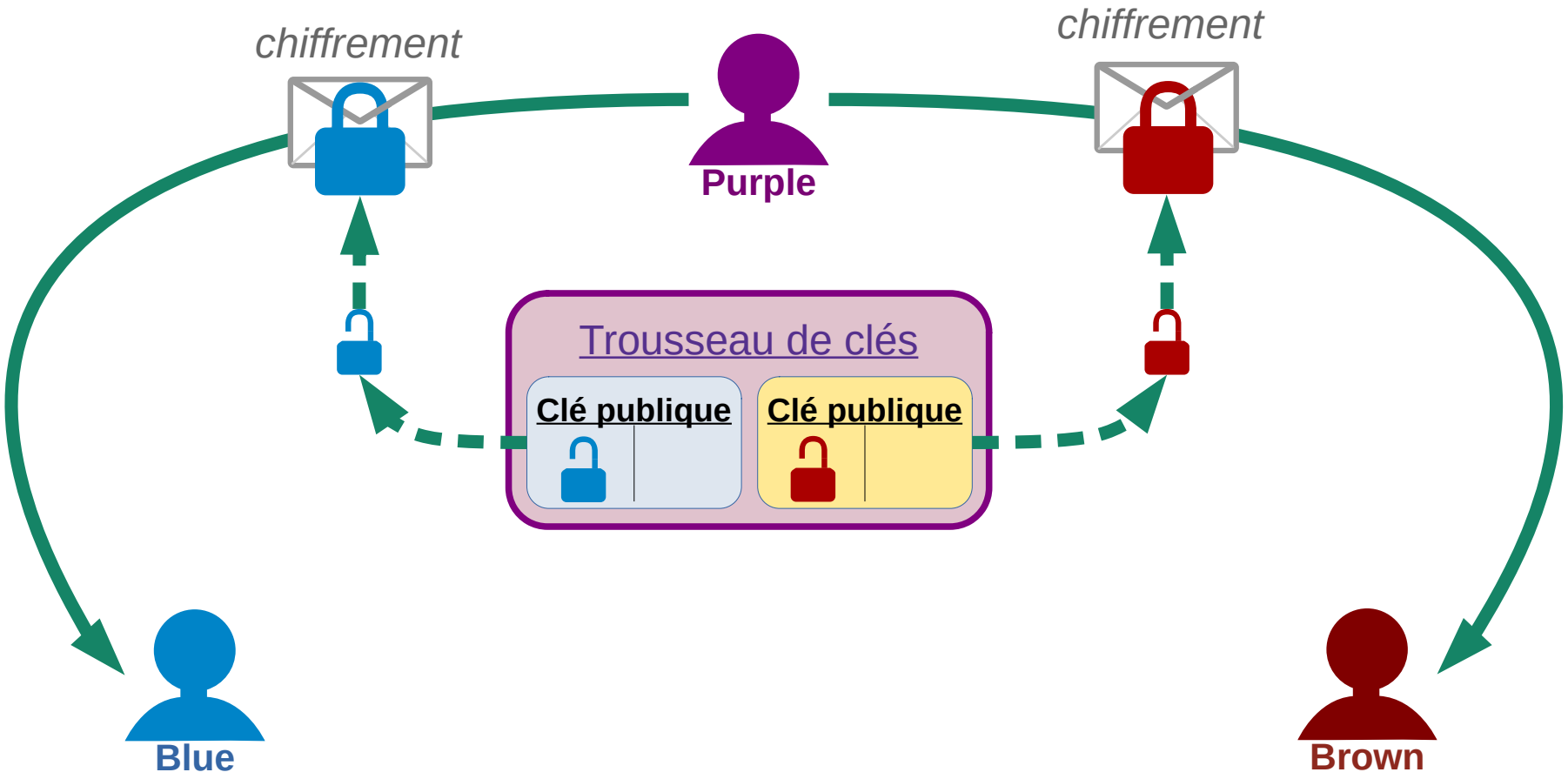
Le courriel chiffré est opérationnel !

Chacun est prêt à envoyer et à recevoir un message chiffré !



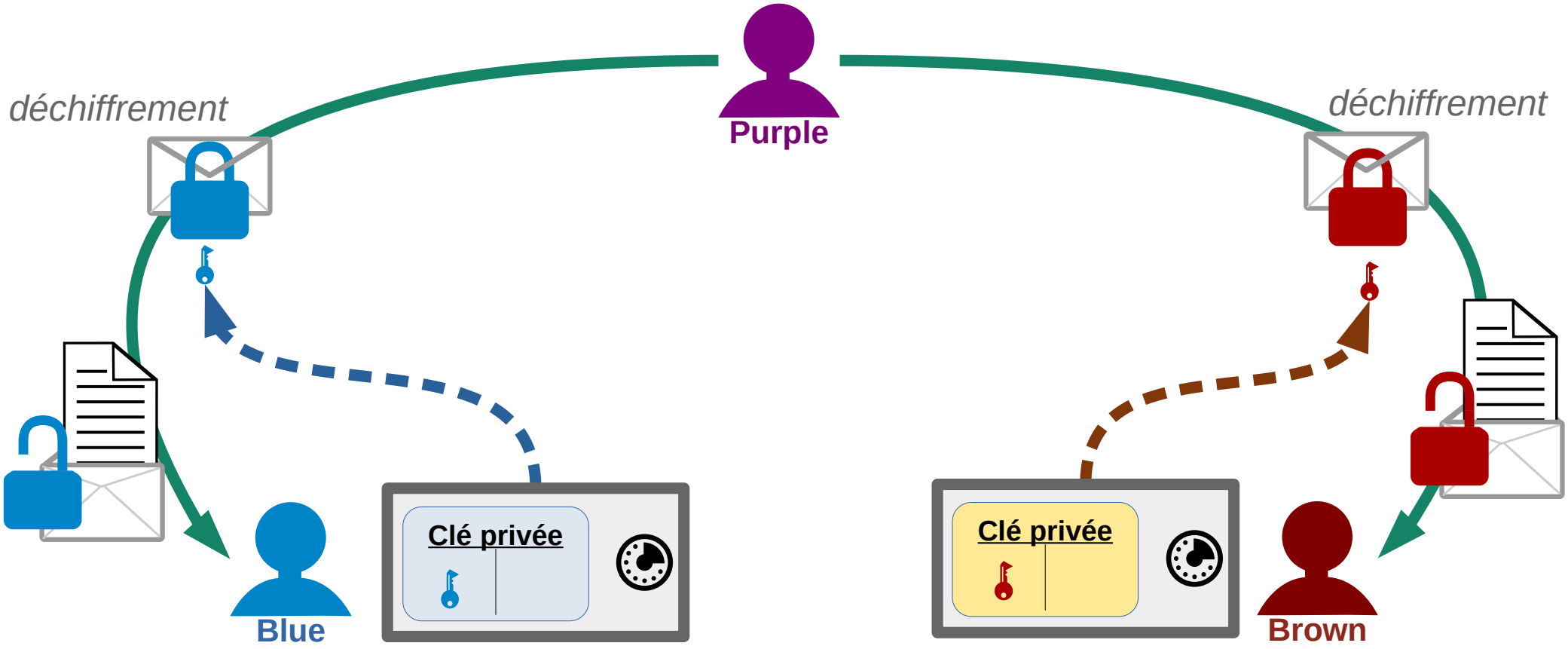
Exemple : envoi...

Purple envoie un message à **Blue** et à **Brown** qui sont **seuls** à pouvoir déchiffrer le message qui leur est destiné.



Exemple : réception...

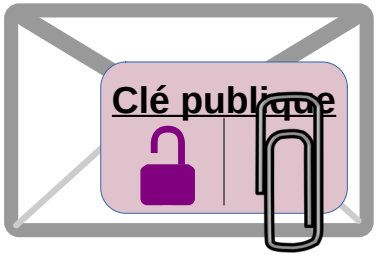
Chacun déchiffre son message avec sa propre **clé privée**.



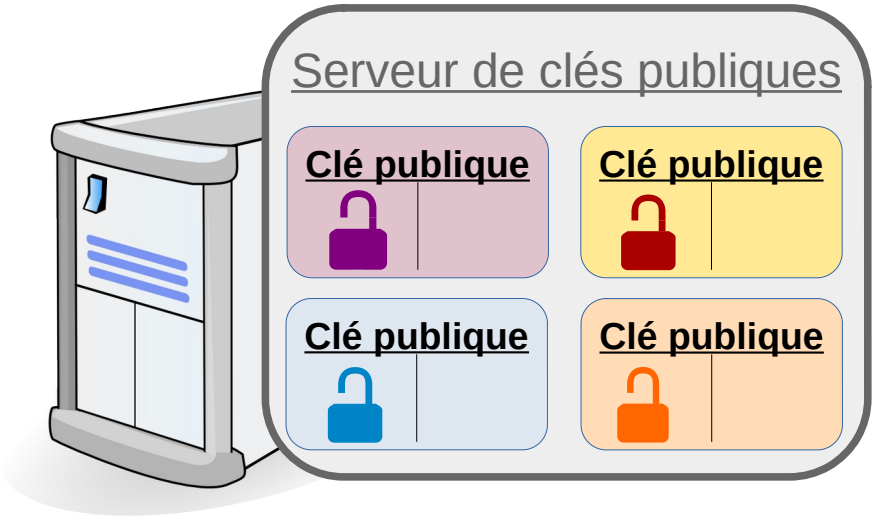
Diffusion de la clé publique

3 canaux pour diffuser sa clé publique :

1. **Envoi direct** au correspondant
   (clé = 1 fichier attaché .asc)



2. Envoi de la clé sur un **serveur officiel de clés publiques**.
   (*déconseillé pour les débutants*)



3. Mode sécurité absolue : support physique (clé USB, etc.) **en main propre**.

Où en sommes-nous avec les objectifs recherchés ?

Objectif 1 atteint !

- [x] **1.** Empêcher la **lecture-modification** du courriel par les intermédiaires.

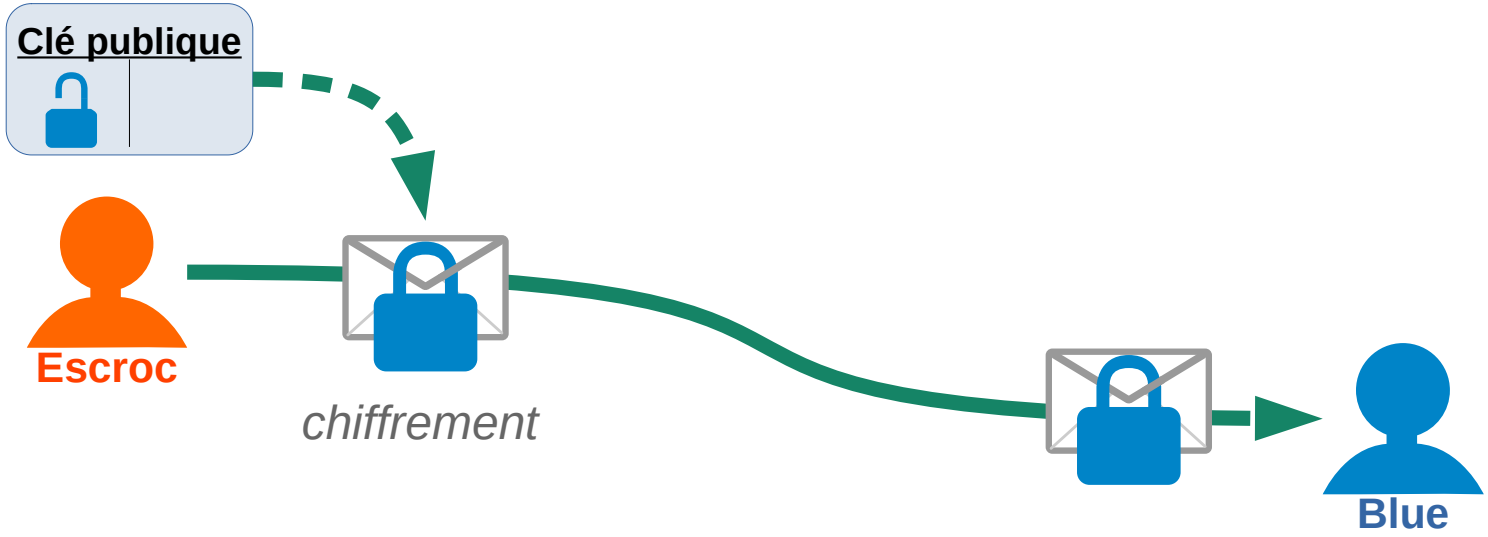
- [ ] **2.** S'assurer de l'**identité** de l'émetteur du courriel.

- [ ] **3.** Solution à **distance**, sans nécessité de contact ou d'échange physique (*ex. clé USB*) entre les interlocuteurs.

Pragmasoft

Objectif 2 : s'assurer de l'identité

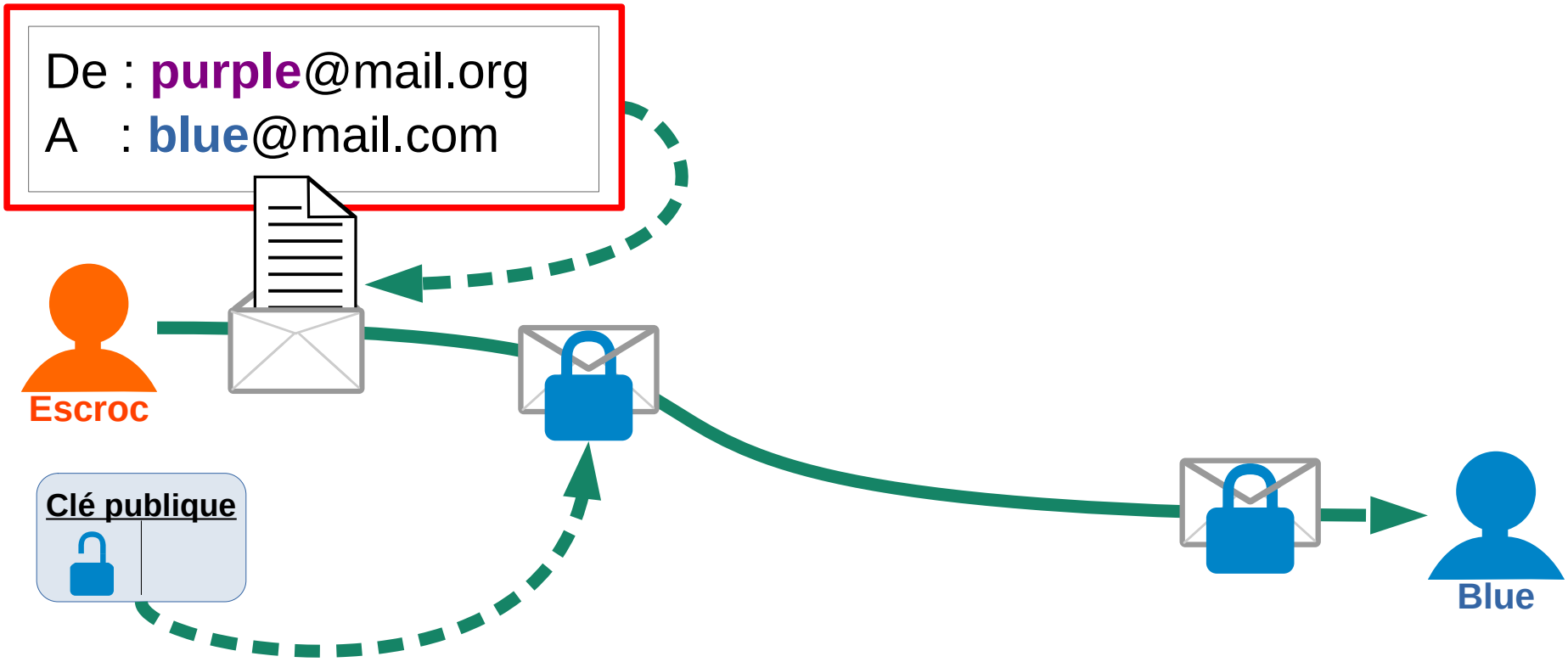
Escroc s'est facilement procuré la **clé publique** de **Blue**.
Il peut donc lui envoyer un message chiffré !



Blue reçoit un message chiffré… C'est bien pour la confidentialité...
Mais comment être sûr de l'expéditeur ?

Objectif 2 : s'assurer de l'identité

Car en effet, **Escroc** peut aussi assez facilement, en trichant sur l'adresse de l'expéditeur, **se faire passer** pour **Purple** !!!



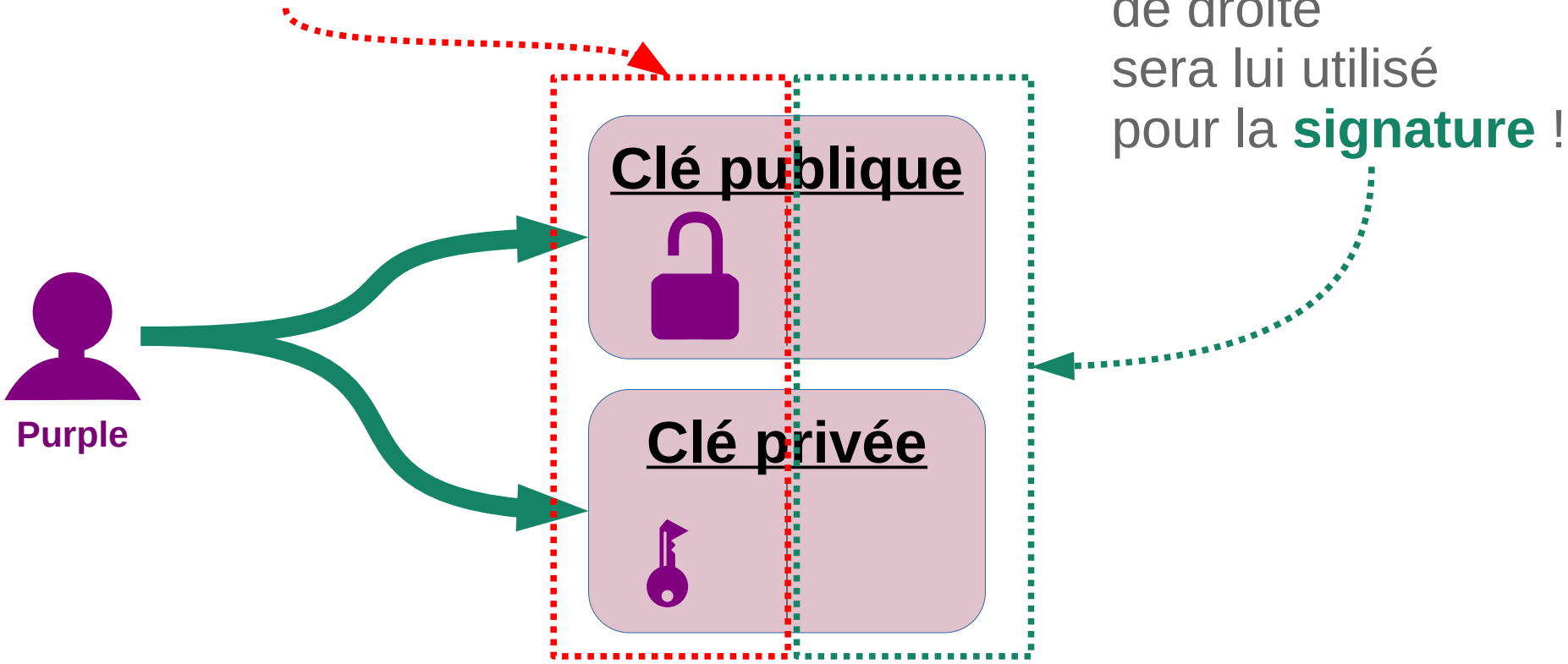
Blue doit donc s'assurer que c'est bien **Purple** qui lui écrit !

Solution : la 2ème partie des « boîtiers »

Rappelez-vous : chaque boîtier - clé a **2** compartiments !

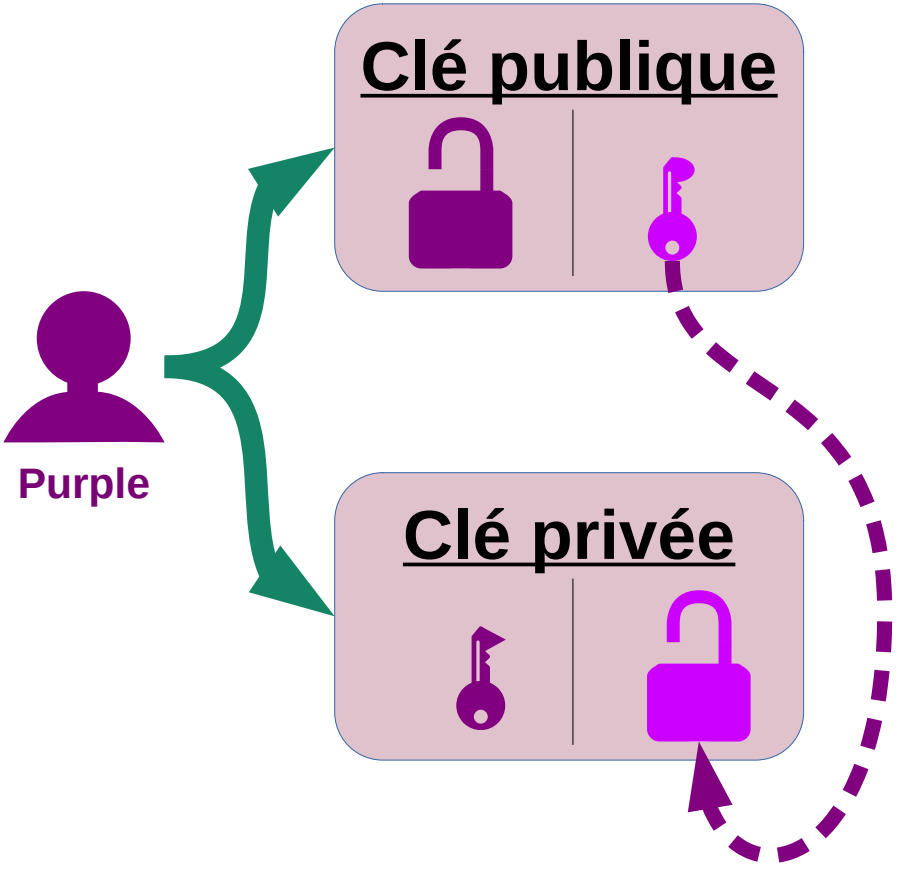
Le compartiment de gauche
est utilisé pour le **chiffrement**.

Le compartiment
de droite
sera lui utilisé
pour la **signature** !



La partie « signature » des « boîtiers »

On ajoute une clé et un cadenas !



Le boîtier « **clé publique** »

- On y ajoute une **clé**, pour ouvrir le nouveau « cadenas de la clé privée ».

Le boîtier « **clé privée** »

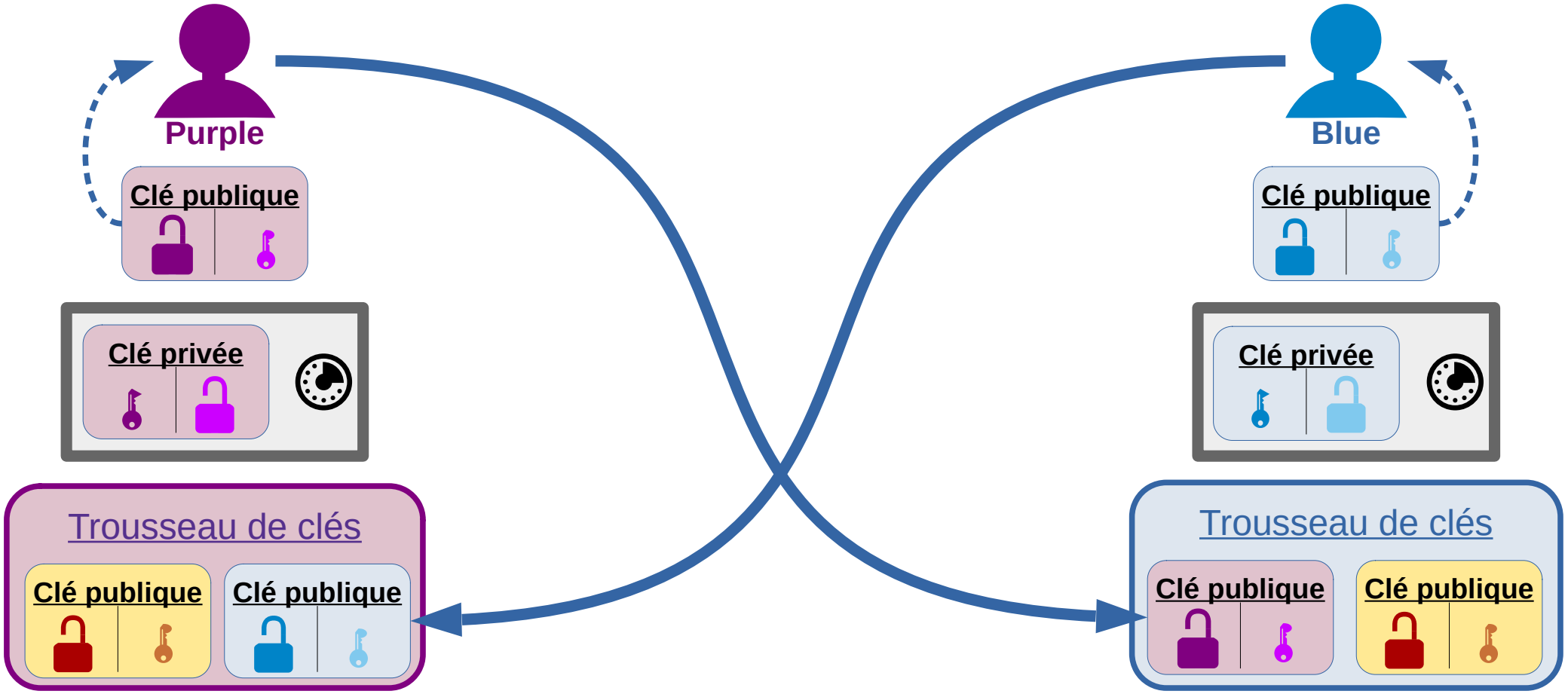
- On y ajoute un « **cadenas ouvert** ».

! ! ! *Notez la **couleur** plus claire des nouveaux clé-cadenas ! ! !*

Le courriel chiffré et signé est opérationnel !

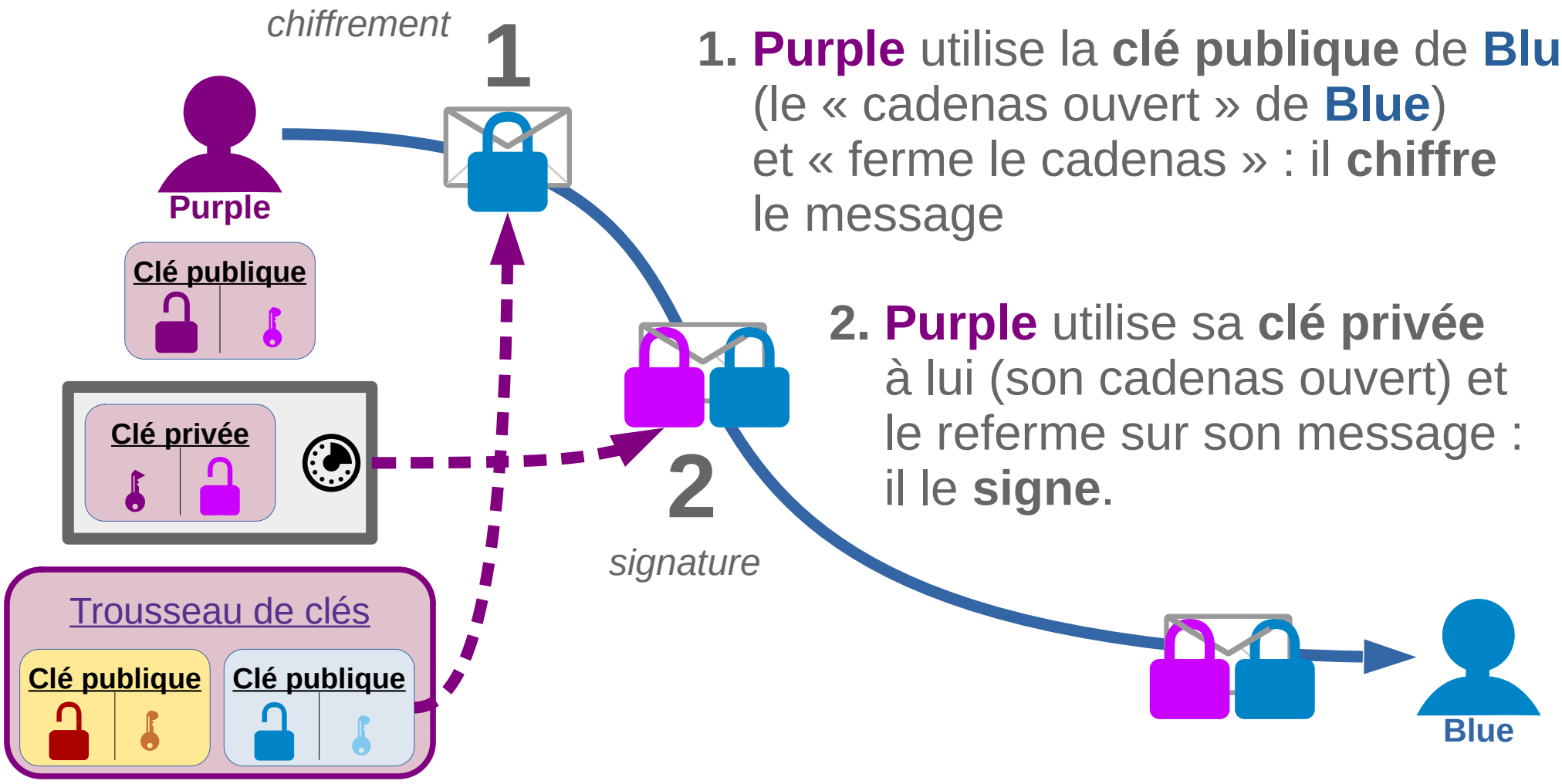
Situation complète des clés publiques et privées.

*Repérez bien les **couleurs foncées et claires** !*



Envoi de courrier chiffré ET signé

Purple envoie un message à **Blue**



1. **Purple** utilise la **clé publique** de **Blue** (le « cadenas ouvert » de **Blue**) et « ferme le cadenas » : il **chiffre** le message

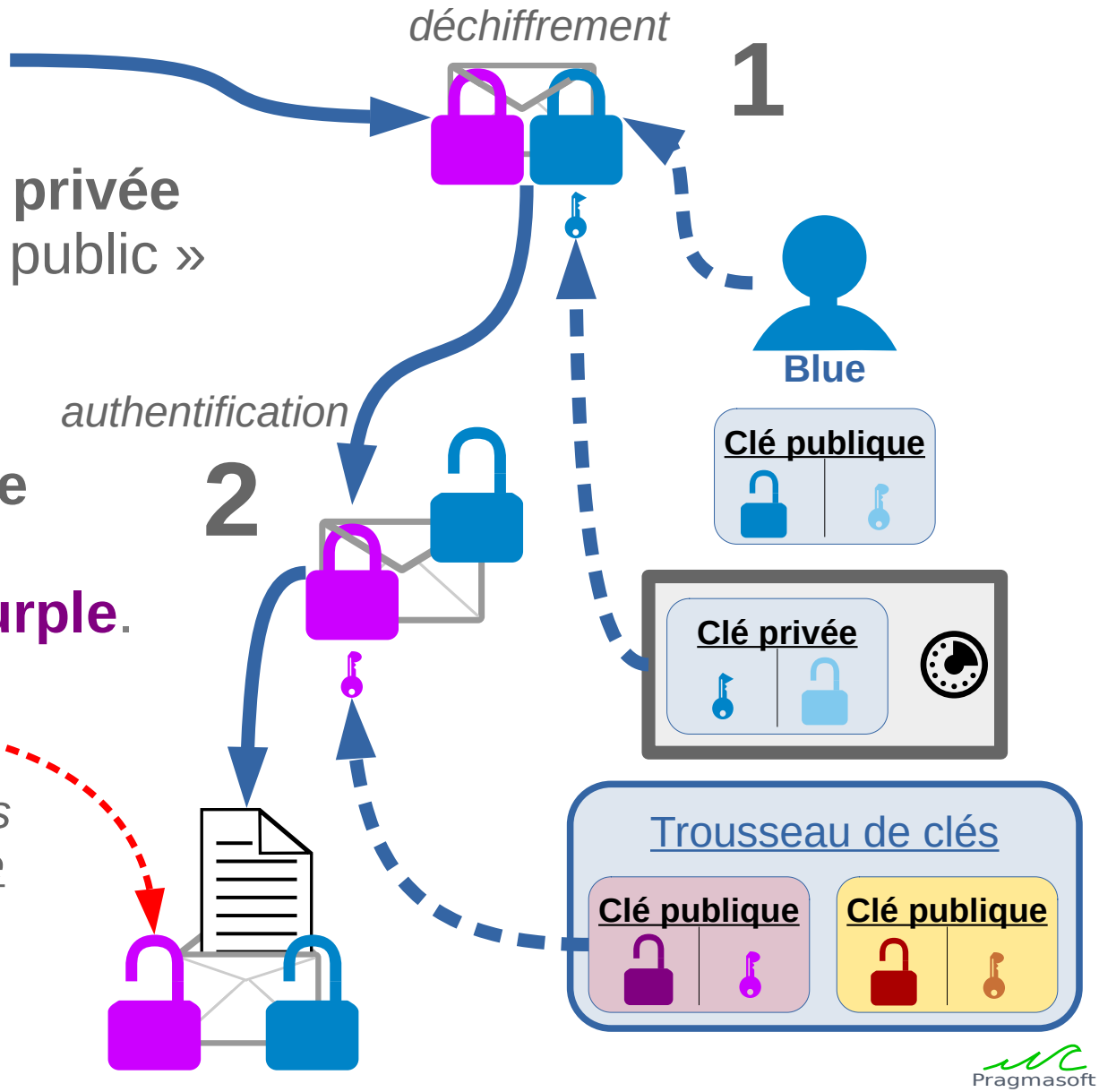
2. **Purple** utilise sa **clé privée** à lui (son cadenas ouvert) et le referme sur son message : il le **signe**.

Réception de courrier chiffré ET signé

Blue reçoit le message.

1. **Blue** utilise d'abord sa **clé privée** pour ouvrir son cadenas « public » (= déchiffrement).

2. **Blue** utilise la **clé publique** de **Purple** pour ouvrir le cadenas « privé » de **Purple**.



*Seul **Purple** a pu mettre ce cadenas (issu de sa clé privée) et donc seule sa clé publique peut l'ouvrir !*

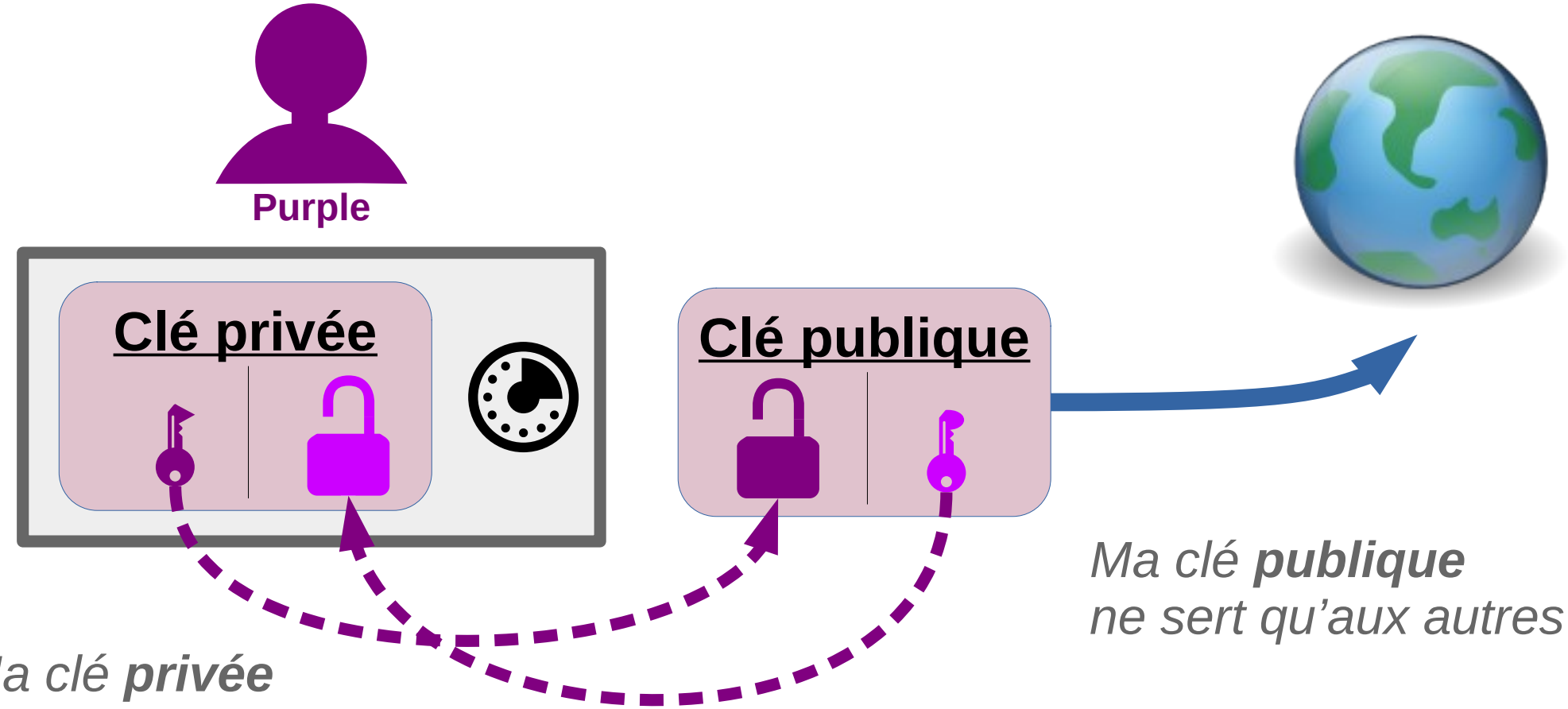
→ ***Blue** est sûr de l'identité de **Purple** !!!*

Pragmasoft

Système à clés publique et privée

Le système à paire de clés :

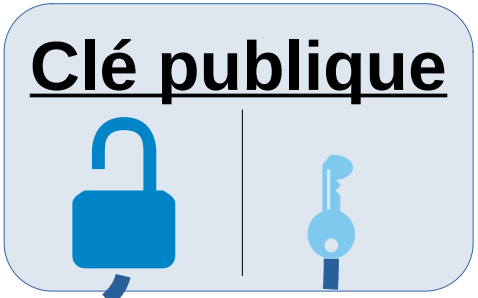
→ **Confidentialité – Identification – A distance**



La clé publique des autres...

Purple

me sert à 2 choses :



- **Quand j'envoie un message :**

  → **à chiffrer** le message destiné au propriétaire de la clé publique

- **Quand je reçois un message :**

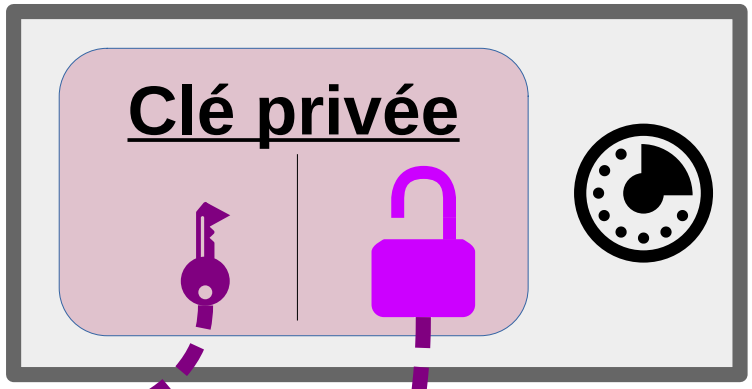
  → à **vérifier l'identité** de l'émetteur

*Exemple : la clé publique de **Blue** sert aux autres à **chiffrer** les messages qu'on lui envoie et aux autres, à **vérifier** qu'il est bien l'auteur des messages qu'il leur envoie.*

Ma clé privée...

Purple

me sert à 2 choses :



- **Quand je reçois un message :**

  → **à déchiffrer** le message qui m'est destiné

- **Quand j'envoie un message :**

  → à **signer** mon message pour prouver mon identité

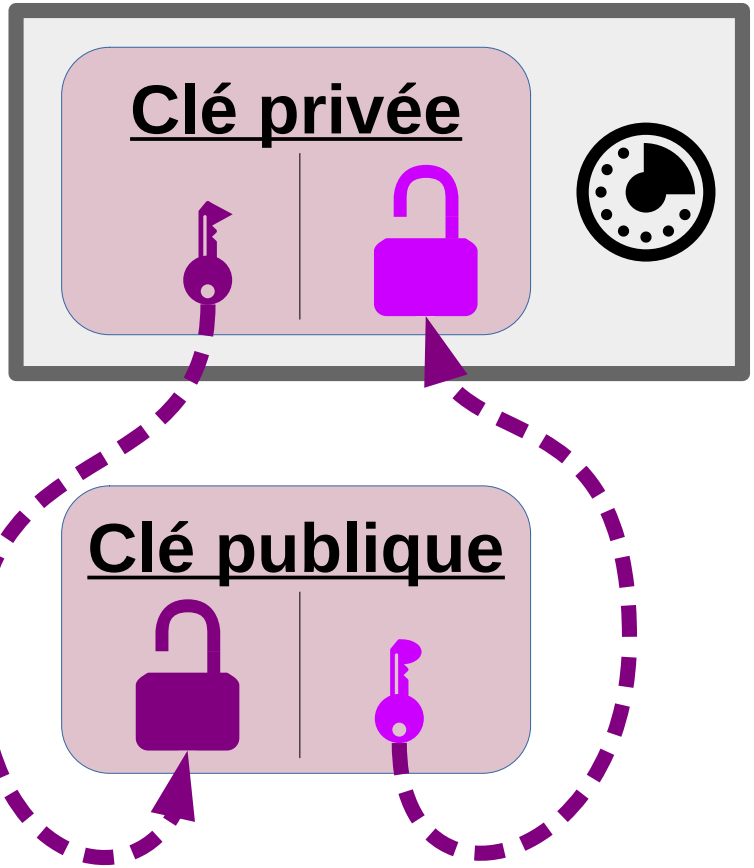
*Exemple : la clé privée de **Purple** lui sert à **déchiffrer** les messages qu'on lui envoie et à **prouver** aux autres qu'il est bien l'auteur des messages qu'il envoie.*

Synthèse

- Chaque utilisateur crée une **paire de clés** de chiffrement asymétriques (une **publique**, l'autre **privée**), et distribue la clé publique.

- Les **signatures** effectuées avec la **clé privée** peuvent être vérifiées en utilisant **la clé publique correspondante**.

- Les messages **chiffrés** avec la **clé publique** sont déchiffrables en utilisant **la clé privée correspondante**.



Où en sommes-nous avec les objectifs ?

Objectifs 2 et 3 atteints !

1. Empêcher la **lecture-modification** du courriel par les intermédiaires.

2. S'assurer de l'**identité** de l'émetteur du courriel.

3. Solution à **distance**, sans nécessité de contact ou d'échange physique (*ex. clé USB*) entre les interlocuteurs.

Sécurité absolue ?

Tout chiffrement peut être piraté..

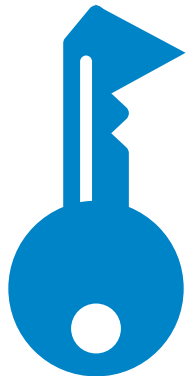
Mais avec PGP, pour cracker un message :

1. Il faudrait un paquet d'ordinateurs ne faisant que cela !
2. Enormément de temps : des semaines voire des années !

Plus de personnes encrypteront leurs courriels...
Et plus la tâche de décryptage devient impossible !

Donc… Encryptez !!!

Annexe : le mot de passe idéal



- Une phrase, pas des mots, et sans espace.
- 50 caractères minimum (100 = mieux !)
  => fastidieux => utiliser un gestionnaire de mot de passe sécurisé
- Lettres majuscules-minuscules, chiffres, ponctuations, caractères spéciaux.
- Pas de suites logiques (123456.. azerty...)
- Mots de plusieurs langues ou mieux : pas de mots d'une langue existante.
- Mots en phonétique : bato
- Aucune donnée privée (dates, lieu de naissance, adresse, téléphone)

- **Le changer tous les 60 jours**
  (60 jours = temps courant de crackage de systèmes simples)

Crédits

Réalisation, design & conception

- Pragma-soft - https://www.pragmasoft.be

Icônes

- Icons (p. 2, 6) by svgrepo.com - https://www.svgrepo.com

Photo

- Photo (p. 8) Zimmermann by Matt Cypto
  https://commons.wikimedia.org/wiki/File:PRZ_closeup.jpg