SÉCURITÉ

SE

Madame Khaoula ElBedoui-Maktouf

2ème année Ingénieur Informatique

Plan

I. Objets protégés et méthodes de protection

II. Protection de l'accès

III. Protection des fichiers

IV. Authentification

Objets et méthodes

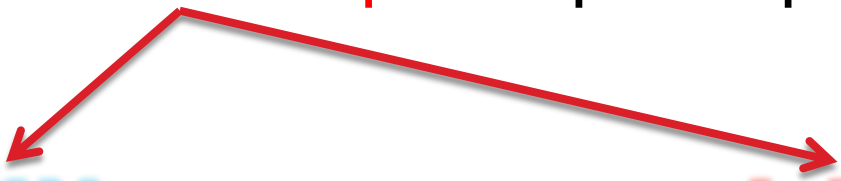
1. Objets protégés

Un Système Informatique est sujet d'attaques

Objets et méthodes

1. Objets protégés

Un Système Informatique est sujet d'attaques



Matériel

- Processeur
- Mémoire
- Périphérique d'E/S

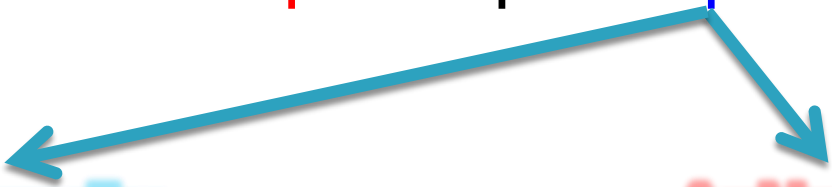
Logiciel

- Processus
- Base des données
- Fichiers

Objets et méthodes

1. Objets protégés

Un Système Informatique est sujet d'attaques



Intentionnelles

- Vols
- Modifications interdites
- Dévulgation

Accidentelles

- Pertes
- Erreurs
- Fausses manipulations

Objets et méthodes

1. Objets protégés

- Un système sécurisé doit vérifier les 4 propriétés suivantes (DICT) :
  - **Disponibilité** : garantir la continuité de service et maintenir son bon fonctionnement.

Objets et méthodes

1. Objets protégés

- Un système sécurisé doit vérifier les 4 propriétés suivantes (DICT) :
  - **Disponibilité** : garantir la continuité de service et maintenir son bon fonctionnement.
  - **Intégrité** : garantir l'exactitude et la validité du système. Éviter sa modification, par erreur ou par malveillance.

Objets et méthodes

1. Objets protégés

- Un système sécurisé doit vérifier les 4 propriétés suivantes (DICT) :
  - **Disponibilité** : garantir la continuité de service et maintenir son bon fonctionnement.
  - **Intégrité** : garantir l'exactitude et la validité du système. Éviter sa modification, par erreur ou par malveillance.
  - **Confidentialité** : garantir que le système n'est ni disponible, ni divulgué aux personnes, entités ou processus non autorisés.

Objets et méthodes

1. Objets protégés

- Un système sécurisé doit vérifier les 4 propriétés suivantes (DICT) :
  - **Disponibilité** : garantir la continuité de service et maintenir son bon fonctionnement.
  - **Intégrité** : garantir l'exactitude et la validité du système. Éviter sa modification, par erreur ou par malveillance.
  - **Confidentialité** : garantir que le système n'est ni disponible, ni divulgué aux personnes, entités ou processus non autorisés
  - **Traçabilité :** garantir la possibilité de reconstituer un traitement à des fins de contrôle (audit) et de preuves

Objets et méthodes

2. Méthodes de protection

- Les **mesures de protection** par critère de sécurité :

  - **Disponibilité** : garantir la continuité de service et maintenir son bon fonctionnement.
  - **Intégrité** : garantir l'exactitude et la validité du système. Éviter sa modification, par erreur ou par malveillance.
  - **Confidentialité** : garantir que le système n'est ni disponible, ni divulgué aux personnes, entités ou processus non autorisés.
  - **Traçabilité :** garantir la possibilité de reconstituer un traitement à des fins de contrôle (audit) et de preuves.

Objets et méthodes

2. Méthodes de protection

- Les **mesures de protection** par critère de sécurité :
  - **Disponibilité** : duplication matérielle et logicielle, sauvegarde, tolérance aux pannes
  - **Intégrité** : garantir l'exactitude et la validité du système. Éviter sa modification, par erreur ou par malveillance.
  - **Confidentialité** : garantir que le système n'est ni disponible, ni divulgué aux personnes, entités ou processus non autorisés.
  - **Traçabilité :** garantir la possibilité de reconstituer un traitement à des fins de contrôle (audit) et de preuves.

Objets et méthodes

2. Méthodes de protection

- Les **mesures de protection** par critère de sécurité :
  - **Disponibilité** : duplication matérielle et logicielle, sauvegarde, tolérance aux pannes
  - **Intégrité** : certification, contrôle d'accès et de la validité du système. Éviter sa modification, par erreur ou par malveillance.
  - **Confidentialité** : garantir que le système n'est ni disponible, ni divulgué aux personnes, entités ou processus non autorisés.
  - **Traçabilité :** garantir la possibilité de reconstituer un traitement à des fins de contrôle (audit) et de preuves.

Objets et méthodes

2. Méthodes de protection

- Les **mesures de protection** par critère de sécurité :
  - **Disponibilité** : duplication matérielle et logicielle, sauvegarde, tolérance aux pannes
  - **Intégrité** : certification, contrôle d'accès et de la validité du système Éviter sa modification, par erreur ou par malveillance.
  - **Confidentialité** : contrôle d'accès et chiffrement , ni divulgué aux personnes, entités ou processus non autorisés.
  - **Traçabilité :** garantir la possibilité de reconstituer un traitement à des fins de contrôle (audit) et de preuves.

Objets et méthodes

2. Méthodes de protection

- Les **mesures de protection** par critère de sécurité :
  - **Disponibilité** : duplication matérielle et logicielle, sauvegarde, tolérance aux pannes
  - **Intégrité** : certification, contrôle d'accès et de la validité du système. Éviter sa modification, par erreur ou par malveillance.
  - **Confidentialité** : contrôle d'accès et chiffrement , ni divulgué aux personnes, entités ou processus non autorisés.
  - **Traçabilité :** authentification, fichiers logs et archivage authentification, reconstitution des données

Objets et méthodes

2. Méthodes de protection

- Les **mesures de protection** par critère de sécurité :
  - **Disponibilité** : duplication matérielle et logicielle, sauvegarde, tolérance aux pannes
  - **Intégrité** : certification, contrôle d'accès et de la validité du système. Éviter sa modification, par erreur ou par malveillance.
  - **Confidentialité** : contrôle d'accès et chiffrement, ni divulgué aux personnes, entités ou processus non autorisés.
  - **Traçabilité** : authentification, fichiers logs et archivage authentification, reconstitution des données

Contrôle d'accès

1. Domaine de protection

- Un objet est une entité dans le système informatique
- Chaque objet peut être utilisé par un ou plusieurs sujets

Contrôle d'accès

1. Domaine de protection

- Un objet est une entité dans le système informatique
- Chaque objet peut être utilisé par un ou plusieurs sujets
- Un sujet est une entité active du système qui agit sur un objet
- le sujet peut être : processus, utilisateur, groupe d'utilisateurs, …
- Chaque sujet a des droits d'accès sur un objet

Contrôle d'accès

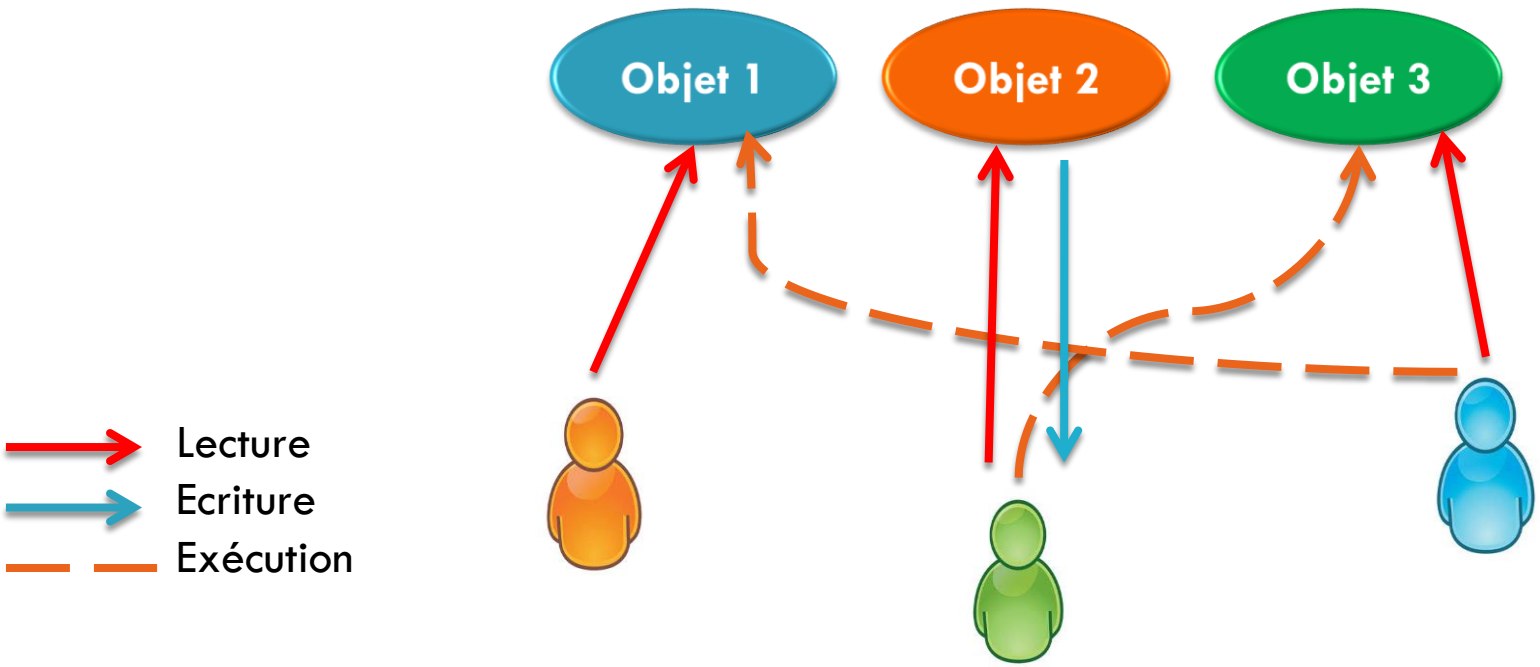
1. Domaine de protection

- Un objet est une entité dans le système informatique
- Chaque objet peut être utilisé par un ou plusieurs sujets
- Un sujet est une entité active du système qui agit sur un objet
- le sujet peut être : processus, utilisateur, groupe d'utilisateurs, …
- Chaque sujet a des droits d'accès sur un objet
- Un domaine = (objet, droits)
- Le domaine correspond à un sujet
- Lampson (1971) propose de modéliser les domaines par une matrice de protection

Contrôle d'accès

1. Domaine de protection

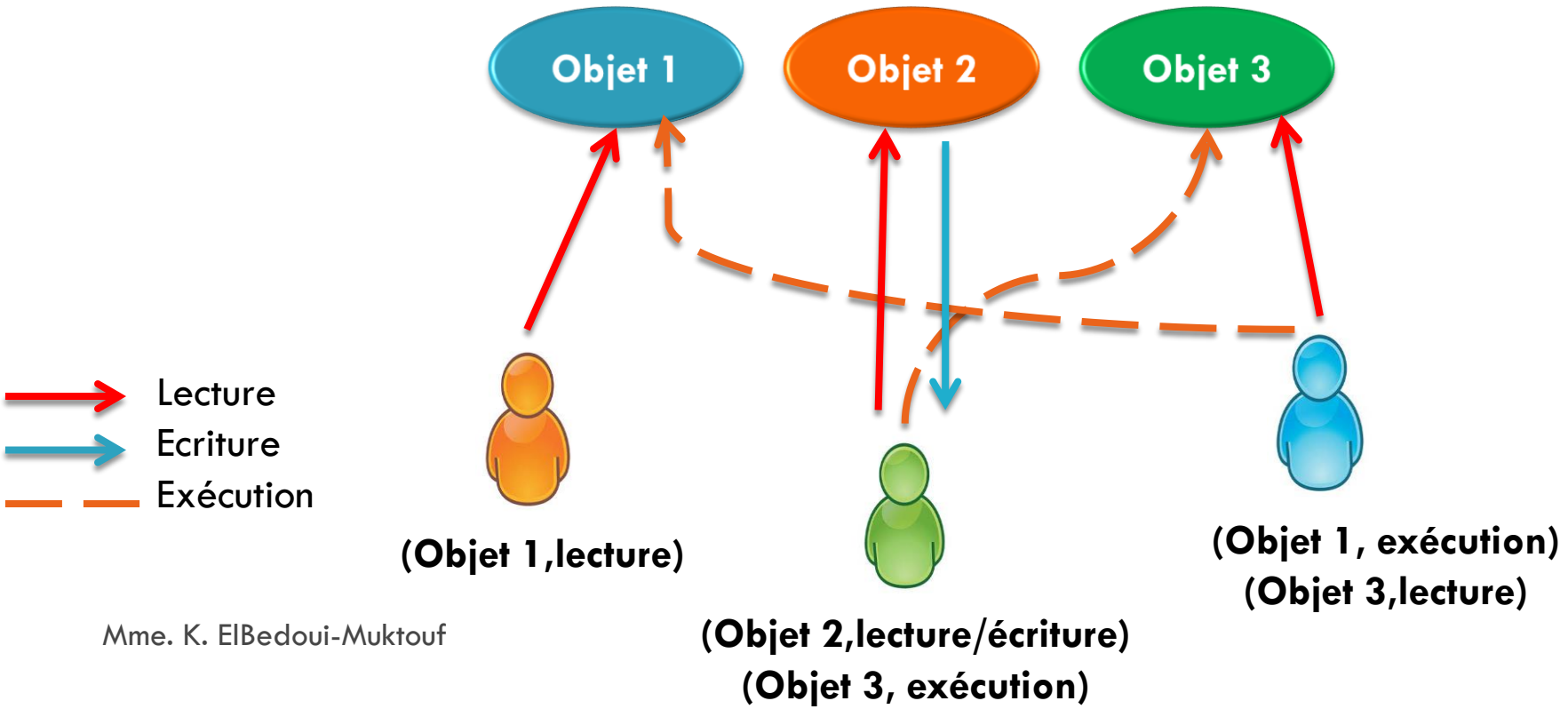
- **Objets et sujets**



Contrôle d'accès

1. Domaine de protection

- **Objets et sujets**



Contrôle d'accès

1. Domaine de protection

- **Matrice de protection**

	Objet 1	Objet 2	Objet 3
Domaine 1	R		
Domaine 2		R W	X
Domaine 3	X		R

(Objet 1,lecture)

(Objet 2,lecture/écriture)
(Objet 3, exécution)

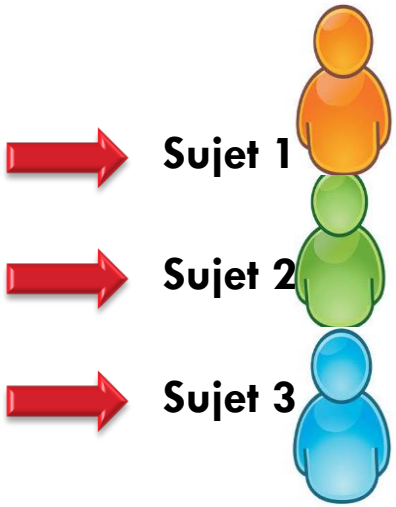
(Objet 1, exécution)
(Objet 3,lecture)

Contrôle d'accès

1. Domaine de protection

- **Matrice de protection**

	Objet 1	Objet 2	Objet 3
Domaine 1	R		
Domaine 2		R W	X
Domaine 3	X		R

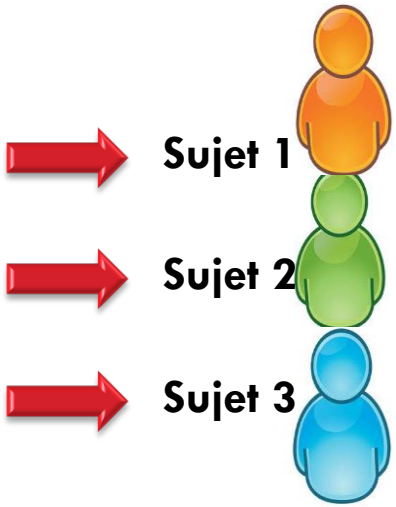


Contrôle d'accès

1. Domaine de protection

- Matrice de protection

	Objet 1	Objet 2	Objet 3
Domaine 1	R		
Domaine 2		R W	X
Domaine 3	X		R



+ Préciser les droits d'accès pour tous les sujets

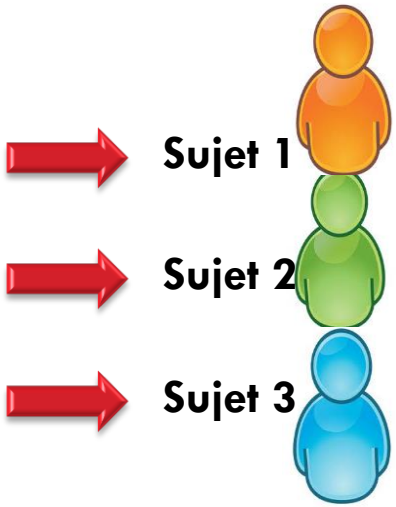
- Matrice imposante et creuse

Contrôle d'accès

1. Domaine de protection

- Matrice de protection

	Objet 1	Objet 2	Objet 3
Domaine 1	R		
Domaine 2		R W	X
Domaine 3	X		R



+ Préciser les droits d'accès pour tous les sujets

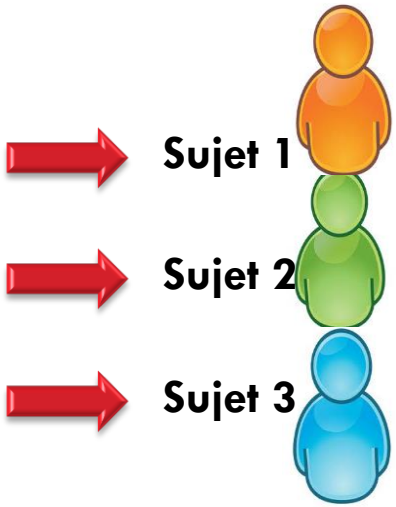
- Matrice imposante et creuse → stocker les cellules non vides

Contrôle d'accès

1. Domaine de protection

- Matrice de protection

	Objet 1	Objet 2	Objet 3
Domaine 1	R		
Domaine 2		R W	X
Domaine 3	X		R



+ Préciser les droits d'accès pour tous les sujets

- Matrice imposante et creuse → stocker les cellules non vides

colonne par colonne ou ligne par ligne

Contrôle d'accès

2. ACL (Access control List)

- Les cellules non vides de la matrice de protection sont stockées **colonne par colonne**

	Objet 1	Objet 2	Objet 3
Domaine 1	R		
Domaine 2		R W	X
Domaine 3	X		R

- A chaque objet on associe une liste qui définit les droits d'accès par sujet

Contrôle d'accès

2. ACL (Access control List)

- Les cellules non vides de la matrice de protection sont stockées **colonne par colonne**

	Objet 1	Objet 2	Objet 3
Domaine 1	R		
Domaine 2		R W	X
Domaine 3	X		R

Objet 1 → Sujet 1: R ; Sujet 3 : X

- A chaque objet on associe une liste qui définit les droits d'accès par sujet

Contrôle d'accès

2. ACL (Access control List)

- Les cellules non vides de la matrice de protection sont stockées **colonne par colonne**

	Objet 1	Objet 2	Objet 3
Domaine 1	R		
Domaine 2		R W	X
Domaine 3	X		R

Objet 1 → Sujet 1: R ; Sujet 3 : X

Objet 2 → Sujet 2 : RW

- A chaque objet on associe une liste qui définit les droits d'accès par sujet

Contrôle d'accès

2. ACL (Access control List)

- Les cellules non vides de la matrice de protection sont stockées **colonne par colonne**

	Objet 1	Objet 2	Objet 3
Domaine 1	R		
Domaine 2		R W	X
Domaine 3	X		R

Objet 1 → Sujet 1: R ; Sujet 3 : X

Objet 2 → Sujet 2 : RW

Objet 3 → Sujet 2 : X ; Sujet 3 : R

- A chaque objet on associe une liste qui définit les droits d'accès par sujet

Contrôle d'accès

2. ACL (Access control List)

- Les cellules non vides de la matrice de protection sont stockées **colonne par colonne**

	Objet 1	Objet 2	Objet 3
Domaine 1	R		
Domaine 2		R W	X
Domaine 3	X		R

Objet 1 → Sujet 1: R ; Sujet 3 : X

Objet 2 → Sujet 2 : RW

Objet 3 → Sujet 2 : X ; Sujet 3 : R

\+ la suppression d'un objet est facile (suppression de son ACL)

\- La suppression d'un sujet est complexe

Contrôle d'accès

3. C-List (Capability List)

- Les cellules non vides de la matrice de protection sont stockées **ligne par ligne**

	Objet 1	Objet 2	Objet 3
Domaine 1	R		
Domaine 2		R W	X
Domaine 3	X		R

Contrôle d'accès

3. C-List (Capability List)

- Les cellules non vides de la matrice de protection sont stockées **ligne par ligne**

	Objet 1	Objet 2	Objet 3
Domaine 1	R		
Domaine 2		R W	X
Domaine 3	X		R

Sujet 1 → Objet 1: R

Contrôle d'accès

3. C-List (Capability List)

- Les cellules non vides de la matrice de protection sont stockées **ligne par ligne**

	Objet 1	Objet 2	Objet 3
Domaine 1	R		
Domaine 2		R W	X
Domaine 3	X		R

Sujet 1 → Objet 1: R

Sujet 2 → Objet 2 : RW ; Objet 3 : X

Contrôle d'accès

3. C-List (Capability List)

- Les cellules non vides de la matrice de protection sont stockées **ligne par ligne**

	Objet 1	Objet 2	Objet 3
Domaine 1	R		
Domaine 2		R W	X
Domaine 3	X		R

Sujet 1 → Objet 1: R

Sujet 2 → Objet 2 : RW ; Objet 3 : X

Sujet 3 → Objet 1 : X ; Objet 3 : R

Contrôle d'accès

3. C-List (Capability List)

- Les cellules non vides de la matrice de protection sont stockées **ligne par ligne**

	Objet 1	Objet 2	Objet 3
Domaine 1	R		
Domaine 2		R W	X
Domaine 3	X		R

Sujet 1 → Objet 1: R

Sujet 2 → Objet 2 : RW ; Objet 3 : X

Sujet 3 → Objet 1 : X ; Objet 3 : R

\+ la suppression d'un sujet est facile (suppression de son C-List)

\- La suppression d'un objet est complexe

Protection des fichiers

1. Chiffrement (cryptographie)

- Consiste à rendre illisible un fichier et ce afin de le protéger
- Le chiffrement se base sur :
  - Clé
  - Algorithme

Protection des fichiers

1. Chiffrement (cryptographie)

- Consiste à rendre illisible un fichier et ce afin de le protéger
- Le chiffrement se base sur :
  - Clé
  - Algorithme

Texte brut

Algorithme de chiffrement

Texte chiffré

Algorithme de déchiffrement

Texte normal

Protection des fichiers

2. Chiffrement symétrique

- Si la clé de chiffrement et la clé de déchiffrement sont les mêmes (la clé doit rester secrète)

  \+ simple

  \- La clé peut être interceptée

Protection des fichiers

2. Chiffrement symétrique

- **Exemple :**

  substitution → clé : chaque lettre est remplacée par son suivant

Bonjour

Texte brut

Algorithme de chiffrement

Cpokpvs

Texte chiffré

Algorithme de déchiffrement

Bonjour

Texte normal

Protection des fichiers

3. Chiffrement asymétrique

- Si la clé de chiffrement et la clé de déchiffrement sont différentes
- La clé de chiffrement = clé publique (destinée à être transmise)
- La clé de déchiffrement = clé privée (gardée secrète)

Texte brut

Algorithme de chiffrement

Texte chiffré

Algorithme de déchiffrement

Texte normal

Protection des fichiers

3. Chiffrement asymétrique

- **Confidentialité = document lu seulement par le destinataire**

Emetteur

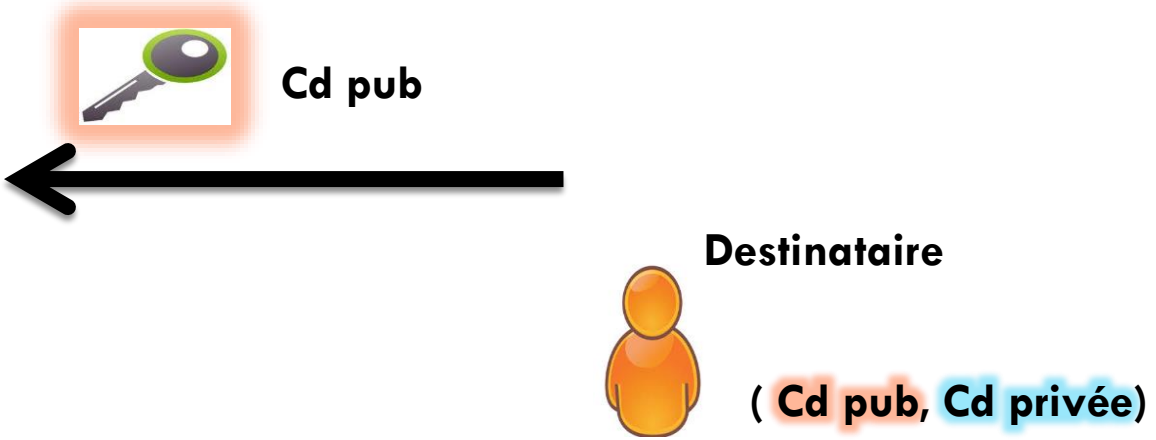
Destinataire

(Cd pub, Cd privée)

Protection des fichiers

3. Chiffrement asymétrique

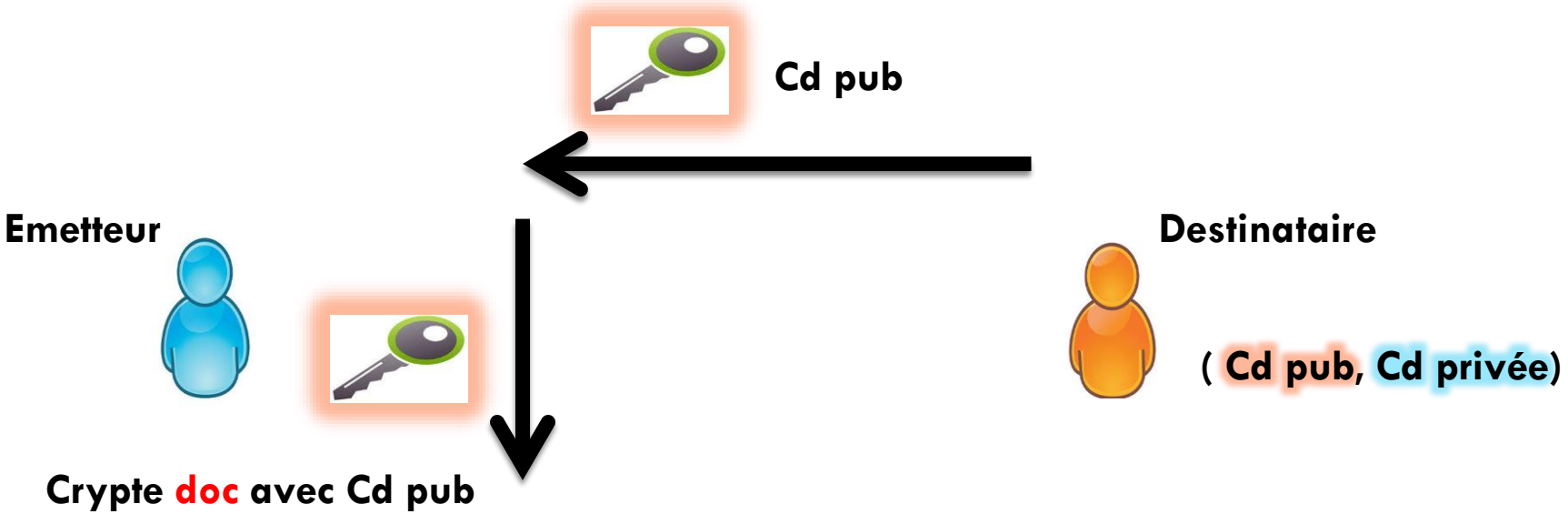
- Confidentialité = document lu seulement par le destinataire



Protection des fichiers

3. Chiffrement asymétrique

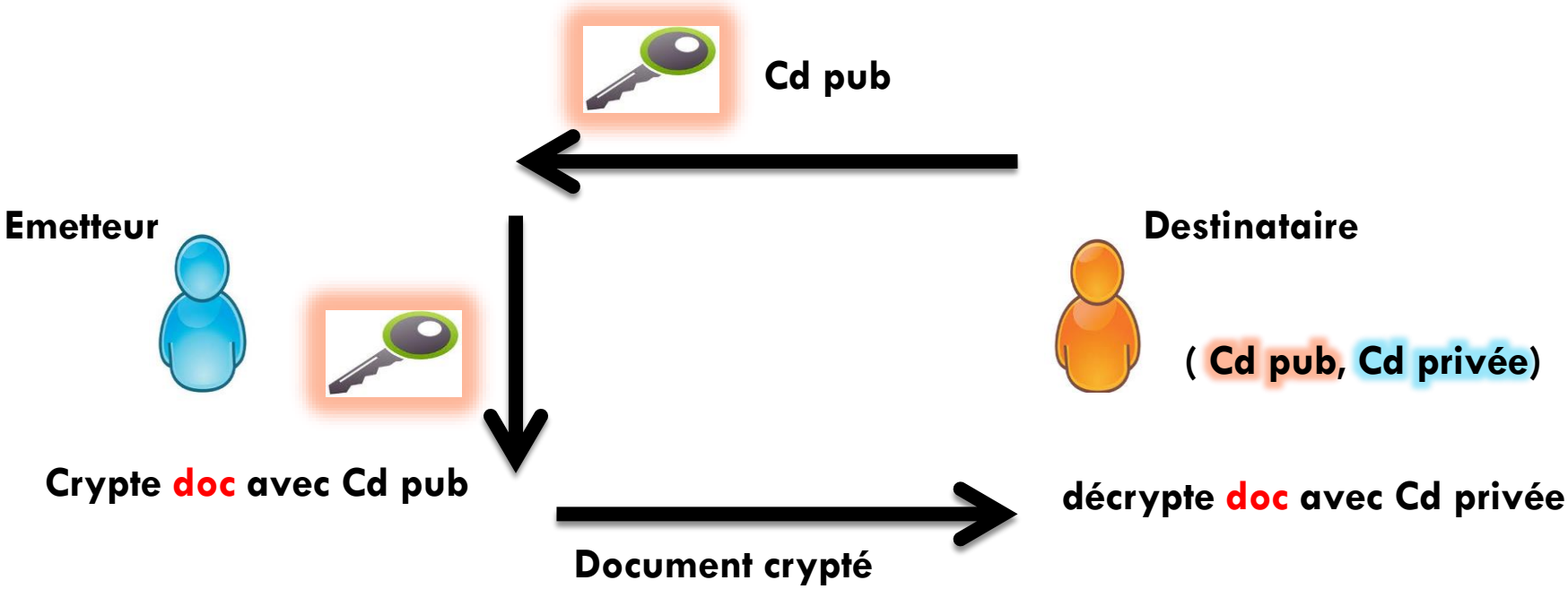
- Confidentialité = document lu seulement par le destinataire



Protection des fichiers

3. Chiffrement asymétrique

- Confidentialité = document lu seulement par le destinataire



Protection des fichiers

3. Chiffrement asymétrique

- **Authentification = s'assurer de l'identité de l'émetteur**

Emetteur

(Ce pub, Ce privée)

Destinataire

Protection des fichiers

3. Chiffrement asymétrique

- **Authentification = s'assurer de l'identité de l'émetteur**

Ce pub

Emetteur

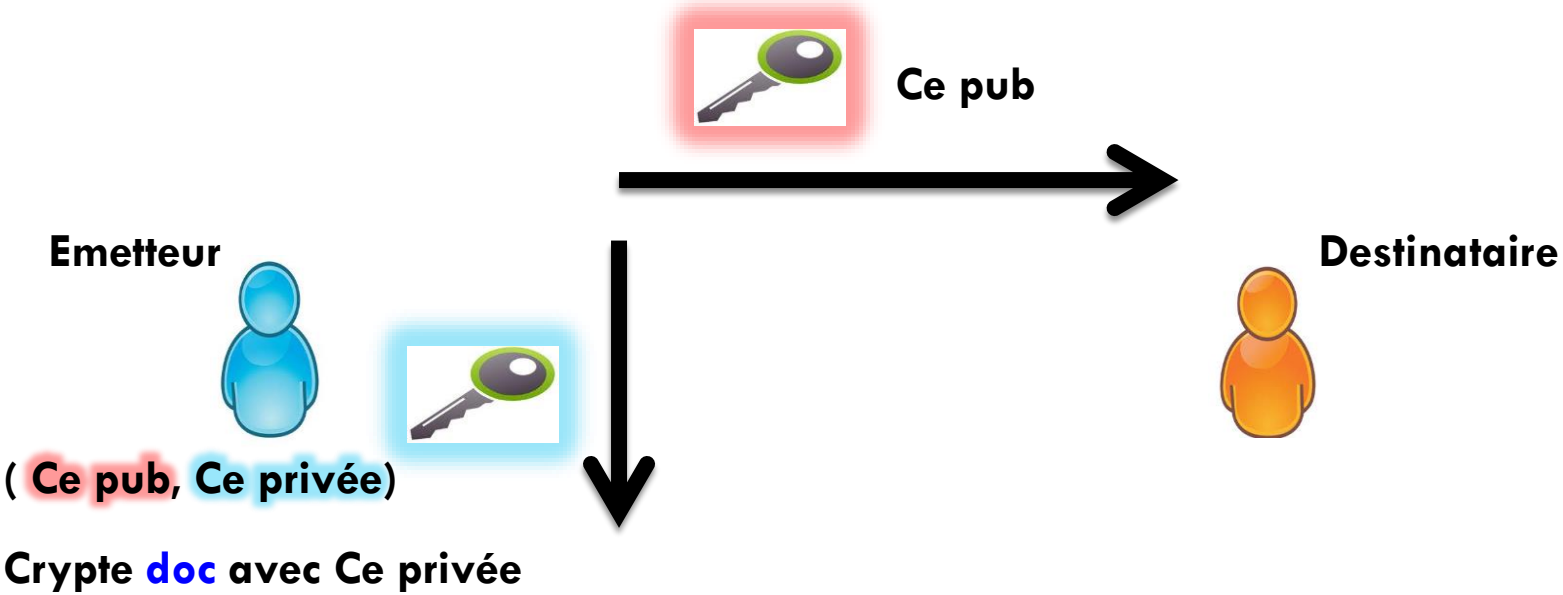
Destinataire

(Ce pub, Ce privée)

Protection des fichiers

3. Chiffrement asymétrique

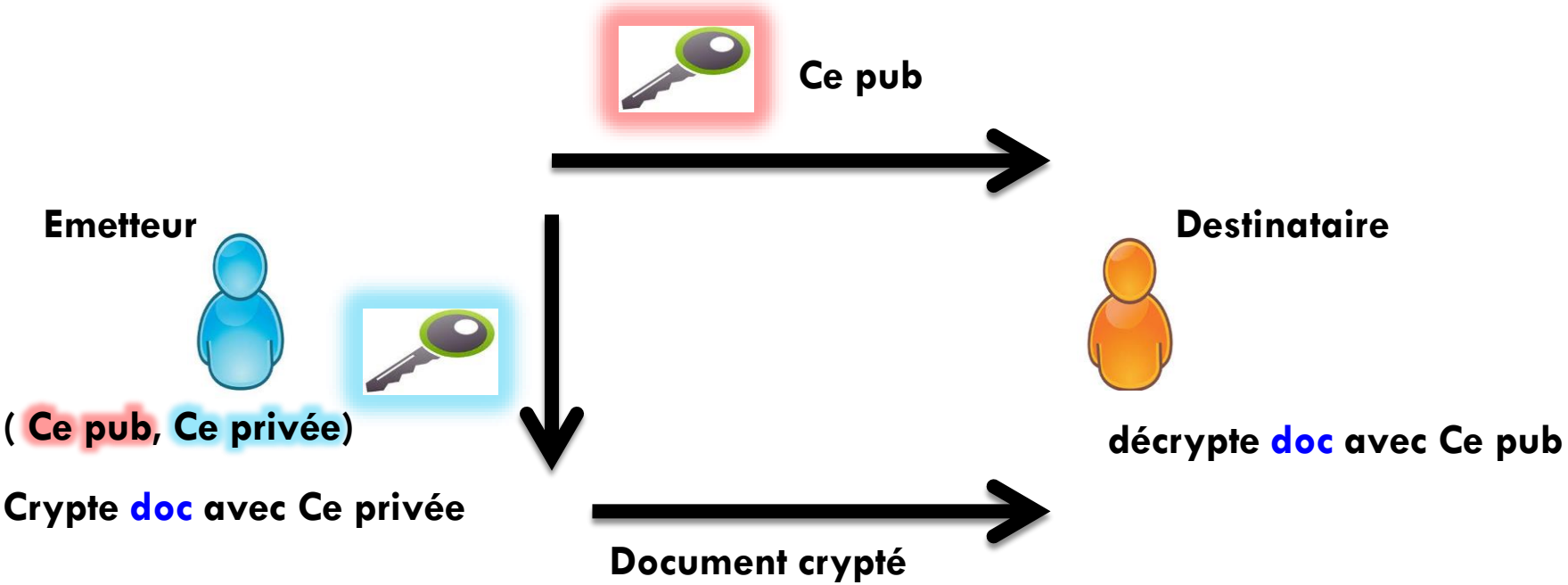
- **Authentification = s'assurer de l'identité de l'émetteur**



Protection des fichiers

3. Chiffrement asymétrique

- Authentification = s'assurer de l'identité de l'émetteur



Protection des fichiers

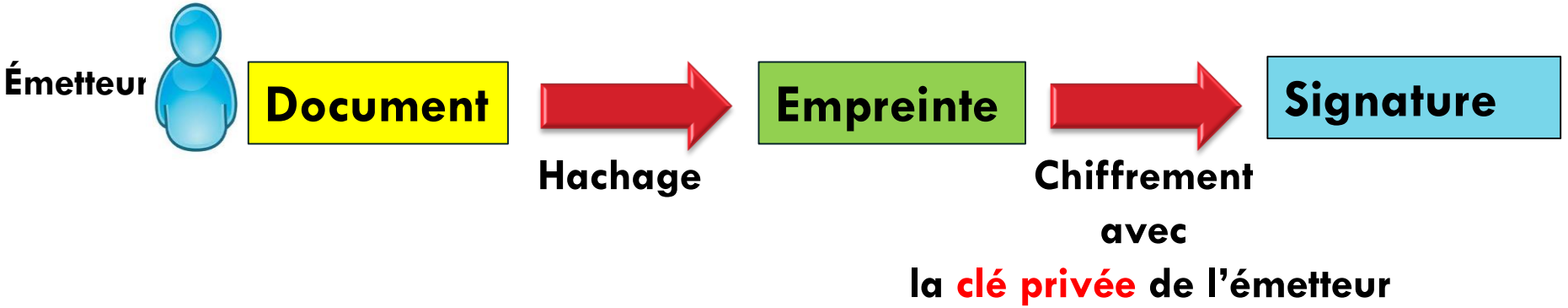
4. Signature électronique

- Permet **d'authentifier** l'émetteur d'un document et de vérifier **l'intégrité** du fichier

Protection des fichiers

4. Signature électronique

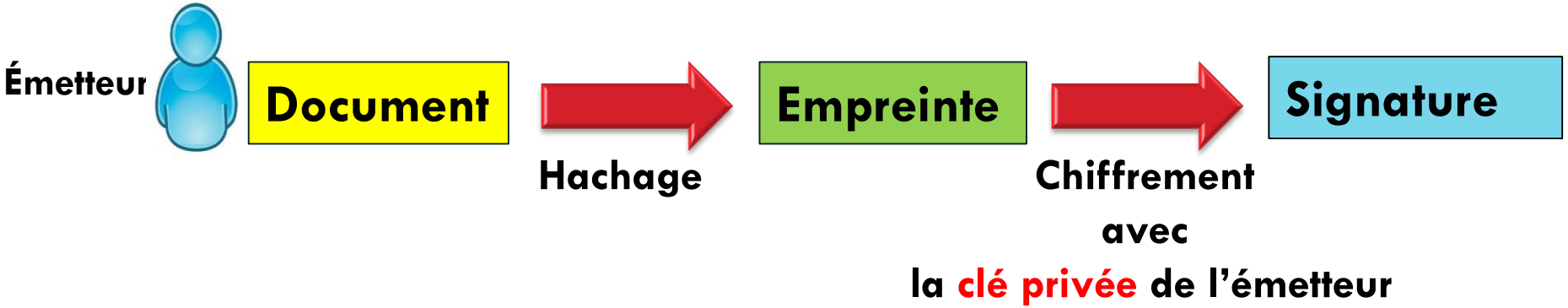
- Permet d'authentifier l'émetteur d'un document et de vérifier l'intégrité du fichier



Protection des fichiers

4. Signature électronique

- Permet d'authentifier l'émetteur d'un document et de vérifier l'intégrité du fichier

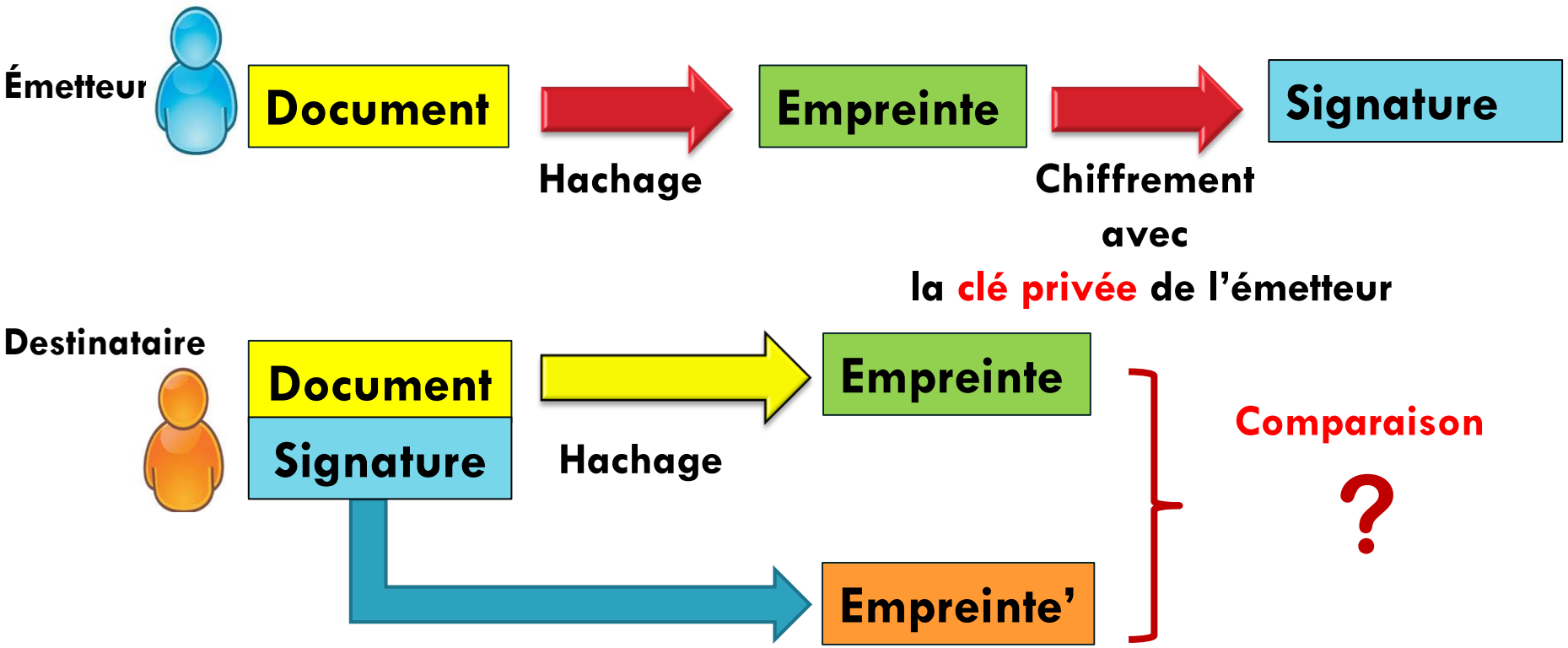


Hachage : permet de condenser le contenu d'un document sur un nombre fixe de bits. Le hachage est sensible : à chaque document correspond un et un seul document haché. La fonction de hachage est à sens unique.

Protection des fichiers

4. Signature électronique

- Permet d'authentifier l'émetteur d'un document et de vérifier l'intégrité du fichier

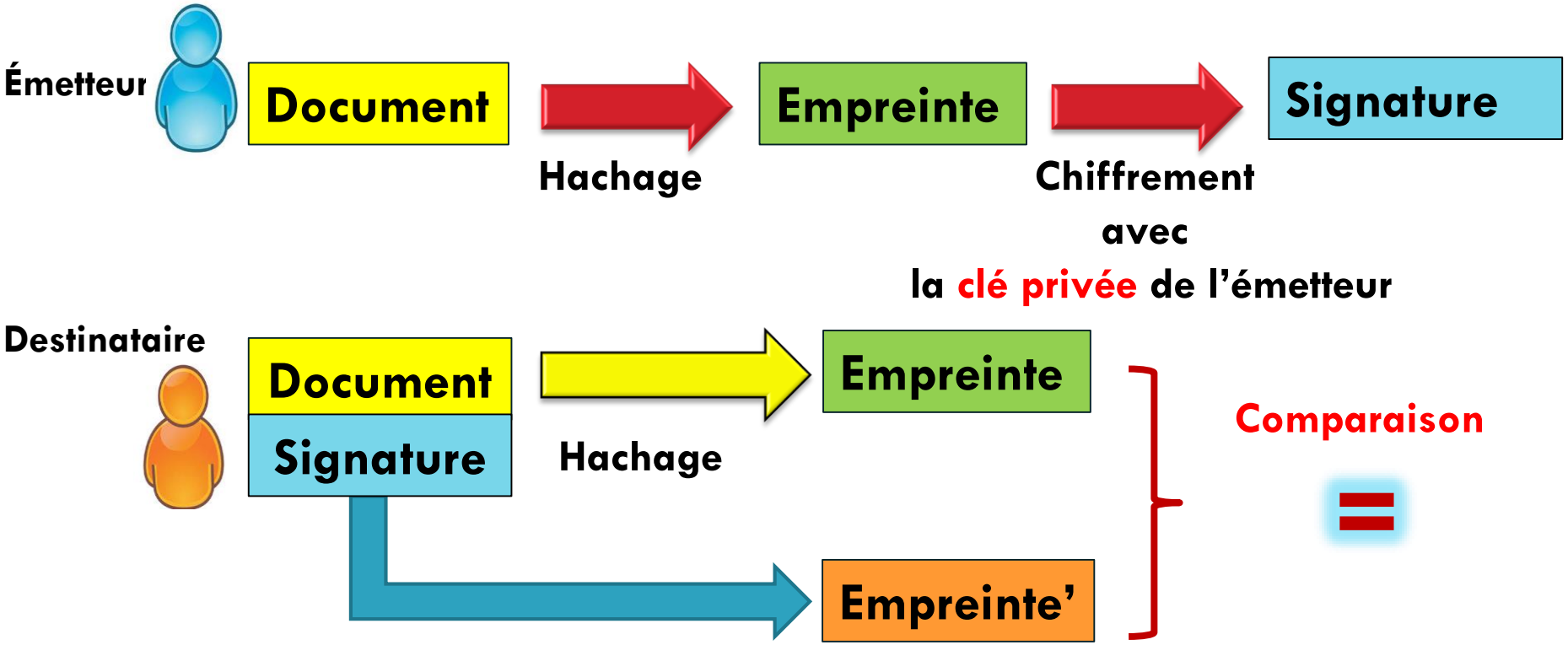


Déchiffrement avec la clé publique de l'émetteur

Protection des fichiers

4. Signature électronique

- Permet d'authentifier l'émetteur d'un document et de vérifier l'intégrité du fichier



Déchiffrement avec la clé publique de l'émetteur

Authentification

1. Logique

- Par un mot de passe
- Par connaissance d'une information (question secrète)

+ Simple

- Risque d'oubli ou de fraude

Authentification

2. Physique

- Par carte magnétique
- Par carte à puce
- Par RFID

+ Simple

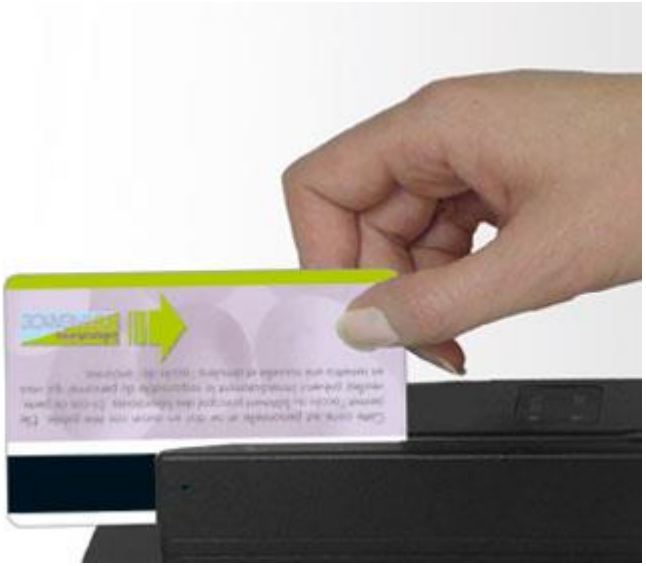
- Risque de perte de vol

- Risque d'oubli de mot de passe

Authentification

2. Physique

- **Par carte magnétique**
  - Bande magnétique (140 Ø)
  - Les informations sont lues par un terminal
  - Le mot de passe est chiffré au moyen d'une clé que seule « la banque » connait



Authentification

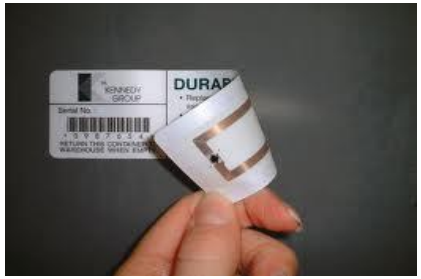
2. Physique

- **Par carte à puce**
  - Les informations sont lues par un terminal qui demande le mot de passe (code PIN)

Authentification

2. Physique

- **Par RFID (R*adio* F*requency* ID*entification*)**
  - Ces puces électroniques contiennent un identifiant et éventuellement des données complémentaires



Authentification

3. Biométrique

Pas de Risque de perte, d'oubli ou de fraude

- **Doit : empreinte (depuis 1960)**
- **Voix: sensible aux variations (âge, état)**
- **Visage : sensible aux variations (âge, état)**
- **Rétine : peu sensible**

FIN

Madame Khaoula ElBedoui-Maktouf

2ème année Ingénieur Informatique